



Informatica®

Informatica® Intelligent Cloud Services  
November 2024

# Connections

Informatica Intelligent Cloud Services Connections  
November 2024

© Copyright Informatica LLC 2006, 2024

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, Informatica Cloud, Informatica Intelligent Cloud Services, PowerCenter, PowerExchange, and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2024-11-06

# Table of Contents

<b>Preface</b> .....	<b>27</b>
Informatica Resources. ....	27
Informatica Documentation. ....	27
Informatica Intelligent Cloud Services web site. ....	27
Informatica Intelligent Cloud Services Communities. ....	27
Informatica Intelligent Cloud Services Marketplace. ....	28
Data Integration connector documentation. ....	28
Informatica Knowledge Base. ....	28
Informatica Intelligent Cloud Services Trust Center. ....	28
Informatica Global Customer Support. ....	28
<b>Chapter 1: Connectors and connections</b> .....	<b>29</b>
Add-on connectors. ....	29
Installing an add-on connector. ....	29
<b>Chapter 2: Connection configuration</b> .....	<b>31</b>
Configuring a connection. ....	32
Configuring a connection using sample data. ....	33
Viewing connection dependencies. ....	34
<b>Chapter 3: ActiveCampaign connection properties</b> .....	<b>35</b>
<b>Chapter 4: Adabas CDC Connection Properties</b> .....	<b>36</b>
<b>Chapter 5: Adabas connection properties</b> .....	<b>39</b>
<b>Chapter 6: Adaptive Insights Connection Properties</b> .....	<b>41</b>
<b>Chapter 7: Adobe Analytics connection properties</b> .....	<b>42</b>
<b>Chapter 8: Adobe Analytics Mass Ingestion connection properties</b> .....	<b>43</b>
<b>Chapter 9: Adobe Experience Platform connection properties</b> .....	<b>45</b>
<b>Chapter 10: Advanced FTP Connection properties</b> .....	<b>46</b>
<b>Chapter 11: Advanced FTP V2 connection properties</b> .....	<b>48</b>
<b>Chapter 12: Advanced FTPS connection properties</b> .....	<b>50</b>
<b>Chapter 13: Advanced FTPS V2 connection properties</b> .....	<b>52</b>

<b>Chapter 14: Advanced SFTP connection properties.....</b>	<b>55</b>
<b>Chapter 15: Advanced SFTP V2 connection properties.....</b>	<b>56</b>
<b>Chapter 16: Amazon Athena connection properties.....</b>	<b>58</b>
Prepare for authentication. . . . .	58
Create an Amazon S3 policy. . . . .	58
Create an AWS Glue data catalog policy. . . . .	59
Create an Amazon Athena policy. . . . .	59
Connect to Amazon Athena. . . . .	60
Before you begin. . . . .	60
Connection details. . . . .	61
Authentication types. . . . .	61
Advanced settings. . . . .	62
Proxy server settings. . . . .	62
<b>Chapter 17: Amazon Aurora connection properties.....</b>	<b>63</b>
<b>Chapter 18: Amazon DynamoDB connection properties.....</b>	<b>65</b>
<b>Chapter 19: Amazon DynamoDB V2 connection properties.....</b>	<b>66</b>
<b>Chapter 20: Amazon Kinesis connection properties.....</b>	<b>68</b>
Amazon Kinesis Firehose connection properties. . . . .	68
Amazon Kinesis Streams connection properties. . . . .	70
<b>Chapter 21: Amazon Redshift connection properties.....</b>	<b>72</b>
<b>Chapter 22: Amazon Redshift V2 connection properties.....</b>	<b>74</b>
Prepare for authentication. . . . .	74
Create a minimal Amazon IAM policy. . . . .	76
Configure IAM authentication. . . . .	76
Configure an assume role for Amazon Redshift. . . . .	77
Generate temporary security credential policies for Amazon Redshift. . . . .	77
Generate temporary security credentials using AssumeRole for EC2. . . . .	79
Configure an assume role for Amazon S3 staging. . . . .	80
Generate temporary security credentials using AssumeRole for Amazon S3 staging. . . . .	81
Generate temporary security credentials using AssumeRole for EC2. . . . .	83
Enable encryption. . . . .	84
Connect to Amazon Redshift. . . . .	85
Before you begin. . . . .	85
Connection details. . . . .	85
Authentication types. . . . .	86



Proxy server settings. . . . .	95
Configure SSL. . . . .	95
Configure SSL with the serverless runtime environment. . . . .	96
Configure client-side encryption with the serverless runtime environment. . . . .	97
Configure SSE-KMS encryption for mappings in advanced mode. . . . .	98
Amazon Redshift Serverless connectivity. . . . .	98
Requirements to use Amazon Redshift Spectrum. . . . .	98
Private communication with Amazon Redshift. . . . .	99
Private communication with Amazon S3. . . . .	99
VPC peering between the serverless runtime environment and Amazon Redshift. . . . .	100
<b>Chapter 23: Amazon S3 connection properties. . . . .</b>	<b>101</b>
<b>Chapter 24: Amazon S3 V2 connection properties. . . . .</b>	<b>103</b>
Prepare for authentication. . . . .	103
Create a minimal Amazon IAM policy. . . . .	103
IAM authentication. . . . .	104
AssumeRole using EC2 role and IAM user . . . . .	105
Credential profile file authentication. . . . .	107
Connect to Amazon S3. . . . .	107
Before you begin. . . . .	108
Connection details. . . . .	108
Authentication types. . . . .	108
Advanced settings. . . . .	117
Private communication with Amazon S3. . . . .	118
Server-side encryption with KMS. . . . .	119
Client-side encryption with serverless runtime environment. . . . .	119
SSE-KMS encryption for mappings in advanced mode. . . . .	120
Proxy server settings. . . . .	120
Bypass proxy server. . . . .	121
Rules and guidelines for AssumeRole via IAM user authentication. . . . .	122
Rules and guidelines for AWS regions. . . . .	123
Rules and guidelines for S3 compatible storage. . . . .	123
<b>Chapter 25: Amplitude connection properties. . . . .</b>	<b>124</b>
<b>Chapter 26: AMQP connection properties. . . . .</b>	<b>125</b>
<b>Chapter 27: Anaplan V2 connection properties. . . . .</b>	<b>127</b>
<b>Chapter 28: Ariba V2 connection properties. . . . .</b>	<b>129</b>
<b>Chapter 29: AS2 connection properties. . . . .</b>	<b>131</b>
Connection properties. . . . .	131

Message properties. . . . .	133
Receipt properties. . . . .	134
Proxy properties. . . . .	135
<b>Chapter 30: BigMachines connection properties. . . . .</b>	<b>136</b>
<b>Chapter 31: Birst Cloud Connect connection properties. . . . .</b>	<b>138</b>
<b>Chapter 32: Box connection properties. . . . .</b>	<b>139</b>
Connect to Box. . . . .	139
Before you begin. . . . .	139
Connection details. . . . .	140
Generate the OAuth access token. . . . .	142
URI request parameters. . . . .	142
<b>Chapter 33: Business 360 connection properties. . . . .</b>	<b>143</b>
<b>Chapter 34: Business 360 Events connection properties. . . . .</b>	<b>144</b>
<b>Chapter 35: Business 360 FEP connection properties. . . . .</b>	<b>145</b>
<b>Chapter 36: CallidusCloud Commissions connection properties. . . . .</b>	<b>146</b>
<b>Chapter 37: CallidusCloud File Processor connection properties. . . . .</b>	<b>148</b>
<b>Chapter 38: Cassandra V2 connection properties. . . . .</b>	<b>150</b>
<b>Chapter 39: Chatter connection properties. . . . .</b>	<b>152</b>
<b>Chapter 40: Cloud Integration Hub connection properties. . . . .</b>	<b>153</b>
<b>Chapter 41: Concur connection properties. . . . .</b>	<b>155</b>
<b>Chapter 42: Concur V2 connection properties. . . . .</b>	<b>157</b>
<b>Chapter 43: Couchbase connection properties. . . . .</b>	<b>159</b>
<b>Chapter 44: Coupa connection properties. . . . .</b>	<b>161</b>
<b>Chapter 45: Coupa V2 connection properties. . . . .</b>	<b>162</b>
Connect to Coupa V2. . . . .	162
Before you begin. . . . .	162
Connection details. . . . .	162
Advanced settings. . . . .	164
Coupa V2 Custom Fields. . . . .	164

Proxy server settings. . . . .	166
Rules and guidelines for Coupa custom fields. . . . .	167
<b>Chapter 46: Cvent connection properties. . . . .</b>	<b>168</b>
Connect to Cvent. . . . .	168
Before you begin. . . . .	168
Connection details. . . . .	168
Advanced settings. . . . .	169
Proxy server settings. . . . .	170
<b>Chapter 47: Databricks connection properties. . . . .</b>	<b>171</b>
Staging prerequisites. . . . .	171
SQL warehouse. . . . .	171
Configure AWS staging. . . . .	171
Configure Azure staging. . . . .	175
All-purpose cluster. . . . .	176
Configure Secure Agent properties. . . . .	176
Job cluster. . . . .	176
Spark configuration. . . . .	177
Configure Secure Agent properties . . . . .	177
Connect to Databricks. . . . .	177
Before you begin. . . . .	177
Connection details. . . . .	178
Authentication type . . . . .	179
Advanced settings. . . . .	180
JDBC URL parameters. . . . .	186
Proxy server settings. . . . .	186
Private links to access Databricks. . . . .	186
Rules and guidelines for personal staging location. . . . .	187
<b>Chapter 48: Datacom CDC Connection Properties. . . . .</b>	<b>188</b>
<b>Chapter 49: Datacom Connection Properties. . . . .</b>	<b>191</b>
<b>Chapter 50: Db2 Data Map connection properties. . . . .</b>	<b>193</b>
<b>Chapter 51: Db2 for i CDC connection properties. . . . .</b>	<b>195</b>
<b>Chapter 52: Db2 for i connection properties. . . . .</b>	<b>198</b>
<b>Chapter 53: Db2 for i Database Ingestion connection properties. . . . .</b>	<b>200</b>
<b>Chapter 54: Db2 for LUW CDC connection properties. . . . .</b>	<b>202</b>

<b>Chapter 55: Db2 for LUW Database Ingestion connection properties.....</b>	<b>205</b>
<b>Chapter 56: Db2 for z/OS Bulk Load connection properties.....</b>	<b>206</b>
<b>Chapter 57: Db2 for z/OS CDC connection properties.....</b>	<b>208</b>
<b>Chapter 58: Db2 for z/OS connection properties.....</b>	<b>211</b>
<b>Chapter 59: Db2 for zOS Database Ingestion connection properties.....</b>	<b>214</b>
<b>Chapter 60: Db2 for z/OS Image Copy connection properties.....</b>	<b>216</b>
<b>Chapter 61: Db2 for z/OS Unload File connection properties.....</b>	<b>218</b>
<b>Chapter 62: DB2 Loader connection properties.....</b>	<b>220</b>
Prerequisites. . . . .	220
Install the DB2 Loader JDBC driver and DB2 client. . . . .	220
Connect to DB2 Loader. . . . .	221
Before you begin. . . . .	221
Connection details. . . . .	221
<b>Chapter 63: Db2 Warehouse on Cloud connection properties.....</b>	<b>225</b>
<b>Chapter 64: Domo connection properties.....</b>	<b>226</b>
<b>Chapter 65: Dropbox connection properties.....</b>	<b>227</b>
<b>Chapter 66: Elasticsearch connection properties.....</b>	<b>229</b>
<b>Chapter 67: Eloqua Bulk API connection properties.....</b>	<b>230</b>
Connect to Eloqua. . . . .	230
Before you begin. . . . .	230
Connection details. . . . .	231
Advanced settings. . . . .	232
Activities or Custom Fields Configuration. . . . .	232
Adding fields which are not part of fields API to the custom objects. . . . .	233
Understanding the Time Zone Offset. . . . .	239
Proxy server settings. . . . .	239
<b>Chapter 68: Eloqua REST connection properties.....</b>	<b>241</b>
<b>Chapter 69: FHIR connection properties.....</b>	<b>242</b>
Connect to FHIR. . . . .	242
Connection details. . . . .	242

Authentication types. . . . .	244
<b>Chapter 70: File List connection properties. . . . .</b>	<b>247</b>
<b>Chapter 71: File Processor connection properties. . . . .</b>	<b>249</b>
<b>Chapter 72: FileIO connection properties. . . . .</b>	<b>250</b>
<b>Chapter 73: Flat file connections. . . . .</b>	<b>251</b>
Flat file connection properties. . . . .	251
Configuring a locale in Linux for flat file connections. . . . .	253
<b>Chapter 74: FTP/SFTP connections. . . . .</b>	<b>255</b>
FTP/SFTP connection properties. . . . .	255
Key exchange algorithms and ciphers. . . . .	256
FTP/SFTP connection rules and guidelines. . . . .	257
<b>Chapter 75: Google Ads connection properties. . . . .</b>	<b>258</b>
<b>Chapter 76: Google Analytics connection properties. . . . .</b>	<b>259</b>
Prerequisites. . . . .	259
Connect to Google Analytics. . . . .	260
Before you begin. . . . .	260
Connection details. . . . .	261
API version. . . . .	261
<b>Chapter 77: Google Analytics Mass Ingestion connection properties. . . . .</b>	<b>263</b>
<b>Chapter 78: Google BigQuery connection properties. . . . .</b>	<b>264</b>
Connection modes. . . . .	265
Connection mode example. . . . .	266
Rules and guidelines for Google BigQuery connection modes. . . . .	269
<b>Chapter 79: Google BigQuery V2 connection properties. . . . .</b>	<b>271</b>
Connect to Google BigQuery. . . . .	271
Before you begin. . . . .	271
Connection details. . . . .	271
Authentication type. . . . .	272
Proxy server settings. . . . .	275
Configure proxy settings for NTLM authentication. . . . .	275
<b>Chapter 80: Google Bigtable connection properties. . . . .</b>	<b>276</b>
<b>Chapter 81: Google Cloud Storage connection properties. . . . .</b>	<b>277</b>

<b>Chapter 82: Google Cloud Storage V2 connection properties.....</b>	<b>278</b>
<b>Chapter 83: Google Drive connection properties.....</b>	<b>280</b>
<b>Chapter 84: Google PubSub - Streaming Ingestion and Replication connection properties.....</b>	<b>281</b>
<b>Chapter 85: Google PubSub connection properties.....</b>	<b>282</b>
<b>Chapter 86: Google PubSub V2 connection properties.....</b>	<b>283</b>
<b>Chapter 87: Google Sheets connection properties.....</b>	<b>284</b>
<b>Chapter 88: Google Sheets V2 connection properties.....</b>	<b>286</b>
<b>Chapter 89: Greenplum connection properties.....</b>	<b>287</b>
Prerequisites. . . . .	287
Configure JDBC and ODBC drivers. . . . .	287
Configuring the Kerberos authentication. . . . .	289
Connect to Greenplum. . . . .	290
Before you begin. . . . .	290
Connection details. . . . .	291
Authentication types. . . . .	291
<b>Chapter 90: Hadoop connection properties.....</b>	<b>294</b>
JDBC URL. . . . .	295
JDBC Driver Class. . . . .	296
<b>Chapter 91: Hadoop Files connection properties.....</b>	<b>297</b>
<b>Chapter 92: Hadoop Files V2 connection properties.....</b>	<b>299</b>
<b>Chapter 93: Hive connection properties.....</b>	<b>302</b>
<b>Chapter 94: HubSpot connection properties.....</b>	<b>304</b>
<b>Chapter 95: IBM MQ connection properties.....</b>	<b>305</b>
<b>Chapter 96: IDMS CDC connection properties.....</b>	<b>307</b>
<b>Chapter 97: IDMS connection properties.....</b>	<b>310</b>
<b>Chapter 98: IMS CDC Connection Properties.....</b>	<b>312</b>
<b>Chapter 99: IMS connection properties.....</b>	<b>315</b>

<b>Chapter 100: JD Edwards EnterpriseOne connection properties.....</b>	<b>317</b>
<b>Chapter 101: JDBC connection properties.....</b>	<b>319</b>
<b>Chapter 102: JDBC V2 connection properties.....</b>	<b>320</b>
Prerequisites. . . . .	320
Install the Type 4 JDBC driver. . . . .	320
Connect to JDBC V2. . . . .	321
Before you begin. . . . .	321
Connection details. . . . .	321
Connect to SSL-enabled databases for mappings in advanced mode. . . . .	323
Use the serverless runtime environment. . . . .	324
<b>Chapter 103: JIRA Cloud connection properties.....</b>	<b>326</b>
<b>Chapter 104: Jira connection properties.....</b>	<b>327</b>
Connect to Jira. . . . .	327
Before you begin. . . . .	327
Connection details. . . . .	327
<b>Chapter 105: JMS connection properties.....</b>	<b>329</b>
<b>Chapter 106: JSON Target connection properties.....</b>	<b>331</b>
<b>Chapter 107: Kafka connection properties.....</b>	<b>332</b>
<b>Chapter 108: Klaviyo connection properties.....</b>	<b>336</b>
<b>Chapter 109: LDAP connection properties.....</b>	<b>337</b>
<b>Chapter 110: Magento V1 connection properties.....</b>	<b>339</b>
<b>Chapter 111: Mailchimp connection properties.....</b>	<b>340</b>
<b>Chapter 112: Marketo V3 connection properties.....</b>	<b>341</b>
Connect to Marketo. . . . .	341
Before you begin. . . . .	341
Connection details. . . . .	341
Advanced settings. . . . .	342
Proxy server settings. . . . .	342
<b>Chapter 113: Microsoft Access connection properties.....</b>	<b>344</b>
<b>Chapter 114: Microsoft Azure Blob Storage connection properties.....</b>	<b>345</b>

<b>Chapter 115: Microsoft Azure Blob Storage V2 connection properties.....</b>	<b>346</b>
<b>Chapter 116: Microsoft Azure Blob Storage V3 connection properties.....</b>	<b>347</b>
Prepare for authentication. . . . .	347
Shared key authentication. . . . .	347
Shared access signature . . . . .	348
Connect to Microsoft Azure Blob Storage V3. . . . .	349
Before you begin. . . . .	349
Connection details. . . . .	350
Authentication types. . . . .	350
Proxy Server Settings. . . . .	351
<b>Chapter 117: Microsoft Azure Cosmos DB SQL API connection properties..</b>	<b>353</b>
Connect to Microsoft Azure Cosmos DB SQL API. . . . .	353
Before you begin. . . . .	353
Connection details. . . . .	353
<b>Chapter 118: Microsoft Azure Data Lake Storage Gen2 connection properties.....</b>	<b>355</b>
Prepare for authentication. . . . .	355
Managed identity authentication. . . . .	356
Connect to Microsoft Azure Data Lake Storage Gen2. . . . .	356
Before you begin. . . . .	356
Connection details. . . . .	356
Authentication types. . . . .	357
Proxy Server Settings. . . . .	359
Bypass the proxy server. . . . .	359
<b>Chapter 119: Microsoft Azure DocumentDB Connection Properties.....</b>	<b>361</b>
<b>Chapter 120: Microsoft Azure Event Hub connection properties.....</b>	<b>362</b>
<b>Chapter 121: Microsoft Azure SQL Data Warehouse - Database Ingestion connection properties.....</b>	<b>364</b>
<b>Chapter 122: Microsoft Azure SQL Data Warehouse connection properties..</b>	<b>366</b>
<b>Chapter 123: Microsoft Azure SQL Data Warehouse V2 connection properties.....</b>	<b>367</b>
<b>Chapter 124: Microsoft Azure Synapse Analytics Database Ingestion connection properties.....</b>	<b>368</b>



<b>Chapter 125: Microsoft Azure Synapse SQL connection properties.....</b>	<b>370</b>
Prerequisites. . . . .	370
Azure Active Directory authentication. . . . .	370
Service principal authentication. . . . .	372
Managed Identity authentication. . . . .	372
Serverless SQL pool. . . . .	373
Connect to Microsoft Azure Synapse SQL. . . . .	373
Before you begin. . . . .	373
Connection details. . . . .	374
Azure storage types. . . . .	376
Advanced settings. . . . .	379
Verify permissions. . . . .	379
<b>Chapter 126: Microsoft CDM Folders V2 connection properties.....</b>	<b>381</b>
<b>Chapter 127: Microsoft Dynamics 365 for Operations connection properties</b>	<b>383</b>
Prepare for authentication. . . . .	383
OAuth 2.0 authentication. . . . .	383
OAuth 2.0 client secret grant authentication. . . . .	383
Set the -Dlog4j.configuration property. . . . .	384
Connect to Microsoft 365 for Operations. . . . .	384
Before you begin. . . . .	384
Connection details. . . . .	384
Authentication types. . . . .	385
Advanced settings. . . . .	386
Proxy server settings. . . . .	386
<b>Chapter 128: Microsoft Dynamics 365 for Sales connections.....</b>	<b>387</b>
Prepare for authentication. . . . .	387
OAuth 2.0 password grant. . . . .	387
OAuth 2.0 client secret grant. . . . .	387
OAuth 2.0 client certificate grant. . . . .	389
Connect to Microsoft Dynamics 365 for Sales. . . . .	391
Before you begin. . . . .	391
Connection details. . . . .	392
Authentication types. . . . .	392
Advanced settings. . . . .	394
Configure the serverless runtime environment. . . . .	395
Troubleshooting a Microsoft Dynamics 365 for Sales connection. . . . .	395
<b>Chapter 129: Microsoft Dynamics 365 Mass Ingestion connection properties.....</b>	<b>396</b>

<b>Chapter 130: Microsoft Dynamics AX V3 connection properties.....</b>	<b>400</b>
<b>Chapter 131: Microsoft Dynamics CRM connection properties.....</b>	<b>401</b>
<b>Chapter 132: Microsoft Dynamics NAV connection properties.....</b>	<b>403</b>
<b>Chapter 133: Microsoft Excel connection properties.....</b>	<b>404</b>
<b>Chapter 134: Microsoft Fabric Data Warehouse connection properties.....</b>	<b>405</b>
<b>Chapter 135: Microsoft Fabric Lakehouse connection properties.....</b>	<b>406</b>
<b>Chapter 136: Microsoft Fabric OneLake connection properties.....</b>	<b>407</b>
<b>Chapter 137: Microsoft Power BI Connection Properties.....</b>	<b>409</b>
<b>Chapter 138: Microsoft SharePoint connection properties.....</b>	<b>411</b>
<b>Chapter 139: Microsoft Sharepoint Online connection properties.....</b>	<b>412</b>
Prepare for authentication. . . . .	412
Access Control Service. . . . .	412
Microsoft Entra ID. . . . .	415
Connect to Microsoft Sharepoint Online. . . . .	417
Before you begin. . . . .	418
Connection details. . . . .	418
SharePoint Online authentication types. . . . .	418
<b>Chapter 140: Microsoft SQL Server CDC connection properties.....</b>	<b>421</b>
<b>Chapter 141: Microsoft SQL Server connection properties.....</b>	<b>424</b>
Prepare for authentication. . . . .	424
Prepare for Kerberos authentication. . . . .	424
Connect to Microsoft SQL Server. . . . .	426
Before you begin. . . . .	426
Connection details. . . . .	426
Authentication types. . . . .	426
Advanced settings. . . . .	431
Configure SSL with the serverless runtime environment. . . . .	432
<b>Chapter 142: Mixpanel connection properties.....</b>	<b>434</b>
<b>Chapter 143: MLLP connection properties.....</b>	<b>435</b>
<b>Chapter 144: MongoDB Mass Ingestion connection properties.....</b>	<b>437</b>

<b>Chapter 145: MongoDB connection properties.....</b>	<b>439</b>
<b>Chapter 146: MongoDB V2 connection properties.....</b>	<b>441</b>
Additional connection properties. . . . .	442
Configure SSL for the serverless runtime environment. . . . .	444
<b>Chapter 147: MQTT connection properties.....</b>	<b>445</b>
<b>Chapter 148: MRI Software connection properties . . . . .</b>	<b>447</b>
<b>Chapter 149: MySQL CDC connection properties.....</b>	<b>448</b>
<b>Chapter 150: MySQL connection properties.....</b>	<b>451</b>
SSL properties. . . . .	452
<b>Chapter 151: Netezza connection properties.....</b>	<b>455</b>
Prerequisites. . . . .	455
Download the Netezza JDBC Driver. . . . .	455
Download the Netezza ODBC Driver. . . . .	456
Connect to Netezza. . . . .	456
Before you begin. . . . .	456
Connection details. . . . .	457
Advanced settings. . . . .	458
Database privileges. . . . .	458
<b>Chapter 152: NetSuite connection properties.....</b>	<b>459</b>
Connect to NetSuite. . . . .	459
Before you begin. . . . .	459
Connection details. . . . .	459
Advanced settings. . . . .	461
NetSuite account-specific service URL. . . . .	462
Token-based authentication. . . . .	463
Rules and guidelines for a NetSuite connection. . . . .	463
Troubleshoot a NetSuite connection. . . . .	464
<b>Chapter 153: NetSuite Mass Ingestion connection properties.....</b>	<b>465</b>
<b>Chapter 154: NetSuite RESTlet V2 connection properties.....</b>	<b>467</b>
<b>Chapter 155: NICE Satmetrix connection properties.....</b>	<b>469</b>
<b>Chapter 156: OData connections properties.....</b>	<b>470</b>
Connect to OData. . . . .	470

Before you begin. . . . .	470
Connection details. . . . .	470
Advanced settings. . . . .	471
Proxy server settings. . . . .	471
<b>Chapter 157: OData consumer connection properties. . . . .</b>	<b>472</b>
Connect to OData Consumer. . . . .	472
Before you begin. . . . .	472
Connection details. . . . .	472
Advanced settings. . . . .	473
Proxy server settings. . . . .	474
Setting up one-way SSL. . . . .	474
<b>Chapter 158: OData V2 Protocol Reader connection properties. . . . .</b>	<b>475</b>
Authorization code authentication. . . . .	476
Client credential authentication. . . . .	478
<b>Chapter 159: OData V2 Protocol Writer connection properties. . . . .</b>	<b>479</b>
<b>Chapter 160: ODBC connection properties. . . . .</b>	<b>481</b>
Prerequisites. . . . .	481
Configure the ODBC driver. . . . .	481
Prepare for Kerberos authentication. . . . .	485
Connect to ODBC. . . . .	486
Before you begin. . . . .	487
Connection details. . . . .	488
Rules and guidelines for an ODBC connection. . . . .	491
Use the serverless runtime environment. . . . .	491
<b>Chapter 161: OpenAir connection properties. . . . .</b>	<b>494</b>
<b>Chapter 162: Open Table connection properties. . . . .</b>	<b>495</b>
Prerequisites. . . . .	495
Adding the Amazon Athena JDBC driver. . . . .	495
Create minimal IAM policies. . . . .	496
Connect to Open Table. . . . .	497
Before you begin. . . . .	497
Connection details. . . . .	498
<b>Chapter 163: Oracle connection properties. . . . .</b>	<b>499</b>
Prerequisites. . . . .	499
SSL configuration. . . . .	499
Kerberos authentication. . . . .	501

Connect to Oracle. . . . .	502
Before you begin. . . . .	502
Connection details. . . . .	503
Authentication types. . . . .	503
Advanced settings. . . . .	504
Configuring SSL with the serverless runtime environment. . . . .	506
Oracle Connection Rules and Guidelines. . . . .	507
<b>Chapter 164: Oracle Autonomous Database connections. . . . .</b>	<b>508</b>
Prerequisites. . . . .	508
Prepare for object storage authentication. . . . .	508
Connect to Oracle Autonomous Database. . . . .	509
Before you begin. . . . .	509
Connection details. . . . .	509
Authentication types. . . . .	510
Object storage authentication types. . . . .	510
<b>Chapter 165: Oracle Business Intelligence Publisher connection properties 512</b>	
Connect to Oracle Business Intelligence Publisher. . . . .	512
Before you begin. . . . .	512
Connection details. . . . .	513
Advanced settings. . . . .	514
Proxy server settings. . . . .	514
<b>Chapter 166: Oracle CDC V2 connection properties. . . . .</b>	<b>515</b>
<b>Chapter 167: Oracle Cloud Object Storage connections. . . . .</b>	<b>518</b>
Prerequisites. . . . .	518
Configure Oracle Cloud Infrastructure policies. . . . .	518
Prepare for authentication. . . . .	519
Connect to Oracle Cloud Object Storage. . . . .	520
Before you begin. . . . .	520
Connection details. . . . .	520
Authentication types. . . . .	520
Proxy server settings. . . . .	522
<b>Chapter 168: Oracle CRM Cloud V1 connections properties. . . . .</b>	<b>523</b>
<b>Chapter 169: Oracle CRM On Demand connection properties. . . . .</b>	<b>524</b>
<b>Chapter 170: Oracle Database Ingestion connection properties. . . . .</b>	<b>525</b>
Prerequisites for Kerberos authentication. . . . .	531
Configuring Kerberos authentication. . . . .	532

<b>Chapter 171: Oracle Financials Cloud V1 connection properties.....</b>	<b>534</b>
Prerequisites. . . . .	534
Access the XLSM template files. . . . .	534
Get the ERP endpoint URL. . . . .	535
Connect to Oracle Financials Cloud. . . . .	535
Before you begin. . . . .	535
Connection details. . . . .	536
Encryption mode . . . . .	537
Proxy server settings. . . . .	538
<b>Chapter 172: Oracle Fusion Cloud Mass Ingestion connection properties... </b>	<b>539</b>
<b>Chapter 173: Oracle HCM Cloud V1 connection properties.....</b>	<b>540</b>
Prerequisites. . . . .	540
Get the WebCenter Content URL. . . . .	540
Verify roles. . . . .	540
Connect to Oracle HCM. . . . .	541
Before you begin . . . . .	541
Connection details. . . . .	541
Advanced settings. . . . .	543
Encryption mode . . . . .	543
Extract definition. . . . .	544
Download the excel templates. . . . .	545
Download and install ADF desktop integration tool. . . . .	547
Set up the excel templates. . . . .	548
Proxy server settings. . . . .	549
<b>Chapter 174: Pinecone connection properties.....</b>	<b>550</b>
Prepare for authentication. . . . .	550
Get the Pinecone API key. . . . .	550
Connect to Pinecone. . . . .	550
Before you begin. . . . .	550
Connection details. . . . .	551
<b>Chapter 175: PostgreSQL CDC connection properties.....</b>	<b>552</b>
<b>Chapter 176: PostgreSQL connection properties.....</b>	<b>555</b>
Prepare for authentication. . . . .	555
Prepare for Kerberos authentication. . . . .	555
Connect to PostgreSQL. . . . .	557
Before you begin. . . . .	557
Connection details. . . . .	557

Authentication types. . . . .	557
Advanced settings. . . . .	559
Configure SSL with serverless runtime environment. . . . .	561
<b>Chapter 177: Power BI connection properties. . . . .</b>	<b>562</b>
<b>Chapter 178: QuickBooks V2 Connection Properties. . . . .</b>	<b>563</b>
<b>Chapter 179: Redis connection properties. . . . .</b>	<b>564</b>
<b>Chapter 180: REST API connection properties. . . . .</b>	<b>566</b>
<b>Chapter 181: REST V2 connection properties. . . . .</b>	<b>567</b>
Prerequisites. . . . .	567
Connect to REST V2. . . . .	567
Before you begin. . . . .	567
Connection details. . . . .	567
Authentication types. . . . .	568
Advanced settings. . . . .	577
Secure communication with TLS authentication. . . . .	578
Generate a truststore. . . . .	579
Generate a keystore. . . . .	579
Configuring one-way or two-way secure communication. . . . .	580
Secure communication in a serverless runtime environment. . . . .	581
Swagger specification file in a serverless runtime environment. . . . .	581
Rules and guidelines for runtime environment. . . . .	582
Rules and guidelines for a REST V2 connection. . . . .	583
<b>Chapter 182: REST V3 Connection Properties. . . . .</b>	<b>584</b>
Authorization Code Authentication. . . . .	585
Client Credential Authentication. . . . .	588
Rules and guidelines for REST V3 connections. . . . .	590
<b>Chapter 183: Salesforce Analytics connection properties. . . . .</b>	<b>591</b>
<b>Chapter 184: Salesforce Commerce Cloud connection properties. . . . .</b>	<b>592</b>
<b>Chapter 185: Salesforce connection properties. . . . .</b>	<b>593</b>
Prepare for authentication. . . . .	593
Standard. . . . .	593
OAuth. . . . .	593
Connect to Salesforce. . . . .	594
Before you begin. . . . .	594
Connection details. . . . .	594

Salesforce connection types . . . . .	595
Firewall configuration. . . . .	596
Proxy server settings. . . . .	597
Connection timeout. . . . .	597
Troubleshooting a Salesforce connection. . . . .	597
<b>Chapter 186: Salesforce Data Cloud connection properties. . . . .</b>	<b>599</b>
Connect to Salesforce Data Cloud. . . . .	599
Before you begin. . . . .	599
Connection details. . . . .	599
<b>Chapter 187: Salesforce Marketing Cloud connection properties. . . . .</b>	<b>601</b>
<b>Chapter 188: Salesforce Mass Ingestion connection properties. . . . .</b>	<b>603</b>
<b>Chapter 189: Salesforce Pardot connection properties. . . . .</b>	<b>607</b>
<b>Chapter 190: SAP connection properties. . . . .</b>	<b>609</b>
Prerequisites. . . . .	609
Download and configure the SAP libraries. . . . .	609
Configure SAP user authorization. . . . .	611
Configure the sapnwrfc.ini file. . . . .	611
Define SAP Connector as a logical system in SAP. . . . .	614
Connect to SAP. . . . .	617
Before you begin. . . . .	617
Connection details. . . . .	618
SAP connection types. . . . .	618
Use the serverless runtime environment. . . . .	620
<b>Chapter 191: SAP ADSO Writer connection properties. . . . .</b>	<b>622</b>
<b>Chapter 192: SAP BAPI connection properties. . . . .</b>	<b>627</b>
Prerequisites. . . . .	627
Download and configure the SAP libraries. . . . .	627
Configure SAP user authorization. . . . .	628
Connect to SAP BAPI. . . . .	628
Before you begin. . . . .	629
Connection details. . . . .	629
Advanced settings. . . . .	630
Configure SAP BAPI Connector as a business service. . . . .	630
Use the serverless runtime environment. . . . .	631



<b>Chapter 193: SAP BW Connector connection properties.....</b>	<b>633</b>
Prerequisites. . . . .	633
Download and configure the SAP libraries. . . . .	633
Configure SAP user authorization. . . . .	635
Install transport files for SAP BW. . . . .	636
Connect to SAP BW. . . . .	637
Before you begin. . . . .	637
Connection details. . . . .	637
Connection types. . . . .	637
Configure HTTPS to connect to SAP. . . . .	641
Create an OpenSSL certificate. . . . .	642
Convert an OpenSSL certificate to PSE format. . . . .	643
Enable the HTTPS service on the SAP system. . . . .	644
Import the certificate to the SAP system truststore. . . . .	644
<b>Chapter 194: SAP BW BEx Query connection properties.....</b>	<b>645</b>
Prerequisites. . . . .	645
Download and configure the SAP libraries. . . . .	645
Configure SAP user authorization. . . . .	646
Connect to SAP BW BEx Query. . . . .	647
Before you begin. . . . .	647
Connection details. . . . .	647
Connection types. . . . .	648
Use the serverless runtime environment. . . . .	651
<b>Chapter 195: SAP HANA CDC Connection Properties.....</b>	<b>653</b>
<b>Chapter 196: SAP HANA connection properties.....</b>	<b>656</b>
Prerequisites. . . . .	656
Adding entries in Linux operating system. . . . .	656
Downloading and configuring libraries. . . . .	657
Connect to SAP HANA. . . . .	657
Before you begin. . . . .	657
Connection details. . . . .	657
Advanced settings. . . . .	659
Use the serverless runtime environment. . . . .	659
<b>Chapter 197: SAP HANA Database Ingestion connection properties.....</b>	<b>661</b>
<b>Chapter 198: SAP IQ connection properties.....</b>	<b>664</b>
Prerequisites. . . . .	664
Install the SAP IQ JDBC driver and Sybase client. . . . .	664

Connect to SAP IQ. . . . .	665
Before you begin. . . . .	665
Connection details. . . . .	665
<b>Chapter 199: SAP Mass Ingestion connection properties. . . . .</b>	<b>667</b>
<b>Chapter 200: SAP OData V2 connection properties. . . . .</b>	<b>673</b>
Prepare for authentication. . . . .	673
Basic. . . . .	673
API key. . . . .	673
Authorization code. . . . .	673
Client credentials. . . . .	674
Connect to SAP OData V2. . . . .	674
Before you begin. . . . .	674
Connection details. . . . .	674
Authentication types. . . . .	675
<b>Chapter 201: SAP OData V4 connection properties. . . . .</b>	<b>683</b>
Prepare for authentication. . . . .	683
Authorization code. . . . .	683
Connect to SAP OData V4. . . . .	683
Before you begin. . . . .	684
Connection details. . . . .	684
Authentication types. . . . .	684
<b>Chapter 202: SAP ODP Extractor connection properties. . . . .</b>	<b>686</b>
Prerequisites. . . . .	686
Verify the required SAP Notes in the SAP server. . . . .	686
Download and configure the SAP libraries. . . . .	686
Configure SAP user authorization. . . . .	688
Configure the Secure Network Communication protocol. . . . .	690
Connect to SAP ODP. . . . .	690
Before you begin. . . . .	691
Connection details. . . . .	691
SAP server connection types. . . . .	691
Advanced settings. . . . .	696
Hierarchical data extraction from SAP ODP objects. . . . .	696
Use the serverless runtime environment. . . . .	697
<b>Chapter 203: SAP Table Connector connection properties. . . . .</b>	<b>699</b>
Prerequisites. . . . .	699
Download and configure the SAP libraries. . . . .	699
Configure SAP user authorization. . . . .	701

Install transport files to read from an SAP table. . . . .	702
Install transport files to write to an SAP table. . . . .	703
Connect to SAP table. . . . .	703
Before you begin. . . . .	703
Connection details. . . . .	704
Configure the sapnwrfc.ini file. . . . .	706
Configure HTTPS to connect to SAP. . . . .	708
Create an OpenSSL certificate. . . . .	709
Convert an OpenSSL certificate to PSE format. . . . .	710
Enable the HTTPS service on the SAP system. . . . .	711
Import the certificate to the SAP system trust store. . . . .	711
Configure the Secure Network Communication protocol. . . . .	711
Enable the Secure Agent to operate as a whitelisted host in SAP (Optional). . . . .	712
Use the serverless runtime environment. . . . .	713
Troubleshooting an SAP Table connection. . . . .	714
<b>Chapter 204: SAS connection properties. . . . .</b>	<b>715</b>
<b>Chapter 205: Satmetrix connection properties. . . . .</b>	<b>716</b>
<b>Chapter 206: Sequential File connection properties. . . . .</b>	<b>717</b>
<b>Chapter 207: ServiceNow connection properties. . . . .</b>	<b>720</b>
Connect to ServiceNow. . . . .	720
Before you begin. . . . .	720
Connection details. . . . .	720
Advanced settings. . . . .	721
Firewall Configuration. . . . .	721
Proxy server settings. . . . .	722
Configure proxy server through proxy.ini file. . . . .	722
Test a ServiceNow connection. . . . .	722
<b>Chapter 208: ServiceNow Mass Ingestion connection properties. . . . .</b>	<b>725</b>
<b>Chapter 209: Shopify connection properties. . . . .</b>	<b>727</b>
Connect to Shopify. . . . .	727
Before you begin. . . . .	727
Connection details. . . . .	727
<b>Chapter 210: Snowflake connection properties. . . . .</b>	<b>729</b>
<b>Chapter 211: Snowflake Data Cloud connection properties. . . . .</b>	<b>731</b>
Prepare for authentication. . . . .	731
Standard. . . . .	731

Authorization code. . . . .	732
Key pair. . . . .	732
Client credentials. . . . .	734
Connect to Snowflake. . . . .	734
Before you begin. . . . .	734
Connection details. . . . .	734
Authentication types. . . . .	735
JDBC URL parameters. . . . .	742
Microsoft Azure Active Directory for external OAuth authorization. . . . .	743
Proxy server settings. . . . .	744
Private links to access Snowflake. . . . .	744
Use the serverless runtime environment with key pair authentication. . . . .	745
<b>Chapter 212: Stripe connection properties. . . . .</b>	<b>746</b>
Connect to Stripe. . . . .	746
Before you begin. . . . .	746
Connection details. . . . .	746
<b>Chapter 213: SuccessFactors LMS connection properties. . . . .</b>	<b>748</b>
<b>Chapter 214: Successfactor ODATA connection properties. . . . .</b>	<b>750</b>
Connect to SuccessFactors. . . . .	750
Before you begin. . . . .	750
Connection details. . . . .	751
Advanced settings. . . . .	751
Proxy server settings. . . . .	752
<b>Chapter 215: SuccessFactors SOAP connection properties. . . . .</b>	<b>753</b>
<b>Chapter 216: SurveyMonkey connection properties. . . . .</b>	<b>754</b>
<b>Chapter 217: Tableau V2 connection properties. . . . .</b>	<b>756</b>
<b>Chapter 218: Tableau V3 connection properties. . . . .</b>	<b>757</b>
<b>Chapter 219: Teradata connection properties. . . . .</b>	<b>759</b>
Prerequisites. . . . .	759
Teradata Parallel Transporter Utilities. . . . .	759
Configuring the Kerberos authentication. . . . .	759
Setting Environment Variables. . . . .	760
Connect to Teradata. . . . .	761
Before you begin. . . . .	761
Connection details. . . . .	761
Authentication types. . . . .	762

Advanced settings. . . . .	763
Database privileges. . . . .	764
<b>Chapter 220: UKGPro V2 connection properties. . . . .</b>	<b>765</b>
<b>Chapter 221: UltiPro connection properties. . . . .</b>	<b>767</b>
<b>Chapter 222: VSAM CDC connection properties. . . . .</b>	<b>769</b>
<b>Chapter 223: VSAM connection properties. . . . .</b>	<b>772</b>
<b>Chapter 224: Web Service Consumer connection properties. . . . .</b>	<b>774</b>
<b>Chapter 225: WebServices V2 connection properties. . . . .</b>	<b>776</b>
<b>Chapter 226: Workday connection properties. . . . .</b>	<b>778</b>
<b>Chapter 227: Workday Mass Ingestion connection properties. . . . .</b>	<b>779</b>
<b>Chapter 228: Workday V2 connection properties. . . . .</b>	<b>782</b>
Connect to Workday. . . . .	782
Connection details. . . . .	782
Advanced settings. . . . .	783
<b>Chapter 229: Xactly connection properties. . . . .</b>	<b>784</b>
<b>Chapter 230: Xero connection properties. . . . .</b>	<b>785</b>
<b>Chapter 231: XML Source connection properties. . . . .</b>	<b>787</b>
<b>Chapter 232: XML Target connection properties. . . . .</b>	<b>788</b>
<b>Chapter 233: Yellowbrick Data Warehouse connection properties. . . . .</b>	<b>789</b>
<b>Chapter 234: Zendesk connection properties. . . . .</b>	<b>791</b>
<b>Chapter 235: Zendesk Mass Ingestion connection properties. . . . .</b>	<b>792</b>
<b>Chapter 236: Zendesk V2 connection properties. . . . .</b>	<b>794</b>
<b>Chapter 237: Zuora AQUA Connection properties. . . . .</b>	<b>796</b>
Connect to Zuora. . . . .	796
Before you begin. . . . .	796
Connection details. . . . .	796
Advanced settings. . . . .	797

<b>Chapter 238: Zuora connection properties.....</b>	<b>798</b>
<b>Chapter 239: Zuora Multi-Entity connection properties.....</b>	<b>799</b>
<b>Chapter 240: Zuora REST V2 connection properties.....</b>	<b>800</b>
<b>Index.....</b>	<b>802</b>

# Preface

Use *Informatica Intelligent Cloud Services™ Connections* to learn how to configure connections between Informatica Intelligent Cloud Services and cloud and on-premises applications, platforms, databases, and flat files. Refer to *Informatica Intelligent Cloud Services Connections* for information about the connection properties for all connectors that can be used with Informatica Intelligent Cloud Services.

## Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

### Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit <https://docs.informatica.com>.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

### Informatica Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at <http://www.informatica.com/cloud>. This site contains information about Informatica Cloud integration services.

### Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

<https://network.informatica.com/community/informatica-network/products/cloud-integration>

Developers can learn more and share tips at the Cloud Developer community:

<https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers>

## Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

<https://marketplace.informatica.com/>

## Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit <https://docs.informatica.com>.

## Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit <https://search.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

## Informatica Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at <https://www.informatica.com/trust-center.html>.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The [Informatica Intelligent Cloud Services Status](#) page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the [Informatica Intelligent Cloud Services Status](#) page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

## Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at <https://www.informatica.com/services-and-training/support-services/contact-us.html>.



# CHAPTER 1

## Connectors and connections

Connections provide access to data in cloud and on-premise applications, platforms, databases, and flat files. They specify the location of sources, lookup objects, and targets that are included in a task.

You use connectors to create connections. You can create a connection for any connector that is installed in Informatica Intelligent Cloud Services. Many connectors are pre-installed. However, you can also use a connector that is not pre-installed by installing an add-on connector created by Informatica or an Informatica partner.

### Add-on connectors

Add-on connectors provide connectivity for connection types that are not installed by default in Informatica Intelligent Cloud Services.

When you install an add-on connector, the connector becomes available as a connection type for the organization and all sub-organizations. Users can create connections of this type and use them in tasks. Some connectors require configuration before you can use them.

If your organization includes sub-organizations, you install add-on connectors in the parent organization. You cannot install add-on connectors in a sub-organization. If a sub-organization should not use a connector that is available to the parent organization, disable the connector license for the sub-organization.

For information about individual connectors, see the help for the appropriate connector.

If you have a request for a connector that is not yet available, or if you would like information about building a connector, contact Informatica Global Customer Support.

### Installing an add-on connector

You can install a free trial version of an Informatica Intelligent Cloud Services add-on connector, or you can buy the connector from Informatica. After you install an add-on connector, it becomes available as a connection type for the organization and all sub-organizations.

**Note:** If you want to install an add-on connector for use in a sub-organization, install the connector in the parent organization. You cannot install an add-on connector in a sub-organization.

1. In Administrator, select **Add-On Connectors**.
2. Perform either of the following steps:

- To start a free trial for an Informatica Intelligent Cloud Services Connector, click **Free Trial** for the connector, and confirm that you want to start the free trial.
- To buy a license for a connector with an expired free trial, click **Contact Us**.

An Informatica representative will contact you.

After you install the connector, it is displayed on the **Add-On Connectors** page with the message, "Connector Available," and the connection type becomes available to your organization and sub-organizations. The connection type uses the naming convention `<connector name> (<publisher name>)`, for example, "Teradata (Informatica Cloud)."

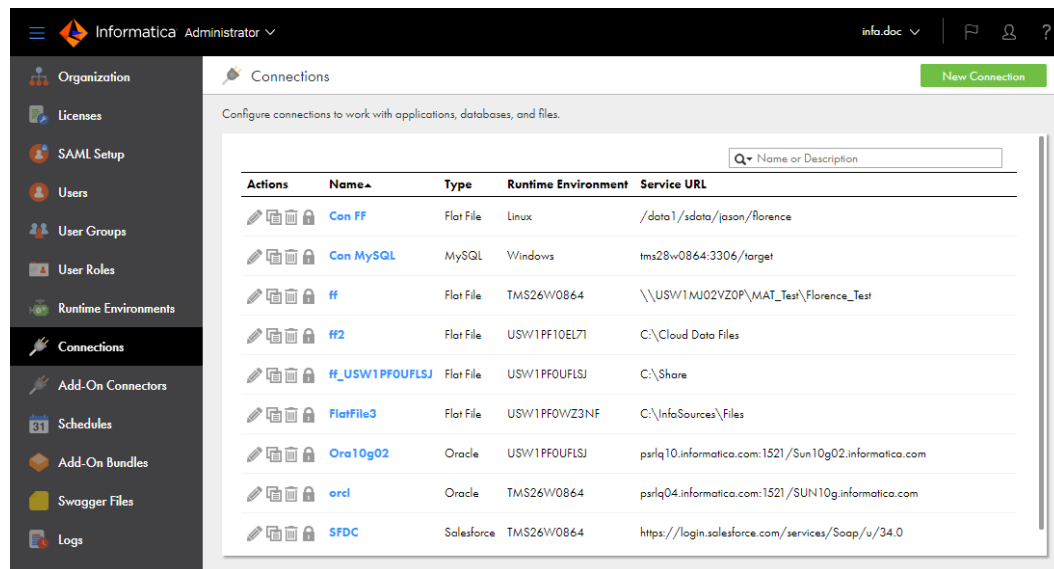
## CHAPTER 2

# Connection configuration

When you configure a connection, the connection becomes available for use within the organization. If you use sub-organizations and you want a connection to be available to multiple sub-organizations, create the connection in each sub-organization.

Configure connections on the **Connections** page. The **Connections** page lists all of the connections that have been configured in the organization. You can create a connection on this page. You can also search for an existing connection by name or description, by name only, or by description only.

The following image shows the **Connections** page:



When you configure a connection, you specify the runtime environment for the connection. The runtime environment must contain an agent that is running. You can override the runtime environment in the connection from the mapping or mapping task.

The runtime environment manages the connection between Informatica Intelligent Cloud Services and the connection endpoint. It helps you perform the following tasks:

- Test the connection to the endpoint.
- Display objects available for the connection and retrieve metadata when you use the connection in an asset. You can preview data in the source, target, or lookup object selected in the asset.
- Run assets that use the connection to read from a source, transform data, or write data to a target.

You can configure a connection to a database, cloud data warehouse, or other endpoint type. When you create a source or target connection to a database or cloud data warehouse, you connect to a table, alias, or view. For example, when you create a Snowflake Data Cloud connection, you connect to a Snowflake table or

view. For more information about creating connections to different types of endpoints, see the help for the appropriate connector.

When you configure connections for sources and targets in a mapping or task, where the connections require you to specify the code page, ensure that the code pages are the same. If the source system and target system in a task use different code pages, the Informatica Intelligent Cloud Services might load unexpected data to the target.

You can delete any connection that you create as long as the connection is not used by a saved query or task.

## Configuring a connection

You can create a connection for connectors that are installed in Informatica Intelligent Cloud Services. You can create a connection on the **Connections** page in Administrator or when you create a source, target, or lookup object in a mapping or task in Data Integration.

**Note:** If your organization is configured to retrieve sensitive connection credentials from an external secrets manager, you need to create and edit connections in Administrator. You can't create and edit connections when you configure mappings and tasks in Data Integration.

When you configure a connection, you specify properties for the connection. Connection properties enable an agent to connect to data sources.

1. Configure the following connection details:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the connection. Maximum length is 255 characters.
Type	Type of connection, such as Salesforce or Oracle.

2. If you use an external secrets manager, select **Use Secret Vault**, select the checkbox next to each property that you store in the secrets manager, and enter the secret name for each property.

Enter the secret name in the following format:

- AWS Secrets Manager: <secret name>:<secret key>
- Azure Key Vault: <secret name>

For example, you configure a relational connection and you store the database password in AWS Secrets Manager. The secret name is MySQLServerCredentials, and the secret key is MyPassword. Select **Use**

**Secret Vault**, enable the checkbox next to the **Password** field, and enter MySQLServerCredentials:MyPassword in the **Password** field, as shown in the following image:

The image shows a configuration form for a connection. It is divided into two sections: 'Connection Details' and 'SQL Server Connection Properties'. In the 'Connection Details' section, 'Connection Name' is 'SQLServer2008\_02', 'Description' is empty, and 'Type' is 'SQL Server'. In the 'SQL Server Connection Properties' section, 'Use Secret Vault' is checked and highlighted with a red box. 'Runtime Environment' is 'redhat8ptfmqa.informatica.com', 'SQL Server Version' is 'SQL Server 2008', 'Authentication Mode' is 'SQL Server Authentication', 'Domain' is empty, 'User Name' is 'jsmith', 'Password' is checked and highlighted with a red box, 'Host' is 'psv46impqa', and 'Port' is '1433'.

3. Select the runtime environment to be used with the connection.

If you use an external secrets manager, the runtime environment you select must contain a local Secure Agent that runs the SecretManagerApp service. The Hosted Agent, serverless agents, and cloud-hosted agents can't connect to an external secrets manager.

4. Configure the connection-specific properties.

For example, if you configure a flat file connection, enter the directory where the files are stored, the date format for date fields in the files, and the code page of the system that hosts the files.

5. To test the connection, click **Test Connection**.
6. Click **Save**.

## Configuring a connection using sample data

You can configure a connection to use sample data. You might want to use sample data when you want to test a mapping without affecting your organization's data.

When you configure a connection to use sample data, you can choose a mock connector from a variety of connector types such as Snowflake, Google BigQuery, and Salesforce. The connection properties are already configured.

1. On the **New Connection** page, select **Sample Data**.
2. Select a mock connector to use for the connection and click **OK**.

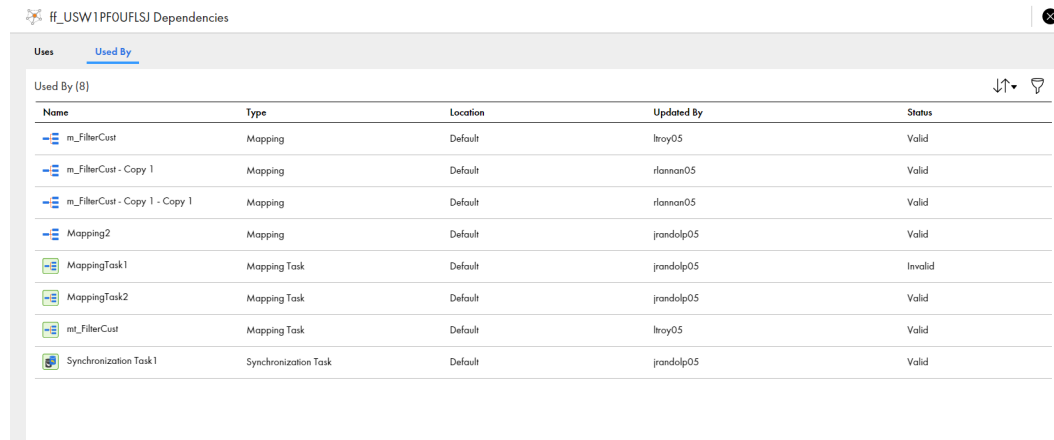
# Viewing connection dependencies

You can view object dependencies for connections. When you view object dependencies for connections, Administrator lists the runtime environments that the connection uses as well as the assets in each service that use the connection.

To view object dependencies for a connection, on the Connections page, click the **Show Dependencies** icon.

The **Dependencies** page opens with showing the Uses tab by default. To see the assets that use the connection, select the Used By tab.

The following image shows the asset dependencies on the Used By tab for a connection:



The screenshot shows the 'Used By' tab for a connection named 'ff\_USW1PFOUFLSJ'. The table lists 8 assets used by the connection, with columns for Name, Type, Location, Updated By, and Status.

Name	Type	Location	Updated By	Status
m_FilterCust	Mapping	Default	liray05	Valid
m_FilterCust - Copy 1	Mapping	Default	rlannan05	Valid
m_FilterCust - Copy 1 - Copy 1	Mapping	Default	rlannan05	Valid
Mapping2	Mapping	Default	grandalp05	Valid
MappingTask1	Mapping Task	Default	grandalp05	Invalid
MappingTask2	Mapping Task	Default	grandalp05	Valid
mt_FilterCust	Mapping Task	Default	liray05	Valid
Synchronization Task1	Synchronization Task	Default	grandalp05	Valid

To sort the objects that appear on the page, click the sort icon and select the column name for the property you want to sort by.

To filter the objects that appear on the dependencies page, click the **Filter** icon. Use filters to find specific objects. To apply a filter, click **Add Field**, select the property to filter by, and then enter the property value. You can specify multiple filters. For example to find a mapping called "MyMapping," add the Type filter and specify Mapping. Then add the Name filter and enter "MyMapping."

## CHAPTER 3

# ActiveCampaign connection properties

When you create an ActiveCampaign connection, configure the connection properties.

The following table describes the ActiveCampaign connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	ActiveCampaign
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
API Base URL	The base URL to connect to the ActiveCampaign application. For example: <a href="https://youraccountname.api-us1.com">https://youraccountname.api-us1.com</a>
API Token	The API token to access the ActiveCampaign account using token-based authentication.

## CHAPTER 4

# Adabas CDC Connection Properties

When you configure an Adabas CDC connection, you must set the connection properties.

The following table describes Adabas CDC connection properties:

Property	Description
Connection Name	A name for the Adabas CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Adabas CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Adabas CDC, the type must be <b>Adabas CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Adabas change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ADACDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Adabas instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Adabas source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.



Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None.</b> Do not use encryption.</li> <li>- <b>AES 128-bit.</b> Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit.</b> Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit.</b> Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.  Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ADACDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Adabas table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 963 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 5

# Adabas connection properties

When you configure an Adabas connection, you must set the connection properties.

The following table describes the Adabas connection properties:

Property	Description
Connection Name	A name for the Adabas connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Adabas connection. Maximum length is 4000 characters.
Type	Type of connection. For Adabas, the type must be <b>Adabas</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Adabas runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example:  ADALSNR:14673
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name in the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processing transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.

Property	Description
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For Adabas data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>
Write Mode	<p>Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> <p>Default is <b>Confirm Write On</b>.</p>

## CHAPTER 6

# Adaptive Insights Connection Properties

You can create a connection on the **Connections** page or when you create a task. When you create an Adaptive Insights connection, you must configure the connection properties. After you create a connection, it becomes available to all users who have access to the organization.

The following table describes the Adaptive Insights connection properties:

Connection Attributes	Description
Username	Required. The username of the registered user.
Password	Required. The password set by the user.
Locale	Optional. The language in which the system response messages appear. It is also used to interpret and format incoming and outgoing numbers and dates.
Instance Code	Required. The code indicates whether a particular user is logged in via default instance or another instance. Default value is <code>https://api.AdaptiveInsights.com/v1.svc</code>
Start Date	Optional. Indicates the range attribute from which the Secure Agent must read the data.
End Date	Optional. Indicates the range attribute till which the Secure Agent must read the data.
Dimensions	Optional. Indicates the dimension in which each row of data is grouped and exported for a particular dimension tag.

## CHAPTER 7

# Adobe Analytics connection properties

When you create an Adobe Analytics connection, configure the connection properties.

The following table describes the Adobe Analytics connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Adobe Analytics
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent or a Hosted Agent.
Client ID	The client ID of the service account.
Client Secret	The client secret of the service account.
Technical Account ID	The technical account ID of the service account.
Organization ID	The organization ID of the service account.
Private Key	The private key generated when you configure the Service Account Integration.
IMS Host	The base URL of Adobe Identity Management System.
IMS Exchange	The exchange URL of Adobe Identity Management System.

## CHAPTER 8

# Adobe Analytics Mass Ingestion connection properties

When you set up an Adobe Analytics Mass Ingestion connection, you must configure the connection properties.

Adobe Analytics uses a JSON Web Token (JWT) to authenticate the Adobe Analytics Mass Ingestion connection. To use an Adobe Analytics Mass Ingestion connection, you must create a Service Account Integration on Adobe Developer Console and then specify the service integration details in the connection properties. For more information about creating a Service Account Integration on Adobe Developer Console, see the [Adobe documentation](#).

The following table describes the connection properties for an Adobe Analytics Mass Ingestion connection:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Adobe Analytics Mass Ingestion</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the Service Account that you created on Adobe Developer Console.
Client Secret	Client secret of the Service Account that you created on Adobe Developer Console.
Technical Account ID	Technical account ID of the Service Account.
Organization ID	Organization ID of the Service Account.
Private Key	Private key that is generated when you create the Service Account Integration. The private key is required to generate the JWT.

<b>Connection property</b>	<b>Description</b>
IMS Host	Base URL of Adobe Identity Management System (IMS). The default value is: <code>ims-na1.adobelogin.com</code>
IMS Exchange	Exchange URL of IMS. The connection use the JWT to obtain an access token from Adobe by making a POST request to the exchange URL. The default value is: <code>https://ims-na1.adobelogin.com/ims/exchange/jwt</code>



## CHAPTER 9

# Adobe Experience Platform connection properties

When you set up an Adobe Experience Platform connection, you must configure the connection properties.

**Important:** Adobe Experience Platform Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

After you generate a service integration, you can get the organization specific properties that are required to generate the access token.

To obtain access token for your integration, you must first create a JSON Web Token (JWT) that encapsulates your client credentials. For each API session, you can exchange your JWT for an access token from Adobe IMS. The token identifies your integration and grants access to the services you have configured.

The following table describes the Adobe Experience Platform connection properties that are required to generate a JWT token every time you connect to Adobe Experience Platform:

Property	Description
Environment	The Adobe Experience Platform environment. Select prod.
Private Key Path	Path of the private key on the Secure Agent machine. Enter the private key path without the drive name. For example, if the private key file resides in the C drive path C:\a_IOD\Files\AdobeExperiencePlatform\key.der then the private key path is: file:///a_IOD/Files/AdobeExperiencePlatform/key.der
Client Id	Client ID in Adobe Experience Platform required for generating a valid access token.
Client Secret	The client secret key in Adobe Experience Platform required for generating a valid access token.
Account Id	The Adobe Experience Platform Account ID.
IMS Org	The Adobe Identity Management System (IMS) Organization ID.
Sandbox Name	Optional. Name of the Adobe Experience Platform sandbox account that you want to connect to.

## CHAPTER 10

# Advanced FTP Connection properties

When you set up an Advanced FTP connection, you must configure the connection properties.

The following table describes the Advanced FTP connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the FTP server.
Port	The port number to use for connecting to the FTP server. If left blank, the default port number is 21.
Username	User name to connect to the FTP server.
Password	Password to connect to the Advanced FTP connection.
Folder Path	The directory to use after connecting to the FTP server.
Use passive mode	Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. The default value is <b>Yes</b> . In Active mode, the server will attempt to connect back to a port on the connection client in order to perform the data transfer. In Passive mode, the server does not need to connect back to a port on the connection client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the server, you may want to change the mode to Passive by selecting <b>Yes</b> for this option.
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.

Connection property	Description
Connection Retry Attempts	The number of times to connect to retry the FTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support international characters.
List Parser	The list parser to use for the server connection. If the field is left blank, the Advanced FTP connection will attempt to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser will be used. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting will ignore any user specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any user-specified values.

# CHAPTER 11

## Advanced FTP V2 connection properties

When you set up an Advanced FTP V2 connection, you must configure the connection properties.

The following table describes the Advanced FTP V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={} \ \ ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced FTP V2</b> connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent.
Host	The host name or IP address of the FTP server.
Port	The port number to use for connecting to the FTP server. If left blank, the default port number 21 is used.
Username	User name to connect to the FTP server.
Password	Password to connect to the FTP server.
Folder Path	The directory to use after connecting to the FTP server.
Use passive mode	Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. The default value is <b>Yes</b> .  In Passive mode, the server does not need to connect back to a port on the connection client, which is a firewall-friendly mode. If you have problems with connecting to the server, you might want to change the mode to Passive by selecting <b>Yes</b> for this option. In Passive mode, depending on the FTP server, the connection may require high port range based on the port availability to transfer data.  In Active mode, the server attempts to connect back to a port on the connection client to perform the data transfer.

Connection property	Description
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the FTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings such as UTF-8 can be specified to support international characters.
List Parser	The list parser to use for the server connection. If the field is left blank, the Advanced FTP V2 Connector attempts to use the MLSD parser. If the MLSD parser is not supported by the server, the UNIX parser is used. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting ignores any user specified value.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting ignores any user-specified value.
Bandwidth	Controls the maximum amount of network resources used for file transfers. The value is applicable for file uploads and downloads. Default is 0. 0 indicates that the bandwidth is not restricted.
Bandwidth Unit	The unit of the network bandwidth used for file transfer. You can choose one of the following units: - Kilobytes per second (KBps) - Megabytes per second (MBps)

**Note:** Advanced FTP V2 connector doesn't support NTLM proxy authentication.

## CHAPTER 12

# Advanced FTPS connection properties

When you set up an Advanced FTPS connection, you must configure the connection properties.

The following table describes the Advanced FTPS connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
Username	User name to connect to the FTPS server.
Password	Password to connect to the FTPS server.
Folder Path	The directory to use after connecting to the server.
Use passive mode	Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. The default value is <b>Yes</b> . In Active mode, the server will attempt to connect back to a port on the connection client in order to perform the data transfer. In Passive mode, the server does not need to connect back to a port on the connection client, which is a more firewall-friendly mode. Therefore, if you have problems with connecting to the server, you may want to change the mode to Passive by selecting <b>Yes</b> for this option.
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.

Connection property	Description
Connection Retry Attempts	The number of times to connect to retry the FTPS connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support international characters.
Trusted Server	Specify whether the FTPS server is a trusted server. The FTPS Connector only supports a trusted server.
List Parser	The list parser to use for the server connection. If the field is empty, the Advanced FTPS Connector tries to use the MLSD parser. If the server does not support the MLSD parser, the connector uses the UNIX parser. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting will ignore any user specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting will ignore any user-specified values.

## CHAPTER 13

# Advanced FTPS V2 connection properties

When you set up an Advanced FTPS V2 connection, you must configure the connection properties.

The following table describes the Advanced FTPS V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced FTPS V2</b> connection type.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
Username	User name to connect to the FTPS server.
Password	Password to connect to the FTPS server.
Folder Path	The directory to use after connecting to the server.
Use passive mode	Indicates whether the connection uses <b>Passive</b> or <b>Active</b> mode. Specify <b>Yes</b> to use <b>Passive</b> mode. Specify <b>No</b> to use <b>Active</b> mode. The default value is <b>Yes</b> . In Passive mode, the server does not need to connect back to a port on the connection client, which is a firewall-friendly mode. If you have problems with connecting to the server, you might want to change the mode to Passive by selecting <b>Yes</b> for this option. In Passive mode, depending on the FTPS server, the connection may require high port range based on the port availability to transfer data. In Active mode, the server attempts to connect back to a port on the connection client to perform the data transfer.



Connection property	Description
Data Connection Start Port	The starting port number to use for the data connection.
Data Connection End Port	The ending port number to use for the data connection.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs will if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the Advanced FTP V2 connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .
Control Encoding	If left blank, the connection uses the ISO standard ISO-8859-1. If supported by the server, other encodings like UTF-8 can be specified to support international characters.
Trusted Server	Specify whether the FTPS server is a trusted server. The Advanced FTP V2 Connector only supports a trusted server.
List Parser	The list parser to use for the server connection. If the field is empty, the Advanced FTP V2 Connector tries to use the MLSD parser. If the server does not support the MLSD parser, the connector uses the UNIX parser. If you experience problems listing directories, select a different list parser.
Date Format	This date format is applied if the server returns a date that is different from the selected list parser default. If your location requires a different date format (for example, d MMM yyyy), specify the date format in this field. Not all list parsers support the date format setting. List parsers that do not support the date format setting ignores any user specified values.
Recent Date Format	Specify the date format to use when parsing the recent last modified date for each file. The recent date format applies in UNIX-based systems and appears on entries less than a year old. If your location requires a specific date format (for example, d MMM HH:mm), specify that pattern in this field. Not all list parsers support the recent date format setting. List parsers that do not support the recent date format setting ignores any user-specified values.
Connection Type	Indicates if the connection type is IMPLICIT_SSL or EXPLICIT_SSL. - IMPLICIT_SSL. The connection automatically starts as an SSL connection. - EXPLICIT_SSL. After initial authentication with the FTPS server, the connection is encrypted with SSL or TLS depending on the security protocol you select. Default is IMPLICIT_SSL.
SecurityProtocol	Indicates whether SSL or TLS is used for EXPLICIT_SSL connections. Default is SSL.
Key Store File	The path and file name of the keystore file. The keystore file contains the certificates to authenticate the FTPS server.
Key Store Password	The password for the keystore file required to access the Trusted Server Certificate Store.

Connection property	Description
Key Alias	The alias of the individual key.
Key Store Type	Indicates if the type of the keystore is Java KeyStore (JKS) or Public Key Cryptology Standard (PKCS12). Default is JKS.
Bandwidth	Controls the maximum amount of network resources used for file transfers. The value is applicable for file uploads and downloads. Default is 0. 0 indicates that the bandwidth is not restricted.
Bandwidth Unit	The unit of the network bandwidth used for file transfer. You can choose one of the following units: <ul style="list-style-type: none"> <li>- Kilobytes per second (KBps)</li> <li>- Megabytes per second (MBps)</li> </ul>

**Note:** Advanced FTPS V2 connector doesn't support NTLM proxy authentication.

## CHAPTER 14

# Advanced SFTP connection properties

When you set up an Advanced SFTP connection, you must configure the connection properties.

The following table describes the Advanced SFTP connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 21.
Username	User name to connect to the SFTP server.
Password	Password to connect to the SFTP server.
Folder Path	The directory to use after connecting to the server.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If left blank, the default timeout is 120 seconds.
Connection Retry Attempts	The number of times to connect to retry the SFTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. <b>Note:</b> For instance, if you want to retry to connect up to 10 times with a five second delay between retries, then specify <b>10</b> for the <b>Connection Retry Attempts</b> and <b>5</b> for the <b>Connection Retry Interval</b> .

## CHAPTER 15

# Advanced SFTP V2 connection properties

When you set up an Advanced SFTP V2 connection, you must configure the connection properties.

The following table describes the Advanced SFTP V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	Select the <b>Advanced SFTP V2</b> connection type.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Host	The host name or IP address of the server. The host name is case insensitive and must be unique within the domain. The name cannot exceed 24 characters. It can contain letters (A to Z), digits (0 to 9), period (.) special character, and minus (-) sign.
Port	The port number to use to connect to the server. Default is 21.
Username	User name to connect to the SFTP server.
Password	Password to connect to the SFTP server.
Folder Path	The directory to use after connecting to the server.
Timeout	The number of seconds to wait when attempting to connect to the server. A timeout occurs if the connection cannot be established in the specified amount of time. If left blank, the default value of 120 seconds is used.
Connection Retry Attempts	The number of times to connect to retry the SFTP connection if a connection cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, no retries will be attempted.

Connection property	Description
Connection Retry Interval	The number of seconds to wait between each connection retry attempt. For example, if you want to retry to connect up to 10 times with a five second delay between retries, then specify 10 for the Connection Retry Attempts and 5 for the Connection Retry Interval.
Private Key File	The name of the SSH private key file along with the path where the file is stored. Ensure that the file path is on the machine that hosts the Secure Agent. For example, C:/SSH/my_keys/key.ppk
Private Key Passphrase	Specify the passphrase to encrypt the SSH private key.
Use Curve Kex Algorithm	Enable additional key exchange algorithms such as curve, and keyed-hash algorithm such as, - hmac-sha2-512, and -hmac-sha2-256.
Bandwidth	Controls the maximum amount of network resources used for file transfers. The value is applicable for file uploads and downloads. Default is 0. 0 indicates that the bandwidth is not restricted.
Bandwidth Unit	The unit of the network bandwidth used for file transfer. You can choose one of the following units: - Kilobytes per second (KBps) - Megabytes per second (MBps)
Use File Integration Proxy Server	The connector connects to the SFTP server through the file integration proxy server. Verify that the following prerequisites are met: - You must have the File Integration Service license to use this option. - You must define a proxy server in File Servers. - If you don't have the File Integration Service proxy, you need to use the agent proxy through the proxy.ini file.
Proxy Server Host Name	Host name or IP address of the outgoing File Integration Service proxy server.
Proxy Server Port	Port number of the outgoing File Integration Service proxy server.

**Note:** Advanced SFTP V2 connector doesn't support NTLM proxy authentication.

## CHAPTER 16

# Amazon Athena connection properties

Create an Amazon Athena connection to read from Amazon Athena.

## Prepare for authentication

You can configure permanent IAM credentials and EC2 instance profile authentication types to access Amazon Athena.

To use the permanent IAM credentials authentication, create an IAM user, attach the required policies, and generate the access and secret key in the AWS Console. Keep these details handy to use in the connection properties.

To use EC2 instance profile authentication, install the Secure Agent on the EC2 instance and attach the EC2 role to the EC2 instance.

Before you configure the connection properties, create the minimal Amazon S3 policy, AWS Glue data catalog policy, and the Amazon Athena policies. Define the required permissions for the IAM user or EC2 role in the policies.

Attach the policies to the IAM user or EC2 role based on the authentication type that you want to configure.

## Create an Amazon S3 policy

Create an Amazon S3 policy in the AWS console and define the permissions to store Amazon Athena results on Amazon S3.

Use the following minimum required permissions to store Amazon Athena results on Amazon S3:

- PutObject
- GetObject
- DeleteObject
- ListBucket
- GetBucketLocation
- ListAllMyBuckets
- GetBucketAcl

You can use the following sample Amazon S3 policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## Create an AWS Glue data catalog policy

You can use AWS IAM to define policies and roles to access resources used by AWS Glue.

Amazon Athena uses the AWS Glue Data Catalog to store and retrieve table metadata for the Amazon S3 data in your AWS account.

You can use the following sample policy for AWS Glue Data Catalog:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## Create an Amazon Athena policy

Specify the minimum required permissions for Amazon Athena Connector to read data from views and external tables in the AWS Glue data catalog and to read and query Amazon S3 files.

You can use the following minimum required permissions:

- GetWorkGroup
- GetTableMetadata
- StartQueryExecution

- GetQueryResultsStream
- ListDatabases
- GetQueryExecution
- GetQueryResults
- GetDatabase
- ListTableMetadata
- GetDataCatalog
- CreatePreparedStatement
- DeletePreparedStatement

You can use the following sample policy for Amazon Athena:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "athena:GetWorkGroup",
        "athena:GetTableMetadata",
        "athena:StartQueryExecution",
        "athena:GetQueryResultsStream",
        "athena:ListDatabases",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetDatabase",
        "athena:ListTableMetadata",
        "athena:GetDataCatalog",
        "athena:CreatePreparedStatement",
        "athena>DeletePreparedStatement"
      ],
      "Resource": [
        "arn:aws:athena:*:*:workgroup/*",
        "arn:aws:athena:*:*:datacatalog/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

## Connect to Amazon Athena

Let's configure the Amazon Athena connection properties to connect to Amazon Athena.

### Before you begin

Before you get started, you'll need to get information from your Amazon Athena account based on the authentication type that you want to configure.

To configure permanent IAM credentials authentication, get the access key and secret key.



To configure EC2 instance profile authentication, set up an EC2 instance and attach the EC2 role to the EC2 instance.

Depending on the authentication method you choose, attach the appropriate policies to the IAM user or EC2 role.

Check out [“Prepare for authentication” on page 58](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Amazon Athena
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.

## Authentication types

You can configure permanent IAM credentials and EC2 instance profile authentication types to access Amazon Athena.

### Permanent IAM credentials

Permanent IAM credentials authentication is the default type that requires the access key and secret key of the IAM user to connect to Amazon Athena.

The following table describes the basic connection properties for permanent IAM credentials authentication:

Property	Description
Access Key	The access key of the IAM user to connect to Amazon Athena.
Secret Key	The secret key of the IAM user to connect to Amazon Athena.
JDBC URL	The URL to connect to Amazon Athena. Enter the JDBC URL in the following format: <code>jdbc:awsathena://AwsRegion=&lt;region_name&gt;;S3OutputLocation=&lt;S3_Output_Location&gt;;</code>

## EC2 instance profile

You can configure AWS Identity and Access Management (IAM) authentication to connect to Amazon Athena when the Secure Agent is installed on an Amazon Elastic Compute Cloud (EC2) system.

The following table describes the basic connection properties for EC2 instance profile authentication:

Property	Description
JDBC URL	The URL of the Amazon Athena connection. Enter the JDBC URL in the following format: <code>jdbc:awsathena://AwsRegion=&lt;region_name&gt;;S3OutputLocation=&lt;S3_Output_Location&gt;;</code>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Customer Master Key ID	The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access when you stage data in Amazon S3. The customer master key serves to encrypt your data at the destination before they are saved in Amazon S3. You can either enter the customer-generated customer master key ID or the default customer master key ID. Ensure that you generate the customer master key for the same region where your Amazon S3 bucket resides. For more information about using customer master keys with Amazon Athena, see <a href="#">Encryption</a> in the AWS documentation.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, you can use the serverless runtime environment to connect to Informatica Intelligent Cloud Services through the proxy server.

You can use the unauthenticated or authenticated proxy server.

To configure proxy settings for the serverless runtime environment, see *Runtime Environments* in the Administrator help.

## CHAPTER 17

# Amazon Aurora connection properties

When you set up an Amazon Aurora connection, configure the connection properties.

**Important:** Amazon Aurora Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use MySQL Connector to access Amazon Aurora MySQL.

The following table describes the Amazon Aurora connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Amazon Aurora connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Host	Amazon Aurora server host name. For example, <code>xyzcloud-cluster.cluster-cj8irzt1lmku.us-west-2.rds.amazonaws.com</code> .
Port	Amazon Aurora directory server port number.
Database Name	Name of the Amazon Aurora database.
Code Page	The code page of the database server defined in the connection. Select one of the following code pages: <ul style="list-style-type: none"><li>- MS Windows Latin 1</li><li>- UTF-8</li><li>- Shift-JIS</li><li>- ISO 8859-15 Latin 9 (Western European)</li><li>- ISO 8859-2 Eastern European</li><li>- ISO 8859-3 Southeast European</li><li>- ISO 8859-5 Cyrillic</li><li>- ISO 8859-9 Latin 5 (Turkish)</li><li>- IBM EBCDIC International Latin-1</li></ul>

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch metadata from the source.</p> <p>For example, <code>connectTimeout=180000</code></p> <p>For more metadata advanced connection properties, see <a href="#">MariaDB Connector for JDBC</a>.</p>
Run-time Advanced Connection Properties	<p>Additional properties for the ODBC driver required at run time.</p> <p>For example, <code>charset=sjis;readtimeout=180</code></p> <p>For more run-time advanced connection properties, see <a href="#">MariaDB Connector for ODBC</a>.</p>
Username	User name of the Amazon Aurora account.
Password	Password of the Amazon Aurora account.

## CHAPTER 18

# Amazon DynamoDB connection properties

When you set up an Amazon DynamoDB connection, you must configure the connection properties.

**Important:** Amazon DynamoDB Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Amazon DynamoDB connection properties:

Connection property	Description
Access Key	The access key ID used to access the Amazon account resources. <b>Note:</b> Ensure that you have valid AWS credentials before you create a connection.
Secret Key	The secret access key used to access the Amazon account resources. This value is associated with the access key and uniquely identifies the account.
Region	The AWS region associated with the account.

## CHAPTER 19

# Amazon DynamoDB V2 connection properties

When you set up an Amazon DynamoDB V2 connection, you must configure the connection properties.

The following table describes the Amazon DynamoDB V2 connection properties:

Connection property	Description
Connection Name	The name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Amazon DynamoDB V2.
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent or serverless runtime environment.
Access Key	The access key to access Amazon DynamoDB. You can optionally enter the access key when you use assume role for an IAM user.
Secret Key	The secret key to access Amazon DynamoDB. This value is associated with the access key and uniquely identifies the account. You can optionally enter the secret key when you use assume role for an IAM user.
Region Name	The AWS region of Amazon DynamoDB that you want to access.
Assume Role	Enables the IAM entity to assume a role.
Assume Role ARN	The ARN of the IAM role assumed by the IAM user to generate the temporary security credentials.

Connection property	Description
External Id	The external ID to generate the temporary security credentials.
Additional Options	<p>Optional properties in key-value pairs that you can configure when you read data from or write data to Amazon DynamoDB. To specify more than one property, separate the key-value pairs with an ampersand. For example, <code>propertyName1=&lt;value1&gt;&amp;propertyName2=&lt;value2&gt;</code></p> <p>You can configure the following parameter: <b>prefixFieldNames=true</b>.</p> <p>If you configure this parameter in the source connection, it prefixes an underscore character to all the columns when you import the table. If you configure this parameter in the target connection, it removes the first character from all the target columns.</p>

## CHAPTER 20

# Amazon Kinesis connection properties

The Amazon Kinesis connection is a messaging connection. Use the Amazon Kinesis connection to access Amazon Kinesis Data Streams or Amazon Kinesis Data Firehose as targets.

## Amazon Kinesis Firehose connection properties

When you set up an Amazon Kinesis Firehose connection, you must configure the connection properties.

The following table describes the Amazon Kinesis Firehose connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identity the connection. The description cannot exceed 4,000 characters.
Type	The Amazon Kinesis connection type. If you do not see the Amazon Kinesis connection type, go to the <b>Add-On Connectors</b> page to enable the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service	The type of Kinesis Service that you want to use. Select <b>Kinesis Firehose</b> .
AWS Access Key ID	The access key ID of the Amazon AWS user account.
AWS Secret Access Key	The secret access key for the Amazon AWS user account.



Property	Description
Region	<p>Region where the endpoint for your service is available. You can select one of the following values:</p> <ul style="list-style-type: none"> <li>- us-east-2. Indicates the US East (Ohio) region.</li> <li>- us-east-1. Indicates the US East (N. Virginia) region.</li> <li>- us-west-1. Indicates the US West (N. California) region.</li> <li>- us-west-2. Indicates the US West (Oregon) region.</li> <li>- ap-northeast-1. Indicates the Asia Pacific (Tokyo) region.</li> <li>- ap-northeast-2. Indicates the Asia Pacific (Seoul) region.</li> <li>- ap-northeast-3. Indicates the Asia Pacific (Osaka-Local) region.</li> <li>- ap-south-1. Indicates the Asia Pacific (Mumbai) region.</li> <li>- ap-southeast-1. Indicates the Asia Pacific (Singapore) region.</li> <li>- ap-southeast-2. Indicates the Asia Pacific (Sydney) region.</li> <li>- ca-central-1. Indicates the Canada (Central) region.</li> <li>- cn-north-1. Indicates the China (Beijing) region.</li> <li>- cn-northwest-1. Indicates the China (Ningxia) region.</li> <li>- eu-central-1. Indicates the EU (Frankfurt) region.</li> <li>- eu-west-1. Indicates the EU (Ireland) region.</li> <li>- eu-west-2. Indicates the EU (London) region.</li> <li>- eu-west-3. Indicates the EU (Paris) region.</li> <li>- sa-east-1. Indicates the South America (São Paulo) region.</li> <li>- us-gov-west-1. Indicates AWS GovCloud (US-West) region.</li> <li>- us-gov-east-1. Indicates AWS GovCloud (US-East) region.</li> </ul> <p>A streaming ingestion and replication task does not support ap-northeast-3 region.</p>
Connection TimeOut (ms)	<p>Optional. Number of milliseconds that the Data Ingestion and Replication service waits to establish a connection to the Kinesis Firehose after which it times out.</p> <p>Default is 10,000 milliseconds.</p>
AWS Credential Profile Name	<p>An AWS credential profile defined in the credentials file.</p> <p>A mapping accesses the AWS credentials through the profile name at run time. If you do not provide an AWS credential profile name, the mapping uses the access key ID and secret access key that you specify when you create the connection.</p>
ARN of IAM Role	<p>The Amazon Resource Name specifying the role of an IAM user. Applies to Cross-Account IAM Roles authentication.</p>
External ID	<p>The external ID for an IAM role is an additional restriction that you can use in an IAM role trust policy to designate who can assume the IAM role. Applies to Cross-Account IAM Roles authentication.</p>

# Amazon Kinesis Streams connection properties

When you set up an Amazon Kinesis Streams connection, you must configure the connection properties.

The following table describes the Amazon Kinesis Streams connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identity the connection. The description cannot exceed 4,000 characters.
Type	The Amazon Kinesis connection type. If you do not see the Amazon Kinesis connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service	The type of Kinesis Service that you want to use. Select <b>Kinesis Streams</b> .
AWS Access Key ID	The access key ID of the Amazon AWS user account.
AWS Secret Access Key	The secret access key for your Amazon AWS user account.
Region	Region where the endpoint for your service is available. You can select one of the following values: <ul style="list-style-type: none"> <li>- us-east-2. Indicates the US East (Ohio) region.</li> <li>- us-east-1. Indicates the US East (N. Virginia) region.</li> <li>- us-west-1. Indicates the US West (N. California) region.</li> <li>- us-west-2. Indicates the US West (Oregon) region.</li> <li>- ap-northeast-1. Indicates the Asia Pacific (Tokyo) region.</li> <li>- ap-northeast-2. Indicates the Asia Pacific (Seoul) region.</li> <li>- ap-northeast-3. Indicates the Asia Pacific (Osaka-Local) region.</li> <li>- ap-south-1. Indicates the Asia Pacific (Mumbai) region.</li> <li>- ap-southeast-1. Indicates the Asia Pacific (Singapore) region.</li> <li>- ap-southeast-2. Indicates the Asia Pacific (Sydney) region.</li> <li>- ca-central-1. Indicates the Canada (Central) region.</li> <li>- cn-north-1. Indicates the China (Beijing) region.</li> <li>- cn-northwest-1. Indicates the China (Ningxia) region.</li> <li>- eu-central-1. Indicates the EU (Frankfurt) region.</li> <li>- eu-west-1. Indicates the EU (Ireland) region.</li> <li>- eu-west-2. Indicates the EU (London) region.</li> <li>- eu-west-3. Indicates the EU (Paris) region.</li> <li>- sa-east-1. Indicates the South America (São Paulo) region.</li> <li>- us-gov-west-1. Indicates AWS GovCloud (US-West) region.</li> <li>- us-gov-east-1. Indicates AWS GovCloud (US-East) region.</li> </ul> A streaming ingestion and replication task does not support ap-northeast-3 region.

<b>Property</b>	<b>Description</b>
Connection TimeOut (ms)	Optional. Number of milliseconds that the Data Ingestion and Replication service waits to establish a connection to the Kinesis Streams after which it times out. Default is 10,000 milliseconds.
AWS Credential Profile Name	An AWS credential profile defined in the credentials file. A mapping accesses the AWS credentials through the profile name at run time. If you do not provide an AWS credential profile name, the mapping uses the access key ID and secret access key that you specify when you create the connection.
ARN of IAM Role	The Amazon Resource Name specifying the role of an IAM user. Applies to Cross-Account IAM Roles authentication.
External ID	The external ID for an IAM role is an additional restriction that you can use in an IAM role trust policy to designate who can assume the IAM role. Applies to Cross-Account IAM Roles authentication.

## CHAPTER 21

# Amazon Redshift connection properties

When you set up an Amazon Redshift connection, you must configure the connection properties.

**Important:** Amazon Redshift Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Amazon Redshift V2 Connector to access Amazon Redshift.

The following table describes the Amazon Redshift connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	User name of the Amazon Redshift account.
Password	Password for the Amazon Redshift account.
Schema	Amazon Redshift schema name. Default is public.
AWS Access Key ID	Optional. Amazon S3 bucket access key ID. To run tasks on Secure Agent installed on an EC2 system, you might leave the Access Key ID blank. To run tasks on Secure Agent that is not installed on an EC2 system, you must provide the Access Key ID.
AWS Secret Access Key	Optional. Amazon S3 bucket secret access key ID. To run tasks on Secure Agent installed on an EC2 system, you might leave the Secret Access Key blank. To run tasks on Secure Agent that is not installed on an EC2 system, you must provide the Secret Access Key.
Master Symmetric Key	Optional. Amazon S3 encryption key. Provide a 256-bit AES encryption key in the Base64 format.
Customer Master Key ID	Optional. Specify the customer master key ID or alias name generated by AWS Key Management Service (AWS KMS). You must generate the customer master key ID for the same region where Amazon S3 bucket reside. You can either specify the customer generated customer master key ID or the default customer master key ID.

Connection property	Description
JDBC URL	Amazon Redshift connection URL.
Number of bytes needed to support multibytes for varchar	<p>Applicable to Create Target. Reads the Varchar precision of the source table and creates the target table with 1x/2x/3x/4x times of the source precision to successfully write multibyte characters in the target table.</p> <p><b>Note:</b> You cannot create a target table if the Varchar precision exceeds 65535 that is maximum allowed.</p>

**Note:** When you test a connection, Secure Agent validates Redshift connection. Validation of AWS Access key and AWS Secret key requires the Amazon S3 bucket name present in the advanced source and target properties. Therefore, Secure Agent validates AWS Access key and AWS Secret key when a synchronization or mapping task is run.

## CHAPTER 22

# Amazon Redshift V2 connection properties

Create an Amazon Redshift V2 connection to read from or write data to Amazon Redshift.

## Prepare for authentication

You can configure **Default** and **Redshift IAM Authentication via AssumeRole** authentication types in an Amazon Redshift V2 connection to connect to Amazon Redshift. Additionally, you need to complete the S3 staging prerequisites to access S3 resources. You can also configure encryption, if required, to connect to Amazon Redshift.

**Note:** Application ingestion and replication and database ingestion and replication tasks do not support Redshift IAM authentication via AssumeRole unless you use an EC2 instance to assume the role.

See the following sections for a summary of the authentication, staging, and encryption prerequisites.

### Authentication prerequisites

Before you begin, you need to have a registered user account with Amazon Redshift.

Get the minimum required details from your Amazon Redshift account from the AWS Console for the authentication type that you want to configure, as listed in the following table:

Default authentication	Redshift IAM Authentication via Assume Role
<ul style="list-style-type: none"><li>- JDBC URL</li><li>- User name</li><li>- Password</li></ul>	<ul style="list-style-type: none"><li>- JDBC URL</li><li>- User name</li><li>- Database name</li><li>- Cluster identifier</li><li>- Redshift IAM role ARN*</li></ul>
<p>*To use the Redshift IAM role ARN, configure the Redshift IAM role ARN with the required trust policies to generate temporary security credentials to access Amazon Redshift. For instructions, see <a href="#">"Configure an assume role for Amazon Redshift" on page 77</a>.</p>	

### Staging prerequisites

To enable staging on Amazon S3 and to gain access to S3 resources when you read or write data, you need to configure the staging properties in the Amazon Redshift V2 connection.

The following table summarizes the staging options that you can configure in the connection for both default and Redshift IAM Authentication via AssumeRole authentication and the tasks that you need to perform to get the required details for S3 staging:

S3 staging options	Tasks
<p>Generate temporary credentials for the IAM user who assumes the S3 IAM role to access S3 staging.</p>	<p><b>AWS configurations</b>            Enable IAM users to assume an S3 IAM role and generate temporary credentials.            For instructions, see the following references:</p> <ul style="list-style-type: none"> <li>- <a href="#">“Generate temporary security credentials using AssumeRole for Amazon S3 staging” on page 81.</a></li> <li>- <a href="#">Using an assume role for Amazon S3 resources</a> How-To Library article.</li> </ul> <p><b>Redshift V2 connection configurations</b></p> <ul style="list-style-type: none"> <li>- Enter the value of the <b>S3 IAM Role ARN</b>.</li> <li>- Enter the <b>S3 Access Key ID</b> and <b>S3 Secret Access Key</b> values.</li> </ul>
<p>Generate temporary security credentials for an EC2 instance that assumes an S3 IAM role to access S3 staging.</p>	<p><b>AWS configurations</b>            Define an EC2 instance to assume an S3 IAM role and generate the temporary credentials for S3 staging.            For instructions, see <a href="#">“Generate temporary security credentials using AssumeRole for EC2” on page 83.</a></p> <p><b>Redshift V2 connection configurations</b>            Configure the following minimum required properties:</p> <ul style="list-style-type: none"> <li>- Enable <b>Use EC2 Role to Assume Role</b>.</li> <li>- Enter the value of the <b>S3 IAM Role ARN</b>.</li> </ul>
<p>Generate the S3 access and secret access keys for the IAM user with access to the S3 bucket.</p>	<p><b>AWS configurations</b>            To generate the credentials, perform the following tasks:</p> <ol style="list-style-type: none"> <li>1. <a href="#">“Create a minimal Amazon IAM policy” on page 76.</a></li> <li>2. Create an IAM user, assign the policy to that user, and then generate the S3 access key ID and S3 secret access key in the AWS console.</li> </ol> <p>For more information about how to create an IAM user and generate keys, see the AWS documentation.</p> <p><b>Redshift V2 connection configurations</b>            Enter the <b>S3 Access Key ID</b> and <b>S3 Secret Access Key</b> values.</p>
<p>Configure IAM authentication</p>	<p><b>AWS configurations</b>            If you have an EC2 instance, and do not want to specify the keys or use the IAM role ARN, then assign the minimum policy to the EC2 with access to the S3 bucket.            For instructions, see <a href="#">“Configure IAM authentication” on page 76.</a></p> <p><b>Redshift V2 connection configurations</b>            In this case, you do not need to enable or specify any of the staging properties in the connection.</p>

### Encryption prerequisites

To configure client-side and server-side encryption for the Default authentication and Redshift IAM authentication via AssumeRole during staging, see [“Enable encryption” on page 84.](#)

# Create a minimal Amazon IAM policy

To stage the data in Amazon S3, you need to create an IAM policy with the minimum required permissions to access the S3 resources.

You can either attach the policy to the IAM user and generate the S3 access key ID and S3 secret access keys to access S3 resources. Or, if you have an EC2 instance, you can assign the minimum policy to the EC2 instance to access the S3 bucket for staging.

You need the following minimum required permissions in the policy:

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads. Applicable only for mappings in advanced mode.

You can use the following sample Amazon IAM policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>/*",
        "arn:aws:s3:::<bucket_name>"
      ]
    }
  ]
}
```

For mappings in advanced mode, you can use different AWS accounts within the same AWS region in the source and target connection. Make sure that the Amazon IAM policy confirms access to the AWS accounts specified in mappings.

**Note:** The **Test Connection** does not validate the IAM policy assigned to users. Hence, ensure that the policy assigned to the user is valid.

## Configure IAM authentication

Configure AWS Identity and Access Management (IAM) authentication and create a minimal Amazon IAM policy for both the EC2 role and Redshift role.

For instructions, see the following How-to-Library article: [Configuring AWS IAM Authentication](#)



# Configure an assume role for Amazon Redshift

To use the Redshift IAM role ARN, configure the Redshift IAM role ARN with the required trust policies to generate temporary security credentials to access Amazon Redshift.

You can use one of the following options to generate the temporary security credentials:

AWS configurations	Connection details
Option 1. Configure an AssumeRole to enable an IAM user.	To use the AssumeRole for the IAM user, specify the following IAM user details: <ul style="list-style-type: none"><li>- Redshift Access Key ID</li><li>- Redshift Secret Access Key</li><li>- Redshift IAM Role ARN</li></ul>
Option 2. Define an EC2 instance to assume a Redshift IAM role.	To use the AssumeRole for Amazon EC2: <ul style="list-style-type: none"><li>- Specify the <b>Redshift IAM Role ARN</b> value.</li><li>- Enable the <b>Use EC2 Role to Assume Role</b> check box.</li></ul>

For application ingestion and replication tasks and database ingestion and replication tasks, use Option 2 to have an EC2 role assume the Redshift IAM role.

For more information about configuring an AssumeRole, see the following How-to-Library article: [Configure AssumeRole authentication for Amazon Redshift V2 Connector](#)

Generate the temporary security credentials based on your requirement.

## Generate temporary security credential policies for Amazon Redshift

To use the temporary security credentials to connect to Amazon Redshift, both the IAM user and IAM role require policies.

The following section lists the policies required for the IAM user and IAM role:

### IAM user

An IAM user must have the `sts:AssumeRole` policy to use the temporary security credentials in the same or different AWS account. The IAM user credentials are used to key-in the Redshift access key and Redshift secret key in the connection properties.

The following sample policy allows an IAM user to use the temporary security credentials in an AWS account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ACCOUNT-HYPHENS>:role/<REDSHIFT-IAM-ROLE-NAME>"
    }
  ]
}
```

**Note:** To run mappings in advanced mode, ensure to assign this policy to the Worker node role.

### Redshift IAM role trust policy

The Redshift IAM role policy pertains to the role that is specified in the Redshift IAM Role ARN. An IAM role must have a trust policy attached with it to allow the IAM user to access Redshift using the temporary security credentials.

The following policy is a sample trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::AWS-account-ID:<IAM-USER>" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

For example, you can specify the role or user in the following format:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<AWS-account>:role/<name-of-the-role>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<AWS-account>:user/<name-of-the-user>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### Redshift IAM role trust policy for mappings in advanced mode

An IAM role must have a trust policy attached with it to allow the worker node to assume the Redshift role and access Amazon Redshift through the AssumeRole.

The following policy is a sample trust policy:

```
{
  "Effect": "Allow",
  "Principal": { "AWS": "arn:aws:iam::<ACCOUNT-ID>:role/<WORKER-NODE-ROLE-ARN>" },
  "Action": "sts:AssumeRole"
}
```

### Minimum permission policies of the Redshift IAM role

The following policy shows the permissions required to the Redshift IAM Role, which will be assumed by an IAM user to connect to the Redshift database using an existing Amazon Redshift user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials",
        "redshift:DescribeClusters"
      ]
    }
  ]
}
```



Consider the following prerequisites when you use temporary security credentials using AssumeRole for EC2:

- To use temporary security credentials using AssumeRole for EC2, install the Secure Agent on an AWS service such as Amazon EC2.
- The EC2 role attached to the AWS EC2 service must not have access to Amazon Redshift but needs to have permission to assume another IAM role.
- The IAM role that needs to be assumed by the EC2 role must have a permission policy and a trust policy attached to it.

To configure an EC2 role to assume the IAM Role provided in the Redshift IAM Role ARN connection property, select the **Use EC2 Role to Assume Role** check box in the connection properties.

#### EC2 service role trust policy

The following is a sample trust policy that is defined in a trust relationship of the EC2 role attached to the EC2 instance:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

The following is a sample trust policy of the Redshift IAM role when you enable EC2 assume role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<Account-ID:role>/ec2_role_attached_to_ec2_instance"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

The permission policy that is required to be attached to the EC2 instance is same as the policy defined for the IAM user.

## Configure an assume role for Amazon S3 staging

To configure AssumeRole authentication for S3 staging, you need to attach the minimum permission policies and trust policies for the IAM user and IAM role in the AWS console.

An IAM user can use the AssumeRole to temporarily gain access to the Amazon S3 resources. For more information about using an assume role for Amazon S3 resources, you can also refer to the How-to-Library article: [Using an assume role for Amazon S3 resources](#)

You can generate temporary security credentials using AssumeRole for Amazon S3 staging to access the Amazon S3 staging bucket. If you want EC2 instances to assume an IAM role to gain access to the S3 staging bucket securely, use the temporary security credentials generated using AssumeRole for EC2 instances.

**Note:** Do not use the root user credentials of the AWS account to generate the temporary security credentials. You need to use the credentials of an IAM user to generate the temporary security credentials.

Generate the temporary security credentials based on your requirement.

## Generate temporary security credentials using AssumeRole for Amazon S3 staging

You can use the temporary security credentials using AssumeRole to access the Amazon S3 staging bucket from the same or different AWS accounts.

Ensure that you have the **sts:AssumeRole** permission and a trust relationship established within the AWS accounts to use the temporary security credentials. The trust relationship is defined in the trust policy of the IAM role when you create the role. The IAM role adds the IAM user as a trusted entity allowing the IAM users to use the temporary security credentials and access the AWS accounts. For more information about how to establish the trust relationship, see the AWS documentation.

When the trusted IAM user requests for the temporary security credentials, the AWS Security Token Service (AWS STS) dynamically generates the temporary security credentials that are valid for a specified period and provides the credentials to the trusted IAM users. The temporary security credentials consist of access key ID, secret access key, and secret token.

To use the dynamically generated temporary security credentials, provide the value of the **S3 IAM Role ARN** connection property when you create an Amazon Redshift V2 connection. The IAM Role ARN uniquely identifies the AWS resources. Then, specify the time duration in seconds during which you can use the temporarily security credentials in the **Temporary Credential Duration** advanced source and target properties.

### External ID

You can specify the external ID for a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account than the IAM user or EC2 instance.

**Note:** Application ingestion and replication and database ingestion and replication tasks do not support use of External ID.

You can optionally specify the external ID in the AssumeRole request to the AWS Security Token Service (STS).

The external ID must be a string. The following sample shows an external ID condition in the assumed IAM role's trust policy:

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "dummy_external_id"
      }
    }
  }
]
```

```

    }
  }
]

```

## Temporary security credentials policy

To use the temporary security credentials to access the Amazon S3 staging bucket, both the IAM user and IAM role require policies.

The following section lists the policies required for the IAM user and IAM role:

### IAM user

An IAM user must have the `sts:AssumeRole` policy to use the temporary security credentials in the same or different AWS account.

The following sample policy allows an IAM user to use the temporary security credentials in an AWS account:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>"
    }
  ]
}

```

The following sample policy allows an IAM user for the China region to use the temporary security credentials in an AWS account:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws-cn:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>"
    }
  ]
}

```

### IAM role

An IAM role must have a `sts:AssumeRole` policy and a trust policy attached with the IAM role to allow the IAM user to access the Amazon S3 bucket using the temporary security credentials. The policy specifies the Amazon S3 bucket that the IAM user can access and the actions that the IAM user can perform. The trust policy specifies the IAM user from the AWS account that can access the Amazon S3 bucket.

The following policy is a sample trust policy:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::AWS-account-ID:<ROLE-NAME>" },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

## Temporary security credentials for KMS

To use the temporary security credentials with AWS Key Management Service (AWS KMS)-managed customer master key and enable encryption with KMS, you must create a KMS policy.

You can perform the following operations to use the temporary security credentials and enable encryption with KMS:

- GenerateDataKey
- DescribeKey
- Encrypt
- Decrypt
- ReEncrypt

You can use the following sample policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": ["arn:aws:kms:region:account:key:<KMS_key>"]
    }
  ]
}
```

When you configure KMS and access an Amazon S3 endpoint in the China region, use the following sample policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
    }
  ]
}
```

## Generate temporary security credentials using AssumeRole for EC2

You can use temporary security credentials using AssumeRole for an Amazon EC2 role to access the Amazon S3 staging bucket from the same or different AWS accounts.

The Amazon EC2 role can assume another IAM role from the same or different AWS account without requiring a permanent access key and secret key. The Amazon EC2 role can also assume another IAM role from a different region.

Consider the following prerequisites when you use temporary security credentials using AssumeRole for EC2:

- To use temporary security credentials using AssumeRole for EC2, install the Secure Agent on an AWS service such as Amazon EC2.
- The EC2 role attached to the AWS EC2 service must not have access to Amazon S3 but needs to have permission to assume another IAM role.
- The IAM role that needs to be assumed by the EC2 role must have a permission policy and a trust policy attached to it.

To configure an EC2 role to assume the IAM Role provided in the **IAM Role ARN** connection property, select the **Use EC2 Role to Assume Role** check box in the connection properties.

# Enable encryption

You can enable client-side and server-side encryption in the Amazon Redshift V2 connection for staging data in Amazon S3.

Complete the prerequisites based on the type of encryption that you want to configure in the Amazon Redshift V2 connection.

## Client-side encryption

Client-side encryption requires a 256-bit AES encryption key in the Base64 format. You can generate a key using a third-party tool.

Specify the key value in the **Master Symmetric Key** field when you create an Amazon Redshift V2 connection.

## Server-side encryption

To enable server-side encryption, create an AWS Key Management Service (AWS KMS)-managed customer master key.

Generate the customer master key ID for the same region where your Amazon S3 staging bucket resides. For more information about generating a customer master key, see the AWS documentation.

To enable encryption with the customer master key, you need to create a minimal KMS policy. You can specify the customer master key ID when you create an Amazon Redshift V2 connection.

**Note:** You cannot configure server-side encryption with the master symmetric key and client-side encryption with the customer master key.

## Create a minimal policy for using AWS KMS

To use the AWS Key Management Service (AWS KMS)-managed customer master key and enable the encryption with KMS, you must create a KMS policy.

You can perform the following operations to enable encryption with KMS:

- GenerateDataKey
- DescribeKey
- Encrypt
- Decrypt
- ReEncrypt

Sample policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": ["arn:aws:kms:region:account:key/<KMS_key>"]
    }
  ]
}
```

When you configure KMS and access an Amazon S3 endpoint in the China region, use the following sample policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "kms:GenerateDataKey", "kms:DescribeKey", "kms:Encrypt", "kms:Decrypt",
```



```

"kms:ReEncrypt*" ],
"Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
}
]
}

```

## Connect to Amazon Redshift

Let's configure the Amazon Redshift V2 connection properties to connect to Amazon Redshift.

### Before you begin

Before you get started, you'll need to get information from your Amazon Redshift account based on the authentication type you want to configure.

Check out ["Prepare for authentication" on page 74](#) to learn about the authentication requirements before you configure a connection.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - , Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Amazon Redshift V2
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	Name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run an application ingestion and replication task, database ingestion and replication task, file ingestion and replication task, or streaming ingestion and replication task on a Hosted Agent or serverless runtime environment. <b>Note:</b> Hosted Agent doesn't apply for mappings that run on an advanced cluster. You also cannot use the Hosted Agent for IAM authentication and EC2 AssumeRole authentication.

## Authentication types

You can configure default and Redshift IAM AssumeRole authentication types to access Amazon Redshift.

**Note:** Application ingestion and replication tasks and database ingestion and replication tasks do not support Redshift IAM AssumeRole authentication without an EC2 instance.

Select the required authentication method and then configure the authentication-specific parameters.

### Default authentication

The following table describes the basic connection properties for default authentication:

Properties	Description
JDBC URL	<p>The JDBC URL to connect to the Amazon Redshift cluster.</p> <p>You can get the JDBC URL from your Amazon AWS Redshift cluster configuration page.</p> <p>Enter the JDBC URL in the following format:</p> <pre>jdbc:redshift://&lt;cluster_endpoint&gt;:&lt;port_number&gt;/&lt;database_name&gt;</pre> <p>where the endpoint includes the Redshift cluster name and region.</p> <p>For example, <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>In the example,</p> <ul style="list-style-type: none"><li>- <code>infa-rs-qa-cluster</code> is the name of the Redshift cluster.</li><li>- <code>us-west-2.redshift.amazonaws.com</code> is the Redshift cluster endpoint, which is the US West (Oregon) region.</li><li>- <code>5439</code> is the port number for the Redshift cluster.</li><li>- <code>rsdb</code> is the specific database instance in the Redshift cluster to which you want to connect.</li></ul>
Username	User name of your database instance in the Amazon Redshift cluster.
Password	Password of the Amazon Redshift database user.
Use EC2 Role to Assume Role	<p>Enables the EC2 instance that assumes an S3 IAM role to access the S3 resources to stage data using the temporary security credentials.</p> <p>The EC2 role must have a policy attached with permissions to assume an S3 IAM role. The S3 IAM role and the EC2 instance can be in the same or different AWS account.</p> <p>Select the check box to enable the EC2 role to assume an S3 IAM role specified in the S3 IAM Role ARN option to access the S3 resources for staging data.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks. By default, this check box is not selected.</p> <p>For instructions, see <a href="#">"Generate temporary security credentials using AssumeRole for EC2" on page 83</a>.</p>
S3 IAM Role ARN	<p>The Amazon Resource Number (ARN) of the IAM role assumed by the IAM user or EC2 to use the dynamically generated temporary security credentials to stage data in Amazon S3.</p> <p>This property applies when you want to generate temporary security credentials to access the S3 staging buckets by using either the EC2 instance or the IAM user who assumes the S3 IAM role.</p> <p>Specify the S3 IAM role name to use the temporary security credentials to access the Amazon S3 staging bucket.</p> <p>For more information about how to get the ARN of the S3 IAM role, see the <a href="#">AWS documentation</a>.</p> <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that use role-based authentication, but not the default role for the AWS cluster, specify an IAM role ARN. If you use the default role, leave this field blank.</p>

## Advanced settings

The following table describes the advanced connection properties for default authentication:

Properties	Description
S3 Access Key ID	<p>Access key of the IAM user to access the Amazon S3 staging bucket.</p> <p>Enter the access key ID when you use the following methods for S3 staging:</p> <ul style="list-style-type: none"> <li>- When the IAM user has access to S3 staging.</li> <li>- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3.</li> </ul> <p>You do not need to enter the S3 access key ID if you use IAM authentication or the assume role for EC2 to access S3.</p> <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that use key-based authentication, provide the access key value.</p>
S3 Secret Access Key	<p>Secret access key to access the Amazon S3 staging bucket.</p> <p>The secret key is associated with the access key and uniquely identifies the account.</p> <p>Enter the secret access key value when you use following methods for S3 staging:</p> <ul style="list-style-type: none"> <li>- When the IAM user has access to S3 staging.</li> <li>- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3.</li> </ul> <p>You do not need to enter the S3 secret access key if you use IAM authentication or the assume role for EC2 to access S3.</p> <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that use key-based authentication, provide the access key value.</p>
S3 VPC Endpoint Type <sup>1</sup>	<p>The type of Amazon Virtual Private Cloud endpoint for Amazon S3.</p> <p>You can use a VPC endpoint to enable private communication with Amazon S3.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint which uses a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.</li> </ul>
Endpoint DNS Name for Amazon S3 <sup>1</sup>	<p>The DNS name for the Amazon S3 interface endpoint.</p> <p>Replace the asterisk symbol with the bucket keyword in the DNS name.</p> <p>Enter the DNS name in the following format:</p> <p>bucket.&lt;DNS name of the interface endpoint&gt;</p> <p>For example, bucket.vpce-s3.us-west-2.vpce.amazonaws.com</p>
STS VPC Endpoint Type <sup>1</sup>	<p>The type of Amazon Virtual Private Cloud endpoint for AWS Security Token Service.</p> <p>You can use a VPC endpoint to enable private communication with Amazon Security Token Service.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon Security Token Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.</li> </ul>
Endpoint DNS Name for AWS STS <sup>1</sup>	<p>The DNS name for the AWS STS interface endpoint.</p> <p>For example, vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</p>

Properties	Description
KMS VPC Endpoint Type <sup>1</sup>	<p>The type of Amazon Virtual Private Cloud endpoint for AWS Key Management Service. You can use a VPC endpoint to enable private communication with Amazon Key Management Service.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon Key Management Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.</li> </ul>
Endpoint DNS Name for AWS KMS <sup>1</sup>	<p>The DNS name for the AWS KMS interface endpoint.</p> <p>For example, <code>vpce-0e722f5c721e19232-g2pkm2r7.kms.us-west-2.vpce.amazonaws.com</code></p>
External ID	<p>The external ID associated with the IAM role.</p> <p>You can specify the external ID if you want to provide a more secure access to the Amazon S3 bucket. The Amazon S3 staging bucket and the IAM role can be in the same or different AWS accounts.</p> <p>If required, you also have the option to specify the external ID in the AssumeRole request to the AWS Security Token Service (STS) using an external ID condition in the assumed IAM role's trust policy.</p> <p>For more information about using an external ID, see <a href="#">External ID when granting access to your AWS resources</a>.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.</p>

Properties	Description
Cluster Region	<p>The AWS cluster region in which the Redshift cluster resides.</p> <p>Select the cluster region from the list if you choose to provide a custom JDBC URL with a different cluster region from that specified in the <b>JDBC URL</b> field property. To continue to use the cluster region name specified in the <b>JDBC URL</b> field property, select <b>None</b> as the cluster region in this property.</p> <p>You can only read data from or write data to the cluster regions supported by the AWS SDK.</p> <p>Select one of the following cluster regions:</p> <ul style="list-style-type: none"> <li>None</li> <li>Asia Pacific(Mumbai)</li> <li>Asia Pacific(Seoul)</li> <li>Asia Pacific(Singapore)</li> <li>Asia Pacific(Sydney)</li> <li>Asia Pacific(Tokyo)</li> <li>Asia Pacific(Hong Kong)</li> <li>AWS GovCloud (US)</li> <li>AWS GovCloud (US-East)</li> <li>Canada(Central)</li> <li>China(Beijing)</li> <li>China(Ningxia)</li> <li>EU(Ireland)</li> <li>EU(Frankfurt)</li> <li>EU(Paris)</li> <li>EU(Stockholm)</li> <li>South America(Sao Paulo)</li> <li>Middle East(Bahrain)</li> <li>US East(N. Virginia)</li> <li>US East(Ohio)</li> <li>US West(N. California)</li> <li>US West(Oregon)</li> </ul> <p>Default is <b>None</b>.</p> <p><b>Note:</b> A region value is required for application ingestion and replication tasks and database ingestion and replication tasks.</p>
Connection Environment SQL	<p>The SQL statement to set up the database environment that applies for the entire session.</p> <p>Separate multiple values with a semicolon (;).</p> <p>Specify only the configurations for the database environment in the SQL statement. Do not specify any DDL or DML commands in the SQL statement.</p>
Master Symmetric Key <sup>1</sup>	<p>A 256-bit AES encryption key in the Base64 format that enables client-side encryption to encrypt your data before you send them for staging in Amazon S3.</p> <p>For more information, see <a href="#">"Enable encryption" on page 84</a>.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.</p>

Properties	Description
Customer Master Key ID	<p>The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access when you stage data in Amazon S3. The customer master key serves to encrypt your data at the destination before they are saved in Amazon S3.</p> <p>You can either enter the customer-generated customer master key ID or the default customer master key ID.</p> <p>You can use a cross account KMS key in a connection in a mapping in advanced mode. The cluster and the staging bucket needs to be in the same region.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.</p>
<p><sup>1</sup>Doesn't apply to mappings in advanced mode.</p>	

## Redshift IAM Authentication via AssumeRole

The Redshift AssumeRole authentication enables the user to assume an IAM role or define an EC2 role configured with required trust policies to generate temporary security credentials to access Amazon Redshift.

**Note:** For application ingestion and replication tasks and database ingestion and replication tasks, you must use an EC2 role.

The following table describes the basic connection properties for Redshift IAM AssumeRole authentication:

Properties	Description
JDBC URL	<p>The JDBC URL to connect to the Amazon Redshift cluster.</p> <p>You can get the JDBC URL from your Amazon AWS Redshift cluster configuration page.</p> <p>Enter the JDBC URL in the following format:</p> <p><code>jdbc:redshift://&lt;cluster_endpoint&gt;:&lt;port_number&gt;/&lt;database_name&gt;</code>, where the endpoint includes the Redshift cluster name and region.</p> <p>For example, <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>In the example,</p> <ul style="list-style-type: none"> <li>- <code>infa-rs-qa-cluster</code> is the name of the Redshift cluster.</li> <li>- <code>us-west-2.redshift.amazonaws.com</code> is the Redshift cluster endpoint, which is the US West (Oregon) region.</li> <li>- <code>5439</code> is the port number for the Redshift cluster.</li> <li>- <code>rsdb</code> is the specific database instance in the Redshift cluster to which you want to connect.</li> </ul>
Username	User name of your database instance in the Amazon Redshift cluster.
Cluster Identifier	<p>The unique identifier of the cluster that hosts Amazon Redshift.</p> <p>Specify the Amazon Redshift cluster name.</p>
Database Name	Name of the Amazon Redshift database where the tables that you want to access are stored.
Redshift IAM Role ARN	<p>The Amazon Resource Number (ARN) of the IAM role assumed by EC2 to use the dynamically generated temporary security credentials to access Amazon Redshift.</p> <p>Enter the Redshift IAM role ARN to access the Amazon Redshift cluster.</p>

Properties	Description
Use EC2 Role to Assume Role	<p>Enables the EC2 role to assume an IAM role, either to connect to Redshift or to stage data using the temporary security credentials:</p> <p><b>Connect to Redshift with IAM authentication using the EC2 role</b></p> <p>Select the check box to enable the EC2 role that assumes a Redshift IAM role specified in the <b>Redshift IAM Role ARN</b> field to access Amazon Redshift.</p> <p>The EC2 role must have a policy attached with permissions to assume a Redshift IAM role from the same or different account.</p> <p><b>Access S3 resources to stage data</b></p> <p>Select the check box to enable the EC2 role to assume an S3 IAM role specified in the <b>S3 IAM Role ARN</b> field and dynamically generate the temporary security credentials to access the S3 staging buckets.</p> <p>The EC2 role must have a policy attached with permissions to assume an S3 IAM role from the same or different AWS account.</p>
S3 IAM Role ARN	<p>The Amazon Resource Number (ARN) of the S3 IAM role assumed by the IAM user or EC2 to use the dynamically generated temporary security credentials to stage data in Amazon S3.</p> <p>This property applies when you want to generate the temporary security credentials to access the S3 staging buckets by using either the EC2 instance or the IAM user who assumes the S3 IAM role.</p> <p>Specify the S3 IAM role name to use the temporary security credentials to access the Amazon S3 staging bucket.</p> <p>For more information about how to get the ARN of the IAM role, see the <a href="#">AWS documentation</a>.</p> <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that uses role-based authentication, but not the default role for the AWS cluster, specify an IAM role ARN. If you use the default role, leave this field blank.</p>

## Advanced settings

The following table describes the advanced connection properties for Redshift IAM AssumeRole authentication:

Properties	Description
Redshift Access Key ID	<p>The access key of the IAM user that has permissions to assume the Redshift IAM AssumeRole ARN.</p> <p>This property doesn't apply to Amazon Redshift AssumeRole authentication with EC2 role.</p>
Redshift Secret Access Key	<p>The secret access key of the IAM user that has permissions to assume the Redshift IAM AssumeRole ARN.</p> <p>This property doesn't apply to Amazon Redshift AssumeRole authentication with EC2 role.</p>
Database Group	<p>The name of the database group to which you want to add the database user when you select the <b>Auto Create DBUser</b> option in this connection property.</p> <p>The user that you add to this database group inherits the specified group privileges.</p> <p>If you do not specify a database group name, the user is added to the public group and inherits its associated privileges.</p> <p>You can also enter multiple database groups, separated by a comma, to add the user to each of the specified database groups.</p>

Properties	Description
Expiration Time	The time duration that the password for the Amazon Redshift database user expires. Specify a value between 900 seconds and 3600 seconds. Default is 900.
Auto Create DBUser	Select to create a new Amazon Redshift database user at run time. The agent adds the user you specified in the <b>Username</b> field to the database group. The added user assumes the privileges assigned to the database group. Default is disabled.
S3 Access Key ID	Access key of the IAM user to access the Amazon S3 staging bucket. Enter the access key ID when you use the following methods for S3 staging: <ul style="list-style-type: none"> <li>- When the IAM user has access to S3 staging.</li> <li>- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3.</li> </ul> You do not need to enter the S3 access key ID if you use IAM authentication or the assume role for EC2 to access S3. <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that use key-based authentication, provide the access key value.</p>
S3 Secret Access Key	Secret access key to access the Amazon S3 staging bucket. The secret key is associated with the access key and uniquely identifies the account. Enter the secret access key value when you use following methods for S3 staging: <ul style="list-style-type: none"> <li>- When the IAM user has access to S3 staging.</li> <li>- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3.</li> </ul> You do not need to enter the S3 secret access key if you use IAM authentication or the assume role for EC2 to access S3. <p><b>Note:</b> If you use the connection for application ingestion and replication or database ingestion and replication tasks that use key-based authentication, provide the access key value.</p>
S3 VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for Amazon S3. You can use a VPC endpoint to enable private communication with Amazon S3. Select one of the following options: <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint which uses a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.</li> </ul>
Endpoint DNS Name for Amazon S3 <sup>1</sup>	The DNS name for the Amazon S3 interface endpoint. Replace the asterisk symbol with the bucket keyword in the DNS name. Enter the DNS name in the following format: <pre>bucket.&lt;DNS name of the interface endpoint&gt;</pre> <p>For example, <code>bucket.vpce-s3.us-west-2.vpce.amazonaws.com</code></p>
STS VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for AWS Security Token Service. You can use a VPC endpoint to enable private communication with Amazon Security Token Service. Select one of the following options: <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon Security Token Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.</li> </ul>



Properties	Description
Endpoint DNS Name for AWS STS <sup>1</sup>	The DNS name for the AWS STS interface endpoint. For example, <code>vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</code>
KMS VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for AWS Key Management Service. You can use a VPC endpoint to enable private communication with Amazon Key Management Service. Select one of the following options: <ul style="list-style-type: none"> <li>- Default. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon Key Management Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.</li> </ul>
Endpoint DNS Name for AWS KMS <sup>1</sup>	The DNS name for the AWS KMS interface endpoint. For example, <code>vpce-0e722f5c721e19232-g2pkm2r7.kms.us-west-2.vpce.amazonaws.com</code>
External ID	The external ID associated with the IAM role. You can specify the external ID if you want to provide a more secure access to the Amazon S3 bucket when the Amazon S3 staging bucket is in same or different AWS accounts. If required, you also have the option to specify the external ID in the AssumeRole request to the AWS Security Token Service (STS) using an external ID condition in the assumed IAM role's trust policy. For more information about using an external ID, see <a href="#">External ID when granting access to your AWS resources</a> . This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.

Properties	Description
Cluster Region	<p>The AWS geographical region in which the Redshift cluster resides.</p> <p>Select the cluster region from the list if you choose to provide a custom JDBC URL with a different cluster region from that specified in the <b>JDBC URL</b> field property. To continue to use the cluster region name specified in the <b>JDBC URL</b> field property, select <b>None</b> as the cluster region in this property.</p> <p>You can only read data from or write data to the cluster regions supported by the AWS SDK.</p> <p>Select one of the following cluster regions:</p> <ul style="list-style-type: none"> <li>None</li> <li>Asia Pacific(Mumbai)</li> <li>Asia Pacific(Seoul)</li> <li>Asia Pacific(Singapore)</li> <li>Asia Pacific(Sydney)</li> <li>Asia Pacific(Tokyo)</li> <li>Asia Pacific(Hong Kong)</li> <li>AWS GovCloud (US)</li> <li>AWS GovCloud (US-East)</li> <li>Canada(Central)</li> <li>China(Beijing)</li> <li>China(Ningxia)</li> <li>EU(Ireland)</li> <li>EU(Frankfurt)</li> <li>EU(Paris)</li> <li>EU(Stockholm)</li> <li>South America(Sao Paulo)</li> <li>Middle East(Bahrain)</li> <li>US East(N. Virginia)</li> <li>US East(Ohio)</li> <li>US West(N. California)</li> <li>US West(Oregon)</li> </ul> <p>Default is <b>None</b>.</p> <p><b>Note:</b> A region value is required for application ingestion and replication tasks and database ingestion and replication tasks.</p>
Connection Environment SQL	<p>The SQL statement to set up the database environment that applies for the entire session.</p> <p>Separate multiple values with a semicolon (;).</p> <p>Specify only the configurations for the database environment in the SQL statement. Do not specify any DDL or DML commands in the SQL statement.</p>
Master Symmetric Key <sup>1</sup>	<p>A 256-bit AES encryption key in the Base64 format that enables client-side encryption to encrypt your data before you send them for staging in Amazon S3.</p> <p>For more information, see <a href="#">“Enable encryption” on page 84</a>.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.</p>

Properties	Description
Customer Master Key ID	<p>The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access when you stage data in Amazon S3. The customer master key serves to encrypt your data at the destination before they are saved in Amazon S3.</p> <p>You can either enter the customer-generated customer master key ID or the default customer master key ID.</p> <p>You can use a cross account KMS key in a connection in a mapping in advanced mode. The cluster and the staging bucket needs to be in the same region.</p> <p>For more information about how to configure server-side encryption, see <a href="#">"Enable encryption" on page 84</a>.</p> <p>This property doesn't apply to application ingestion and replication tasks and database ingestion and replication tasks.</p>
<p><sup>1</sup>Doesn't apply to mappings in advanced mode.</p>	

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

**Note:** If you enable both HTTP and SOCKS proxies, SOCKS proxy is used by default. If you want to use HTTP proxy instead of SOCKS proxy, set the value of the **DisableSocksProxy** property to true in the System property.

## Configure SSL

To use SSL to connect to Amazon Redshift, you need to configure the Secure Agent for SSL and enable SSL through the JDBC URL in the Amazon Redshift V2 connection properties.

1. Download the Amazon Redshift certificate from the following location: <https://s3.amazonaws.com/redshift-downloads/redshift-ssl-ca-cert.pem>.

2. At the command prompt, run the following command to add the certificate file to the key store: `$ {JAVA_HOME}/bin/keytool -keystore {JAVA_HOME}/lib/security/cacerts -import -alias <string_value> -file <certificate_filepath>`.
3. In Administrator, select **Runtime Environments**.
4. Select the Secure Agent from the list of Secure Agents.
5. In the upper-right corner, click **Edit**.
6. In the **System Configuration Details** section, change the **Type** to **DTM**.
7. Click the **Edit Agent Configuration** icon next to **JVMOption1** and add the following command: `-Djavax.net.ssl.trustStore=<keystore_name>`.
8. Click the **Edit Agent Configuration** icon next to **JVMOption2** and add the following command: `-Djavax.net.ssl.trustStorePassword=<password>`.
9. Add the following parameter to the JDBC URL that you specify in the Amazon Redshift V2 connection properties: `ssl=true`.  
For example, `jdbc:redshift://mycluster.xyz789.us-west-2.redshift.amazonaws.com:5439/dev?ssl=true`.
10. Click **OK** to save your changes.

## Configure SSL with the serverless runtime environment

You can use the serverless runtime environment in an Amazon Redshift V2 connection to connect to an SSL-enabled Amazon Redshift database.

Before you configure a secure Amazon Redshift V2 connection using the serverless runtime environment, perform the following tasks:

- Add the SSL certificate in the Amazon S3 bucket or Azure container.
- Configure the `.yml` serverless configuration file.
- Configure the serverless environment.
- Configure the connection properties to use SSL.

### Add the SSL certificate in the Amazon S3 bucket or Azure container

Perform the following steps to configure an SSL connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
`<Supplementary file location>/serverless_agent_config`
2. Add the certificate name and source path in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: `<Supplementary file location>/serverless_agent_config/SSL`

### Configure the `.yml` serverless configuration file

Perform the following steps to configure the `.yml` serverless configuration file in the serverless runtime environment and add the certificate name and path entries so that Amazon Redshift V2 Connector can use SSL:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
```

```
- fileCopy:
  sourcePath: SSL/<cert_name>
- importCerts:
  certName: <cert_name>
  alias: <alias name of the certificate>
```

where the source path is the directory path of the certificate files in AWS or Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`  
When the `.yml` file runs, the SSL certificates are copied from the AWS or Azure location to the `serverless agent` directory.

#### Configure the serverless environment

Configure the `JVMOption1` and `JVMOption2` properties for SSL in the serverless runtime environment:

1. Navigate to your serverless runtime environment properties, and click **Edit**.
2. On the **Runtime Configuration Properties** tab, click **JVMOption1** and add the following property:  
`-Djavax.net.ssl.trustStore=/home/cldagnt/SystemAgent/jdk/jre/lib/security/cacerts`
3. Click **JVMOption2** and add the following property:  
`-Djavax.net.ssl.trustStorePassword=changeit`
4. Click **Save**.
5. Redeploy the runtime environment.

#### Configure the connection properties to use SSL

After you set the runtime properties in the serverless runtime environment, specify `ssl=true` in the **JDBC URL** connection property.

For example, `jdbc:redshift://mycluster.xyz789.us-west-2.redshift.amazonaws.com:5439/dev?ssl=true`

## Configure client-side encryption with the serverless runtime environment

You can use the serverless runtime environment to configure client-side encryption when you connect to Amazon Redshift.

Before you configure client-side encryption using the serverless runtime environment, configure the `.yml` serverless configuration file.

#### Configure the `.yml` serverless configuration file

Perform the following steps to configure the `.yml` serverless configuration file in the serverless runtime environment so that Amazon Redshift V2 Connector can use client-side encryption:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      jdk:
        security:
```

```
policyJars:
  - local_policy.jar
  - US_export_policy.jar
```

2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location:  
`<Supplementary file location>/serverless_agent_config`

When the .yml file runs, the policy jars are copied from the AWS or Azure location to the serverless agent directory.

3. After you update the .yml configuration file, redeploy the serverless runtime environment.

Specify the master symmetric key in the connection properties and the client-side encryption type in the advanced source and target properties.

## Configure SSE-KMS encryption for mappings in advanced mode

To use SSE-KMS encryption for connections used in mappings in advanced mode, perform one of the following tasks:

- To use the credentials from the `~/.aws/credentials` location, create the master instance profile and the worker instance profile in AWS, attach the KMS policy to the worker profile, and specify the profiles in the cluster configuration.
- Use the Secure Agent on Amazon EC2, create the master instance profile and the worker instance profile in AWS, and attach the KMS policy to the worker profile.
- Use the Secure Agent on Amazon EC2, use the default IAM role, and attach the KMS policy to the Secure Agent role.

## Amazon Redshift Serverless connectivity

Amazon Redshift Serverless is a serverless offering of Amazon Web Services (AWS) that allows the same scalability and capability of Amazon Redshift without the need to set up and manage the provisioned Redshift cluster.

Amazon Redshift V2 Connector provides out-of-the-box support to connect to the Amazon Redshift Serverless endpoint.

For more information about how to access the Amazon Redshift serverless endpoint, see the How-to-Library article: [Using Amazon Redshift Serverless with Cloud Data Integration](#)

## Requirements to use Amazon Redshift Spectrum

When you use a connection in a mapping to read data from an Amazon Redshift Spectrum external table, provide the required authorization to the Amazon Redshift cluster to access the data catalog and the data files in Amazon S3.

**Important:** The Amazon Redshift cluster and the Amazon S3 bucket that contains the data files must belong to the same region. The Amazon Redshift cluster must be of version 1.0.1294 or later.

1. Create an AWS Identity and Access Management (IAM) role to authorize the Amazon Redshift cluster access to the external data catalog and data files in Amazon S3.
2. Associate the IAM role with the specified Amazon Redshift cluster.
3. Create an external schema.
4. Provide Amazon Redshift role ARN for the IAM role in the external schema.
5. Create an external table within the external schema and specify the Amazon S3 location from where you want to read the data. For more information about creating external tables, see the AWS documentation.
6. To access the data catalog and the data files in Amazon S3 by using Amazon Redshift Spectrum, ensure that the Amazon Redshift cluster has the required authorization.

## Private communication with Amazon Redshift

If you do not want to expose your traffic to the public internet, you can enable private communication with Amazon Redshift by configuring a gateway endpoint on the AWS console.

To establish a private connection with Amazon Redshift, ensure that the Secure Agent is a part of the subnet in the AWS Virtual Private Cloud (VPC). You can create a gateway endpoint and stage the Amazon S3 data to Amazon Redshift.

To configure private communication to connect to Amazon Redshift, you need to perform the following tasks:

- Create a cluster subnet group.
- Create a Redshift-managed VPC endpoint.
- Configure the gateway endpoint.

You can then specify the gateway endpoint in the Amazon Redshift V2 connection properties.

For more information, see

[Configuring private communication with Amazon Redshift using the Amazon Redshift V2 Connector.](#)

## Private communication with Amazon S3

You can configure an Amazon Redshift V2 connection to establish private communication with Amazon S3 for staging.

You need to configure an interface endpoint on the AWS console to enable private communication to stage data in Amazon S3. The AWS S3 VPC endpoint enables an S3 request to be routed to the Amazon S3 service, without connecting to the internet.

Consider the following guidelines to establish private communication with Amazon S3:

- When an Amazon Redshift Cluster is spawned, an Elastic Network Interface (ENI) is generated for the cluster within the subnet. Ensure that the route table of the S3 gateway endpoint corresponds to the same subnet where your Redshift cluster ENI is created.
- To connect to an Amazon S3 bucket using a VPC endpoint, the Amazon Redshift cluster and the Amazon S3 bucket that it connects to must be in the same AWS region.

# VPC peering between the serverless runtime environment and Amazon Redshift

When you use the serverless runtime environment and if the serverless runtime environment and the Amazon Redshift cluster reside in different VPCs, you need to configure VPC peering.

For more information about configuring VPC peering, see the How-to-Library article:

[Configure VPC peering between Amazon Redshift clusters](#)



## CHAPTER 23

# Amazon S3 connection properties

When you set up an Amazon S3 connection, you must configure the connection properties.

**Important:** Amazon S3 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Amazon S3 V2 Connector to access Amazon S3.

The following table describes the Amazon S3 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Access Key	The access key ID used to access the Amazon account resources. Required if you do not use AWS Identity and Access Management (IAM) authentication. <b>Note:</b> Ensure that you have valid AWS credentials before you create a connection.
Secret Key	The secret access key used to access the Amazon account resources. This value is associated with the access key and uniquely identifies the account. You must specify this value if you specify the access key ID. Required if you do not use AWS Identity and Access Management (IAM) authentication.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, <bucket name>/<my folder name>
Master Symmetric Key	Optional. Provide a 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a key using a third-party tool. If you specify a value, ensure that you specify the encryption type as client side encryption in the advanced target properties in the <b>Schedule</b> page.

<b>Connection property</b>	<b>Description</b>
Code Page	<p>The code page compatible with the Amazon S3 source. Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode and non-Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>
Region Name	<p>Specify the name of the region where the Amazon S3 bucket is available and for which you generated the customer master key ID. Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Asia Pacific (Tokyo)</li> <li>- Asia Pacific (Seoul)</li> <li>- Asia Pacific (Singapore)</li> <li>- Asia Pacific (Sydney)</li> <li>- AWS GovCloud</li> <li>- China (Beijing)</li> <li>- EU (Ireland)</li> <li>- EU (Frankfurt)</li> <li>- South America (Sao Paulo)</li> <li>- US East (N. Virginia)</li> <li>- US West (N. California)</li> <li>- US West (Oregon)</li> <li>- US East (Ohio)</li> <li>- Canada (Central)</li> <li>- Asia Pacific (Mumbai)</li> </ul> <p>You can only read from or write data to the regions supported by AWS SDK used by the Amazon S3 connector.</p>

## CHAPTER 24

# Amazon S3 V2 connection properties

Create an Amazon S3 V2 connection to read from and write to Amazon S3.

## Prepare for authentication

You can configure multiple authentication types to access Amazon S3.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

- Basic authentication requires access key and secret key values from your AWS account.
- IAM authentication requires attaching policies to the EC2 role to grant access to specific folder paths and access Amazon S3 objects .
- AssumeRole with EC2 role authentication requires you to enable the EC2 role to assume another IAM role specified by the IAM Role ARN.
- AssumeRole with IAM user authentication requires the access key and secret key values of the IAM user and the ARN of the IAM role.
- Credential profile file authentication requires the credential profile file path and profile name.
- Federated user single sign-on authentication requires the user name and password of the federated user, IdP SSO URL, ARN of the SAML identity provider, and ARN of the IAM role assumed by the federated user. You can only use ADFS 3.0 (IDP) for SSO.

## Create a minimal Amazon IAM policy

You can configure an IAM policy through the AWS console. Use AWS IAM authentication to securely control access to Amazon S3 resources.

Use the following minimum required policies for users to read data from an Amazon S3 bucket:

- GetObject
- ListBucket

Use the following minimum required policies for users to write data to an Amazon S3 bucket:

- PutObject
- GetObject

- DeleteObject
- ListBucket
- ListBucketMultipartUploads. Applicable only for mappings in advanced mode.

The following sample policy shows the minimal Amazon IAM policy to write data to an Amazon S3 bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>/*",
        "arn:aws:s3:::<bucket_name>"
      ]
    }
  ]
}
```

For bucket level access in advanced mode, you need to provide the `AllowListBucketMultipartUploads` permission at the bucket level in addition to the `ListBucketMultipartUploads` permission.

The following sample policy shows the minimal Amazon IAM policy to access the S3 bucket at the bucket level in advanced mode:

```
{
  "Sid": "AllowListBucketMultipartUploads",
  "Action": [
    "s3:ListBucketMultipartUploads"
  ],
  "Effect": "Allow",
  "Resource": [
    "arn:aws:s3:::infa.qa.minimum.access.bucket"
  ]
},
```

For mappings in advanced mode, you can use different AWS accounts within the same AWS region. Make sure that the Amazon IAM policy confirms access to the AWS accounts used in the mapping.

## IAM authentication

To configure IAM authentication, the Secure Agent needs to run on an Amazon Elastic Compute Cloud (EC2) system. If you prefer not to specify the keys or use the IAM role ARN, then assign the minimum policy to the EC2 with access to the S3 bucket.

When you use a serverless runtime environment, you cannot configure IAM authentication.

If you do not provide the access key and the secret key in the connection, Amazon S3 V2 Connector uses AWS credentials provider chain that looks for credentials in the following order:

1. The `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY` or `AWS_ACCESS_KEY` and `AWS_SECRET_KEY` environment variables.
2. The `aws.accessKeyId` and `aws.secretKey` java system properties.
3. The credential profiles file at the default location, `~/.aws/credentials`.

4. The instance profile credentials delivered through the Amazon EC2 metadata service.

Perform the following steps to configure IAM authentication on EC2:

1. Create a minimal Amazon IAM policy.
2. Create the Amazon EC2 role. The Amazon EC2 role is used when you create an EC2 system. For more information about creating the Amazon EC2 role, see the AWS documentation.
3. Link the minimal Amazon IAM policy with the Amazon EC2 role.
4. Create an EC2 instance. Assign the Amazon EC2 role that you created in step 2 to the EC2 instance.
5. Install the Secure Agent on the EC2 system.

## AssumeRole using EC2 role and IAM user

You can configure AssumeRole using EC2 role or IAM user to connect to Amazon S3.

You can use the temporary security credentials using AssumeRole to access AWS resources from the same or different AWS accounts.

When you configure AssumeRole using EC2 role or IAM user, ensure that you have the **sts:AssumeRole** permission and a trust relationship established within the AWS accounts to use the temporary security credentials. The trust relationship is defined in the trust policy of the IAM role when you create the role. The IAM role adds the EC2 role or IAM user as a trusted entity allowing the EC2 role or IAM user to use the temporary security credentials and access the AWS accounts.

For more information about how to establish the trust relationship, see the AWS documentation.

When the trusted EC2 role or IAM user requests for the temporary security credentials, the AWS Security Token Service (AWS STS) dynamically generates the temporary security credentials that are valid for a specified period and provides the credentials to the trusted EC2 role or IAM user.

### AssumeRole using EC2 role

To configure an EC2 role to assume the IAM role provided in the **IAM Role ARN** connection property, select the **Use EC2 Role to Assume Role** check box in the Amazon S3 V2 connection properties.

The Amazon EC2 role can assume another IAM role from the same or different AWS account without requiring a permanent access key and secret key. The Amazon EC2 role can also assume another IAM role from a different region.

Consider the following prerequisites before you configure AssumeRole using EC2 role:

- Install the Secure Agent on an AWS service such as Amazon EC2.
- The EC2 role attached to the AWS EC2 service must not have access to Amazon S3 but needs to have permission to assume another IAM role.
- The IAM role that needs to be assumed by the EC2 role must have a permission policy and a trust policy attached to it.

### AssumeRole using IAM user

To configure AssumeRole using IAM user, provide the value of the **IAM Role ARN** connection property when you create an Amazon S3 V2 connection. The IAM Role ARN uniquely identifies the AWS resources. Then, specify the time duration in seconds during which you can use the temporarily security credentials in the **Temporary Credential Duration** advanced source and target properties.

You need to follow some guidelines when you configure AssumeRole using IAM user. For more information, see [#unique\\_88/unique\\_88\\_Connect\\_42\\_GUID-23C83356-8E09-4ECA-A67A-CF00C885784Don page 122](#).

## External ID

You can specify the external ID of your AWS account for a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in same or different AWS account.

You can optionally specify the external ID in the AssumeRole request to the AWS Security Token Service (STS).

The external ID must be a string.

The following sample shows an external ID condition in the assumed IAM role's trust policy:

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "dummy_external_id"
      }
    }
  }
]
```

## AssumeRole policy

To use the temporary security credentials to access the AWS resources, both the IAM user and IAM role require policies.

The following section lists the policies required for the IAM user and IAM role:

### IAM user

An IAM user must have the `sts:AssumeRole` policy to use the temporary security credentials in the same or different AWS account.

The following sample policy allows an IAM user to use the temporary security credentials in an AWS account:

```
{
  "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole",
  "Resource": "arn:aws:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

The following sample policy allows an IAM user for the China region to use the temporary security credentials in an AWS account:

```
{
  "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole",
  "Resource": "arn:aws-cn:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

### IAM role

An IAM role must have a `sts:AssumeRole` policy and a trust policy attached with the IAM role to allow the IAM user to access the AWS resource using the temporary security credentials. The policy specifies the AWS resource that the IAM user can access and the actions that the IAM user can perform. The trust policy specifies the IAM user from the AWS account that can access the AWS resource.

The following policy is a sample trust policy:

```
{
  "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal":
  { "AWS": "arn:aws:iam::AWS-account-ID:root" },
```

```
"Action": "sts:AssumeRole" }
]
}
}
```

Here, in the `Principal` attribute, you can also provide the ARN of IAM user, which allows the designated user to dynamically generate temporary security credentials and helps to restrict further access.

For example,

```
"Principal" : { "AWS" : "arn:aws:iam:: AWS-account-ID :user/ user-name " }
```

## Credential profile file authentication

You can provide the credentials required to establish the connection with Amazon S3 through the credential profile file.

If you do not specify the credential profile file path, the default credential file path is used. If you do not specify the profile name, the credentials are used from the default profile in the credential file.

Consider the following rules for a credential profile file:

- The credential file must be on the same machine where you installed the Secure Agent.
- The credential profile file name must end with `.credentials`.
- If you do not specify the credential profile path, the Secure Agent uses the credential profile file present in the following default location in your home directory:

```
~/.aws/credentials
```

**Note:** On Windows, you can refer to your home directory by using the environment variable `%UserProfile` `%`. On Unix-like systems, you can use the environment variable `$HOME`.

The following sample shows a credential profile file:

```
[default]
aws_access_key_id = 1233333
aws_secret_access_key = abcabcabc

[test-profile]
aws_access_key_id = 1233333
aws_secret_access_key = abcabcabc
aws_session_token = jahaheieomdrftflmlioerp
```

The `aws_access_key_id` and `aws_secret_access_key` are the AWS access key and secret key used as part of credentials to authenticate the user.

The `aws_session_token` is the AWS session token used as part of the credentials to authenticate the user. A session token is required only if you specify temporary security credentials.

## Connect to Amazon S3

Let's configure the Amazon S3 connection properties to connect to Amazon S3.

## Before you begin

Before you get started, you'll need to get information from your Amazon S3 account based on the authentication type that you want to configure.

Check out ["Prepare for authentication" on page 103](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Amazon S3 V2
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run an application ingestion task or a database ingestion task on a Hosted Agent or serverless runtime environment.

## Authentication types

You can configure basic, AWS Identity and Access Management (IAM), temporary security credentials, assume role for EC2, credential profile file, and federated user single sign-on authentication types to access Amazon S3.

Select the required authentication method and then configure the authentication-specific parameters.

### Basic authentication

Basic authentication requires access key and secret key values from your AWS account.



The following table describes the basic connection properties for basic authentication:

Property	Description
Access Key	Access key to access the Amazon S3 bucket.
Secret Key	Secret key to access the Amazon S3 bucket. The secret key is associated with the access key and uniquely identifies the account.
Folder Path	<p>Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored.</p> <p>For example, &lt;bucket name&gt;/&lt;my folder name&gt;</p> <p>For application ingestion and database ingestion tasks, add a trailing slash. For example: &lt;bucket name&gt;/&lt;my folder name&gt;/.</p>
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>

## IAM authentication

IAM authentication requires only the folder path to the Amazon S3 objects. The EC2 role must have access to the folder.

The following table describes the basic connection properties for AWS IAM authentication:

Property	Description
Folder Path	<p>Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored.</p> <p>For example, &lt;bucket name&gt;/&lt;my folder name&gt;</p> <p>For application ingestion and database ingestion tasks, add a trailing slash. For example: &lt;bucket name&gt;/&lt;my folder name&gt;/.</p>
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>

## AssumeRole via EC2 role authentication

AssumeRole via EC2 role authentication requires you to enable the EC2 role to assume another IAM role specified in the IAM Role ARN option.

The following table describes the basic connection properties for AssumeRole via EC2 role authentication:

Property	Description
Folder Path	<p>Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored.</p> <p>For example, &lt;bucket name&gt;/&lt;my folder name&gt;</p> <p>For application ingestion and database ingestion tasks, add a trailing slash. For example: &lt;bucket name&gt;/&lt;my folder name&gt;/.</p>
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>
IAM Role ARN	<p>The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role assumed by the user to use the dynamically generated temporary security credentials.</p> <p>Enter the ARN value if you want to use the temporary security credentials to access AWS resources.</p> <p>This property is not applicable to an application ingestion task.</p> <p><b>Note:</b> Even if you remove the IAM role that grants the agent access to the Amazon S3 bucket, the test connection is successful.</p> <p>For more information about how to get the ARN of the IAM role, see the AWS documentation.</p>

Property	Description
External ID	The external ID of your AWS account. External ID provides a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account.
Use EC2 Role to Assume Role	Enables the EC2 role to assume another IAM role specified in the IAM Role ARN option. By default, this property is not selected. <b>Note:</b> The EC2 role must have a policy attached with permissions to assume an IAM role from the same or different account. <b>Note:</b> Enter a value for the IAM Role ARN property when you enable this property for a streaming ingestion task.

## AssumeRole via IAM user authentication

AssumeRole via IAM user authentication requires the access key and secret key values of the IAM user and the ARN of the IAM role.

The following table describes the basic connection properties for AssumeRole via IAM user authentication:

Property	Description
Access Key	Access key to access the Amazon S3 bucket.
Secret Key	Secret key to access the Amazon S3 bucket. The secret key is associated with the access key and uniquely identifies the account.
Folder Path	Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored. For example, <bucket name>/<my folder name> For application ingestion and database ingestion tasks, add a trailing slash. For example: <bucket name>/<my folder name>/.

Property	Description
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>
IAM Role ARN	<p>The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role assumed by the user to use the dynamically generated temporary security credentials.</p> <p>Enter the value of this property if you want to use the temporary security credentials to access the AWS resources.</p> <p>This property is not applicable to an application ingestion task.</p> <p><b>Note:</b> Even if you remove the IAM role that enables the agent to access the Amazon S3 bucket and create a connection, the test connection is successful.</p> <p>For more information about how to get the ARN of the IAM role, see the AWS documentation.</p>
External ID	<p>The external ID of your AWS account.</p> <p>External ID provides a more secure access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account.</p>

## Credential profile file authentication

Credential profile file authentication requires the credential profile file path and profile name.

The following table describes the basic connection properties for credential profile file authentication:

Property	Description
Folder Path	<p>Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored.</p> <p>For example, &lt;bucket name&gt;/&lt;my folder name&gt;</p> <p>For application ingestion and database ingestion tasks, add a trailing slash. For example: &lt;bucket name&gt;/&lt;my folder name&gt;/.</p>
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>
Other Authentication Type <sup>1</sup>	<p>Determines whether you want to use the credential profile file authentication to connect to Amazon S3.</p> <p>Select one the following authentication types:</p> <ul style="list-style-type: none"> <li>- NONE. Select if you do not want to credential profile file authentication.</li> <li>- Credential Profile File Authentication. Select to use credential profile file authentication to access the Amazon S3 credentials from a credential file.</li> </ul> <p>Enter the credential profile file path and profile name to connect to Amazon S3. You can use permanent IAM credentials or temporary session tokens when you configure the credential profile file authentication.</p> <p>Default is NONE.</p>

Property	Description
Credential Profile File Path <sup>1</sup>	<p>The credential profile file path.</p> <p>If you don't enter the credential profile path, the Secure Agent uses the credential profile file available in the following default location in your home directory:</p> <pre>~/.aws/credentials</pre> <p><b>Note:</b> Database Ingestion and Replication has not been certified with the <b>Credential Profile File Path</b> and <b>Profile Name</b> connection properties. Database Ingestion and Replication finds AWS credentials by using the default credential provider chain that is implemented by the DefaultAWSCredentialsProviderChain class, which includes the credential profile file.</p>
Profile Name <sup>1</sup>	<p>Name of the profile in the credential profile file used to get credentials to access Amazon S3 resources.</p> <p>If you don't enter the profile name, the credentials from the default profile in the credential profile file are used.</p>
<sup>1</sup> Applies only to mappings.	

## Federated single sign-on authentication

Federated user single sign-on authentication requires the user name and password of the federated user, IdP SSO URL, ARN of the SAML identity provider, and ARN of the IAM role assumed by the federated user. You can only use ADFS 3.0 (IDP) for SSO.

The following table describes the basic connection properties for federated single sign-on authentication:

Property	Description
Folder Path	<p>Amazon S3 bucket name or the folder path within the Amazon S3 bucket where the Amazon S3 objects are stored.</p> <p>For example, &lt;bucket name&gt;/&lt;my folder name&gt;</p> <p>For application ingestion and database ingestion tasks, add a trailing slash. For example: &lt;bucket name&gt;/&lt;my folder name&gt;/.</p>
Region Name	<p>The AWS region of the bucket that you want to access.</p> <p>Select one of the following regions:</p> <ul style="list-style-type: none"> <li>- Africa(Cape Town)</li> <li>- Asia Pacific(Mumbai)</li> <li>- Asia Pacific(Jakarta)</li> <li>- Asia Pacific (Osaka)</li> <li>- Asia Pacific(Seoul)</li> <li>- Asia Pacific(Singapore)</li> <li>- Asia Pacific(Sydney)</li> <li>- Asia Pacific(Tokyo)</li> <li>- Asia Pacific(Hong Kong)</li> <li>- AWS GovCloud(US)</li> <li>- AWS GovCloud(US-East)</li> <li>- Canada(Central)</li> <li>- China(Beijing)</li> <li>- China(Ningxia)</li> <li>- EU(Ireland)</li> <li>- EU(Frankfurt)</li> <li>- EU(London)</li> <li>- EU(Milan)</li> <li>- EU(Paris)</li> <li>- EU(Stockholm)</li> <li>- South America(Sao Paulo)</li> <li>- Middle East(Bahrain)</li> <li>- Middle East(UAE)</li> <li>- US East(N. Virginia)</li> <li>- US East(Ohio)</li> <li>- US ISO East</li> <li>- US ISOB East(Ohio)</li> <li>- US ISO West</li> <li>- US West(N. California)</li> <li>- US West(Oregon)</li> </ul> <p>Default is US East(N. Virginia).</p>
Federated SSO IdP <sup>1</sup>	<p>SAML 2.0-enabled identity provider for the federated user single sign-on to use with the AWS account.</p> <p>You can only use ADFS 3.0 (IDP) for SSO.</p> <p>Select <b>None</b> if you don't want to use federated user single sign-on.</p> <p><b>Note:</b> Federated user single sign-on doesn't apply to mappings in advanced mode.</p> <p><b>Note:</b> Federated user single sign-on is not applicable to application ingestion tasks, database ingestion tasks, and streaming ingestion tasks.</p>
Federated User Name	User name of the federated user to access the AWS account through the identity provider.
Federated User Password	Password for the federated user to access the AWS account through the identity provider.



Property	Description
IdP SSO URL	Single sign-on URL of the identity provider for AWS. Doesn't apply to a streaming ingestion task.
SAML Identity Provider ARN	ARN of the SAML identity provider that the AWS administrator created to register the identity provider as a trusted provider.
Role ARN	ARN of the IAM role assumed by the federated user.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
S3 Account Type	The type of the Amazon S3 account. Select from the following options: <ul style="list-style-type: none"> <li>- Amazon S3 Storage. Enables you to use the Amazon S3 services.</li> <li>- S3 Compatible Storage. Enables you to use the endpoint for a third-party storage provider such as Scalify RING or MinIO.</li> </ul> Default is Amazon S3 storage.
REST Endpoint	The S3 storage endpoint required for S3 compatible storage. Enter the S3 storage endpoint in HTTP or HTTPs format. For example, <code>http://s3.isv.scality.com</code> .
S3 VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for Amazon S3. You can use a VPC endpoint to enable private communication with Amazon S3. Select one of the following options: <ul style="list-style-type: none"> <li>- None. Select if you do not want to use a VPC endpoint.</li> <li>- Gateway Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint. A gateway endpoint is a target for a route in your route table that is used to forward S3 traffic to the S3 gateway endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint which uses a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.</li> </ul> Default is None. Doesn't apply to an application ingestion task or database ingestion task.
Endpoint DNS Name for Amazon S3 <sup>1</sup>	The DNS name for the Amazon S3 interface endpoint. Enter the DNS name in the following format: <code>bucket.&lt;DNS name of the interface endpoint&gt;</code> Doesn't apply to an application ingestion task or database ingestion task.
STS VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for AWS Security Token Service. This option applies when you select the S3 VPC interface endpoint and when use AssumeRole via IAM user or EC2 role authentication or Federated SSO IdP authentication. Doesn't apply to an application ingestion task, streaming ingestion task, or database ingestion task.

Property	Description
Endpoint DNS Name for AWS STS <sup>1</sup>	The DNS name for the AWS STS interface endpoint. Doesn't apply to an application ingestion task or database ingestion task.
KMS VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for AWS Key Management Service. This option applies when you select the S3 VPC interface endpoint and required when you specify the customer master key ID. Doesn't apply to an application ingestion task or database ingestion task.
Endpoint DNS Name for AWS KMS <sup>1</sup>	The DNS name for the AWS KMS interface endpoint. Doesn't apply to an application ingestion task or database ingestion task.
Master Symmetric Key	A 256-bit AES encryption key in the Base64 format when you use client-side encryption. You can generate a key using a third-party tool. Doesn't apply to an application ingestion task, database ingestion task, or streaming ingestion task.
Customer Master Key ID	The customer master key ID or alias name generated by AWS Key Management Service (AWS KMS) or the Amazon Resource Name (ARN) of your custom key for cross-account access. <b>Note:</b> Cross-account access is not available for mappings in advanced mode. You must generate the customer master key for the same region where the Amazon S3 bucket resides. You can specify the following master keys: <ul style="list-style-type: none"> <li>- Customer generated customer master key. Enables client-side or server-side encryption.</li> <li>- Default customer master key. Enables client-side or server-side encryption. Only the administrator user of the account can use the default customer master key ID to enable client-side encryption.</li> </ul> Doesn't apply to an application ingestion task, database ingestion task, or streaming ingestion task.
<sup>1</sup> Applies only to mappings.	

## Private communication with Amazon S3

You can enable private communication with Amazon S3 by configuring a gateway endpoint or interface endpoint on AWS console and in the Amazon S3 V2 connection.

You can configure Amazon S3 V2 Connector to establish private communication with Amazon S3 without exposing your traffic to the public internet. To access Amazon S3, ensure that the Secure Agent is a part of the subnet in the AWS Virtual Private Cloud (VPC). AWS S3 VPC endpoint enables an S3 request to be routed to the Amazon S3 service, without having to connect a subnet to an internet gateway. You can create an interface endpoint or a gateway endpoint.

For more information, see

[Configuring private communication with Amazon S3 using the Amazon S3 V2 Connector.](#)

# Server-side encryption with KMS

To use the customer master key managed by AWS Key Management Service (AWS KMS) and enable the encryption with KMS, you need to create a KMS policy.

You can perform the following operations to use the temporary security credentials and enable the encryption with KMS:

- GenerateDataKey
- DescribeKey
- Encrypt
- Decrypt
- ReEncrypt

See the following sample KMS policy for reference:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": ["arn:aws:kms:region:account:key/<KMS_key>"]
    }
  ]
}
```

When you configure KMS and access an Amazon S3 endpoint in the China region, use the following sample policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
    }
  ]
}
```

# Client-side encryption with serverless runtime environment

You can use the serverless runtime environment with Amazon S3 V2 Connector to configure client-side encryption.

Before you configure client-side encryption using the serverless runtime environment, you must configure the .yaml serverless configuration file.

## Configure the .yaml serverless configuration file

Perform the following steps to configure the .yaml serverless configuration file in the serverless runtime environment so that Amazon S3 V2 Connector can use client-side encryption:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      jdk:
```

```
security:
  policyJars:
    - local_policy.jar
    - US_export_policy.jar
```

2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location:  
`<Supplementary file location>/serverless_agent_config`

When the .yml file runs, the policy jars are copied from the AWS or Azure location to the serverless agent directory.

3. After you update the .yml configuration file, redeploy the serverless runtime environment.

Specify the master symmetric key in the connection properties and the client-side encryption type in the advanced source and target properties.

## SSE-KMS encryption for mappings in advanced mode

To enable encryption with KMS, create an AWS Key Management Service (AWS KMS) policy and an AWS KMS-managed customer master key.

To use SSE-KMS encryption for mappings in advanced mode, perform one of the following tasks:

- To use the credentials from the `~/.aws/credentials` location, create the master instance profile and the worker instance profile in AWS, attach the KMS policy to the worker profile, and specify the profiles in the cluster configuration.
- Configure the Secure Agent on Amazon EC2, create the master instance profile and the worker instance profile in AWS, and attach the KMS policy to the worker profile.
- Configure the Secure Agent on Amazon EC2, use the default IAM role, and attach the KMS policy to the Secure Agent role.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux.

You can use only an unauthenticated proxy server to connect to Informatica Intelligent Cloud Services.

To configure the proxy settings for the Secure Agent, perform the following tasks:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.  
For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.
- Configure the proxy server properties in the `proxy.ini` file.

When you use a serverless runtime environment, you cannot use a proxy server to connect to Informatica Intelligent Cloud Services.

**Note:** If you enable both HTTP and SOCKS proxies, SOCKS proxy is used by default. If you want to use HTTP proxy instead of SOCKS proxy, set the value of the **DisableSocksProxy** property to true in the System property.

## Bypass proxy server

If your organization uses an outgoing proxy server to connect to the internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

However, if you want to exclude certain IP addresses and host names from the proxy, you can bypass the proxy. Set the *InfaAgent.NonProxyHost* property in the `proxy.ini` file and the `-Dhttp.nonProxyHosts` property in the JVM options of the Secure Agent properties and include the IP addresses and host names that you want to exclude.

The following table shows the proxy setting that you can configure through the `proxy.ini` file or the JVM options:

Proxy configuration	Proxy Flag Setting
Proxy.ini	<p><code>InfaAgent.NonProxyHost=localhost &lt;your_bucket_name&gt;.s3. 127.* [\:\:1]</code></p> <p>For example, to bypass a single S3 Bucket <code>iam.qa.bucket</code>, use the following proxy setting:</p> <p><code>InfaAgent.NonProxyHost=localhost iam.qa.bucket.s3. 127.* [\:\:1]</code></p> <p>To bypass all S3 buckets, use the following proxy setting:</p> <p><code>InfaAgent.NonProxyHost=localhost *.s3.* 127.* [\:\:1]</code></p>
JVM option	<p><code>-Dhttp.nonProxyHosts=localhost &lt;your_bucket_name&gt;.s3. 127.* [\:\:1]</code></p> <p>For example, to bypass a single S3 Bucket, <code>iam.qa.bucket</code>, use the following proxy setting:</p> <p><code>-Dhttp.nonProxyHosts=localhost iam.qa.bucket.s3. 127.* [\:\:1]</code></p> <p>To bypass all S3 buckets, use the following proxy setting:</p> <p><code>-Dhttp.nonProxyHosts=localhost *.s3.* 127.* [\:\:1]</code></p>

### Bypass the proxy server in advanced mode

To bypass the proxy server, you must update the `NonProxyHost` value in the `proxy.ini` file. You can set the property in the agent core path to configure the `NonProxyHost` in the advanced cluster configuration.

To bypass the proxy at the Amazon S3 endpoint, perform the following steps:

1. Edit the `proxy.ini` file and set the property in the `NonProxyHost` with the cluster region.
2. Enter the appropriate region name in the property in the following format:

```
InfaAgent.NonProxyHost=localhost|127.*|[\:\:1]|
169.254.169.254|. <REGION_NAME>.elb.amazonaws.com|*. <REGION_NAME>.elb.amazonaws.com
```

The following example shows how you can update the `NonProxyHost` for the US West region in the `proxy.ini` file:

```
InfaAgent.NonProxyHost=localhost|127.*|[\:\:1]|169.254.169.254|.us-
west-2.elb.amazonaws.com|*.us-west-2.elb.amazonaws.com|s3.us-west-2.amazonaws.com|
*.s3.us-west-2.amazonaws.com|s3.amazonaws.com
```

3. After you edit the `proxy.ini` file, you must set the property `ccs.enable.storage.proxy.settings` to false in the runtime properties of the advanced cluster. Perform the following steps to set the property:
  - a. Go to **Administrator**.

- b. In the **Advanced Clusters** page, select the name of the configuration that you want to edit from the list of advanced configurations.
- c. Set the property `ccs.enable.storage.proxy.settings` to `false` and save the cluster configuration in the **Runtime Properties** for the particular cluster.

The following image shows the configured cluster runtime properties:

Key	Value
ccs.enable.storage.proxy.settings	false
ccs.k8s.api.access.cidr	172.31.74.13/32
ccs.k8s.ssh.access.cidr	172.31.74.13/32
ccs.ssh.access.cidr	172.31.74.13/32

## Rules and guidelines for AssumeRole via IAM user authentication

Consider the following guidelines for Assume Role via IAM user authentication:

- The IAM user or IAM role that requests for the temporary security credentials must not have access to any AWS resources.
- Only authenticated IAM users or IAM roles can request for the temporary security credentials from the AWS Security Token Service (AWS STS).
- Before you run a task, ensure that you have enough time to use the temporary security credentials for running the task. You cannot extend the time duration of the temporary security credentials for an ongoing task.  
For example, when you read from and write to Amazon S3 and if the temporary security credentials expire, you cannot extend the time duration of the temporary security credentials which causes the task to fail.
- After the temporary security credentials expire, AWS does not authorize the IAM users or IAM roles to access the resources using the credentials. You must request for new temporary security credentials before the previous temporary security credentials expire in a mapping.
- For mappings in advanced mode, the temporary security credentials do not expire even after the configured time in the **Temporary Credential Duration** advanced source property elapses.
- Do not use the root user credentials of an AWS account to use the temporary security credentials. You must use the credentials of an IAM user to use the temporary security credentials.
- If both the source and target in a mapping point to the same Amazon S3 bucket, use the same Amazon S3 connection in the Source and Target transformations. If you use two different Amazon S3 connections, configure the same values in the connection properties for both the connections.
- If the source and target in a mapping point to different Amazon S3 buckets, you can use two different Amazon S3 connections.

You can configure different values in the connection properties for both the connections. However, you must select the **Use EC2 Role to Assume Role** check box in the connection property. You must also specify the same value for the **Temporary Credential Duration** field in the source and target properties.

- In a mapping, if you configure two or more Amazon S3 data sources from the same Amazon S3 bucket with different IAM roles, each IAM role must be able to access the data source of the other IAM role.
- In a mapping with two data sources, if you set up one Amazon S3 data source to use user credentials and another to use an IAM role, consider the following rules:
  - The IAM user for the first data source must also be able to assume the IAM role of the second Amazon S3 data source.
  - The IAM role that you configured for the second data source must also have access to the first Amazon S3 data source.

## Rules and guidelines for AWS regions

Consider the following rules and guidelines when you configure the region name of the bucket in the connection properties:

- When you change the runtime environment of an existing connection, the region is changed to the default region US East (N. Virginia). Select the region manually to change the default region.
- When you edit an existing connection, you see duplicate entries for regions. Use the regions that contain spaces because these regions are populated from AWS SDK. For example, use US West (Oregon) instead of US West(Oregon).

## Rules and guidelines for S3 compatible storage

Consider the following rules and guidelines when you configure S3 compatible storage in an Amazon S3 V2 connection:

- You can only configure basic authentication when you use S3 compatible storage.
- You cannot configure SSE-KMS encryption for the Scality RING S3 compatible storage. You cannot configure SSE and SSE-KMS encryption for MinIO S3 compatible storage.
- You cannot configure SQL ELT optimization to load data from Amazon S3 sources to Amazon Redshift.

## CHAPTER 25

# Amplitude connection properties

When you create an Amplitude connection, configure the connection properties.

The following table describes the Amplitude connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Amplitude
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent or a Hosted Agent.
API Key	The API key to access the Amplitude account.
Secret Key	The secret key of the Amplitude account.



## CHAPTER 26

# AMQP connection properties

When you set up an AMQP connection, you must configure the connection properties.

The following table describes the AMQP connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identity the connection. The description cannot exceed 4,000 characters.
Type	The AMQP connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Host Name	Network address of the AMQP broker.
Port	Port number of the AMQP broker to which the underlying TCP connection is made. Default is 5672.
Virtual Host	Virtual host name that identifies the AMQP system. Use the virtual host name for enhanced security.
Username	Username for the AMQP broker.
Password	Password for the AMQP broker.
Use SSL	Enable this option to use SSL for secure transmission. If you enable the SSL authentication, ensure that you provide both keystore and truststore details for using the AMQP connection in a streaming ingestion and replication task.
Keystore File Name	Contains the keys and certificates required for secure communication.
Keystore Password	Password for the keystore filename.

Property	Description
Keystore Type	<p>Type of keystore that you want to use.</p> <p>Keystore type defines the storage and data format of the keystore information and the algorithms used to protect private keys in the keystore.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- JKS. Stores private keys and certificates.</li> <li>- PKCS12. Stores private keys, secret keys, and certificates.</li> </ul>
Truststore File Name	Name of the truststore file.
Truststore Password	Password for the truststore file.
Truststore Type	<p>Type of truststore that you want to use.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- JKS</li> <li>- PKCS 12</li> </ul>
TLS Protocol	<p>Transport protocols that you want to use.</p> <p>Use one of the following types:</p> <ul style="list-style-type: none"> <li>- SSL</li> <li>- SSLv2Hello</li> <li>- SSLv3</li> <li>- TLS</li> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul>
Client Authentication	<p>Client authentication policy when connecting to the secured AMQP broker.</p> <p>Use one of the following property values when you define and enable an SSL context.</p> <ul style="list-style-type: none"> <li>- WANT</li> <li>- REQUIRED</li> <li>- NONE</li> </ul>

## CHAPTER 27

# Anaplan V2 connection properties

When you set up an Anaplan V2 connection, you must configure the connection properties.

The following table describes the Anaplan V2 connection properties:

Connection property	Description
Connection Name	A name for the Anaplan V2 connection. This name must be unique within the organization.
Description	Description of the Anaplan V2 connection.
Type	Type of connection. Select Anaplan V2.
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
Auth Type	The type of authentication that the connector must use to log in to Anaplan. Select the authentication method that the connector must use to login to the Anaplan. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Auth. Requires Anaplan account username and password to connect to Anaplan.</li><li>- Cert Auth. Requires Certificate Authority (CA) to obtain an authentication token.</li><li>- OAuth Device Flow. Requires an OAuth 2.0 client credential to authenticate user data across apps.</li></ul> Default is Basic Auth.
Username	The user name to log in to Anaplan. For example, <code>firstname.lastname@anaplan.com</code> . <b>Note:</b> Do not leave this field blank. Even though you want to establish a connection using certificate based authentication, you need to enter a random value or string in this field.
Password	Password that is associated with the user name that is specified in the Username property.
Certificate Path Location	Path to the Anaplan authentication certificate. Certificate Path Location is required only if you want to configure a connection with the certificate issued by Anaplan and you want to use API version 1.3. This implies that the Certification Path Location is required only if Auth type = Cert Auth, Major Version = 1, and Minor Version = 3 .
Workspace ID	The name or ID of the workspace. To fetch the ID, open the Anaplan model and copy the value after <code>selectedWorkspaceId=</code> from the URL.

Connection property	Description
Model ID	The name or ID of the model. To fetch the ID, open the Anaplan model and copy the value after <code>selectedModelId=</code> from the URL.
API Base URL	Enter the API Base URL. For example, <code>https://api.anaplan.com</code>
Auth URL	Specifies the URL for the authentication service required to generate the authentication token. For example, <code>https://us1a.app.anaplan.com</code>
API Major Version	The Anaplan API version has two parts: Major Version and Minor Version. Example: For API version 1.3, the Major Version is 1 and the Minor Version is 3. By default, the API Major Version is set to 1. <ul style="list-style-type: none"> <li>- To use certificate issued by Anaplan, select 1. API version 1.x supports certificate issued by Anaplan.</li> <li>- To use certificate issued by a certificate authority, select 2. API version 2.x supports certificate issued by a certificate authority.</li> </ul>
API Minor Version	By default, the API Minor Version is set to 3. <ul style="list-style-type: none"> <li>- Select 3 if you want to use API version x.3. For example, version 1.3</li> <li>- Select 0 if you want to use API version x.0. For example, version 2.0</li> </ul>
Max Task Retry Count	By default, the Max Task Retry Count is set to 2. If you select a greater value, it may slow down the synchronization tasks.
Error Dump Path Location	The absolute path of the error file on the Secure Agent machine. The Secure Agent creates a sub-folder in the Error Dump Path Location for each process operation.
Use API Based Metadata	You can import API based metadata from Anaplan and use API based field mapping instead of File based field mapping in a synchronization task. When you import API based metadata, Anaplan V2 Connector reads the column header information from Anaplan APIs directly without referring to files in Anaplan.
KeyStore Path Location	Path to the JAVA KeyStore file on the system with the Secure Agent. <b>Note:</b> The KeyStore Path Location, KeyStore Alias, and Keystore Password is required only if you want to configure a connection with the certificate issued by a certificate authority and you want to use API version 2.0.
KeyStore Alias	Alias of the certificate saved in the KeyStore file.
Keystore Password	Password for the certificate alias in the KeyStore file.
ClientId	Required for OAuth Device Flow. The client identifier issued to the client during the application registration process.
Token	Required for OAuth Device Flow. The refresh token is used to get new access tokens. You can select one of the following options: <ul style="list-style-type: none"> <li>- Rotatable. Uses the refresh token once during the lifespan.</li> <li>- Non-rotatable. Uses the refresh token several times. The non-rotatable token does not expire.</li> </ul>

## CHAPTER 28

# Ariba V2 connection properties

When you set up an Ariba V2 connection, you must configure the connection properties.

You can create an ITK or SOAP connection. When you create an ITK connection, Ariba allows authentication using shared secret or SSL certificate.

The following table describes the Ariba V2 connection properties:

Connection Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Connection Type	Type of Connection. You can select SOAP or ITK.
Service URL	URL for the Ariba service.
Realm/Site	Realm of the Ariba instance.
Data Dictionary File Location	Location of the data dictionary file on your local machine.
Use SSL Certificate	Applicable for ITK connection. Determines whether the Secure Agent establishes a secure connection to Ariba. When you select this option, the Secure Agent establishes an encrypted connection. SSL authentication requires Client Keystore, Client Keystore Password, and Client Key Password.
Shared Secret	Shared Secret for the ITK connection. Leave the Shared Secret blank if you authenticate using SSL certificate on Ariba Network.
Client Keystore	The location of the client keystore file.
Client Keystore Password	The password for the client keystore file required for secure communication.
Client Key Password	The password for the client key.

<b>Connection Property</b>	<b>Description</b>
User Name	Required for a SOAP connection. User name for the Ariba account.
Password	Required for a SOAP connection. Password for the Ariba account.

## CHAPTER 29

# AS2 connection properties

Configure connection properties for an AS2 server.

Configure the following properties on the **Connection** page in Administrator:

- AS2 connection properties, which define the connection and enable access to the AS2 server.
- Message properties, which specify access to private and public keys and message encryption preferences. The message properties also define how to pass messages to the organization such as whether to compress messages and whether to send or receive message receipts.
- Receipt properties, which specify whether to request MDN receipts, certificate and transfer encoding properties, and method of receiving MDN receipts.
- Proxy properties, which specify whether to use a proxy server and the proxy server details.

## Connection properties

The following table describes AS2 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment that contains the Secure Agent that you want to run the tasks.
URL	URL of the server that receives the messages. The URL syntax must refer to a valid server and location. The host name can be an IP address or a domain name. The port number is the port on which the AS2 server listens.
AS2 From ID	Name or ID of the sender. If the receiving server filters by this ID, the IDs must match. Value is case sensitive and can contain 1 to 128 ASCII printable characters in length. The value cannot contain white spaces.
AS2 To ID	Name or ID of the recipient. Value is case sensitive and can contain 1 to 128 ASCII printable characters in length. The value cannot contain white spaces.
Username	User name to connect to the remote AS2 server.
Password	Password to connect to the remote AS2 server.

Connection property	Description
Connection Timeout	<p>Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection does not occur in the specified amount of time.</p> <p>If the value is 0 or blank, the wait time is infinite.</p> <p>Default is 60 seconds.</p>
Read Timeout	<p>Maximum number of seconds to wait when attempting to read a file from the server. A timeout occurs if the file is not read in the specified amount of time.</p> <p>If the value is 0 or blank, the wait time is infinite.</p> <p>Default is 0 seconds.</p>
Connection Retry Attempts	<p>Number of times to retry connecting to the AS2 server if a successful connection does not occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections.</p> <p>If the value is blank, no retries are attempted.</p> <p>Default is blank.</p>
Connection Retry Interval	<p>Number of seconds to wait between each connection retry attempt.</p> <p>For example, to retry to connect up to 10 times with a five second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5.</p> <p>If the value is blank, the interval is 0 seconds.</p> <p>Default is blank.</p>
Follow Redirects	<p>Whether or not to follow redirect links when creating a connection.</p> <p>Default is false.</p>
User Agent	<p>Value used in the message header to indicate what application created or sent the message.</p>
Use Chunked Encoding	<p>Whether or not to pre-calculate the length of the request or send the request in chunks. Pre-calculating the content length might slow performance when sending large files. However, not all AS2 servers support chunked encoding.</p> <p>Default is false.</p>
Client Certificate Alias	<p>Alias of the key within the default keystore to use for client authentication when required by the receiving AS2 server.</p>
SSL Context Protocol	<p>Protocol to use when creating the SSLContext. The protocol that you specify depends on the security providers installed in the Java Runtime Environment (JRE).</p> <p><b>Note:</b> In most cases, the default value of SSL is appropriate. However, for some IBM JRE implementations, the default value of SSL will not work if the server you are connecting to does not support SSLv3.</p> <p>Default is SSL.</p>



# Message properties

The following table describes AS2 connection message properties:

Connection property	Description
Trust Store Location	Path to the truststore that stores the public key certificates. Must be on the Secure Agent machine or on a server accessible to the Secure Agent.
Trust Store Password	Password to access the truststore.
Encrypt Messages	Whether or not to encrypt messages during transmission. Encrypting the message within the encrypted tunnel is optional, but highly recommended. Default is false.
Encryption Algorithm	Algorithm to use to encrypt messages. Choose one of the following algorithms: <ul style="list-style-type: none"> <li>- AES128</li> <li>- AES256</li> <li>- CAST5</li> <li>- IDEA</li> <li>- TRIPLE-DES</li> <li>- RC2</li> </ul> Default is AES128.
Encryption Certificate Alias	Certificate alias to use in the default trusted certificate keystore to encrypt the outgoing message.
Sign Messages	Whether or not to sign the message with a digital signature. Signing messages is optional, but highly recommended. Default is false.
Private Keystore Location	Location of the keystore that stores private keys and associated certificates. Applicable when signing messages is enabled.
Private Keystore Password	Password to access the keystore. Applicable when signing messages is enabled.
Signature Algorithm	Algorithm to use to sign messages. Applicable when signing messages is enabled. Choose one of the following algorithms: <ul style="list-style-type: none"> <li>- SHA1</li> <li>- SHA224</li> <li>- SHA256</li> <li>- SHA384</li> <li>- SHA512</li> <li>- MD5</li> </ul> Default is SHA1.
Signature Certificate Alias	Private key alias to use to sign the message. The private key is located in the default private keystore.
Compress Messages	Whether or not to compress messages to reduce bandwidth. If you enable this option, Informatica Intelligent Cloud Services compresses messages using the zlib format. Default is false.
Content Type	MIME type of the source files. Default is application/EDI-Consent.

# Receipt properties

The following table describes AS2 connection receipt properties:

Connection property	Description
Receipt Certificate Alias	<p>Alias for the receipt certificate. Applicable when you configure the connection to require a signed receipt.</p> <p>AS2 Connector uses the receipt certificate to verify that the certificate that signed the receipt is a certificate in the default trusted certificate keystore.</p> <p>Optional if the receipt signature contains an embedded certificate. If the receipt signature does not contain an embedded certificate, you must specify the receipt certificate alias.</p>
Receipt Transfer Encoding	<p>Type of encoding to use for message receipts. This is useful when the receipt does not include the transfer encoding.</p> <p>Use one of the following values:</p> <ul style="list-style-type: none"> <li>- base64</li> <li>- quoted-printable</li> <li>- 7bit</li> <li>- 8bit</li> <li>- binary</li> </ul>
Request Receipt	<p>Whether or not to request a MDN receipt when the server receives the message. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- None. Do not require a receipt.</li> <li>- Signed. Require a receipt signed with a digital signature.</li> <li>- Unsigned. Require a receipt without a digital signature.</li> </ul> <p>Default is none.</p>
Destination	<p>Mode with which to receive the MDN. Applicable when you request a receipt.</p> <p>Select one of the following values:</p> <ul style="list-style-type: none"> <li>- Joblog. Receive MDN in the job log, accessible in Monitor.</li> <li>- File. Receive MDN in a file.</li> <li>- Email. Receive MDN in an email.</li> <li>- URL. Receive MDN through an URL.</li> <li>- Discard. Discard MDN.</li> </ul> <p>Default is joblog.</p>
File	<p>Path including the file name to store the MDN. Applicable for a file destination.</p>
When File Exists	<p>Determines how to resolve name conflict when a receipt file already exists. Applicable for a file destination.</p> <p>Select one of the following values:</p> <ul style="list-style-type: none"> <li>- Rename. Rename the new receipt file by adding a sequential number. For example, fileMdn 2.txt, fileMdn 3.txt</li> <li>- Append. Append receipt to the existing file.</li> <li>- Overwrite. Overwrite contents of the existing receipt file.</li> <li>- Skip. Do not upload the receipt.</li> <li>- Error. Duplicate file name causes error.</li> </ul> <p>Default is rename.</p>
Email Address	<p>Email address to send the receipts. Applicable for an email destination.</p>
Receipt URL	<p>URL to post the receipts. Applicable for an URL destination.</p>

# Proxy properties

The following table describes AS2 connection proxy properties:

Connection property	Description
Enabled	Determines if a proxy server is enabled for the connector. Default is disabled.
Proxy Type	Type of proxy server to use for the connection. Select one of the following types: <ul style="list-style-type: none"><li>- SOCKS. You can use SOCKS version 4 or 5.</li><li>- HTTPS.</li><li>- Informatica File Server proxy.</li></ul> Verify with your network administrator which proxy server type to use.
Host	Host name or IP address of the proxy server on your network.
Alternate Host	Host name or IP address of an alternate proxy server on your network. The alternate proxy server is used when the primary proxy server is unavailable.
Port	Port number of the proxy server on your network. If left blank, the default port for HTTP is 80 and the default port for SOCKS is 1080.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server. Required if your network uses the proxy server to create HTTP or HTTPS connections.

## CHAPTER 30

# BigMachines connection properties

When you set up a BigMachines connection, you must configure the connection properties.

**Important:** BigMachines Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use REST V2 Connector to access BigMachines.

The following table describes BigMachines connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	BigMachines.
Runtime Environment	Name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	Username of the BigMachines account.
Password	Password of the BigMachines account.
DataTables Schema Path	Provide the path of the data table schema file. For example, <code>...\BigMachines\config\Datatables.tbl</code> <b>Note:</b> The Data Table schema file name must contain a <code>.tbl</code> extension. The table header names mentioned in the schema file must have a separate <code>.sch</code> file in the same directory. The <code>.sch</code> files define field details of the table names present in the schema file.
WSDL Folder Path	Provide the WSDL file path. <b>Note:</b> If you do not specify WSDL URL in the connection properties, the default WSDL file path is selected as WSDL URL. The default WSDL URL file path is: <code>&lt;Secure Agent installation directory&gt;\downloads\&lt;latest connector zip package&gt;\package\plugins\&lt;Plugin ID&gt;\&lt;WSDL&gt;</code>
Endpoint URL	Path of the BigMachines endpoint URL.

Property	Description
Attribute Control File Path	Provide the attribute control path. The attribute control path controls the metadata. The default control file path is <Secure Agent installation directory>\downloads \<latest connector zip package>\package\plugins\
Enable Logging	Select the property to enable logging.
PagingSize	Number of records to fetch for each request.
Transaction Schema Name	Name of the REST document to fetch a transaction.
Transaction Line Item Schema Name	Name of the REST document to fetch the transaction line item details.
Batch Size	Specify the batch size to perform a bulk upsert operation on a Data Tables object.

## CHAPTER 31

# Birst Cloud Connect connection properties

When you set up a Birst Cloud Connect connection, you must configure the connection properties.

The following table describes the Birst Cloud Connect connection properties:

Connection property	Description
Connection Name	Name of Birst Cloud Connect Connector.
Description	Description of Birst Cloud Connect Connector.
Type	Select Birst Cloud Connect connection.
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	User name for Birst Cloud Connect application.
Password	Password for Birst Cloud Connect application.
Endpoint URL	Birst Web Services end-point URL.
Space ID	UDID of Birst Space in which you want to upload data.
Enable Debug Logger	Select to enable debug logging.
Configuration Location	Temporary storage for internal configuration.

## CHAPTER 32

# Box connection properties

Create a Box connection to read from or write data to Box.

## Connect to Box

Let's configure the Box connection properties to connect to Box.

### Before you begin

Before you get started, you need to configure OAuth for your Box account.

When you configure OAuth, specify the `redirect_URI` parameter. Box verifies that the `redirect_uri` parameter passed in the authorization URL in your Box connection matches with the redirect URI configured for the application.

When you configure a Box connection, you have the option to either autogenerate the access token in the connection, or manually generate the token. If you prefer to handle the token generation process yourself, you can manually generate the access token, along with the grant type, client ID, and client secret when you configure OAuth in Box.

For more information on how to set up OAuth to access Box, see the Box documentation.

The following video shows you how to autogenerate the OAuth access token when you configure a Box connection:



## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Box
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent doesn't apply to mappings in advanced mode.
Access Token Type	The access token to authenticate and authorize access to resources in the endpoint server. You can select from the following options: - Auto Generated. Box autogenerates the access token in the connection when you click <b>Get Token</b> . - Manual. Get the OAuth details from your Box account and enter the details manually in the connection. Default is <b>Auto Generated</b> .

### Autogenerate the access token

The connection is by default selected to autogenerate.

The following table describes the property and action required to autogenerate the access token from Box:

Property	Description
OAuth Access Token	Access token generated by Box. Click <b>Get Token</b> so that Box generates the access token and populates this field for you. For more information, see " <a href="#">Generate the OAuth access token</a> " on page 142. For a visual presentation, you can check out the <a href="#">Generating the access token video</a> .

### Manually generate the access token

To manually enter the OAuth properties, select the **Access Token Type** as **Manual**, and then enter the required properties:



The following table describes the OAuth properties that you need to connect to Box manually:

Property	Description
Access Token	Enter the manually generated OAuth access token value in Box.
Client Id	The client identifier issued to the client during the application registration process in Box.
Client Secret	The client secret key issued to the client during the application registration process in Box.
Grant Type	The grant type to connect to Box. Enter the string <b>refresh_token</b> .
Refresh Token	Enter the refresh token value. If the access token expires, you can use the refresh token to generate a new access token. <b>Note:</b> When you use the manual access token type and the refresh token expires, you need to re-enter the connection properties.

### Advanced settings

The following table describes the advanced connection properties:

Property	Description
URI Request Parameters	Parameters to search for files or folders in Box. Specify the search string in the following format: <code>query=search_string;content_types=&lt;name description file_content comments tags;limit=&lt;number&gt;;offset=&lt;number&gt;</code> For example, to search for objects that contain the word "generate", you can enter the following string: <code>query=generate;content_types=name;limit=0;offset=0</code> . You can use wildcard characters and enclose phrases or multiple query strings within double quotes to refine your search criteria. For more information, see <a href="#">"URI request parameters" on page 142</a> .
Source File Path	This property doesn't apply to the Box connection.
Target File Path	Optional. A directory on the Secure Agent machine where you can download objects from Box. Enter a path to download files or folders to a specific directory. By default, the Secure Agent downloads all the Box objects to the root directory in the Secure Agent machine.
Response Folder Path	This property doesn't apply to a Box connection.
Box File or Folder ID	File ID or the folder ID of the file or folder in Box from where you want to read data from or write data to Box. You can get the file ID or folder ID from the Box URL of the file or folder. For example, the Reports folder in Box has the following URL: <code>https://app.box.com/folder/50016834230</code> In the URL, 50016834230 is the folder ID of Reports. <b>Note:</b> You can override this value when you read from or write to CSV files in Box.

# Generate the OAuth access token

You need to generate an OAuth access token when you create a Box connection. The Secure Agent uses the token to securely connect to Box.

1. In the **OAuth Access Token** field on the **Connections** page , click **Get Token**.  
The **Log In** page for Box appears.
2. Enter the user credentials. You can choose one of the following options:
  - To use Box user account credentials, enter an email address and password associated with the user.
  - To use the single sign-on option, click **Use Single Sign On (SSO)** and enter the email address associated with the user.
3. Click **Authorize**.
4. Click **Grant access to Box**.

The **OAuth Access Token** field in the **Connection** page is updated with the generated token.

# URI request parameters

Use the URI request parameters to search Box objects.

Specify the search string in the **URI Request Parameters** field using the following syntax:

```
query=search_string;content_types=<name|description|file_content|comments|tags;limit=<number>;offset=<number>
```

The following table describes the **URI Request Parameters** field options:

Options	Description
Query	Searches the Box objects based on the word or phrase you specify. When you specify a phrase, verify that you enclose the phrase in single quote.
content_types	Specifies the scope of the search. You can use one of the following values: <ul style="list-style-type: none"><li>- Name - Searches based on the names of Box objects.</li><li>- Description - Searches based on the description associated with Box objects.</li><li>- File_content - Searches based on contents in the Box objects.</li><li>- Comments - Searches based on comments associated with Box objects.</li><li>- Tags - Searches based on tags associated with Box objects.</li></ul>
limit	Limits the number of search results that the Secure Agent writes to the target.
offset	Offsets the search results based on the specified offset value. For example, if you specify the offset value as 12, the Secure Agent ignores the first 11 rows in the search results and writes the results from the 12th row.

## CHAPTER 33

# Business 360 connection properties

When you create the Business 360 connection, you must configure the connection properties.

The following table describes the Business 360 connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={[] \:;'"'<, >. ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360</b> .
Runtime Environment	The name of the runtime environment where you want to run the mappings. Select a Secure Agent. <b>Note:</b> Ensure that you don't select a Hosted Agent or serverless runtime environment when you create a Business 360 connection.
Runtime Parameter	A system-generated job instance ID to process the ingress and export jobs. <b>Note:</b> Ensure that you do not modify this attribute.

## CHAPTER 34

# Business 360 Events connection properties

When you create the Business 360 Events connection, you must configure the connection properties.

The following table describes the Business 360 Events connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360 Events</b> .
Runtime Environment	The name of the runtime environment where you want to run the mappings. Specify a Secure Agent, Hosted Agent, or a serverless runtime environment.
Start Timestamp	A system-generated timestamp variable to set the start of a time range for which you want to get events from the Business 360 data store. <b>Note:</b> You can't modify this attribute.
End Timestamp	A system-generated timestamp variable to set the end of a time range for which you want to get events from the Business 360 data store. <b>Note:</b> You can't modify this attribute.

## CHAPTER 35

# Business 360 FEP connection properties

When you create the Business 360 FEP connection, you must configure the connection properties.

The following table describes the Business 360 FEP connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 100 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={[] \:;'"'<, > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Business 360 FEP Connector</b> .
Runtime Environment	The name of the runtime environment where you want to run the mappings. Select a Secure Agent. <b>Note:</b> Ensure that you don't select a Hosted Agent or serverless runtime environment when you create a Business 360 connection.
Runtime Parameter	A system-generated job instance ID to process the ingress jobs. <b>Note:</b> Ensure that you do not modify this attribute.

## CHAPTER 36

# CallidusCloud Commissions connection properties

When you create a CallidusCloud Commissions connection, you must configure the connection properties.

The following table describes the CallidusCloud Commissions connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
UserName	User name for the CallidusCloud portal login.
Password	Password of the CallidusCloud portal login.
BaseURL	The base URL to connect to the CallidusCloud application. Use the following sample to specify the base URL: <code>https://&lt;domainName&gt;/TrueComp-SaaS/services/rest/</code>
PageSize	The page size for the read operation. Default value is 10.

### Guidelines for a CallidusCloud Commissions connection

You can set the values for the session timeout properties as per your requirement through the JVM options for the Secure Agent.

You can configure the following properties:

- Session timeout: The time in seconds after which the session with the CallidusCloud Commissions endpoint times out.
- Attempts: The number of attempts to reconnect to the CallidusCloud Commissions endpoint.
- Wait time to re-attempt: The time in seconds between 2 attempts.

You must set the values for the properties higher than the default values, else the default values are considered.

The default values are:

```
-Dconnection.sessionTimeout=50
```

```
-Dconnection.attempts=3
```

```
-Dconnection.waitTimeToReattempt=5
```

Perform the following steps to configure the JVM options:

1. In Administrator, select the Secure Agent listed on the **Runtime Environments** tab.
2. Click **Edit**.
3. In the **System Configuration Details** section, select **Data Integration Server** as the service and **DTM** as the type.
4. Specify the values for the JVM options.

Custom Configuration Details

Service	Type	Sub-type	Name	Value	
Data Integration Server	DTM		JVMOption6	-Dconnection.sessionTimeout=60	+ X
Data Integration Server	DTM		JVMOption7	-Dconnection.attempts=4	+ X
Data Integration Server	DTM		JVMOption8	-Dconnection.waitTimeToReattempt=5	+ X

5. Click **Save**.

## CHAPTER 37

# CallidusCloud File Processor connection properties

When you create a CallidusCloud File Processor connection, you must configure the connection properties.

The following table describes the CallidusCloud File Processor connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
UserName	The user name to use for connecting to the SFTP server.
Password	The password to use for connecting to the SFTP server.
SFTP Key	The private key to use for connecting to the SFTP server. You must specify the SFTP key in a single line.
SFTP Key Pass Phrase	The pass phrase to connect to the SFTP server. You must specify the SFTP Key Pass Phrase in a single line
Host	The host name of the SFTP server.
Port	The port number to use for connecting to the server. If left blank, the default port number is 22.
Remote Directory	The directory on the SFTP host accessible to the Secure Agent. <b>Note:</b> Add / at the end of the specified path.



Property	Description
Charset	<p>Specify the character set to use for encoding data.</p> <p>CallidusCloud File Processor Connector supports the following character sets:</p> <ul style="list-style-type: none"> <li>- Big5</li> <li>- Big5-HKSCS</li> <li>- CESU-8</li> <li>- EUC-JP</li> <li>- EUC-KR</li> <li>- GB18030</li> <li>- GB2312</li> <li>- GBK</li> <li>- IBM00858</li> <li>- IBM01140</li> <li>- IBM01141</li> <li>- IBM01142</li> <li>- IBM01143</li> <li>- IBM01144</li> <li>- IBM01145</li> <li>- UTF-8</li> </ul> <p>The default value is UTF-8, which works well for all character data.</p>
Delimiter	<p>Delimiter used in the file to separate columns of data.</p> <p>Select the delimiter. The default delimiter is Comma.</p>
Compression Mode	<p>The compression format for binary files. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- gzip</li> </ul> <p>Default is None.</p>
Encryption Mode	<p>The type of encryption that the SFTP server uses to encrypt the data. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- GPG</li> </ul> <p>Default is None.</p>
Encryption Public Key	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the public key in a single line to encrypt data.</p>
Encryption Private Key	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the private key in a single line to decrypt data.</p>
Encryption Pass Phrase	<p>Required when you select <b>GPG</b> as the <b>Encryption Mode</b>. You must specify the pass phrase in a single line to encrypt data.</p>

For more information about converting multiline key file or pass phrase to single line key string, see the CallidusCloud File Processor documentation.

## CHAPTER 38

# Cassandra V2 connection properties

When you create a Cassandra V2 connection, you must configure the connection properties.

The following table describes the Cassandra V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + , Maximum length is 255 characters.
Description	
Type	The Cassandra V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Cassandra server.
Port	Port number of the Cassandra server. Default is <b>9042</b> .
Datacenter	Name of the Cassandra Datacenter to connect to. Default is <b>datacenter1</b> .
Keyspace	Name of the Cassandra Keyspace within the Cassandra Datacenter to connect to.
Username	User name to access the Cassandra server.
Password	Password to access the Cassandra server.
SSL Enabled	Choose from the following options: - Yes. Enable the SSL encryption. - No. Disable the SSL encryption. Default is <b>No</b> .

<b>Property</b>	<b>Description</b>
SSL KeyStore File Path	Applicable if you enable SSL. Absolute path of the SSL KeyStore file in the Secure Agent machine that contains private keys and certificates for the SSL server.
SSL KeyStore Password	Applicable if you enable SSL. Password for the SSL KeyStore.
SSL TrustStore File Path	Applicable if you enable SSL. Absolute path of the SSL TrustStore file in the Secure Agent machine that contains private keys and certificates for the SSL server.
SSL TrustStore Password	Applicable if you enable SSL. Password for the SSL TrustStore.

## CHAPTER 39

# Chatter connection properties

To use the Chatter Connector in a synchronization task, you must create a connection in Data Integration and configure the connection properties.

**Important:** Chatter Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Chatter connection properties:

Connection property	Description
Connection Name	Name of the connection.
Type	Type of connection. Select <b>Chatter</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
User Name	User name of the Chatter account.
Password	Password of the Chatter account.
Security Token	The security token generated from Salesforce.
Service URL	The service endpoint URL with the API version. The Chatter Connector supports up to API version 34.0. For example: <code>https://login.salesforce.com/services/Soap/u/34.0</code>
Attachment Path	The path where the attachments of the feeds need to be copied.

# CHAPTER 40

## Cloud Integration Hub connection properties

You can view the Cloud Integration Hub connection only if your organization is provisioned with Cloud Integration Hub. Do not edit, modify, or delete this connection. Do not modify any connection property apart from the **Do not use intermediate staging for subscription flows** and **Use JDBC for Private Publication Repository** properties.

The following table describes the connection properties for a Cloud Integration Hub connection:

Connection Property	Description	Editable
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ] }   \ : ; " ' < , > . ? /	Do not edit.
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.	Yes
Type	<b>Cloud Integration Hub</b> connection type.	Do not edit.
Enable Secret Vault	Stores the publication repository password for the connection in the Secret Manager in the runtime environment that is configured for your organization. This property appears only if secrets manager is set up for your organization. Select this option to use the credentials from the Secret Manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.	Do not edit.
Runtime Environment	Name of the runtime environment where you want to run the tasks.	Do not edit.

Connection Property	Description	Editable
Do not use intermediate staging for subscription flows	Disables writing to intermediate staging. Enable this property if you do not want to write to the intermediate staging, the Data Integration task reads the data from Cloud Integration Hub and then writes the data directly to the target location. Disabling writing to intermediate staging might affect system performance.	Yes
Use JDBC for Private Publication Repository	<p>To configure zero downtime for a private publication repository. Enable this property to ensure uninterrupted access to data on the private publication repository. You can enable zero downtime for publications and subscriptions that trigger a Data Integration task.</p> <p>On a hosted publication repository, Cloud Integration Hub applies zero downtime by default for all publication and subscription types.</p>	Yes

# CHAPTER 41

## Concur connection properties

To use Concur Connector in a synchronization task, you must create a connection in Data Integration.

**Important:** Concur Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

Perform the following steps to create Concur connection in Data Integration.

1. Click **Administrator > Connections**, and then click **New Connection** to create a connection.

The **New Connection** page appears.

**OK** **Cancel** **Test**

---

**Connection Details**

Connection Name:\*

Description:

Type:\*

---

**concur (ICL) Connection Properties**

Secure Agent:\*

Username\*

Password\*

Key\*

Company Domain

Service URL\*

Enable Logging

Paging Size

- Specify the following details:

Connection Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select Concur from the list.
Secure Agent	Select the appropriate Secure Agent from the list.
Username	Enter relevant username.
Password	Enter relevant password.
Key	Enter Concur OAUTH 2.0 key. For details, see <i>Key</i> .
Company Domain	Enter Concur company domain address, part of the Concur authentication using OAUTH 2.0.
Service URL	Enter service URL to connect to Concur account.
Enable Logging	Select to enable logging.
Paging Size	Enter the number of records to be pushed to Concur. The default value is 100.

- Click **Test Connection** to test the connection.
- Click **Save** to save the connection.



## CHAPTER 42

# Concur V2 connection properties

When you set up a Concur V2 connection, you can specify OAuth 2 or consumer key authentication to authenticate users and authorize access to Concur data. Informatica recommends that you use the OAuth 2 connection type.

The following table describes the basic connection properties

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Concur V2
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication	Authentication method for the connection. Ensure that you select <b>Concur V2</b> for the connection.
User name	The user name to log in to the Concur web page.
Password	The password associated with the user name.
Use OAuth 2	Uses OAuth 2 to authenticate users and authorize access to Concur data. Select OAuth 2. If you do not select OAuth 2, the connection uses consumer key authentication. Get the OAuth 2 credentials from SAP Concur.
Base URL for authentication	The URL for authentication that you received from Concur when you created your account. The base URL for authentication is derived from the authorization URL. For example, if the authorization URL is <a href="https://us-impl.api.concursolutions.com/oauth2/v0/token">https://us-impl.api.concursolutions.com/oauth2/v0/token</a> , the base URL for authentication is <a href="https://us-impl.api.concursolutions.com">https://us-impl.api.concursolutions.com</a> .
Base URL for API Invocation	The URL for API invocation that you received from Concur when you created your account.
Client ID	The unique ID of your application to complete the OAuth Authentication in the Active Directory.

Property	Description
Secret ID	The password of your application to complete the OAuth Authentication in the Active Directory.
Folder	The relative path to the objects that you want to access from Concur. For example, if the URL for API invocation is <code>https://us-impl.api.concursolutions.com</code> and the absolute path to invoke the API to retrieve the expense reports from Concur is <code>https://us-impl.api.concursolutions.com/api/expense/report</code> , enter the following relative path: <code>expense/report</code>

The following table describes the advanced connection properties:

Property	Description
Consumer Key	The key that is generated when a Concur administrator registers a partner application for your organization. To use consumer key authentication, ensure that you specify the user name and password of the Concur account in the connection properties. <b>Note:</b> Informatica intends to drop consumer key authentication support in a future release. Informatica requests you to transition to use OAuth authentication before the consumer key authentication is dropped.

## CHAPTER 43

# Couchbase connection properties

When you create a Couchbase connection, you must configure the connection properties.

The following table describes the Couchbase connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ ; : " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The connection type. Select <b>Couchbase</b> .
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Host Name	Host name or IP address of the Couchbase server.
Port	Couchbase server port number. Default is 9042.
Username	User name to access the Couchbase server.
Password	Password corresponding to the user name to access the Couchbase server.
SSL Mode	Not applicable for Couchbase Connector. Select <b>disabled</b> .

Property	Description
SSL Certificate Path	Not applicable for Couchbase Connector.
Additional Connection Properties	<p>Enter one or more JDBC connection parameters in the following format:            &lt;param1&gt;=&lt;value&gt;;&lt;param2&gt;=&lt;value&gt;;&lt;param3&gt;=&lt;value&gt;</p> <p>Couchbase Connector supports the following connection parameters:</p> <p><b>QueryMode</b></p> <p>It is used to send queries to Couchbase Server.</p> <p><b>LogLevel</b></p> <p>Species whether the Secure Agent logs error messages in the session log.</p> <p><b>LogPath</b></p> <p>The complete path to the folder where the driver saves log files when logging is enabled.</p> <p><b>AuthMech</b></p> <p>The authentication mechanism that the driver uses to connect to the Couchbase server.</p>

## CHAPTER 44

# Coupa connection properties

When you set up a Coupa connection, configure the connection properties.

**Important:** Coupa Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Coupa V2 Connector to access Coupa.

The following table describes the Coupa connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Coupa connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment for a mapping.
Domain Name	Coupa domain name.
Coupa API Key	Coupa unique API key.
UTC Time Zone	Coupa UTC time zone. Enter the timezone in the date and time fields. The time zone is appended to the filter values for the date and time fields.
Enable Logging	Enables logging for the task. When you enable logging, you can view the session log for the log details.

## CHAPTER 45

# Coupa V2 connection properties

Create a Coupa V2 connection to securely read data from or write data to Coupa.

## Connect to Coupa V2

Let's configure the Coupa V2 connection properties to connect to Coupa.

### Before you begin

Before you get started, configure OAuth authentication for your Coupa account based on the client secret authentication to register to the Coupa success portal to get the client details.

Log in to Coupa Cloud and get the following details:

- Identifier
- Secret
- Scope

Specify the identifier as client ID, secret as client secret, and the scopes in the connection properties.

**Note:** The scope values have to be space separated.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Coupa V2

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Hosted Agent doesn't apply to mappings in advanced mode.</p>
Authentication	Select Coupa V2.
Base Url	<p>Base URL to connect to Coupa API.</p> <p>Specify the base URL in the following format:</p> <p><code>https://{instance_name}.coupahost.com/</code></p> <p>For example, <code>https://companyname.coupahost.com/</code></p>
Client ID	<p>The Coupa client ID required to generate a valid access token.</p> <p>Specify the Coupa identifier as the client ID.</p>
Client Secret	<p>The Coupa client secret required to generate a valid access token.</p> <p>Specify the Coupa secret as the client secret.</p>
Scope	<p>The scope used to authorize access to Coupa.</p> <p>Enter the scope defined for the user in Coupa. To enter multiple scopes, separate each scope with a space.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Custom Field Config	<p>Specify custom fields for Coupa objects.</p> <p>Specify the custom fields in Coupa using the following format, where <code>FieldName</code> is value of the custom field name in Coupa, <code>FieldType</code> is the type of custom field, and <code>IsAPIGlobalNamespace</code> determines whether a custom field appears under root tag or custom-field tag in the <b>Field Mapping</b> tab:</p> <pre>Object1=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName3,FieldType,DataType,IsAPIGlobalNamespace Object2=FieldName1,FieldType,DataType, IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType, IsAPIGlobalNamespace Object3=FieldName1,FieldType,DataType,IsAPIGlobalNamespace;\ FieldName2,FieldType,DataType,IsAPIGlobalNamespace;\ FieldName3,FieldType,DataType,IsAPIGlobalNamespace</pre> <p><b>Coupa V2 Connector supports only simple custom fields.</b></p> <p><b>For example:</b></p> <pre>user-summary=custom_field1,Simple,String,true;\ custom_field2,Simple,String, false requisition-header=requisition_cf1,Simple,String,true;\ requisition_cf2,Simple,Integer,false;\ requisition_cf3,Simple,Integer user=user_customfield1,Simple,String,false;\ user_customfield_2,Simple,String,true</pre> <p>For more information about the objects and rules and guidelines for custom fields in Coupa V2, see <a href="#">"Coupa V2 Custom Fields" on page 164</a> and <a href="#">"Rules and guidelines for Coupa custom fields" on page 167</a>.</p> <p><b>Note:</b> The Secure agent replaces underscore in the custom field name with hyphen and displays the custom field name in the <b>Field Mapping</b> tab.</p>

## Coupa V2 Custom Fields

Use Coupa to create custom fields. You can use Coupa V2 Connector to read data from the custom fields that are present in the following Coupa resources:

- User
- Expense Reports
- Expense Categories
- Advance Ship Notices
- Punchout Sites
- Forms
- Warehouse
- Asset Tag
- Lookup Values



- Address
- Contracts
- Suppliers
- Items
- Department
- Commodities
- Invoices
- Receipts
- Purchase Orders
- Requisitions

To read data from or insert data to custom fields in Coupa, you must configure the **Custom Field Config** property when you create a Coupa V2 connection.

When you specify a custom field for a Coupa resource in the **Custom Field Config** connection property, you must specify the object name based on the Coupa metadata file.

The following table lists the object names based on the Coupa metadata file:

Coupa Resource Name	Coupa Sub Resources	Object Name
Expense Reports	Items	expense-report
		item
Advance Ship Notices	Headers	asn-header-summary
	Lines	asn-line-summary
Suppliers	Supplier Sites	supplier
		supplier-site
Items	Supplier Items	item
		supplier-item
Invoices	Lines	invoice-header
		invoice-line-summary
Purchase Orders	Lines	order-header
		order-line-summary
Requisitions	Items	requisition-header
		item
Receipts	NA	inventory-transaction
Commodities	NA	commodity-summary

Coupa Resource Name	Coupa Sub Resources	Object Name
Department	NA	department
Contracts	NA	contract
Address	NA	address
Lookup Values	NA	lookup-value
Asset Tag	NA	asset-tag-summary
Warehouse	NA	warehouse-summary
Forms	NA	form-summary
Punchout Sites	NA	punchout-site-summary
User	NA	user

When you want to read data from or insert data to a custom field in Coupa, you must always specify the **Field Name** that is generated by Coupa.

The following table displays the various custom fields and data types that Coupa V2 Connector supports:

Coupa Field Type	Data Type
Check Box	Boolean
Date	Date/Time
Drop Down (Single Select)	String
Number	Integer
Radio Group	String
Text Field	String

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux.

Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.

For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help .

Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Rules and guidelines for Coupa custom fields

Consider the following rules and guidelines to read data from or insert data to custom fields in Coupa:

- When you specify the custom field in the **Custom Field Config** connection property, you must specify the custom fields for different objects separated by a line break.
- When you specify multiple custom fields for a particular object, you must separate the custom fields with an empty new line.
- When you specify the custom fields for an Coupa object, you must specify ; \ at the end of the line except for the last entry.
- Before you specify a value for the **IsAPIGlobalNamespace** field for a custom field, you must verify whether the **API global namespace** check box is available for the custom field in Coupa. If the custom field does not contain the **API global namespace** check box, you must specify the value of **IsAPIGlobalNamespace** field as false.
- If you do not specify a value for the **IsAPIGlobalNamespace** field, Coupa V2 Connector considers true as the default.
- When you specify the value of the **IsAPIGlobalNamespace** as true, the custom field appears under the **root** tag in the **Field Mapping** tab.
- When you specify the value of the **IsAPIGlobalNamespace** as false, the custom field appears under the **custom-field** tag in the **Field Mapping** tab.

## CHAPTER 46

# Cvent connection properties

You can create a Cvent connection to securely read data from Cvent.

Use Cvent connections to specify sources in synchronization tasks and mapping tasks. Create a connection and associate it with synchronization tasks, mappings, or mapping tasks.

## Connect to Cvent

Let's configure the Cvent connection properties to connect to Cvent.

### Before you begin

Before you configure the connection properties, you'll need to get the API user name and endpoint URL from your Cvent account.

The following video shows you how to get the information you need:



### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + , Maximum length is 255 characters.
Description	

Property	Description
Type	Cvent.
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p>
Account Number	Specify the account number.
User Name	User name of the Cvent API.
Password	Password for the Cvent API.
Endpoint Url	The endpoint URL of the Cvent application.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Batch Size	<p>Number of records to be retrieved at a time.</p> <p>Maximum is 200.</p>
UTC Time Zone	<p>Cvent UTC time zone.</p> <p>Enter the timezone in the date and time fields.</p> <p>The time zone is appended to the filter values for the date and time fields.</p>
Enable Logging	<p>Enables logging for the task.</p> <p>When you enable logging, you can view the session log for the log details.</p>

# Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 47

# Databricks connection properties

Create a Databricks connection to securely read data from or write data to Databricks.

## Staging prerequisites

Before you create a connection, you must perform certain prerequisite tasks to configure the staging environment to connect to SQL warehouse, all-purpose cluster, or job cluster.

## SQL warehouse

Configure either the AWS or Azure staging environment for the SQL warehouse based on the deployed environment. You also need to configure the Spark parameters for the SQL warehouse to use Azure and AWS staging.

You can use a SQL warehouse on the Windows and Linux operating systems.

For more information on the types of SQL warehouses that you can connect to, see the [Databricks SQL warehouses](#) Knowledge Base article.

## Configure AWS staging

Configure IAM AssumeRole authentication to use AWS staging for the SQL warehouse.

### IAM AssumeRole authentication

You can enable IAM AssumeRole authentication in Databricks for secure and controlled access to the Amazon S3 staging bucket when you run mappings and mapping tasks.

You can configure IAM authentication when the Secure Agent runs on an Amazon Elastic Compute Cloud (EC2) system. When you use a serverless runtime environment, you cannot configure IAM authentication.

**Note:** Data Ingestion and Replication does not support IAM authentication for access to Amazon S3 staging.

Perform the following steps to configure IAM authentication on EC2:

1. Create a minimal Amazon IAM policy.
2. Create the Amazon EC2 role. The Amazon EC2 role is used when you create an EC2 system. For more information about creating the Amazon EC2 role, see the *AWS documentation*.

3. Link the minimal Amazon IAM policy with the Amazon EC2 role.
4. Create an EC2 instance. Assign the Amazon EC2 role that you created to the EC2 instance.
5. Install the Secure Agent on the EC2 system.

## Temporary security credentials using AssumeRole

You can use temporary security credentials using AssumeRole to access AWS resources from same or different AWS accounts.

**Note:** Data Ingestion and Replication does not support using temporary security credentials for IAM users.

Ensure that you have the **sts:AssumeRole** permission and a trust relationship established within the AWS accounts to use temporary security credentials. The trust relationship is defined in the trust policy of the IAM role when you create the role. The IAM role adds the IAM user as a trusted entity allowing the IAM users to use temporary security credentials and access AWS accounts.

For more information about how to establish the trust relationship, see the *AWS documentation*.

When the trusted IAM user requests for temporary security credentials, the AWS Security Token Service (AWS STS) dynamically generates the temporary security credentials that are valid for a specified period and provides the credentials to the trusted IAM users. The temporary security credentials consist of access key ID, secret access key, and secret token.

To use the dynamically generated temporary security credentials, provide a value for the **IAM Role ARN** connection property when you create a Databricks connection. The IAM Role ARN uniquely identifies the AWS resources. Then, specify the time duration in seconds during which you can use the temporarily security credentials in the **Temporary Credential Duration** advanced source and target properties.

### External ID

You can specify the external ID for a more secure cross-account access to the Amazon S3 bucket when the Amazon S3 bucket is in a different AWS account.

Optionally, you can specify the external ID in the AssumeRole request to the AWS Security Token Service (STS).

The external ID must be a string.

The following sample shows an external ID condition in the assumed IAM role trust policy:

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "dummy_external_id"
      }
    }
  }
]
```

**Note:** Data Ingestion and Replication does not support External ID.

### Temporary security credentials policy

To use temporary security credentials to access AWS resources, both the IAM user and IAM role require policies.



## Amazon S3 permission policy

Attach the following S3 permission policy to allow access to the Amazon S3 bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketAcl"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::com.amk"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketAcl"
      ],
      "Resource": "arn:aws:s3:::com.amk/*"
    }
  ]
}
```

The following section lists the policies required for IAM user and IAM role:

### IAM user

An IAM user must have the `sts:AssumeRole` policy to use temporary security credentials in same or different AWS account.

The following sample policy allows an IAM user to use the temporary security credentials in an AWS account:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

### IAM role

An IAM role must have the `sts:AssumeRole` policy and a trust policy attached with the IAM role to allow the IAM user to access the AWS resource using temporary security credentials. The policy specifies the AWS resource that the IAM user can access and the actions that the IAM user can perform. The trust policy specifies the IAM user from the AWS account that can access the AWS resource.

The following policy is a sample trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::AWS-account-ID:root" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```

    }
  }
}

```

Here, in the `Principal` attribute, you can also provide the ARN of IAM user who can use the dynamically generated temporary security credentials and to restrict further access. For example,

```
"Principal" : { "AWS" : "arn:aws:iam:: AWS-account-ID :user/ user-name " }
```

## Temporary security credentials using AssumeRole for EC2

You can use temporary security credentials using AssumeRole for an Amazon EC2 role to access AWS resources from same or different AWS accounts.

The Amazon EC2 role would be able to assume another IAM Role from the same or a different AWS account without requiring the permanent access key and secret key.

Consider the following prerequisites when you use temporary security credentials using AssumeRole for EC2:

- Install the Secure Agent on an AWS service such as Amazon EC2.
- The EC2 role attached to the AWS EC2 service does not need access to Amazon S3 but needs permission to assume another IAM role.
- The IAM role that needs to be assumed by the EC2 role must have a permission policy and a trust policy attached to it.

To configure an EC2 role to assume the IAM role provided in the **IAM Role ARN** connection property, select the **Use EC2 Role to Assume Role** check box in the connection properties.

## Create a minimal Amazon IAM policy

To stage the data in Amazon S3, use the following minimum required permissions: :

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads. Applicable only for mappings in advanced mode.

You can use the following sample Amazon IAM policy:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3::<bucket_name>/*",
        "arn:aws:s3::<bucket_name>"
      ]
    }
  ]
}

```

For mappings in advanced mode, you can use different AWS accounts within the same AWS region. Make sure that the Amazon IAM policy confirms access to the AWS accounts used in these mappings.

**Note:** The **Test Connection** does not validate the IAM policy assigned to users. You can specify the Amazon S3 bucket name in the source and target advanced properties.

This information does not apply to Data Ingestion and Replication.

## Configure Spark parameters for AWS staging

Before you use the Databricks SQL warehouse to run mappings, configure the Spark parameters for SQL warehouse on the Databricks SQL Admin console.

On the Databricks SQL Admin console, navigate to **SQL Warehouse Settings > Data Security**, and then configure the Spark parameters for AWS under **Data access configuration**.

Add the following Spark configuration parameters and restart the SQL warehouse:

- `spark.hadoop.fs.s3a.access.key` <S3 Access Key value>
- `spark.hadoop.fs.s3a.secret.key` <S3 Secret Key value>
- `spark.hadoop.fs.s3a.endpoint` <S3 Staging Bucket endpoint value>

For example, the S3 staging bucket warehouse value is `s3.ap-south-1.amazonaws.com`.

Ensure that the configured access key and secret key have access to the S3 buckets where you store the data for Databricks tables.

## Configure Azure staging

Before you use Microsoft Azure Data Lake Storage Gen2 to stage files, perform the following tasks:

- Create a storage account to use with Microsoft Azure Data Lake Storage Gen2 and enable **Hierarchical namespace** in the Azure portal.

You can use role-based access control to authorize the users to access the resources in the storage account. Assign the Contributor role or Reader role to the users. The contributor role grants you full access to manage all resources in the storage account, but does not allow you to assign roles. The reader role allows you to view all resources in the storage account, but does not allow you to make any changes.

**Note:** To add or remove role assignments, you must have write and delete permissions, such as an Owner role.

- Register an application in Azure Active Directory to authenticate users to access the Microsoft Azure Data Lake Storage Gen2 account.

You can use role-based access control to authorize the application. Assign the Storage Blob Data Contributor or Storage Blob Data Reader role to the application. The Storage Blob Data Contributor role lets you read, write, and delete Azure Storage containers and blobs in the storage account. The Storage Blob Data Reader role lets you only read and list Azure Storage containers and blobs in the storage account.

- Create an Azure Active Directory web application for service-to-service authentication with Microsoft Azure Data Lake Storage Gen2.

**Note:** Ensure that you have superuser privileges to access the folders or files created in the application using the connector.

- To read and write complex files, set the JVM options for type DTM to increase the `-Xms` and `-Xmx` values in the system configuration details of the Secure Agent to avoid java heap space error. The recommended `-Xms` and `-Xmx` values are 512 MB and 1024 MB respectively.

## Configure Spark parameters for Azure staging

Before you use the Databricks SQL warehouse to run mappings, configure the Spark parameters for SQL warehouse on the Databricks SQL Admin console.

On the Databricks SQL Admin console, navigate to **SQL Warehouse Settings > Data Security**, and then configure the Spark parameters for Azure under **Data access configuration**.

Add the following Spark configuration parameters and restart the SQL warehouse:

- `spark.hadoop.fs.azure.account.oauth2.client.id.<storage-account-name>.dfs.core.windows.net <value>`
- `spark.hadoop.fs.azure.account.auth.type.<storage-account-name>.dfs.core.windows.net OAuth`
- `spark.hadoop.fs.azure.account.oauth2.client.secret.<storage-account-name>.dfs.core.windows.net <Value>`
- `spark.hadoop.fs.azure.account.oauth.provider.type.<storage-account-name>.dfs.core.windows.net org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider`
- `spark.hadoop.fs.azure.account.oauth2.client.endpoint.<storage-account-name>.dfs.core.windows.net https://login.microsoftonline.com/<Tenant ID>/oauth2/token`

Ensure that the configured client ID and client secret have access to the file systems where you store the data for Databricks tables.

## All-purpose cluster

Enable the Secure Agent properties for design-time processing on the all-purpose cluster. You can use all-purpose cluster only on the Linux operating system.

### Configure Secure Agent properties

To connect to all-purpose cluster, enable the Secure Agent properties for design time.

1. In **Administrator**, select the Secure Agent listed on the **Runtime Environments** tab.
2. Click **Edit**.
3. In the **System Configuration Details** section, select Data Integration Server as the **Service** and Tomcat JRE as the **Type**.
4. Edit the **JRE\_OPTS** field and set the value to `-DUseDatabricksSql=false`.

TomcatJRE	JRE_OPTS	<code>!-Xrs -DUseDatabricksSql=false</code>
-----------	----------	---

## Job cluster

Configure the Spark parameters for job cluster to use Azure and AWS staging based on where the cluster is deployed.

You also need to enable the Secure Agent properties for runtime processing on the job cluster.

You can use job cluster only on the Linux operating system.

## Spark configuration

Before you connect to the job cluster, you must configure the Spark parameters on AWS and Azure.

### Configuration on AWS

Add the following Spark configuration parameters for the job cluster and restart the cluster:

- `spark.hadoop.fs.s3a.access.key <value>`
- `spark.hadoop.fs.s3a.secret.key <value>`
- `spark.hadoop.fs.s3a.endpoint <value>`

Ensure that the access and secret key configured has access to the buckets where you store the data for Databricks tables.

### Configuration on Azure

Add the following Spark configuration parameters for the job cluster and restart the cluster:

- `fs.azure.account.oauth2.client.id.<storage-account-name>.dfs.core.windows.net <value>`
- `fs.azure.account.auth.type.<storage-account-name>.dfs.core.windows.net <value>`
- `fs.azure.account.oauth2.client.secret.<storage-account-name>.dfs.core.windows.net <Value>`
- `fs.azure.account.oauth.provider.type.<storage-account-name>.dfs.core.windows.net org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider`
- `fs.azure.account.oauth2.client.endpoint.<storage-account-name>.dfs.core.windows.net https://login.microsoftonline.com/<Tenant ID>/oauth2/token`

Ensure that the client ID and client secret configured has access to the file systems where you store the data for Databricks tables.

## Configure Secure Agent properties

To connect to job cluster, enable the Secure Agent properties for runtime.

**Note:** This topic does not pertain to Data Ingestion and Replication.

1. In **Administrator**, select the Secure Agent listed on the **Runtime Environments** tab.
2. Click **Edit**.
3. In the **System Configuration Details** section, select Data Integration Server as the **Service** and DTM as the **Type**.
4. Edit the **JVMOption** field and set the value to `-DUseDatabricksSql=false`.



The screenshot shows a configuration table with three columns: 'DTM', 'JVMOption2', and a text input field. The 'DTM' column contains the text 'DTM'. The 'JVMOption2' column contains the text 'JVMOption2'. The text input field contains the value '-DUseDatabricksSql=false'.

## Connect to Databricks

Let's configure the Databricks connection properties to connect to Databricks.

### Before you begin

You can use a Databricks connection to read from and write to Databricks tables.

You can configure the following compute resources to connect to Databricks:

- **SQL warehouse (Recommended)**  
The Secure Agent connects to the SQL warehouse at design time and runtime.
- **All-purpose cluster and job cluster**  
The Secure Agent connects to the all-purpose cluster to import the metadata at design time and to the job cluster to run the mappings.

**Note:** If you're using an all-purpose or job cluster, Informatica recommends transitioning to the SQL warehouse. The all-purpose and job clusters will no longer receive new feature updates or enhancements, although they will still receive critical security updates to maintain their stability and safety. By switching to the SQL warehouse, you will benefit from the latest features and enhancements.

Before you get started, you'll need to configure the AWS or Azure staging environment to use Databricks connection.

To learn about prerequisites for the Azure or AWS environment, check out ["Staging prerequisites" on page 171](#).

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Databricks
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.

Property	Description
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.            Select a Secure agent, Hosted Agent, or serverless runtime environment.            Hosted Agent is not applicable for mappings in advanced mode.            You cannot run an application ingestion and replication, database ingestion and replication, or streaming ingestion and replication task on a Hosted Agent or serverless runtime environment.</p>
SQL Warehouse JDBC URL	<p>Databricks SQL Warehouse JDBC connection URL.            This property is required only for Databricks SQL warehouse. Doesn't apply to all-purpose cluster and job cluster.            To get the SQL Warehouse JDBC URL, go to the Databricks console and select the JDBC driver version from the JDBC URL menu.            For JDBC driver version 2.6.25 or later (recommended), use the following syntax:  <pre>jdbc:databricks://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/&lt;SQL endpoint cluster ID&gt;;</pre>           For JDBC driver version 2.6.22 or earlier, use the following syntax:  <pre>jdbc:spark://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/&lt;SQL endpoint cluster ID&gt;;</pre> <b>Important:</b> Effective in the October 2024 release, Simba JDBC driver versions 2.6.22 and earlier entered deprecation. While you can use the Simba driver in the current release, Informatica intends to drop support for Simba JDBC driver versions 2.6.22 and earlier in the April 2025 release. Informatica recommends that you use the Databricks JDBC driver version 2.6.38. For more information on how to use the Databricks JDBC driver for Databricks Connector, see <a href="#">Databricks JDBC driver</a> Knowledge Base article.            Application ingestion and replication and database ingestion and replication tasks can use JDBC URL version <b>2.6.25 or later</b> or <b>2.6.22 or earlier</b>. The URLs must begin with the prefix  <pre>jdbc:databricks://, as follows:</pre> <pre>jdbc:databricks://&lt;Databricks Host&gt;:443/default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/&lt;SQL endpoint cluster ID&gt;;</pre>           Ensure that you set the required environment variables in the Secure Agent. Also specify the correct <b>JDBC Driver Class Name</b> under advanced connection settings.  <b>Note:</b> Specify the database name in the Database Name connection property. If you specify the database name in the JDBC URL, it is not considered.</p>

## Authentication type

You can configure personal access token and OAuth machine-to-machine authentication types to access Databricks.

Select the required authentication method and then configure the authentication-specific parameters.

Personal access token authentication requires the personal access token and OAuth machine-to-machine authentication requires the client ID and client secret of your Databricks account.

For more information on how to get the personal access token, client ID, and client secret, see the Databricks documentation.

### Personal access token authentication

Personal access token authentication requires the personal access token of your Databricks account.

The following table describes the connection properties for personal access token authentication:

Property	Description
Databricks Token	Personal access token to access Databricks. This property is required for SQL warehouse, all-purpose cluster, and job cluster.
Catalog Name	If you use Unity Catalog, the name of an existing catalog in the metastore. This property is optional for SQL warehouse. Doesn't apply to all-purpose cluster and job cluster. The catalog name cannot contain special characters. For more information about Unity Catalog, see the <i>Databricks documentation</i> .

## OAuth machine-to-machine authentication

OAuth machine-to-machine authentication requires the client ID and client secret of your Databricks account. OAuth machine-to-machine authentication doesn't apply to all-purpose cluster and job cluster can be used only with JDBC driver versions 2.6.25 or later.

The following table describes the connection properties for OAuth machine-to-machine authentication:

Property	Description
Client ID	The client ID of the service principal.
Client Secret	The client secret associated with the Client ID of the service principal.
Catalog Name	If you use Unity Catalog, the name of an existing catalog in the metastore. This property is optional for SQL warehouse. Doesn't apply to all-purpose cluster and job cluster. The catalog name cannot contain special characters. For more information about Unity Catalog, see the <i>Databricks documentation</i> .

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Database	The name of the schema in Databricks. The name can contain only alphanumeric characters and hyphen (-). This property is optional for SQL warehouse, all-purpose cluster, and job cluster. For Data Integration, if you do not specify a value, all databases available in the workspace are listed. The value you specify overrides the schema specified in the <b>SQL Warehouse JDBC URL</b> connection property. If you do not specify a value, all databases available in the workspace are listed. The value you specify overrides the schema specified in the <b>SQL Warehouse JDBC URL</b> connection property.
JDBC Driver Class Name	The name of the JDBC driver class. This property is optional for SQL warehouse, all-purpose cluster, and job cluster. Default is <code>com.databricks.client.jdbc.Driver</code>



Property	Description
Staging Environment	<p>The staging environment where your data is temporarily stored before processing. This property is required for SQL warehouse, all-purpose cluster, and job cluster.</p> <p>Select one of the following options as the staging environment:</p> <ul style="list-style-type: none"> <li>- AWS. Select if Databricks is hosted on the AWS platform.</li> <li>- Azure. Select if Databricks is hosted on the Azure platform.</li> <li>- Personal Staging Location. Select to stage data in a local personal storage location. Personal staging location doesn't apply to all-purpose cluster and job cluster. Personal staging location doesn't apply to mappings in advanced mode.</li> </ul> <p><b>Important:</b> Effective in the October 2024 release, personal staging location entered deprecation. While you can use the functionality in the current release, Informatica intends to drop support for the functionality in a future release. Informatica recommends that you use a Volume to stage the data.</p> <ul style="list-style-type: none"> <li>- Volume. Select to stage data in a volume in Databricks. Volumes are Unity Catalog objects used to manage and secure non-tabular datasets such as files and directories. To use a volume, ensure that your Databricks workspace is enabled for unity catalog. Volume doesn't apply to all-purpose cluster and job cluster. You can use a volume only on a Linux machine and with JDBC driver versions 2.6.25 or later. Volume doesn't apply to mappings in advanced mode.</li> </ul> <p>Default is Volume.</p> <p>If you select Personal Staging Location for a connection that Data Ingestion and Replication uses, the Parquet data files for application ingestion and replication jobs or database ingestion and replication jobs can be staged to a local personal storage location, which has a data retention period of 7 days. You must also specify a Database Host value. If you use Unity Catalog, note that a personal storage location is automatically provisioned.</p> <p>You cannot use personal staging location with Databricks unmanaged tables.</p> <p><b>Note:</b> You cannot switch between clusters after you establish a connection.</p>
Volume Path	<p>The absolute path to the files within a volume in Databricks.</p> <p>Specify the path in the following format:</p> <pre data-bbox="516 1247 1373 1297">/Volumes/&lt;catalog_identifier&gt;/&lt;schema_identifier&gt;/&lt;volume_identifier&gt;/&lt;path&gt;</pre>
Databricks Host	<p>The host name of the endpoint the Databricks account belongs to.</p> <p>This property is required only for all-purpose cluster and job cluster. Doesn't apply to SQL warehouse.</p> <p>You can get the Databricks Host from the JDBC URL. The URL is available in the Advanced Options of JDBC or ODBC in the Databricks all-purpose cluster.</p> <p>The following example shows the Databricks Host in JDBC URL:</p> <pre data-bbox="516 1524 1373 1575">jdbc:spark://&lt;Databricks Host&gt;:443/ default;transportMode=http; ssl=1;httpPath=sql/protocolv1/o/&lt;Org Id&gt;/&lt;Cluster ID&gt;; AuthMech=3; UID=token; PWD=&lt;personal-access-token&gt;</pre> <p>The value of PWD in Databricks Host, Organization Id, and Cluster ID is always &lt;personal-access-token&gt;.</p>

Property	Description
Cluster ID	<p>The ID of the cluster.</p> <p>This property is required only for all-purpose cluster and job cluster. Doesn't apply to SQL warehouse.</p> <p>You can get the cluster ID from the JDBC URL. The URL is available in the Advanced Options of JDBC or ODBC in the Databricks all-purpose cluster</p> <p>The following example shows the Cluster ID in JDBC URL:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/ default;transportMode=http; ssl=1;httpPath=sq/ protocolv1/o/&lt;Org Id&gt;/&lt;Cluster ID&gt;; AuthMech=3;UID=token; PWD=&lt;personal-access-token&gt;</pre>
Organization ID	<p>The unique organization ID for the workspace in Databricks.</p> <p>This property is required only for all-purpose cluster and job cluster. Doesn't apply to SQL warehouse.</p> <p>You can get the Organization ID from the JDBC URL. The URL is available in the Advanced Options of JDBC or ODBC in the Databricks all-purpose cluster</p> <p>The following example shows the Organization ID in JDBC URL:</p> <pre>jdbc:spark://&lt;Databricks Host&gt;:443/ default;transportMode=http; ssl=1;httpPath=sq/ protocolv1/o/&lt;Organization ID&gt;/ &lt;Cluster ID&gt;;AuthMech=3;UID=token; PWD=&lt;personal-access- token&gt;</pre>
Min Workers <sup>1</sup>	<p>The minimum number of worker nodes to be used for the Spark job. Minimum value is 1.</p> <p>This property is required only for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p>
Max Workers <sup>1</sup>	<p>The maximum number of worker nodes to be used for the Spark job. If you don't want to autoscale, set Max Workers = Min Workers or don't set Max Workers.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p>
DB Runtime Version <sup>1</sup>	<p>The version of job cluster to spawn when you connect to job cluster to process mappings.</p> <p>This property is required only for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>Select the Databricks runtime version 9.1 LTS or 13.3 LTS.</p>
Worker Node Type <sup>1</sup>	<p>The worker node instance type that is used to run the Spark job.</p> <p>This property is required only for all-purpose cluster and job cluster. Doesn't apply to SQL warehouse.</p> <p>For example, the worker node type for AWS can be i3.2xlarge. The worker node type for Azure can be Standard_DS3_v2.</p>
Driver Node Type <sup>1</sup>	<p>The driver node instance type that is used to collect data from the Spark workers.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>For example, the driver node type for AWS can be i3.2xlarge. The driver node type for Azure can be Standard_DS3_v2.</p> <p>If you don't specify the driver node type, Databricks uses the value you specify in the worker node type field.</p>

Property	Description
Instance Pool ID <sup>1</sup>	<p>The instance pool ID used for the Spark cluster.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>If you specify the Instance Pool ID to run mappings, the following connection properties are ignored:</p> <ul style="list-style-type: none"> <li>- Driver Node Type</li> <li>- EBS Volume Count</li> <li>- EBS Volume Type</li> <li>- EBS Volume Size</li> <li>- Enable Elastic Disk</li> <li>- Worker Node Type</li> <li>- Zone ID</li> </ul>
Elastic Disk <sup>1</sup>	<p>Enables the cluster to get additional disk space.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>Enable this option if the Spark workers are running low on disk space.</p>
Spark Configuration <sup>1</sup>	<p>The Spark configuration to use in the job cluster.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>The configuration must be in the following format:</p> <pre>"key1"="value1";"key2"="value2";...</pre> <p>For example, "spark.executor.userClassPathFirst"="False"</p> <p>Doesn't apply to Data Ingestion and Replication tasks.</p>
Spark Environment Variables <sup>1</sup>	<p>The environment variables to export before launching the Spark driver and workers.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>The variables must be in the following format:</p> <pre>"key1"="value1";"key2"="value2";...</pre> <p>For example, "MY_ENVIRONMENT_VARIABLE"="true"</p> <p>Doesn't apply to Data Ingestion and Replication tasks.</p>
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## AWS staging environment

The following table describes the properties for the AWS staging environment:

Property	Description
S3 Authentication Mode	<p>The authentication mode to connect to Amazon S3.</p> <p>Select one of the following authentication modes:</p> <ul style="list-style-type: none"> <li>- Permanent IAM credentials. Uses the S3 access key and S3 secret key to connect to Amazon S3.</li> <li>- IAM Assume Role<sup>1</sup>. Uses the AssumeRole for IAM authentication to connect to Amazon S3. This authentication mode applies only to SQL warehouse.</li> </ul>
S3 Access Key	The key to access the Amazon S3 bucket.
S3 Secret Key	The secret key to access the Amazon S3 bucket.
S3 Data Bucket	The existing S3 bucket to store the Databricks data.

Property	Description
S3 Staging Bucket	The existing bucket to store the staging files.
S3 VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for Amazon S3. You can use a VPC endpoint to enable private communication with Amazon S3. Select one of the following options: <ul style="list-style-type: none"> <li>- None. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint which uses a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.</li> </ul>
Endpoint DNS Name for S3 <sup>1</sup>	The DNS name for the Amazon S3 interface endpoint. Replace the asterisk symbol with the bucket keyword in the DNS name. Enter the DNS name in the following format: <code>bucket.&lt;DNS name of the interface endpoint&gt;</code> For example, <code>bucket.vpce-s3.us-west-2.vpce.amazonaws.com</code>
IAM Role ARN <sup>1</sup>	The Amazon Resource Number (ARN) of the IAM role assumed by the user to use the dynamically generated temporary security credentials. Set the value of this property if you want to use the temporary security credentials to access the Amazon S3 staging bucket. For more information about how to get the ARN of the IAM role, see the <i>AWS documentation</i> .
Use EC2 Role to Assume Role <sup>1</sup>	Optional. Select the check box to enable the EC2 role to assume another IAM role specified in the IAM Role ARN option. The EC2 role must have a policy attached with a permission to assume an IAM role from the same or different AWS account.
STS VPC Endpoint Type <sup>1</sup>	The type of Amazon Virtual Private Cloud endpoint for AWS Security Token Service. You can use a VPC endpoint to enable private communication with Amazon Security Token Service. Select one of the following options: <ul style="list-style-type: none"> <li>- None. Select if you do not want to use a VPC endpoint.</li> <li>- Interface Endpoint. Select to establish private communication with Amazon Security Token Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.</li> </ul>
Endpoint DNS Name for AWS STS <sup>1</sup>	The DNS name for the AWS STS interface endpoint. For example, <code>vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</code>
S3 Service Regional Endpoint	The S3 regional endpoint when the S3 data bucket and the S3 staging bucket need to be accessed through a region-specific S3 regional endpoint. This property is optional for SQL warehouse. Doesn't apply to all-purpose cluster and job cluster. Default is <code>s3.amazonaws.com</code> .
S3 Region Name <sup>1</sup>	The AWS cluster region in which the bucket you want to access resides. Select a cluster region if you choose to provide a custom JDBC URL that does not contain a cluster region name in the JDBC URL connection property.

Property	Description
Zone ID <sup>1</sup>	<p>The zone ID for the Databricks job cluster.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p>Specify the Zone ID only if you want to create a Databricks job cluster in a particular zone at runtime.</p> <p>For example, us-west-2a.</p> <p><b>Note:</b> The zone must be in the same region where your Databricks account resides.</p>
EBS Volume Type <sup>1</sup>	<p>The type of EBS volumes launched with the cluster.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p>
EBS Volume Count <sup>1</sup>	<p>The number of EBS volumes launched for each instance. You can choose up to 10 volumes.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p> <p><b>Note:</b> In a Databricks connection, specify at least one EBS volume for node types with no instance store. Otherwise, cluster creation fails.</p>
EBS Volume Size <sup>1</sup>	<p>The size of a single EBS volume in GiB launched for an instance.</p> <p>This property is optional for job cluster. Doesn't apply to SQL warehouse and all-purpose cluster.</p>
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## Azure staging environment

The following table describes the properties for the Azure staging environment:

Property	Description
ADLS Storage Account Name	The name of the Microsoft Azure Data Lake Storage account.
ADLS Client ID	The ID of your application to complete the OAuth Authentication in the Active Directory.
ADLS Client Secret	The client secret key to complete the OAuth Authentication in the Active Directory.
ADLS Tenant ID	The ID of the Microsoft Azure Data Lake Storage directory that you use to write data.
ADLS Endpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and client secret is completed.
ADLS Filesystem Name	The name of an existing file system to store the Databricks data.
ADLS Staging Filesystem Name	The name of an existing file system to store the staging data.

## JDBC URL parameters

You can utilize the additional JDBC URL parameters field in the Databricks connection to customize and set any additional parameters required to connect to Databricks.

You can configure the following properties as additional JDBC URL parameters in the Databricks connection:

- To connect to Databricks using the proxy server, enter the following parameters:

```
jdbc: spark://<Databricks Host>:443/  
default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/warehouses/  
219fe3013963cdce;UseProxy=<Proxy=true>;ProxyHost=<proxy host IPaddress>;ProxyPort=<proxy  
server port number>;ProxyAuth=<Auth_true>;
```

**Note:** Data Ingestion and Replication does not support use of a proxy server to connect to Databricks.

- To connect to SSL-enabled Databricks, specify the value in the JDBC URL in the following format:

```
jdbc:spark://<Databricks Host>:443/  
default;transportMode=http;ssl=1;AuthMech=3;httpPath=/sql/1.0/endpoints/<SQL endpoint  
cluster ID>;
```

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server to connect to Informatica Intelligent Cloud Services.

To configure the proxy settings for the Secure Agent, perform the following tasks:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

You can configure proxy settings only when you use the AWS staging environment. You cannot use a proxy server when you use a serverless runtime environment.

Data Ingestion and Replication does not support proxy server settings.

**Note:** If you enable both HTTP and SOCKS proxies, SOCKS proxy is used by default. If you want to use HTTP proxy instead of SOCKS proxy, set the value of the `DisableSocksProxy` property to true in the System property.

## Private links to access Databricks

You can access Databricks using Azure Private Link endpoints.

To connect to the Databricks account over the private Azure network, see [Secure connectivity to Azure Data Services](#).

Data Ingestion and Replication does not support using Azure Private Link for access to Databricks.

# Rules and guidelines for personal staging location

When you select the personal staging location as a staging environment, the data is first staged in a java temporary location and then copied to a personal staging location of the unity catalog. Both the staged files will be deleted after the task runs successfully.

However, to stage the data in a different directory, configure the DTM property `-Djava.io.tmpdir=/my/dir/path` in the JVM options in the system configuration settings of the Administrator service.

To enable data staging in a different directory, you should have read and write permission and enough disk space to stage the data in the directory.

When you specify a personal staging location in the Databricks connection properties for staging, consider the following rules and guidelines:

- You can only specify unity enabled catalog in the SQL warehouse JDBC URL.
- You cannot use personal staging location as the staging environment with OAuth machine-to-machine authentication.
- All mappings that are configured run without SQL ELT optimization.
- The data is staged in the folder `stage://tmp/<user_name>` where the `<user_name>` is picked from the Databricks token provided in the connection and requires read and write access to the personal staging location in root location of AWS and Azure.

**Important:** Effective in the October 2024 release, personal staging location entered deprecation. While you can use the functionality in the current release, Informatica intends to drop support for the functionality in a future release. Informatica recommends that you use a Volume to stage the data.

## CHAPTER 48

# Datacom CDC Connection Properties

When you configure a Datacom CDC connection, you must set the connection properties.

The following table describes Datacom CDC connection properties:

Property	Description
Connection Name	A name for the Datacom CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Datacom CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Datacom CDC, the type must be <b>Datacom CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Datacom change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ADACDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Datacom instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Datacom source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.



Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None.</b> Do not use encryption.</li> <li>- <b>AES 128-bit.</b> Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit.</b> Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit.</b> Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: ADACDC01:25100 <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Datacom table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="509 590 964 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="509 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 49

# Datacom Connection Properties

When you configure a Datacom connection, you must set the connection properties.

The following table describes Datacom connection properties:

Property	Description
Connection Name	A name for the Datacom connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Datacom connection. Maximum length is 4000 characters.
Type	Type of connection. For Datacom, the type must be <b>Datacom</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Datacom runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name: port_number</i>  For example:  LSNR1:1467?
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.

Property	Description
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>
Write Mode	<p>Write Mode. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

## CHAPTER 50

# Db2 Data Map connection properties

When you configure a Db2 Data Map connection, you must set the connection properties.

The following table describes the Db2 Data Map connection properties:

Property	Description
Connection Name	A name for the Db2 Data Map connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Optional description for the Db2 Data Map connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 data maps, the type must be <b>Db2 Data Map</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 Data Map runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.

Property	Description
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the filtering of data and bulk data processing to the target.</li> <li>- <b>Filter Before.</b> Filters data on the source system and offloads bulk data processing to the target.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the Secure Agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>The size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds after the initial connection attempt fails that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener. If a connection cannot be established within the retry period, the mapping task fails. The default value is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 51

# Db2 for i CDC connection properties

When you configure a Db2 for i CDC connection, you must set the connection properties.

The following table describes Db2 for i CDC connection properties:

Property	Description
Connection Name	A name for the Db2 for i CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for i CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for i CDC, the type must be <b>Db2 for i CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  DB2CDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Db2 for i instance name that is specified in the <b>Instance</b> field for the registration group that contains the capture registrations for the Db2 source tables. This instance name is also specified in the INST parameter in the AS4J CAPI_CONNECTION statement in the DBMOVER member. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> . Default is Rows.
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: DB2CDC01:25100 <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 for i table on the CDC source system.



Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 959 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1403 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 52

# Db2 for i connection properties

When you configure a Db2 for i connection, you must set the connection properties.

The following table describes Db2 for i connection properties:

Property	Description
Connection Name	A name for the Db2 for i connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for i connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for i, the type must be <b>Db2 for i</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for i runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  DB2ILSNR:14675
Database Name	The Db2 for i subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the Db2 for i source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.

Property	Description
Isolation Level	The Db2 for i isolation level to use for the source database. Options are: <ul style="list-style-type: none"> <li>- ALL</li> <li>- CS</li> <li>- CHG</li> <li>- None</li> <li>- RR</li> </ul> Default is CS
Database File Overrides:	A value to override the database file default. This value overrides the value in the DB_FILE statement in the PowerExchange DBMOVER configuration file.
Library List:	The name of the Db2 for i Library List to use for the connection.
Environment SQL	SQL commands that run in the database environment.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 for i connections in PowerCenter.
Write Properties	Write Mode. Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> <li>- <b>Asynchronous with Fault Tolerance.</b> Combines the speed of <b>Confirm Write Off</b> with the error detection of <b>Confirm Write On</b>. This mode buffers the data and sends it asynchronously to the PowerExchange Listener. When an SQL error occurs, PowerExchange creates a reject file on the target machine, which contains the data records that the writer could not write to the target. View the file contents to identify and correct the errors without reloading the entire table. You can also specify how to handle specific SQL return codes.</li> </ul> Default is <b>Confirm Write On</b> .
Reject File	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the Write Mode is Asynchronous with Fault Tolerance. <b>Note:</b> Enter PWXDISABLE to prevent creation of the reject files.

## CHAPTER 53

# Db2 for i Database Ingestion connection properties

When you define a Db2 for i Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion and replication tasks, which you configure in the Data Ingestion and Replication service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is <b>Db2 for i Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for i instance.
Password	The password to use for connecting to the Db2 for i instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Location Name	The name of the Db2 for i location that you want to access. Your system administrator can determine the name of the Db2 location by using the WRKRDBDIRE command. In the output, find the name of the database that is listed as *LOCAL and then use that value as the value of this property.
JDBC Driver	The type of JDBC driver. Select one of the following options: - Data Direct - JTOpen Default is Data Direct.

Property	Description
Code Page for Bit Data	The code page that Database Ingestion and Replication uses to read character data that is stored as bit data. This value must be a canonical name for the java.io API and java.lang API. For more information, see the supported encodings in the Oracle Java documentation. Specify this property if you have FOR BIT DATA source columns.
Advanced Connection Properties	<p>Advanced properties for the JDBC driver which is used to connect to the Db2 for i source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;).</p> <p>For information about the DataDirect JDBC driver connection properties, see <a href="#">Progress DataDirect documentation</a>. For example, you can set the ConnectionRetryCount property to control the number of times the driver retries attempts to connect to the primary database server.</p> <p>For information about the JTOpen JDBC driver connection properties, see <a href="#">IBM Toolbox for Java JDBC properties</a>.</p>
Encryption Method	<p>The data encryption method for the JTOpen JDBC Driver.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Encryption</li> <li>- SSL</li> </ul> <p>Default is No Encryption.</p> <p>If you select SSL, you must add the required certificates to the Informatica Cloud Secure Agent JRE cacerts keystore in one of the following locations:</p> <p>For Linux:</p> <pre>Secure Agent Directory\jdk\jre\lib\security\cacerts</pre> <p>For Windows:</p> <pre>Secure Agent Directory\apps\jdkLatestVersion\jre</pre>

## CHAPTER 54

# Db2 for LUW CDC connection properties

When you configure a Db2 for LUW CDC connection, you must set the connection properties.

The following table describes Db2 for LUW CDC connection properties:

Property	Description
Connection Name	<p>A name for the Db2 for LUW CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name.</p> <p>Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	<p>Description of the Db2 for LUW CDC connection. Maximum length is 4000 characters.</p>
Type	<p>Type of connection. For Db2 for LUW CDC, the type must be <b>Db2 for LUW CDC</b>.</p>
Runtime Environment	<p>Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.</p>
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for LUW run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <p><i>host_name:port_number</i></p> <p>For example:</p> <p>DB2RHL1:1467</p>
User Name	<p>A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i>.</p>
Password	<p>Password that is associated with the user name that is specified in the <b>User Name</b> property.</p>

Property	Description
Collection Name	Db2 instance name that is specified in the <b>Database</b> field of the registration group that contains capture registrations for the Db2 source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None.</b> Do not use encryption.</li> <li>- <b>AES 128-bit.</b> Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit.</b> Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit.</b> Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Enter the host name or IP address of the system that contains the extraction maps. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: DB2UNIX2B:25100  The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.

Property	Description
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>



## CHAPTER 55

# Db2 for LUW Database Ingestion connection properties

When you define a Db2 for LUW Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion and replication tasks, which you configure in the Data Ingestion and Replication service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is <b>Db2 for LUW Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for LUW instance.
Password	The password to use for connecting to the Db2 for LUW instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Database Name	The name of the Db2 for LUW database that you want to access.
Advanced Connection Properties	Advanced properties for the Progress DataDirect JDBC DB2 driver, which is used to connect to the Db2 for LUW source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;).  The driver properties that you can enter in this field are described in the Progress DataDirect for JDBC <a href="#">connection properties</a> . For example, you can set the EncryptionMethod property to control whether data is encrypted and decrypted when transmitted over the network between the driver and database server.

## CHAPTER 56

# Db2 for z/OS Bulk Load connection properties

When you configure a Db2 for z/OS Bulk Load connection, you must set the connection properties.

The following table describes Db2 for z/OS Bulk Load connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Bulk Load connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Bulk Load connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Bulk Load, the type must be <b>Db2 for z/OS Bulk Load</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Bulk Load runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467?
Database Name	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.

Property	Description
Environment SQL	SQL commands that run in the database environment.
Correlation ID	A value to use as the Db2 Correlation ID for Db2 requests. This value overrides the value in the SESSID statement in the PowerExchange DBMOVER configuration file.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Write Mode	Options are: <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 57

# Db2 for z/OS CDC connection properties

When you configure a Db2 for z/OS CDC connection, you must set the connection properties.

The following table describes Db2 for z/OS CDC connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS CDC, the type must be <b>Db2 for zOS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for Db2 change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  DB2CDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The Db2 for z/OS subsystem ID or data-sharing group name that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the Db2 source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None.</b> Do not use encryption.</li> <li>- <b>AES 128-bit.</b> Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit.</b> Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit.</b> Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: DB2CDC01:25100 <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a Db2 for z/OS table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 963 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 58

# Db2 for z/OS connection properties

When you configure a Db2 for z/OS connection, you must set the connection properties.

The following table describes Db2 for z/OS connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS, the type must be <b>Db2 for z/OS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467?
DB2 Subsystem ID	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.

Property	Description
Environment SQL	SQL commands that run in the database environment.
Correlation ID	A value to use as the Db2 Correlation ID for Db2 requests. This value overrides the value in the SESSID statement in the PowerExchange DBMOVER configuration file.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before.</b> Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> Default is No.
Offload Threads	The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning. Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) Db2 for z/OS connections in PowerCenter.
Asynchronous With Fault Tolerance	Combines the speed of <b>Confirm Write Off</b> with the error detection of <b>Confirm Write On</b> . This mode buffers the data and sends it asynchronously to the PowerExchange Listener. When an SQL error occurs, PowerExchange creates a reject file on the target machine, which contains the rows that the writer could not write to the target. View the file contents to identify and correct the errors without reloading the entire table. You can also specify how to handle specific SQL return codes. To stop session execution when the session encounters non-fatal errors, specify a value greater than 0 in the <b>Stop on errors</b> session attribute on the <b>Config Object</b> tab of the Edit Tasks dialog box. Default is <b>Confirm Write On</b> .



Property	Description
Write Properties	<p>Write Mode. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>
Reject File	<p>Overrides the default prefix of PWXR for the reject file.</p> <p>PowerExchange creates the reject file on the target machine when the Write Mode is Asynchronous with Fault Tolerance.</p> <p><b>Note:</b> Enter PWXDISABLE to prevent creation of the reject files.</p>

## CHAPTER 59

# Db2 for zOS Database Ingestion connection properties

When you define a Db2 for zOS Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion and replication tasks, which you configure in the Data Ingestion and Replication service.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is <b>Db2 for zOS Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.
User Name	The user name to use for connecting to the Db2 for z/OS instance.
Password	The password to use for connecting to the Db2 for z/OS instance.
Host	The name of the machine that hosts the database server.
Port	The network port number used to connect to the database server.
Location Name	The name of the Db2 for z/OS location that you want to access. For Db2 for z/OS, your system administrator can determine the name of your Db2 location using the command DISPLAY DDF.
Code Page for Bit Data	The code page that Database Ingestion and Replication uses to read character data that is stored as bit data. This value must be a canonical name for the java.io API and java.lang API. For more information, see the supported encodings in the Oracle Java documentation. Specify this property if you have FOR BIT DATA source columns.
CDC Stored Procedure Schema	For incremental change data capture processing, the name of the schema for the z/OS stored procedure that is required to collect change data from the Db2 log. This value is specified in the #STPINST data set that you customized when setting up the stored procedure on z/OS. No default value is provided.

Property	Description
CDC Stored Procedure Name	For incremental change data capture processing, the name of the z/OS stored procedure that is required to collect change data from the Db2 log. This value is specified in the #STPINST data set that you customized when setting up the stored procedure on z/OS. The default value is INFALOG.
Advanced Connection Properties	<p>Advanced properties for the Progress DataDirect JDBC Db2 driver, which is used to connect to the Db2 for z/OS source. If you specify more than one <i>property=value</i> entry, separate them with a semicolon (;).</p> <p>The driver properties that you can enter in this field are described in the Progress DataDirect documentation at <a href="https://docs.progress.com/bundle/datadirect-connect-jdbc-51/page/Connection-Properties_10.html">https://docs.progress.com/bundle/datadirect-connect-jdbc-51/page/Connection-Properties_10.html</a>. For example, you can set the ConnectionRetryCount property to control the number of times the driver retries attempts to connect to the primary database server.</p>

## CHAPTER 60

# Db2 for z/OS Image Copy connection properties

When you configure a Db2 for z/OS Image Copy connection, you must set the connection properties.

The following table describes Db2 for z/OS Image Copy connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Image Copy connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Image Copy connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Image Copy, the type must be <b>Db2 for z/OS Image Copy</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Image Copy runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467?
DB2 Subsystem ID	The Db2 subsystem or database name.
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	Schema used for the source or target.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.

Property	Description
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before.</b> Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the Integration Service machine. Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading. If you use reader or writer pipeline partitioning, accept the default value of 0. You cannot use both multiple offload threads and partitioning.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	Valid values are from 1 through 5000. Default is 25.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Connection Retry Period	Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre data-bbox="505 1234 959 1262">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 61

# Db2 for z/OS Unload File connection properties

When you configure a Db2 for z/OS Unload File connection, you must set the connection properties.

The following table describes the Db2 for z/OS Unload File connection properties:

Property	Description
Connection Name	A name for the Db2 for z/OS Unload File connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Db2 for z/OS Unload File connection. Maximum length is 4000 characters.
Type	Type of connection. For Db2 for z/OS Unload Files, the type must be <b>Db2 for z/OS Unload File</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for Db2 for z/OS Unload File runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.

Property	Description
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before.</b> Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs. Valid values are 1 through 64. Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For VSAM data sets and Db2 for z/OS Unload Files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions. For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size. Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre data-bbox="500 1392 954 1415">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support. <b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

# CHAPTER 62

## DB2 Loader connection properties

Create a DB2 Loader connection to securely write data to DB2.

### Prerequisites

Before you create a DB2 Loader connection to write to DB2, be sure to complete the prerequisites.

#### Install the DB2 Loader JDBC driver and DB2 client

To write data to DB2 databases, you need to install the DB2 Loader JDBC driver and DB2 client on the Secure Agent machine.

- Install the DB2 Loader JDBC driver on the Secure Agent machine.  
To install the driver, perform the following steps:
  1. To get the DB2 Loader JDBC driver, contact Informatica Global Customer Support.
  2. Create the `informatica.db2loader` folder manually in the following directory based on whether the Secure Agent machine is a Windows or a Linux machine:

Secure Agent machine	Directory
Linux	<Secure Agent installation directory>/ext/connectors/thirdparty/informatica.db2loader
Windows	<Secure Agent installation directory>\ext\connectors\thirdparty\informatica.db2loader

3. Copy the DB2 Loader JDBC driver to the `informatica.db2loader` folder.
- Install the DB2 LUW client on the Secure Agent machine.  
To install the DB2 LUW client, perform the following steps:
    1. Download and install the DB2 LUW client and instance from the IBM website.



- Set the following environmental variables based on whether the Secure Agent machine is a Windows or a Linux machine:

Secure Agent machine	Environmental variable
Linux	<ul style="list-style-type: none"> <li>- setenv DB2INSTANCE &lt;DB2 instance directory&gt;</li> <li>- setenv DB2CLP DB20FADE</li> <li>- setenv PATH &lt;DB2 client directory&gt;/bin</li> <li>- setenv LD_LIBRARY_PATH &lt;DB2 client directory&gt;/lib64</li> </ul>
Windows	setenv DB2CLP DB20FADE

After you install the DB2 Loader JDBC driver and set the environmental variables, you need to restart the Secure Agent.

## Connect to DB2 Loader

Let's configure the DB2 Loader connection properties to connect to a DB2 database.

### Before you begin

Before you get started, you'll need to install the DB2 Loader JDBC driver and DB2 client on the Secure Agent machine to establish a DB2 Loader connection.

Check out ["Prerequisites" on page 220](#) to learn more about the configuration prerequisites.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	db2loader

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent.</p>
Host Name	The name of the machine that hosts the DB2 database server.
Database	The name of the DB2 database.
Port	<p>The port number that connects to the DB2 database server.</p> <p>Default is 50000.</p>
Schema	<p>The schema name in the DB2 database server to fetch the metadata.</p> <p>This property doesn't apply when you configure a DB2 Loader connection.</p>
User Name	The user name to connect to the DB2 account.
Password	The password to connect to the DB2 account.
Connection String	The alias name to connect to the DB2 database.

### Advanced settings

The following table describes the advanced connection properties:

Property	Description
Encryption Method	<p>Encrypts data exchanged between the Secure Agent and the database server.</p> <p>Select one of the following encryption methods from the list:</p> <ul style="list-style-type: none"> <li>- No Encryption. Establishes a connection without using SSL. Data is not encrypted.</li> <li>- SSL. Establishes a connection using SSL. Data is encrypted using SSL.</li> </ul> <p>Default is No Encryption.</p>
Validate Server Certificate	<p>Determines whether the Secure Agent validates the certificate that is sent by the database server.</p> <p>This property appears only if you select the encryption method as <b>SSL</b>.</p> <p>Select one of the following options from the list:</p> <ul style="list-style-type: none"> <li>- False. The Secure Agent does not validate the certificate.</li> <li>- True. The Secure Agent validates the certificate.</li> </ul> <p>Default is False.</p>

Property	Description
Truststore	<p>The path and file name of the truststore file that contains the SSL certificate to connect to DB2. This property appears only if you select the encryption method as <b>SSL</b> and validate server certificate as <b>True</b>.</p> <p>Specify both the directory and file name in the following format:  <code>/root/&lt;folder name&gt;/&lt;truststore file name&gt;.p12</code></p>
Truststore Password	<p>The password to access the truststore file that contains the SSL certificate. This property appears only if you select the encryption method as <b>SSL</b> and validate server certificate as <b>True</b>.</p>
Host name in Certificate	<p>The name of the machine that hosts the secure database. This property appears only if you select the encryption method as <b>SSL</b> and validate server certificate as <b>True</b>.</p> <p>The Secure Agent validates the host name specified in this property with the host name in the SSL certificate.</p>
Authentication Method	<p>The authentication method that the driver uses to establish a connection. Select one of the following authentication methods from the list:</p> <ul style="list-style-type: none"> <li>- Clear Text. Sends the user ID and password in clear text to the DB2 server for authentication.</li> <li>- Encrypted Password. Sends the user ID in clear text and encrypted password to the DB2 server for authentication.</li> </ul> <p>Default is Clear Text.</p>
Is Staged	<p>Method to load data. Select <b>Is Staged</b> to load data to a flat file staging area before loading to the database. Default is disabled.</p>
Recoverable	<p>Sets the DB2 tablespace in backup pending state. Before you enable the <b>Recoverable</b> option and run a mapping, you need to fully back up the database to perform any other operation on the tablespace. Default is enabled.</p>
DB2 Server Location	<p>The DB2 database server location. Select one of the following locations from the list:</p> <ul style="list-style-type: none"> <li>- Remote. The DB2 database server resides on another machine.</li> <li>- Local. The DB2 database server resides on the Secure Agent machine.</li> </ul> <p>Default is Remote.</p>
External Loader Executable	<p>The DB2 external loader executable file name. The Secure Agent uses the DB2 external loader executable file of the IBM data server client 9.5 version and later. Default is db2load.</p>

Property	Description
Operation Mode	<p>The operation for DB2 external loader to perform.</p> <p>Select one of the following operation modes to determine how the DB2 external loader writes data to the target table based on the mode that you selected in the DB2 external loader:</p> <ul style="list-style-type: none"> <li>- Insert. Loads data to the table.</li> <li>- Replace. Deletes existing data from the table, and then adds data to the table.</li> <li>- Restart. Restarts a previously interrupted load operation.</li> <li>- Terminate. Terminates a previously interrupted load operation and rolls back the operation to the starting point, even if consistency points are passed.</li> </ul> <p>Default is Insert.</p>
Additional Metadata Connection Properties	<p>Additional metadata connection properties that you want to pass to the driver. If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, &lt;parameter name1&gt;=&lt;value1&gt; ; &lt;parameter name2&gt;=&lt;value2&gt;</p>

## CHAPTER 63

# Db2 Warehouse on Cloud connection properties

When you set up a Db2 Warehouse on Cloud connection, you must configure the connection properties.

The following table describes the Db2 Warehouse on Cloud connection properties:

Connection property	Description
Connection name	The name of the connection.
Description	Description of the Db2 Warehouse on Cloud connection. Maximum length is 255 characters.
Type	Type of connection. Select <b>Db2 Warehouse on Cloud</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
User ID	User ID to log into IBM Db2 Warehouse on Cloud.
Password	Password for the user ID to connect to IBM Db2 Warehouse on Cloud.
Host name	Host name of IBM Db2 Warehouse on Cloud.
Port number	Network port number used to connect to the IBM Db2 Warehouse server.
Database name	Database name of IBM Db2 Warehouse that you want to connect to.
SSL connection	Determines whether the Secure Agent establishes a secure connection with IBM Db2 Warehouse. Select SSL to establish a secure connection to IBM Db2 Warehouse. <b>Note:</b> When you use a serverless runtime environment, you cannot configure a Db2 Warehouse connection to use SSL to securely communicate with the Db2 Warehouse database.
Advanced connection properties	Optional. Additional connection parameters that you want to use. Specify the connection parameters as key-value pairs in the following format, and separate each key-value pair with a semicolon: <param1>=<value>&<param2>=<value>&<param3>=<value>...
Schema	The schema name in IBM Db2 Warehouse on Cloud from where you want to fetch the metadata. <b>Note:</b> The Secure Agent browses all schemas in IBM Db2 Warehouse on Cloud if you do not specify a schema name.

## CHAPTER 64

# Domo connection properties

When you set up a Domo connection, you must configure the connection properties.

The following table describes the Domo connection properties:

Connection property	Description
Connection Name	Name of the Domo connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Domo connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Customer	User name to connect to the Domo account.
Dev Token	Access token to connect to the Domo account.
UpdateMode	You can select one of the following options to update data: <ul style="list-style-type: none"><li>- APPEND</li><li>- REPLACE</li><li>- UPSERT</li></ul>
Upsert Keys	Applicable for UPSERT mode. Enter unique values and separate each value with a comma.

## CHAPTER 65

# Dropbox connection properties

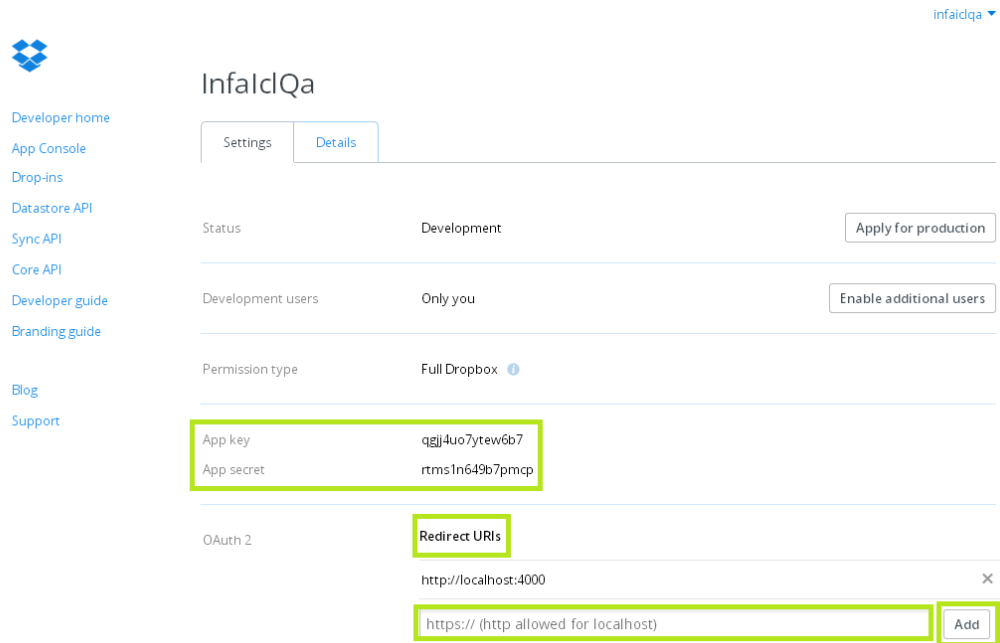
When you set up an Dropbox connection, you must configure the connection properties.

**Important:** Dropbox Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Dropbox connection properties:

Connection property	Description
Connection Name	Name for the connection.
Description	Description for the connection.
Type	Type of connection. Select Dropbox from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
App Key	Dropbox account name. Enter the App Key obtained from the <b>Dropbox App Console</b> .
App Secret	Dropbox account password. Enter the App Secret obtained from the <b>Dropbox App Console</b> .
Agent Hosted on this system	Specify if the system hosts the agent or not.
Authorization code	<ul style="list-style-type: none"><li>- Not applicable, when the system hosts the Secure Agent.</li><li>- When system does not host the Secure Agent, you need to enter the authorization code to get the access token. After specifying the Target folder in connection parameters, test the connection. When you test the connection, an URL link appears in the connection page which specifies the Authorization code.</li></ul>
Access Token	Access token obtained after testing the connection.
Target Folder	Location of target directory to save the files that Dropbox downloads. For example, <code>\\..\..\Dropbox\Target\</code>
Enable Logging	Logs the user, who creates the connection. Select the checkbox to enable logging.

**Note:** While creating a connection, mention the redirect URI `http://localhost:4000` in the Dropbox App settings page.



Developer home  
App Console  
Drop-ins  
Datastore API  
Sync API  
Core API  
Developer guide  
Branding guide  
Blog  
Support

InfalclQa

Settings Details

Status Development Apply for production

Development users Only you Enable additional users

Permission type Full Dropbox ⓘ

App key qgjj4uo7ytew6b7  
App secret rtms1n649b7pmcp

OAuth 2 Redirect URIs

http://localhost:4000 ×

https:// (http allowed for localhost) Add



## CHAPTER 66

# Elasticsearch connection properties

When you create an Elasticsearch connection, you must configure the connection properties.

The following table describes the Elasticsearch connection properties:

Property	Description
Connection Name	The name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Elasticsearch connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Elasticsearch server.
Port	Elasticsearch server port number. Default is 9243.
Authentication	Authentication method to access the Elasticsearch resources. Basic authentication uses user name and password credentials to connect to the Elasticsearch server.
User Name	User name to access the Elasticsearch server.
Password	Password corresponding to the user name to access the Elasticsearch server.

## CHAPTER 67

# Eloqua Bulk API connection properties

Create an Eloqua Bulk API connection to read data from and write data to Eloqua Bulk API. You can use Coupa V2 connections in mappings and mappings tasks. You can use Eloqua Bulk API connections to specify sources and targets in mappings and mappings tasks.

## Connect to Eloqua

Let's configure the Eloqua Bulk API connection properties to connect to Eloqua.

### Before you begin

Before you configure the connection properties, you'll need to get information from your Oracle Eloqua account. You can configure basic and OAuth authentication types to access Oracle Eloqua.

To use basic authentication, you need your Oracle Eloqua base URL, domain name, user name, and password.

To use OAuth authentication, you additionally need the the client ID and client secret for your application.

For more information on how to generate these details, see the [Oracle Eloqua documentation](#).

You can watch the following video to learn where to get the information you need:



## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - ; Maximum length is 255 characters.
Description	
Type	Eloqua Bulk API
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Base URL	The base URL to connect to the Eloqua application. Use one of the following formats to specify the base URL: - https://secure.eloqua.com - https://<host>.eloqua.com/api/bulk/<version number> For the host, you can enter secure, www02.secure, or secure.p03 based on the pod that hosts the Eloqua instance. In the https://<host>.eloqua.com/api/bulk/2.0 URL, 2.0 represents the version number. When you do not mention the version number in the base URL, the Secure Agent considers the default version. For more information about the base URL to connect to the Eloqua application, see <a href="#">Determining Base URL</a> .
Authentication Type	The type of user authentication to connect to the Eloqua application.
Domain Name	The company name of your Eloqua application.
User name	The user name of your Eloqua account.
Password	The password for your Eloqua account.
Client ID	The client ID to complete the OAuth 2.0 authentication to connect to Eloqua. Applies if you select the OAuth 2.0 authentication type.
Client Secret	The client secret key to complete the OAuth 2.0 authentication to connect to Eloqua. Applies if you select the OAuth 2.0 authentication type.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Time Zone Offset	The time zone in the Eloqua application relative to GMT. For more information, see <a href="#">"Understanding the Time Zone Offset" on page 239</a>
Enable Debug Logger	Determines if the debug logger registers the SOAP request and response in the session log. If you enable the debug logger in the connection and run a task, you can view only the response but not the request in the session logs for the read operation. For the write operation, the request appears in the session log, but the response does not appear in the session logs. Default is enabled.
Fetch Data for Preview	Fetches the first 10 rows of the first five columns in an Eloqua Bulk API object for preview. Default is enabled.
Activities or Custom Fields Configuration	The Activities object and custom fields of Contact and Account objects in Eloqua that you want to read from or write. Use the metadata populated in this field to read from or write to the Activities object and custom fields of Contact and Account objects. If you want to include other fields or metadata, ensure that you add them in the JSON format, beginning with an anonymous root structure. For example, {"address" : { "city": "city name", "state": "state name", }} For more information, see <a href="#">"Activities or Custom Fields Configuration" on page 232</a> . For more information about including fields in the custom objects that are not included in the fields API, see the <a href="#">"Adding fields which are not part of fields API to the custom objects" on page 233</a> topic.

## Activities or Custom Fields Configuration

You can read from or write to the Activities object and custom fields of Contact and Account objects.

Add the metadata information in JSON format in the **Activities or Custom Fields Configuration** property under the Eloqua Bulk connection properties. The specification of Activities object and custom fields contains the following sections:

### Activities

Lists all the activities as a name-value pair, where the value is an array of field names. For example,

```
{"EmailAddress", "johns@gmail.com"},  
{"FirstName", "Johns"}
```

### ActivityItem

Defines an array of fields. Each field has the following name-value pairs:

- **name:** Name of the field. The field name must be the same as the field name that you enter in the Activities section.
- **internalName:** Name of the field label. Displays the name and unique name.

- **datatype**: Data type of the field. Default is String data type. The activities or custom fields supports the following data types:
  - Number or Integer
  - Date or Timestamp
  - String
- **maxLength**: Maximum length or precision of the data type field.
- **hasReadOnlyConstraint**: Indicates whether the field is read only.
- **hasNotNullConstraint**: Indicates whether the field is mandatory.
- **hasUniquenessConstraint**: Indicates whether the field is a key.
- **statement**: The statement used in Eloqua REST request.

#### ContactItem

Defines an array of Contact custom fields. Each field has a name-value pair for the ActivityItem section.

#### AccountItem

Defines an array of Account custom fields. Each field has a name-value pair for the ActivityItem section.

## Adding fields which are not part of fields API to the custom objects

Perform the following steps to add the fields that are not part of standard fields in a custom object.

1. Edit the Eloqua Bulk connection.
2. In the **Activities or Custom fields Configuration** connection attribute, add the following JSON element to the JSON template available in the connection attribute:

```
"CustomObjects" :{
  "CO_CustomObject1": ["MappedEntityId","UniqueId"],
  "CO_CustomObject2": ["MappedEntityId","UniqueId"]
}
```

where CO\_CustomObject1 and CO\_CustomObject2 are the names of custom objects and MappedEntityId and UniqueId are the fields.

3. Now add the following field details to the JSON template:

These are the details of the fields that you defined in the CustomObjects element added in the previous step.

```
"CustomItem": [
  {
    "name": "MappedEntityId",
    "internalName": "MappedEntityId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{CustomObject[id].MappedEntityId}}"
  },
  {
    "name": "UniqueId",
    "internalName": "UniqueId",
    "dataType": "integer",
```

```

        "hasReadOnlyConstraint": true,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": true,
        "statement": "{{CustomObject[id].UniqueId}}"
    }
}
]

```

After adding the above details, confirm that the JSON structure is valid.

4. Click **Test Connection**.
5. Click **Save**.

When you use the connection in a new mapping, the fields that you defined in the JSON template appear in the mapping. For an existing mapping from an earlier release, you must refresh the field mapping and map to the target.

6. For an existing mapping, if the above defined fields are required, then refresh the field mapping, and map to the target.

The following example shows a sample Activities or Custom fields configuration:

```

{
  "Activities": {
    "EmailOpen": ["ActivityId", "ActivityType", "ActivityDate", "EmailAddress",
    "ContactId", "IpAddress", "VisitorId", "EmailRecipientId", "AssetType", "AssetName",
    "AssetId", "SubjectLine", "EmailWebLink", "VisitorExternalId", "CampaignId",
    "ExternalId", "DeploymentId", "EmailSendType"],
    "EmailClickthrough": ["ActivityId", "ActivityType", "ActivityDate",
    "EmailAddress", "ContactId", "IpAddress", "VisitorId", "EmailRecipientId",
    "AssetType", "AssetName", "AssetId", "SubjectLine", "EmailWebLink",
    "EmailClickedThruLink", "VisitorExternalId", "CampaignId", "ExternalId",
    "DeploymentId", "EmailSendType"],
    "EmailSend": ["ActivityId", "ActivityType", "ActivityDate", "EmailAddress",
    "ContactId", "EmailRecipientId", "AssetType", "AssetId", "AssetName", "SubjectLine",
    "EmailWebLink", "CampaignId", "ExternalId", "DeploymentId", "EmailSendType"],
    "Subscribe": ["ActivityId", "ActivityType", "AssetId", "ActivityDate",
    "EmailAddress", "EmailRecipientId", "AssetType", "AssetName", "CampaignId",
    "ExternalId"],
    "Unsubscribe": ["ActivityId", "ActivityType", "AssetId", "ActivityDate",
    "EmailAddress", "EmailRecipientId", "AssetType", "AssetName", "CampaignId",
    "ExternalId"],
    "Bounceback": ["ActivityId", "ActivityType", "AssetId", "ActivityDate",
    "EmailAddress", "AssetType", "AssetName", "CampaignId", "ExternalId"],
    "WebVisit": ["ActivityId", "ActivityType", "ActivityDate", "ContactId",
    "VisitorId", "VisitorExternalId", "ReferrerUrl", "IpAddress", "NumberOfPages",
    "FirstPageViewUrl", "Duration", "ExternalId"],
    "PageView": ["ActivityId", "ActivityType", "ActivityDate", "ContactId",
    "CampaignId", "VisitorId", "VisitorExternalId", "WebVisitId", "Url", "ReferrerUrl",
    "IpAddress", "IsWebTrackingOptedIn", "ExternalId"],
    "FormSubmit": ["ActivityId", "ActivityType", "ActivityDate", "ContactId",
    "VisitorId", "VisitorExternalId", "AssetType", "AssetId", "AssetName", "RawData",
    "CampaignId", "ExternalId"]
  },
  "CustomObjects": {
    "CO_CustomObject1": ["MappedEntityId", "UniqueId"],
    "CO_CustomObject2": ["MappedEntityId", "UniqueId"]
  },
  "ActivityItem": [{
    "name": "ActivityId",
    "internalName": "ActivityId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{Activity.Id}}"
  },
  {
    "name": "ActivityType",
    "internalName": "ActivityType",

```

```

        "dataType": "string",
        "maxLength": 100,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Type}}"
    },
    {
        "name": "ActivityDate",
        "internalName": "ActivityDate",
        "dataType": "date",
        "hasReadOnlyConstraint": true,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.CreatedAt}}"
    },
    {
        "name": "EmailAddress",
        "internalName": "EmailAddress",
        "dataType": "emailAddress",
        "maxLength": 400,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailAddress)}}"
    },
    {
        "name": "ContactId",
        "internalName": "ContactId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Contact.Id}}"
    },
    {
        "name": "IpAddress",
        "internalName": "IpAddress",
        "dataType": "string",
        "maxLength": 50,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(IpAddress)}}"
    },
    {
        "name": "VisitorId",
        "internalName": "VisitorId",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Visitor.Id}}"
    },
    {
        "name": "EmailRecipientId",
        "internalName": "EmailRecipientId",
        "dataType": "string",
        "maxLength": 38,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(EmailRecipientId)}}"
    },
    {
        "name": "AssetType",
        "internalName": "AssetType",
        "dataType": "string",
        "maxLength": 100,

```

```

    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Asset.Type}}"
  },
  {
    "name": "AssetName",
    "internalName": "AssetName",
    "dataType": "string",
    "maxLength": 100,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Asset.Name}}"
  },
  {
    "name": "AssetId",
    "internalName": "AssetId",
    "dataType": "integer",
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Asset.Id}}"
  },
  {
    "name": "SubjectLine",
    "internalName": "SubjectLine",
    "dataType": "string",
    "maxLength": 500,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(SubjectLine)}}"
  },
  {
    "name": "EmailWebLink",
    "internalName": "EmailWebLink",
    "dataType": "string",
    "maxLength": 8192,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(EmailWebLink)}}"
  },
  {
    "name": "VisitorExternalId",
    "internalName": "VisitorExternalId",
    "dataType": "string",
    "maxLength": 38,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Visitor.ExternalId}}"
  },
  {
    "name": "CampaignId",
    "internalName": "CampaignId",
    "dataType": "integer",
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Campaign.Id}}"
  },
  {
    "name": "ExternalId",
    "internalName": "ExternalId",
    "dataType": "string",
    "maxLength": 20,
    "hasReadOnlyConstraint": false,

```



```

    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.ExternalId}}"
  },
  {
    "name": "DeploymentId",
    "internalName": "DeploymentId",
    "dataType": "integer",
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(EmailDeploymentId)}}"
  },
  {
    "name": "EmailSendType",
    "internalName": "EmailSendType",
    "dataType": "string",
    "maxLength": 100,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(EmailSendType)}}"
  },
  {
    "name": "EmailClickedThruLink",
    "internalName": "EmailClickedThruLink",
    "dataType": "string",
    "maxLength": 8192,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(EmailClickedThruLink)}}"
  },
  {
    "name": "RawData",
    "internalName": "RawData",
    "dataType": "string",
    "maxLength": 64000,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(RawData)}}"
  },
  {
    "name": "ReferrerUrl",
    "internalName": "ReferrerUrl",
    "dataType": "string",
    "maxLength": 8192,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(ReferrerUrl)}}"
  },
  {
    "name": "WebVisitId",
    "internalName": "WebVisitId",
    "dataType": "integer",
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": false,
    "statement": "{{Activity.Field(WebVisitId)}}"
  },
  {
    "name": "Url",
    "internalName": "Url",
    "dataType": "string",
    "maxLength": 8192,
    "hasReadOnlyConstraint": false,
    "hasNotNullConstraint": false,

```

```

        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(Url)}}"
    },
    {
        "name": "IsWebTrackingOptedIn",
        "internalName": "IsWebTrackingOptedIn",
        "dataType": "boolean",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(IsWebTrackingOptedIn)}}"
    },
    {
        "name": "NumberOfPages",
        "internalName": "NumberOfPages",
        "dataType": "integer",
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(NumberOfPages)}}"
    },
    {
        "name": "FirstPageViewUrl",
        "internalName": "FirstPageViewUrl",
        "dataType": "string",
        "maxLength": 8192,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(FirstPageViewUrl)}}"
    },
    {
        "name": "Duration",
        "internalName": "Duration",
        "dataType": "string",
        "maxLength": 100,
        "hasReadOnlyConstraint": false,
        "hasNotNullConstraint": false,
        "hasUniquenessConstraint": false,
        "statement": "{{Activity.Field(Duration)}}"
    }
},
"ContactItem": [{
    "name": "ContactId",
    "internalName": "ContactId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{Contact.Id}}"
}],
"AccountItem": [],
"CustomItem": [{
    "name": "MappedEntityId",
    "internalName": "MappedEntityId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{CustomObject[id].MappedEntityId}}"
},
{
    "name": "UniqueId",
    "internalName": "UniqueId",
    "dataType": "integer",
    "hasReadOnlyConstraint": true,
    "hasNotNullConstraint": false,
    "hasUniquenessConstraint": true,
    "statement": "{{CustomObject[id].UniqueId}}"
}

```

```
}  
  ]  
}
```

## Understanding the Time Zone Offset

The time zone configured in the Eloqua Bulk API connection must synchronize with the time zone of your Eloqua application.

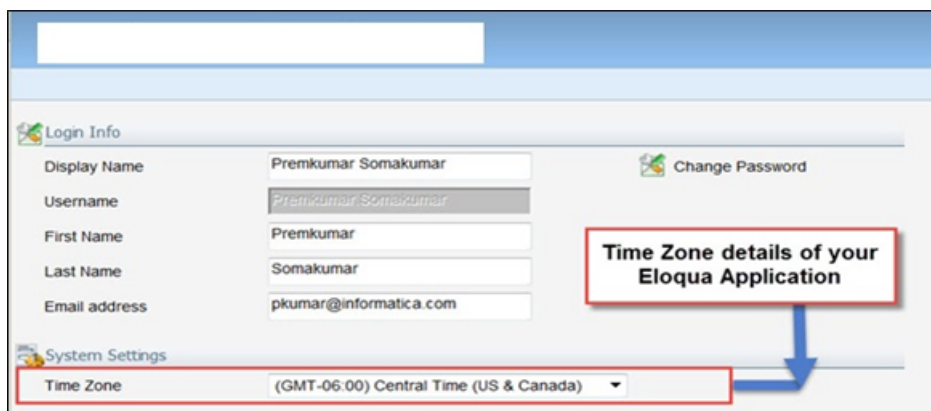
Perform the following tasks to configure the time zone of your Eloqua application:

1. Log in to Eloqua application account.
2. Click **Setup**.
3. Select **My Settings**.

The My Settings page appears.

4. Click **Edit Agent Settings**, and enter the applicable time zone.

The following image shows an example of the time zone set in Eloqua:



For example, if the time zone of the Eloqua application is GMT+06:00, you need to enter +06:00 in this field.

When daylight saving time is in effect, make adjustments to the time. For example, if the time zone is GMT-06:00, enter -06:00 into this field.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 68

# Eloqua REST connection properties

When you create an Eloqua REST connection, you must configure the connection properties.

The following table describes the Eloqua REST connection properties:

Property	Description
Runtime Environment	Runtime environment that contains Secure Agent used to access Eloqua.
Base Url	Endpoint URL of the Eloqua application server. Do not specify the query parameters with the Base URL. For example, <a href="https://rest.apisandbox.eloqua.com">https://rest.apisandbox.eloqua.com</a>
Username	User name of the Eloqua application.
Domain	Domain of the Eloqua application.
Password	Password for the Eloqua application.
Client ID	The client ID created in the Eloqua application. You must enter the client ID if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Client Secret	The client secret key created in the Eloqua application. You must enter the client secret key if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Authentication Type	The type of user authentication to connect to the Eloqua application. Select the authentication type that Eloqua REST Connector must use to login to the Eloqua application. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Auth</li><li>- OAuth 2.0</li></ul> Default is OAuth 2.0.
Enable Debug Logger	Displays the message in the session logs to debug the mapping. Default is false.
Eloqua Swagger	The swagger file that you want to use for the Eloqua REST connection. Select <b>Eloqua Swagger API V1_2017_09_06</b> .

## CHAPTER 69

# FHIR connection properties

Create a FHIR connection to read from and write to a FHIR (Fast Healthcare Interoperability Resources) server.

## Connect to FHIR

Let's configure the FHIR connection properties to connect to a FHIR server.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	FHIR
Runtime Environment	Name of the runtime environment where you want to run tasks. Select a Secure Agent.
Host	Host name or IP address of the FHIR server, including the port number. Enter the value in the following format, where host_name can be a host name or IP address: <code>host_name:port_number</code>
HTTP Method	HTTP method used to send requests. Select one of the following HTTP methods: - HTTP - HTTPS Default is HTTP.

Property	Description
Connection Timeout	Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection doesn't occur in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 30 seconds.
Keep Alive	Indicates whether to keep the connection open for multiple HTTP requests or responses. Default is true.
Follow Redirects	Indicates whether to follow redirect links when creating a connection. Default is true.
Connection Retry Attempts	Number of times to retry connecting to the FHIR server if a successful connection doesn't occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections. Default is 0.
Connection Retry Interval	Number of seconds to wait between each connection retry attempt. For example, to retry to connect up to 10 times with a five-second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5. Default is 0.
Base Path	Base path for the FHIR server. The initial URL segment of the API.
Test Connection Resource Path	Resource path to append to the base path to test the connection.
Content Type	Media type of the request. Select one of the following options: <ul style="list-style-type: none"> <li>- application/fhir+xml</li> <li>- application/fhir+json</li> <li>- application/xml</li> <li>- application/json</li> </ul>
Accept	Media type of the response. Select one of the following options: <ul style="list-style-type: none"> <li>- application/fhir+xml</li> <li>- application/fhir+json</li> <li>- application/xml</li> <li>- application/json</li> </ul>
Additional Headers	Additional headers that the connection requires. Define headers in JSON format. For example: <pre>[{"Name": "Content-Type", "Value": "application/fhir+json"}, {"Name": "accept", "Value": "text/xml"}]</pre>

Property	Description
Authentication Type	<p>Authentication method that the connector must use to connect to the REST endpoint.</p> <p>You can use one of the following options:</p> <ul style="list-style-type: none"> <li>- None</li> <li>- Basic. For more information, see <a href="#">"Basic authentication" on page 245</a>.</li> <li>- OAuth 2.0 authorization code. For more information, see <a href="#">"OAuth 2.0 authorization code authentication" on page 245</a>.</li> <li>- OAuth 2.0 client credentials. For more information, see <a href="#">"OAuth 2.0 client credentials authentication" on page 246</a>.</li> </ul> <p>Default is None.</p>
Trust Store File Path	<p>Absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API.</p> <p>Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.</p>
Trust Store Password	<p>Password for the truststore file that contains the SSL certificate.</p>
Key Store File Path	<p>Absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API.</p> <p>Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.</p>
Key Store Password	<p>Password for the keystore file required for secure communication.</p>
Proxy Type	<p>Type of proxy.</p> <p>You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- No Proxy. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Platform Proxy. Considers the proxy configured at the agent level.</li> <li>- Custom Proxy. Considers the proxy configured at the connection level.</li> </ul> <p>Not applicable when you use a serverless runtime environment.</p>
Proxy Config	<p>Host name or IP address of the proxy server, including the port number.</p> <p>Enter the value in the following format, where host_name can be a host name or IP address:</p> <pre>host_name:port_number</pre>

## Authentication types

You can configure basic, OAuth 2.0 authorization code, and OAuth 2.0 client credentials authentication to access the FHIR server.

Select the required authentication method and then configure the authentication-specific parameters.



## Basic authentication

Basic authentication requires the user name and password from the FHIR server.

The following table describes the connection properties for basic authentication:

Property	Description
Auth User ID	User name to log in to the web service application.
Auth Password	Password associated with the user name.

## OAuth 2.0 authorization code authentication

Configure authentication properties in the FHIR connection to use an OAuth 2.0 authorization code.

To use authorization code authentication, register the following Informatica redirect URL in your application:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires and you receive error code 400, 401, or 403 in the response, the Informatica redirect URL tries to connect to the endpoint and retrieve a new access token. Note that the Informatica redirect URL is usually outside the organization firewall.

The following table describes the authentication properties for a FHIR connection that uses an OAuth 2.0 authorization code:

Property	Description
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	Specifies access control if the API endpoint defines custom scopes. Separate scope attributes using a space. For example: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in JSON format. For example: <code>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</code>
Client Authentication	Select an option to send the client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .

Property	Description
Access Token	<p>Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.</p> <p>To generate the access token through a proxy server, configure an unauthenticated proxy server on the Secure Agent. The FHIR connection-level proxy configuration doesn't apply when generating the access token.</p>
Refresh Token	<p>Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent generates a new access token through the refresh token.</p> <p>If the refresh token expires, you must either enter a valid refresh token or generate a new refresh token by clicking <b>Generate Access Token</b>.</p>

## OAuth 2.0 client credentials authentication

Configure authentication properties in the FHIR connection to use OAuth 2.0 client credentials.

The following table describes the authentication properties for a FHIR connection that uses OAuth 2.0 client credentials:

Property	Description
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	<p>Specifies access control if the API endpoint defines custom scopes. Separate scope attributes using a space.</p> <p>For example: <code>root_readonly root_readwrite manage_app_users</code></p>
Access Token Parameters	<p>Additional parameters to use with the access token URL. Define parameters in JSON format.</p> <p>For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code></p>
Client Authentication	<p>Select an option to send the client ID and client secret for authorization either in the request body or in the request header.</p> <p>Default is <b>Send Client Credentials in Body</b>.</p>
Access Token	<p>Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.</p> <p>To generate the access token through a proxy server, configure an unauthenticated proxy server on the Secure Agent. The FHIR connection-level proxy configuration doesn't apply when generating the access token.</p>

## CHAPTER 70

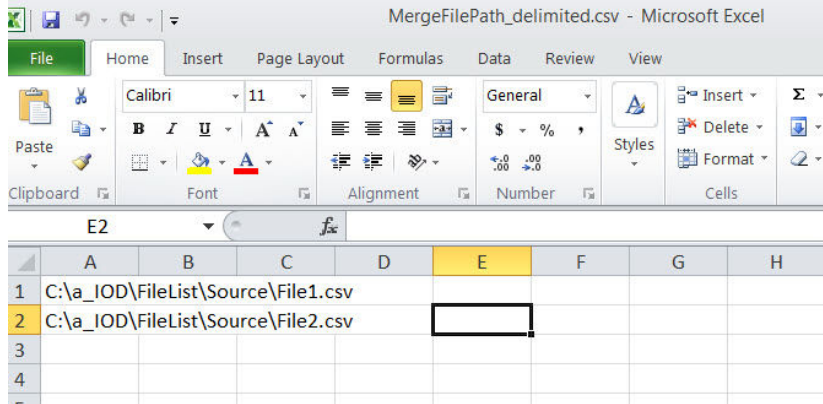
# File List connection properties

When you set up a File List connection, you must configure the connection properties.

**Important:** File List Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Flat File Connector to access flat files.

The following table describes the File List connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a description for the connection.
Type	Select File List from the list.
Secure Agent	Select the Secure Agent from the list.
File Type	Select the file format from the list. The connection supports fixed-width and delimiter file types.
Delimiter	Select the delimiter. The default delimiter is Comma.
Schema File Path	Specify the schema file path. A sample schema file is present in Informatica Secure Agent folder. The path is <Secure Agent installation directory>\apps\ \Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<<plugin ID>
Custom Header File Path	Specify the header file path. You can find header.hdr file in Informatica Secure Agent folder. The path is <Secure Agent installation directory>\apps\ \Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\<<plugin ID>
Skip First N lines	Specify the number of rows you want to skip while merging the files. This helps you to skip the rows from the beginning of the file.
Skip Last N lines	Specify the number of rows you want to skip while merging the files. This helps you to skip the rows from the end of the file.

Connection property	Description
Merge File Path	<p>It is the file which contains details of all the multiple files you need to merge using the File List Connector.</p> <p>Provide the path where this file resides. The following image shows a sample of merge file path where file1 and file 2 are the two files to be merged:</p>  <p>The screenshot shows a Microsoft Excel spreadsheet titled 'MergeFilePath_delimited.csv'. The spreadsheet has columns A through H and rows 1 through 4. Row 1 contains the path 'C:\a_IOD\FileList\Source\File1.csv' in column A. Row 2 contains the path 'C:\a_IOD\FileList\Source\File2.csv' in column A. The cell in column E, row 2 is highlighted with a black border.</p>
Rows Per Batch	Mention the required batch size to optimize the performance. The default value is 100.
Date Format	Mention the Date format. The default date format is dd-MM-yyyy HH:mm:ss.

## CHAPTER 71

# File Processor connection properties

When you set up a File Processor connection, you must configure the connection properties.

The following table describes the File Processor connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Source File Directory	The location that contains files you want to transfer.
Target File Directory	The location where you want to place the transferred files.
Select File	The files that you want to transfer. You can select files based on the fields.
File Pattern	The pattern of the files that you want to transfer. For example, to select a file based on a date pattern, you can specify the date format as DD/MM/YYYY, MM-dd-yyyy, yyyy-MM-dd, or yyyy-MM-d in the file pattern field. Note: The File Pattern field is not applicable when you select <b>all</b> in the <b>Select File</b> connection property.
Days Calculation	Selects files that are created or modified before the specified date or after the specified date. Select files based on Contains Date Pattern and specify the <b>days calculation</b> value so that you can select files that are modified before or after the specified date. Specify the value in terms of days. You cannot specify the value in terms of month and year. You can specify the following date formats: DD/MM/YYYY, MM-dd-yyyy or yyyy-MM-d format. For example, to select a file based on Contains Date Pattern and use the data filters to specify the LastModDate as 02/02/2016, and specify days calculation as -1. Files that are modified till 01/02/2016 are selected.
PassKey	The credentials to connect to FTP or SFTP server. For example, you can specify the password and passphrase of the FTP or SFTP server as passkey1 and passkey2 values.

## CHAPTER 72

# FileIO connection properties

When you set up a FileIO connection, you must configure the connection properties.

The following table describes the FileIO connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select <b>FileIo</b> from the list.
Secure Agent	Select the appropriate secure agent from the list.
Parent Directory	Enter the parent directory path. The parent directory is the folder that contains the files to perform read and write operations. The parent directory must contain an <code>.infaccess</code> empty file. Create a folder within the parent directory with any name other than <code>inprocess</code> , <code>success</code> , and <code>error</code> . For example, you can create a <code>read</code> , <code>write</code> , or <code>test</code> folder. The empty file will be listed as objects when you select this connection as source or target in the task.
Process File Content As	Select the required option from the list of available options to process the file content. The following file processing options are available: <ul style="list-style-type: none"><li>- Binary: When you select Binary, you must map <code>FileContentAsBinary</code> in the <b>Field Mapping</b> tab of the synchronization task.</li><li>- base64 encoded string: By default this option is selected. When you select this option, you must map <code>FileContentAsBase64String</code> in the <b>Field Mapping</b> tab of the synchronization task.</li></ul>
Overwrite Target Files	Check the box to enable overwrite target files. Otherwise the file containing same names will be created in the incrementing naming order using a counter. For example, when you do not enable overwrite target file option, the existing file ABCD will not be overwritten. Instead a new file ABCD(1) will be created.
Auto Archive Source Files	Check the box to enable automatic archiving of source files. This option allows you to move the files from source directory after the file is processed.
In Process Directory	Mention the directory path to be used for file processing. By default, parent directory is considered.
Success Directory	Mention the directory path where the files will be moved after processing. By default, parent directory is considered. Mention the success directory path only when <b>Auto Archive Source Files</b> option is enabled.
Error Directory	Mention the error directory path. When there are issues/errors in file processing. Such files are moved to error directory.

## CHAPTER 73

# Flat file connections

Flat file connections enable you to create, access, and store flat files. You can use flat file connections in mappings and in tasks such as mapping tasks, PowerCenter tasks, replication tasks, and synchronization tasks.

When you configure a flat file connection, you must select the runtime environment to be used with the connection. If you select a runtime environment with Secure Agents that run on Linux, you cannot specify a Windows directory for a flat file target.

A flat file connection cannot use a Secure Agent that runs on NTT. Therefore, do not select a runtime environment with Secure Agents that run on NTT.

In a serverless runtime environment that has data disks configured, you can choose one of the mounted directories or their sub directories to use in the flat file connection.

When you select a flat file connection in a mapping or task, you choose the formatting options for the flat file. When you choose the formatting options in a Source, Lookup, or Target transformation, you specify whether the flat file is a delimited flat file or a fixed-width flat file. If the flat file is a fixed-width flat file, you select a fixed-width format from a list of fixed-width formats that you configured. If you plan to use a fixed-width flat file, you need to create at least one fixed-width format before you select a fixed-width flat file in the Mapping Designer.

## Flat file connection properties

Defines the properties you need to assign to for a flat file source connection.

The following table describes the flat file connection properties:

Connection Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Flat File</b> connection type.

Connection Property	Description
Runtime Environment	<p>Runtime environment that contains the Secure Agent to use for accessing the flat files. Or for Data Integration, a serverless runtime environment that contains the mounted EFS or NFS directories which contain the flat files.</p> <p><b>Note:</b> Do not select a runtime environment with Secure Agents that run on NTT. A flat file connection cannot use a Secure Agent that runs on NTT.</p>
Directory	<p>Directory where the flat file is stored. Must be accessible by all Secure Agents in the selected runtime environment.</p> <p>Enter the full directory or click <b>Browse</b> to locate and select the directory.</p> <p>When you use the connection, you can select a file that's contained in the directory or in any of its subdirectories.</p> <p>This directory is also used in any data disks configured for a serverless runtime environment. Maximum length is 100 characters. Directory names can contain alphanumeric characters, spaces, and the following special characters:</p> <p>/ \ : _ ~</p> <p>The directory is the service URL for this connection type.</p> <p><b>Note:</b> On Windows, the <b>Browse for Directory</b> dialog box doesn't display mapped drives. You can browse My Network Places in Windows Explorer to locate the directory and copy the location from the address bar or enter the directory name in the following format: \&lt;server_name&gt;\&lt;directory_path&gt;. If network directories do not display, you can configure a login for the Secure Agent service. This functionality might not be available on newer versions of Windows.</p> <p>Do not include the name of the flat file. You specify the file name when you create the task.</p> <p>In a serverless runtime environment, this directory must be one of the mounted directories or their subdirectories in the data disk.</p>
Browse button	Use to locate and select the directory where flat files are stored.
Date Format	Date format for date fields in the flat file. Default date format is: MM/dd/yyyy HH:mm:ss



Connection Property	Description
Code Page	<p>The code page of the system that hosts the flat file. Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data</li> <li>- UTF-8. Select for Unicode data</li> <li>- UTF-16 encoding of Unicode (Big Endian)</li> <li>- UTF-16 encoding of Unicode (Lower Endian)</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European)</li> <li>- ISO 8859-2 Eastern European</li> <li>- ISO 8859-3 Southeast European</li> <li>- ISO 8859-5 Cyrillic</li> <li>- ISO 8859-9 Latin 5 (Turkish)</li> <li>- IBM EBCDIC International Latin-1</li> <li>- Japanese EUC (with \ &lt;-&gt; Yen mapping)</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- Chinese EUC</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- EBCDIC Hebrew (updated with new sheqel, control characters)</li> <li>- IBM EBCDIC US English IBM037</li> <li>- UTF-32 encoding of Unicode (Lower Endian)</li> <li>- ISO 8859-1 Western European.</li> <li>- IBM EBCDIC French</li> <li>- ISO 8859-10 Latin 6 (Nordic) *</li> <li>- EBCDIC Finland, Sweden</li> <li>- MOS-DOS Thai, superset of TIS 620</li> <li>- 7-bit ASCII</li> <li>- EBCDIC Finland, Sweden (w/euro update)</li> <li>- MS-DOS Windows Latin 2 (Central Europe)</li> <li>- Japanese EBCDIC-Kana Fujitsu</li> </ul> <p>In advanced mappings, flat file objects in cloud storage connections must use UTF-8 encoding.</p> <p>If the file contains supplementary characters with UTF-16 encoding, the task fails.</p> <p><b>Note:</b> When you use a flat file connection with the Shift-JIS code page and a UTF data object, be sure to install fonts that fully support Unicode.</p>
<p>* Data preview uses a similar ISO 8859-4 Scandinavian/Baltic code page, but runtime processing uses ISO 8859-10 Latin 6 (Nordic), so data preview and runtime encoding won't match.</p>	

## Configuring a locale in Linux for flat file connections

On Linux, for synchronization or replication tasks that use a flat file connection, to support multibyte data you need to set the default locale to UTF-8.

1. To display the current locale, in a shell command line, enter `locale`.

2. To set the default locale to UTF-8, see the following examples:

- For bash and related UNIX shells:

```
export LC_ALL=en_US.UTF-8
```

- For csh and related UNIX shells:

```
setenv LC_ALL en_US.UTF-8
```

3. Restart the Secure Agent.

## CHAPTER 74

# FTP/SFTP connections

File Transfer Protocol (FTP) connections enable you to use FTP to access source and target files. Secure File Transfer Protocol (SFTP) connections use secure protocols, such as SSH, to access source and target files.

When you configure an FTP/SFTP connection, you define the following directories:

### Local directory

Directory local to the Secure Agent that contains a copy of the source or target files.

### Remote directory

Location of the files you want to use as sources or targets.

Informatica Intelligent Cloud Services validates the file in the local directory, not the remote directory. When you configure FTP/SFTP connections, ensure that the local directory contains valid copies of all source and target files. When you configure a task with an FTP/SFTP connection, Informatica Intelligent Cloud Services uses the file structure of the local file to define the source or target for the task. The file structure of the local file must match the source or target file in the remote directory. Informatica Intelligent Cloud Services also uses the local file to generate data preview. If the data in the local file does not match the data in the source or target file in the remote directory, data preview might display inaccurate results.

When Informatica Intelligent Cloud Services runs a data integration task with a FTP/SFTP target connection, it creates a target file based on the target defined in the task. As it completes the task, Informatica Intelligent Cloud Services writes the target file to the remote directory, overwriting the existing file.

## FTP/SFTP connection properties

The following table describes the FTP/SFTP connection properties:

Connection property	Description
Runtime Environment	Runtime environment that contains the Secure Agent to use to access the files.
User Name	User name used to log in to the FTP server.
Password	Password for the user name used to log in to the FTP server.
Host	Host name or IP address of the FTP/SFTP host.

Connection property	Description
Port	Network port number used to connect to FTP/SFTP connection. Default port is 21 for FTP and 22 for SFTP.
Local Directory	Directory on a local machine that stores the local file. The local machine must also run the Secure Agent used to run the corresponding task. Enter a local directory or use the Browse button to select a local directory.
Remote Directory	Directory on the FTP/SFTP host that stores the remote flat file. Depending on the FTP/SFTP server, you might have limited options to enter directories. For more information, see the FTP/SFTP server documentation.
Date Format	Date format for date fields in the flat file. Default date format is: MM/dd/yyyy HH:mm:ss
Code Page	Code page compatible with the system where the source or target flat file resides. Select one of the following code pages: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> <li>- Japanese EUC (with \ &lt;-&gt; Yen mapping</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- Chinese EUC</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- EBCDIC Hebrew (updated with new sheqel, control characters)</li> </ul>
This is a Secure FTP Connection	Indicates whether the connection is secure or not secure. Select to create an SFTP connection.

## Key exchange algorithms and ciphers

You can use the following key exchange algorithms and ciphers for SFTP connections:

### Key exchange algorithms

- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1

## Ciphers

- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc (rijndael-cbc@lysator.liu.se)
- aes192-cbc
- aes128-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- arcfour
- arcfour128
- none

# FTP/SFTP connection rules and guidelines

Consider the following rules and guidelines for FTP/SFTP connections:

- Informatica Intelligent Cloud Services does not lock the target file while writing to the file. To prevent data corruption, verify that only one task writes to a target file at any given time.
- If metadata in the local target file and remote target file are different, Informatica Intelligent Cloud Services overwrites the metadata of the remote target file with the local target file at run time.
- To find the row count of rows loaded into the local target file, open the job details from the **All Jobs** or **My Jobs** page.
- In Windows, you cannot select FTP/SFTP directory on a mapped drive through the **Browse for Directory** dialog box. You can access a network directory by browsing My Network Places. You can also enter the directory with the following format:

```
\\<server_name>\<directory_path>
```

If the **Browse for Directory** dialog box does not display My Network Places, you might need to configure a network login for the Secure Agent service.

- Error messages for FTP/SFTP connections might only reference FTP or SFTP. Read any error message that references FTP or SFTP as an error message for an FTP/SFTP connection.

## CHAPTER 75

# Google Ads connection properties

When you create a Google Ads connection, you must configure the connection properties.

The following table describes the Google Ads connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client ID	Required. The OAuth 2.0 client ID from Google Developer Console.
Client Secret	Required. The OAuth 2.0 client secret from Google Developer Console.
Refresh Token	Required. The OAuth 2.0 refresh token received after you exchange the authorization code for Google Ads.
Developer Token	Required. The developer token from the Google Ads manager account.
Account Customer ID	Required. Unique login customer ID to access the Google Ads account through a manager account.

## CHAPTER 76

# Google Analytics connection properties

Create a Google Analytics connection to read data from a Google Analytics report. You can use Google Analytics connections in mapping tasks and mappings.

## Prerequisites

Before you configure Google Analytics Connector, complete the following prerequisite tasks:

1. Create a Google account to access Google Analytics.
2. On the **Credentials** page, navigate to the APIs and auth section, and Click **Create service account**.
3. In the **Create service account** dialog box, select **Furnish a new private key** and **Enable G Suite Domain-wide Delegation**.

**Note:** You must select **JSON** as the **Key type** and save the generated key as `client_secrets.json`.

4. Click **Create**.
5. After you create the service account, you can download a JSON file that contains the `client_email` and `private_key` values. You will need to enter these details when you add a user in the Google Analytics account and also when you create a Google Analytics connection in Data Integration.

The following image shows the **Credentials** page where you can create the service account and key:

**Create service account**

Service account name <sup>?</sup>  Role <sup>?</sup>

Service account ID

**Furnish a new private key**  
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

**Key type**

JSON  
Recommended

P12  
For backward compatibility with code using the P12 format

**Enable G Suite Domain-wide Delegation**  
Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their part. [Learn more](#)

**CANCEL** **CREATE**

6. Do the following steps to enable the Analytics API:
  - Note:** The Google Analytics Connector uses Google Analytics 4 API to integrate with Google Analytics.
  - a. Go to the following website: <https://console.developers.google.com/>
  - b. On the **Dashboards** page, enable the **Analytics API**.
7. Create an account and property in Google Analytics.
8. Verify that you have the following permissions for the Google Analytics account:
  - Collaborate
  - Edit
  - Manage Users
  - Read and Analyze

## Connect to Google Analytics

Let's configure the Google Analytics connection properties to connect to Google Analytics.

### Before you begin

Before you get started, you need to create the Google service account, enable the Analytics API, and configure the Google Analytics account.

Check out ["Prerequisites" on page 259](#) to learn more about these tasks.



The following video shows you how to get information from your Google service account to configure the Google Analytics connection:



## Connection details

The following table describes the Google Analytics connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Google Analytics
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Service Account Email	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.

## API version

You can configure the default Google Analytics 4 API to read from Google Analytics reports. Select the Google Analytics 4 API and then configure the specific parameters.

The Google Analytics Connector dropped support for the Analytics Reporting API v4 and Core Reporting API v3.

## Google Analytics 4

The following table describes the connection property for Google Analytics 4:

Property	Description
Property ID	The Google Analytics property ID associated with the Google Analytics project. Specify the property ID to read data from the following reports: <ul style="list-style-type: none"><li>- Content Grouping</li><li>- Ecommerce</li><li>- Goal Conversions</li></ul> When you read data from any other report, leave the property blank.

## Core Reporting API v3

The following table describes the connection properties for Core Reporting API v3:

Property	Description
Account ID	Not applicable for Google Analytics Connector.
Property ID	Not applicable for Google Analytics Connector.
View ID	Not applicable for Google Analytics Connector.

## Analytics Reporting API v4

The following table describes the connection properties for Analytics Reporting API v4:

Property	Description
Account ID	Not applicable for Google Analytics Connector.
Property ID	Not applicable for Google Analytics Connector.
View ID	Not applicable for Google Analytics Connector.

## CHAPTER 77

# Google Analytics Mass Ingestion connection properties

When you set up a Google Analytics Mass Ingestion connection, you must configure the connection properties.

The following table describes the connection properties for a Google Analytics Mass Ingestion connection:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -  Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Google Analytics Mass Ingestion</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Service Account ID	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.

## CHAPTER 78

# Google BigQuery connection properties

When you create a Google BigQuery connection, you must configure the connection properties.

**Important:** Effective in the November 2024 release, Google BigQuery Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Google BigQuery V2 Connector to access Google BigQuery.

The following table describes the Google BigQuery connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ ` ! \$ % ^ & * ( ) - + = { }   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The Google BigQuery connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service Account ID	Specifies the client_email value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value present in the JSON file that you download after you create a service account.
Connection mode	The mode that you want to use to read data from or write data to Google BigQuery. Select one of the following connection modes: <ul style="list-style-type: none"><li>- Simple. Flattens each field within the Record data type field as a separate field in the mapping.</li><li>- Hybrid. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the mapping.</li><li>- Complex. Displays all the columns in the Google BigQuery table as a single field of the String data type in the mapping.</li></ul> Default is Simple.

Property	Description
Schema Definition File Path	<p>Specifies a directory on the Secure Agent machine where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. The JSON file name is the same as the Google BigQuery table name.</p> <p>Alternatively, you can specify a storage path in Google Cloud Storage where the Secure Agent must create a JSON file with the sample schema of the Google BigQuery table. You can download the JSON file from the specified storage path in Google Cloud Storage to a local machine.</p> <p>The schema definition file is required if you configure complex connection mode in the following scenarios:</p> <ul style="list-style-type: none"> <li>- You add a Hierarchy Builder transformation in a mapping to read data from relational sources and write data to a Google BigQuery target.</li> <li>- You add a Hierarchy Parser transformation in a mapping to read data from a Google BigQuery source and write data to relational targets.</li> </ul>
Project ID	<p>Specifies the project_id value present in the JSON file that you download after you create a service account.</p> <p>If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.</p>
Dataset ID	<p>Name of the dataset that contains the source table and target table that you want to connect to.</p> <p><b>Note:</b> Google BigQuery supports the datasets that reside only in the US region.</p>
Storage Path	<p>This property applies when you read or write large volumes of data. Required if you read data in staging mode or write data in bulk mode.</p> <p>Path in Google Cloud Storage where the Secure Agent creates a local stage file to store the data temporarily.</p> <p>You can either enter the bucket name or the bucket name and folder name.</p> <p>For example, enter <code>gs://&lt;bucket_name&gt;</code> or <code>gs://&lt;bucket_name&gt;/&lt;folder_name&gt;</code></p>

**Note:** Ensure that you specify valid credentials in the connection properties. The test connection is successful even if you specify incorrect credentials in the connection properties.

## Connection modes

You can configure a Google BigQuery connection to use one of the following connection modes:

### Simple mode

If you use simple mode, Google BigQuery Connector flattens each field within the Record data type field as a separate field in the field mapping.

### Hybrid mode

If you use hybrid mode, Google BigQuery Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the field mapping.

### Complex mode

If you use complex mode, Google BigQuery displays all the columns in the Google BigQuery table as a single field of the String data type in the field mapping.

## Connection mode example

Google BigQuery Connector reads and writes the Google BigQuery data based on the connection mode that you configure for the Google BigQuery connection.

You have a Customers table in Google BigQuery that contains primitive fields and the **Address** field of the Record data type. The Address field contains two primitive sub-fields, **City** and **State**, of the String data type.

The following image shows the schema of the Customers table in Google BigQuery:

<b>ID</b>	INTEGER	NULLABLE
<b>Name</b>	STRING	NULLABLE
<b>Address</b>	RECORD	NULLABLE
<b>Address.City</b>	STRING	NULLABLE
<b>Address.State</b>	STRING	NULLABLE
<b>Mobile</b>	STRING	REPEATED
<b>Totalpayments</b>	FLOAT	NULLABLE
<b>age</b>	INTEGER	REPEATED

The following table shows the Customers table data in Google BigQuery:

<b>ID</b>	<b>Name</b>	<b>Address.City</b>	<b>Address.State</b>	<b>Mobile</b>	<b>Totalpayments</b>
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
				+1-8267389993	
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
				+1-9876553784	
				+1-8456437848	

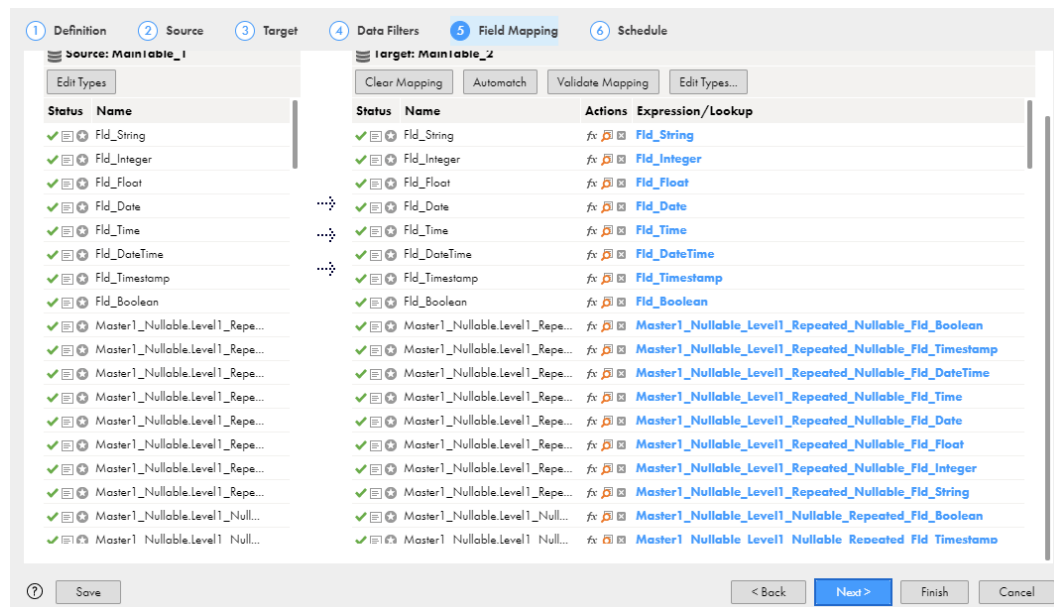
### Simple mode

If you use simple connection mode, Google BigQuery Connector flattens each field within the Record data type field as a separate field in the **Field Mapping** tab.

The following table shows two separate fields, Address\_City and Address\_State, for the respective sub-fields within the Address Record field in the Customers table:

ID	Name	Address_City	Address_State	Mobile	Totalpayments
14	John	LOS ANGELES	CALIFORNIA	+1-9744884744	18433.90
14	John	LOS ANGELES	CALIFORNIA	+1-8267389993	18433.90
29	Jane	BOSTON	MANHATTAN	+1-8789390309	28397.33
29	Jane	BOSTON	MANHATTAN	+1-9876553784	28397.33
29	Jane	BOSTON	MANHATTAN	+1-8456437848	28397.33

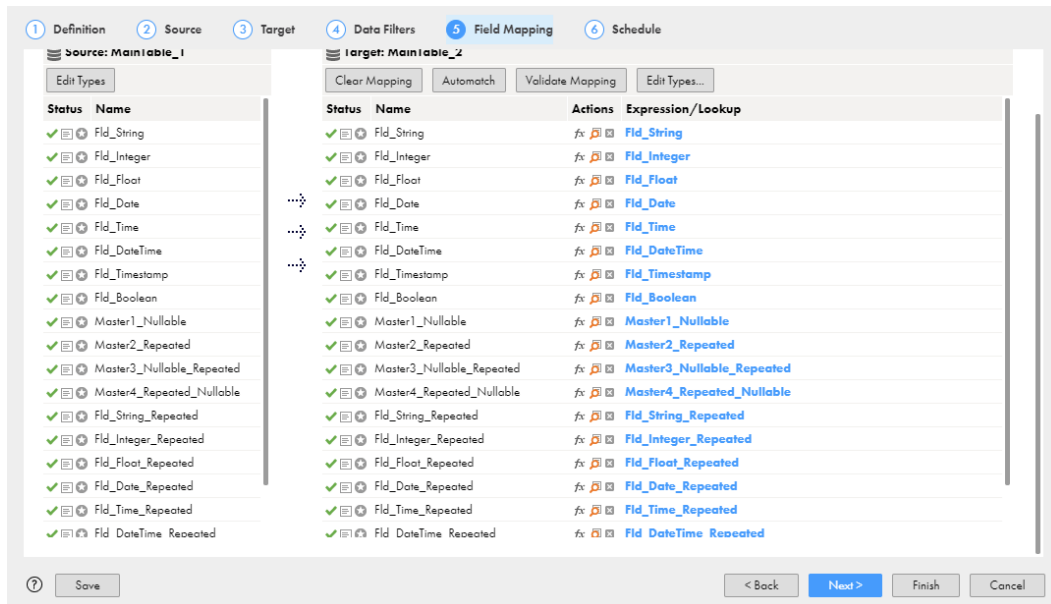
The following image shows the fields in the **Field Mapping** tab of a synchronization task:



### Hybrid mode

If you use hybrid connection mode, Google BigQuery Connector displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery Connector displays the top-level Record data type field as a single field of the String data type in the **Field Mapping** tab.

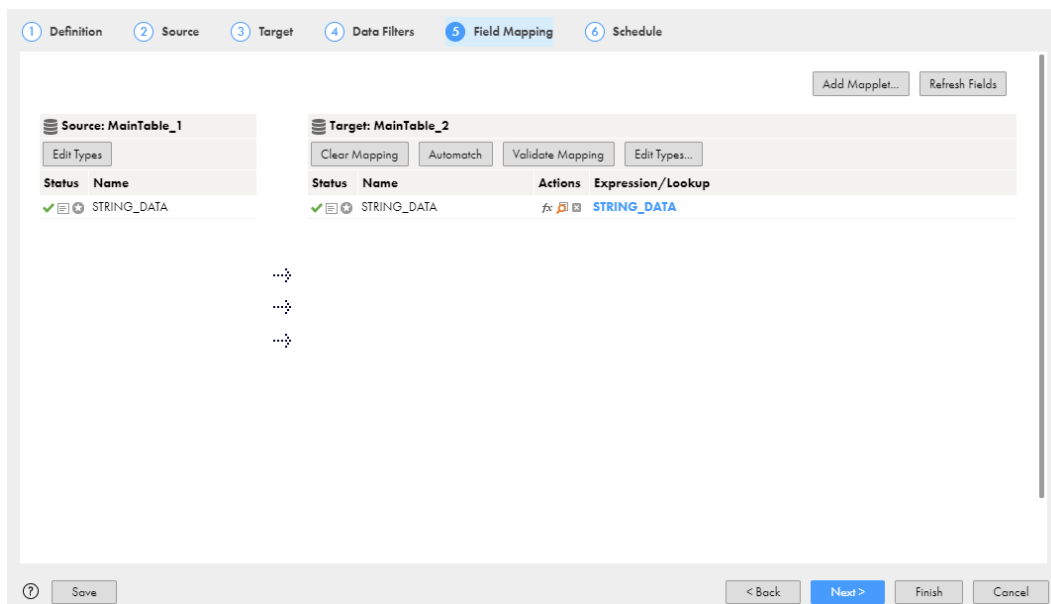
The following image shows the **Field Mapping** tab of a synchronization task:



## Complex mode

If you use complex connection mode, Google BigQuery Connector displays all the columns in the Google BigQuery table as a single field of the String data type in the **Field Mapping** tab.

The following image shows the STRING\_DATA field in the **Field Mapping** tab of a synchronization task:





# Rules and guidelines for Google BigQuery connection modes

## Simple mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use simple connection mode:

- You cannot create a Google BigQuery target table that contains repeated columns using the **Create Target** option.
- If the Google BigQuery source table contains repeated columns, you cannot configure data filters for these columns.
- If the Google BigQuery table contains more than one repeated column, you cannot preview data.
- If the Google BigQuery target table contains repeated columns, you cannot configure update and delete operations for these columns.
- You cannot configure upsert operations for columns of the Record data type and repeated columns.
- When you read data from a Google BigQuery source, you must not map more than one repeated column in a single mapping. You must create multiple mappings for each repeated column.

## Hybrid mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use hybrid connection mode:

- You cannot preview data.
- You cannot create a Google BigQuery target table using the **Create Target** option.
- If the Google BigQuery source table contains columns of the Record data type and repeated columns, you cannot configure data filters for these columns.
- You cannot configure update, upsert, and delete operations for columns of the Record data type and repeated columns.
- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties. You can use CSV format as the data format of the staging file unless the Google BigQuery table contains columns of the Record data type or repeated columns.
- The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows

## Complex mode

Consider the following rules and guidelines when you configure a Google BigQuery connection to use complex connection mode:

- You cannot preview data.
- You cannot create a Google BigQuery target table using the **Create Target** option.
- When you configure a Google BigQuery source connection to use complex connection mode, you cannot configure data filters for the source.
- You cannot configure update, upsert, and delete operations.

- You must select JSON (Newline Delimited) format as the data format of the staging file under the advanced target properties.
- You cannot use CSV format as the data format of the staging file. The following CSV formatting options in the advanced target properties are not applicable:
  - Allow Quoted Newlines
  - Field Delimiter
  - Allow Jagged Rows
- You cannot use key range partitioning for Google BigQuery sources.

## CHAPTER 79

# Google BigQuery V2 connection properties

Create a Google BigQuery V2 connection to securely read data from or write data to Google BigQuery.

## Connect to Google BigQuery

Let's configure the Google BigQuery V2 connection properties to connect to Google BigQuery.

### Before you begin

Before you configure a connection, ensure that you download the Google service account key file in JSON format. The service account key file is created when you create a Google service account.

You require the client email, private key, and project ID from the service account key JSON file to create a Google BigQuery connection.

The following video shows you how to get the information you need from your Google BigQuery account:



### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.

Property	Description
Type	Google BigQuery V2
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run an application ingestion, database ingestion, or streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>

## Authentication type

Select the Service Account authentication type to access Google BigQuery and configure the authentication-specific parameters.

### Service Account authentication

Service Account authentication requires at a minimum your Google BigQuery service account email, service account key, and project ID.

The following table describes the basic connection properties for Service Account authentication:

Property	Description
Service Account Email	The client_email value from the Google service account key JSON file.
Service Account Key	The private_key value from the Google service account key JSON file.
Project ID	<p>The project_id value from the Google service account key JSON file.</p> <p>If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.</p>

**Note:** If you want to validate the credentials for the Service Account Email, Service Account Key, and Project ID during a test connection, set the flag `CredentialValidation:true` in the **Provide Optional Properties** field in advanced settings.

## Advanced settings

The following table describes the advanced connection properties for Service Account authentication:

Property	Description
Enable BigQuery Storage API	Select this option to use Google BigQuery Storage to stage the files when you read or write data. Default is unselected.
Storage Path	<p>Path in Google Cloud Storage where the agent creates a local stage file to store the data temporarily. The agent uses this storage when it reads data in staging mode or writes data in bulk mode.</p> <p>Use one of the following formats:</p> <ul style="list-style-type: none"><li>- gs://&lt;bucket_name&gt;</li><li>- gs://&lt;bucket_name&gt;/&lt;folder_name&gt;</li></ul> <p>When you enable cross-region replication in Google BigQuery, enter a Google Cloud Storage path that supports dual region storage.</p> <p>This property is not applicable if you use Google BigQuery Storage to stage the files.</p>
Connection Mode	<p>The mode that you want to use to read data from or write data to Google BigQuery.</p> <p>Select one of the following connection modes:</p> <ul style="list-style-type: none"><li>- Simple. Flattens each field within the Record data type field as a separate field in the mapping.</li><li>- Hybrid<sup>1</sup>. Displays all the top-level fields in the Google BigQuery table including Record data type fields. Google BigQuery V2 Connector displays the top-level Record data type field as a single field of the String data type in the mapping.</li><li>- Complex<sup>1</sup>. Displays all the columns in the Google BigQuery table as a single field of the String data type in the mapping.</li></ul> <p>Default is Simple.</p> <p>This property is applicable if you use Google Cloud Storage to stage the files.</p>
Use Legacy SQL for Custom Query <sup>1</sup>	<p>Select this option to use legacy SQL to define a custom query. If you clear this option, use standard SQL to define a custom query.</p> <p>This property is applicable if you use Google Cloud Storage to stage the files.</p> <p>This property doesn't apply if you configure the Google BigQuery V2 connection in hybrid or complex mode.</p>
Dataset Name for Custom Query <sup>1</sup>	<p>When you define a custom query, specify a Google BigQuery dataset.</p>
Schema Definition File Path <sup>1</sup>	<p>Directory on the Secure Agent machine where the Secure Agent creates a JSON file with the sample schema of the Google BigQuery table. The JSON file name is the same as the Google BigQuery table name.</p> <p>Alternatively, you can specify a storage path in Google Cloud Storage where the Secure Agent creates a JSON file with the sample schema of the Google BigQuery table. You can download the JSON file from the specified storage path in Google Cloud Storage to a local machine.</p> <p>The schema definition file is required if you configure complex connection mode in the following scenarios:</p> <ul style="list-style-type: none"><li>- You add a Hierarchy Builder transformation in a mapping to read data from relational sources and write data to a Google BigQuery target.</li><li>- You add a Hierarchy Parser transformation in a mapping to read data from a Google BigQuery source and write data to relational targets.</li></ul> <p>When you use a serverless runtime environment, specify a storage path in Google Cloud Storage.</p> <p>This property is applicable if you use Google Cloud Storage to stage the files.</p>

Property	Description
Region ID	The region name where the Google BigQuery dataset that you want to access resides. <b>Note:</b> Ensure that you specify a bucket name or the bucket name and folder name in the <b>Storage Path</b> property that resides in the specified region. For more information about the regions supported by Google BigQuery, see <a href="#">Dataset locations</a> .
Staging Dataset <sup>1</sup>	The Google BigQuery dataset name where you want to create the staging table to stage the data. You can define a Google BigQuery dataset that is different from the source or target dataset. This property is applicable if you use Google Cloud Storage to stage the files.
Provide Optional Properties <sup>1</sup>	Comma-separated key-value pairs of custom properties in the Google BigQuery V2 connection to configure certain source and target functionalities. For more information about the list of custom properties that you can specify, see <a href="#">Optional Properties configuration</a> Knowledge Base.
Enable Retry <sup>1</sup>	Select this option if you want the Secure Agent to attempt a retry to receive the response from the Google BigQuery endpoint. You can configure the retry strategy to read data from Google BigQuery in direct or staging mode and write data to Google BigQuery in bulk mode. The retry strategy is not applicable in the CDC and streaming modes when you write data to a Google BigQuery target. The connection retry option also applies to a connection configured to use the proxy server to connect to the endpoint. Default is unselected.
Maximum Retry Attempts	Appears only if you select the <b>Enable Retry</b> property. The maximum number of retry attempts that the Secure Agent performs to receive the response from the Google BigQuery endpoint. If the Secure Agent fails to connect to Google BigQuery within the maximum retry attempts, the connection fails. Default is 6 attempts.
Initial Retry Delay	Appears only if you select the <b>Enable Retry</b> property. The initial wait time in seconds before the Secure Agent attempts to retry the connection. Default is 1 second.
Retry Delay Multiplier	Appears only if you select the <b>Enable Retry</b> property. The multiplier that the Secure Agent uses to exponentially increase the wait time between successive retry attempts up to the maximum retry delay time. Default multiplier is 2.0. You can also use fractional values.
Maximum Retry Delay	Appears only if you select the <b>Enable Retry</b> property. The maximum wait time in seconds that the Secure Agent waits between successive retry attempts. Default is 32 seconds.
Total Timeout	Appears only if you select the <b>Enable Retry</b> property. The total time duration in seconds that the Secure Agent attempts to retry the connection after which the connection fails. Default is 50 seconds.
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

# Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

Use one of the following methods to configure the proxy settings:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure the proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Configure proxy settings for NTLM authentication

You can use a proxy server that uses NTLM authentication to connect to Google BigQuery. To configure the proxy settings for NTLM authentication, perform the following steps:

1. In Administrator, select **Runtime Environments**.
2. Select the Secure Agent for which you want to configure from the list of available Secure Agents.
3. In the upper-right corner, click **Edit**.
4. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Server.
5. Edit the **JVMOption1** and add the following value:  
`-Dhttp.auth.ntlm.domain=<domain name>`
6. Select the **Type** as **Platform** for the Data Integration Server.
7. Edit the **INFA\_DEBUG** property and add the following value:  
`-Dhttp.auth.ntlm.domain=<domain name>`
8. Click **Save**.
9. Restart the Secure Agent.

## CHAPTER 80

# Google Bigtable connection properties

When you create a Google Bigtable connection, you must configure the connection properties.

The following table describes the Google Cloud Bigtable connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*() - + = { [ ]   \ ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>googleBigTable</b> connection type.
Runtime Environment	Runtime environment that contains the Secure Agent used to access Google Cloud Bigtable.
Project ID	Specifies the <code>project_id</code> value present in the JSON file that you download after you create a service account.
Service Account ID	Specifies the <code>client_email</code> value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the <code>private_key</code> value present in the JSON file that you download after you create a service account.



## CHAPTER 81

# Google Cloud Storage connection properties

When you create a Google Cloud Storage connection, you must configure the connection properties.

**Important:** Effective in the November 2024 release, Google Cloud Storage Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Google Cloud Storage V2 Connector to access Google Cloud Storage.

The following table describes the Google Cloud Storage connection properties:

Property	Description
Runtime Environment	Runtime environment that contains the Secure Agent used to access Google Cloud Storage.
Project ID	Specifies the <code>project_id</code> value present in the JSON file that you download after you create a service account. If you have created multiple projects with the same service account, enter the ID of the project that contains the bucket that you want to connect to.
Service Account ID	Specifies the <code>client_email</code> value present in the JSON file that you download after you create a service account.
Service Account Key	Specifies the <code>private_key</code> value present in the JSON file that you download after you create a service account.
File Path	Path in Google Cloud Storage where you want to read or write data. You can either enter the bucket name or the bucket name and folder name. For example, enter <code>&lt;bucket name&gt;</code> or <code>&lt;bucket name&gt;/&lt;folder name&gt;</code>

## CHAPTER 82

# Google Cloud Storage V2 connection properties

When you create a Google Cloud Storage V2 connection, configure the connection properties.

The following table describes the Google Cloud Storage connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Google Cloud Storage V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion and replication task or streaming ingestion and replication task on a Hosted Agent or serverless runtime environment.
Service Account Email	The client_email value in the JSON file that you download after you create a service account.
Service Account Key	The private_key value in the JSON file that you download after you create a service account.
Project ID	The project_id value in the JSON file that you download after you create a service account. If you created multiple projects with the same service account, enter the ID of the project that contains the bucket that you want to connect to.
Is Encrypted File <sup>1</sup>	Specifies whether a file is encrypted. Select this option when you import an encrypted file from Google Cloud Storage. Default is unselected.
Private Key ID	The private_key_id value in the JSON file that you download after you create a service account. This property applies only to a database ingestion and replication or streaming ingestion and replication task.

Property	Description
Client ID	The <code>client_id</code> value in the JSON file that you download after you create a service account. This property applies only to a database ingestion and replication or streaming ingestion and replication task.
Bucket Name	The Google Cloud Storage bucket name that you want to connect to. When you select a source object or target object in a mapping, the Package Explorer lists files and folder available in the specified Google Cloud Storage bucket. If you do not specify a bucket name, you can select a bucket from the Package Explorer to select a source or target object.

<sup>1</sup> Applies only to mappings in advanced mode.

## CHAPTER 83

# Google Drive connection properties

When you create a Google Drive connection, you must configure the connection properties.

The following table describes the Google Drive connection properties:

Property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client ID	The Client ID from Google Developer Console.
Client Secret	The Client Secret from Google Developer Console.
Refresh Token	The Refresh Token received after exchanging authorization code.
File Download Path	The directory where file needs to be downloaded.
File Upload Path	The directory where file is stored and needs to be uploaded.
PageSize	The page size for the read operation. Default value is 10.

## CHAPTER 84

# Google PubSub - Streaming Ingestion and Replication connection properties

When you define a Google PubSub Streaming Ingestion and Replication connection, you must configure connection properties. You can use this connection type in streaming ingestion and replication tasks, which you configure in the Data Ingestion and Replication service.

The following table describes the Google PubSub connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ]   \ ; ; " ' < , > . ? /
Description	Optional. Description that you use to identify the connection. The description must not exceed 4,000 characters.
Type	The <b>Google PubSub</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Client Email	The <code>client_email</code> value available in the JSON file that you download after you create a service account.
Client ID	The <code>client_id</code> value available in the JSON file that you download after you create a service account.
Private Key ID	The <code>private_key_id</code> value available in the JSON file that you download after you create a service account.
Private Key	The <code>private_key</code> value available in the JSON file that you download after you create a service account.
Project ID	The <code>project_id</code> value available in the JSON file that you download after you create a service account.

**Note:** The test connection for the Google PubSub connector does not fail even if you enter incorrect values for **Client ID** and **Private Key ID**.

## CHAPTER 85

# Google PubSub connection properties

When you create a Google PubSub connection, you must configure the connection properties.

The following table describes the Google PubSub connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. The description of the connection. The description must not exceed 4,000 characters.
Type	The <b>GooglePubSub</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service Account ID	Specifies the client_email value available in the JSON file that you download after you create a service account.
Service Account Key	Specifies the private_key value available in the JSON file that you download after you create a service account in a secured way.
Project ID	Specifies the project_id value available in the JSON file that you download after you create a service account.
maxMessageForBatch	Specifies the number of messages that the Secure Agent can publish in a batch. Default is 100. The maximum value is 1000.

## CHAPTER 86

# Google PubSub V2 connection properties

When you create a Google PubSub V2 connection, you must configure the connection properties.

The following table describes the Google PubSub V2 connection properties:

Property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ `! \$ % ^ & * ( ) - + = { [ ]   \ ; ; " ' < , > . ? /
Description	Optional. The description of the connection. The description must not exceed 4,000 characters.
Type	The <b>GooglePubSubV2</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Service Account ID	Specifies the <code>client_email</code> value available in the JSON file that you download after you create a service account.
Service Account Key	Specifies the <code>private_key</code> value available in the JSON file that you download after you create a service account in a secured way.
Project ID	Specifies the <code>project_id</code> value available in the JSON file that you download after you create a service account.

## CHAPTER 87

# Google Sheets connection properties

When you create a Google Sheets connection, configure the connection properties.

The following table describes the Google Sheets connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Google Sheets
Runtime Environment	Name of the runtime environment where you want to run tasks.
ClientId	Required. The Client ID from Google Developer Console.
ClientSecret	Required. The Client Secret from Google Developer Console.
RefreshTokenForSheet	Required. The Refresh Token received after exchanging authorization code for Google Sheets.
RefreshTokenForDrive	Optional. The Refresh Token received after exchanging authorization code for Google Drive. This option is required when you enter the spreadsheet name in the <b>SpreadSheetName</b> field.
SpreadSheetName	Name of the spreadsheet in Google Sheets.
SpreadSheetId	ID of the spreadsheet in Google Sheets.
InitialColumnRange	Specifies the first column name from a data range in a Google Sheets spreadsheet from where you want to start reading the data. For example, specify the InitialColumnRange value as Sheet1!C5.
FinalColumnRange	Specifies the last column name from a data range in a Google Sheets spreadsheet from where you want to stop reading the data. For example, specify the FinalColumnRange value as Sheet1!G20.



<b>Property</b>	<b>Description</b>
HeaderPresent	Select this option to indicate that the sheet contains a header. If you select this option and the sheet does not contain a header, the first row is treated as the header.
CreateNewSpreadsheet	Select this option to create a new spreadsheet in Google Sheets. The Google Sheets Connector creates an empty spreadsheet with the name that you specified in the <b>SpreadSheetName</b> field. Once you test the connection, disable this option. Otherwise, the Google Sheets Connector will create a new spreadsheet with the same name everytime

## CHAPTER 88

# Google Sheets V2 connection properties

When you create a Google Sheets V2 connection, configure the connection properties.

The following table describes the Google Sheets V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Google Sheets V2
Runtime Environment	Name of the runtime environment where you want to run tasks.
Client ID	Required. The client ID from Google Developer Console.
Client Secret	Required. The client secret from Google Developer Console.
Refresh Token	Required. The refresh token received after you exchange authorization code for Google Sheets.
Spreadsheet ID	ID of the spreadsheet in Google Sheets.
Header Present	Indicates that the sheet contains a header. If you select this option and the sheet does not contain a header, the first row is treated as the header.

## CHAPTER 89

# Greenplum connection properties

Create a Greenplum connection to securely read data from or write data to Greenplum.

## Prerequisites

Before you use Greenplum Connector, ensure that you meet the prerequisites.

Perform the following prerequisite tasks:

1. Install the Greenplum loaders package on the Secure Agent machine. The loaders package contains the gload utility. You can download the Greenplum loaders package from the Pivotal Greenplum website.
2. Configure the DataDirect Greenplum ODBC and JDBC drivers on the Secure Agent machine.
3. Configure the authentication prerequisites to connect to a Greenplum database. You can configure Database or Kerberos authentication. Keep the following authentication details handy based on the authentication type that you want to use:
  - To configure Database authentication, you need the user name, password, host name, port, database name from your Greenplum account.
  - To configure Kerberos authentication, you need the service principal name, host name, port, and database name from your Greenplum account.

## Configure JDBC and ODBC drivers

Before you use Greenplum Connector, configure DataDirect Greenplum JDBC and ODBC drivers on Windows and Linux.

### Configure the DataDirect Greenplum JDBC Driver on Linux

1. Download the DataDirect Greenplum JDBC driver version 6.x from the Pivotal Greenplum website.
2. Copy the Greenplum JDBC driver to the following directory on the Secure Agent machine: `<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra/Greenplum`

**Note:** You must create the `deploy_to_main/bin/rdtm-extra` directory manually.
3. Restart the Secure Agent.

### Configure the DataDirect Greenplum JDBC driver on Windows

1. Download the DataDirect Greenplum JDBC driver version 6.x from the Pivotal Greenplum website.

2. Copy the Greenplum JDBC driver to the following directory on the Secure Agent machine:  
`<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\Greenplum`  
 You must create the `deploy_to_main\bin\rdtm-extra\Greenplum` directory manually.
3. Restart the Secure Agent.

## Configure the DataDirect Greenplum ODBC driver on Linux

1. Download the DataDirect Greenplum ODBC driver version 7.1.6 from the Pivotal website and install the DataDirect Greenplum ODBC driver on the Secure Agent machine.
2. Add the following driver entries to the `odbcinst.ini` file in the following directory: `<Secure Agent installation directory>/odbcinst.ini`  
 Use the following syntax:

```
[DataDirect 7.1 Greenplum Wire Protocol]
Driver=<ODBC driver path>/lib/ddgplm27.so
Setup=<ODBC driver path>/lib/ddgplm27.so
DriverODBCVer=<ODBC Driver version>
HelpRootDirectory=<ODBC Driver path>/help
GSSClient=libgssapi_krb5.so.2
```

For example:

```
[DataDirect 7.1 Greenplum Wire Protocol]
Driver=/opt/Progress/DataDirect/Connect64_for_ODBC_71/lib/ddgplm27.so
Setup=/opt/Progress/DataDirect/Connect64_for_ODBC_71/lib/ddgplm27.so
APILevel=0
ConnectFunctions=YYY
DriverODBCVer=3.52
FileUsage=0
HelpRootDirectory=/opt/Progress/DataDirect/Connect64_for_ODBC_71/help
SQLLevel=0
GSSClient=libgssapi_krb5.so.2
```

3. Set the `GPHOME_LOADERS`, `PATH`, and `LD_LIBRARY_PATH` environmental variables for the driver.  
 Perform the following tasks:
  - a. Set the `GPHOME_LOADERS` environmental variable to the directory that contains the Greenplum loader libraries. Using a C shell and run the following command:  
`setenv GPHOME_LOADERS /export/qa_adp/thirdparty/greenplum/rhel.64/loaders`
  - b. Set the `PATH` environmental variable to the directory that contains the Greenplum loader libraries. Using a C shell and run the following command:  
`setenv PATH ${GPHOME_LOADERS}/bin:${PATH}`
  - c. Set the `LD_LIBRARY_PATH` environmental variable to include the following directories that contain the Greenplum drivers and the DataDirect Greenplum ODBC libraries. Using a C shell and run the following command:  
`setenv LD_LIBRARY_PATH .:${GPHOME_LOADERS}/lib:/export/qa_adp/thirdparty/greenplum/rhel.64/loaders/ext/python/lib`  
`setenv LD_LIBRARY_PATH /opt/Progress/DataDirect/Connect64_for_ODBC_71/lib:${LD_LIBRARY_PATH}`
4. Restart the Secure Agent after you update the environment variables.

## Configure the DataDirect Greenplum ODBC driver on Windows

1. Download the DataDirect Greenplum ODBC driver version 7.1.6 from the Pivotal website and install the DataDirect Greenplum ODBC driver on the Secure Agent machine.

2. Install Python 2.5.4 32-bit.
3. Install the 5.18 Greenplum Clients software for Windows.
4. Install the 5.18 Greenplum loaders software for Windows.
5. Set the following environmental variables for the driver:
  - Set the GPHOME\_LOADERS environment variable to the folder that contains the Greenplum loader libraries:  
For example, Set GPHOME\_LOADERS = C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0
  - Set the GPHOME\_CLIENTS environment variable to the folder that contains the Greenplum clients libraries:  
For example, set GPHOME\_CLIENTS=C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\
  - Set the PYTHONPATH environment variable:  
Set PYTHONPATH=%GPHOME\_LOADERS%\bin\lib
  - Set the DDCPATH environment variable to the folder containing the DataDirect libraries.  
For example, DDCPATH=C:\Program Files\Progress\DataDirect\Connect64\_for\_ODBC\_71\drivers;C:\Program Files\Progress\DataDirect\Connect64\_for\_ODBC\_71\jre\bin;C:\Program Files\Progress\DataDirect\Connect64\_for\_ODBC\_71\jre\bin\server
  - Set the Path environment variable to the folder that contains the Greenplum clients, Greenplum loaders, Python and Greenplum ODBC Datadirect driver libraries:  
For example, Path=C:\Python25;C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0\lib;C:\Program Files (x86)\Greenplum\greenplum-loaders-5.18.0\bin;C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\lib;C:\Program Files (x86)\Greenplum\greenplum-clients-5.18.0\bin;%DDCPATH%

## Configuring the Kerberos authentication

Before you use Kerberos authentication to connect to Greenplum on Linux or Windows, the organization administrator needs to perform the prerequisite tasks.

1. To configure the Java Authentication and Authorization Service configuration file (JAAS), perform the following tasks:

- a. Create a JAAS configuration file on the Secure Agent machine.
- b. Add the following entries to the JAAS configuration file:

```
JDBC_DRIVER_01 {
  com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;
};
```

2. To configure the `krb5.conf` file, perform the following tasks:

- a. Create a `krb5.conf` file on the Secure Agent machine.
- b. Add the details of the Key Distribution Center (KDC) and admin server to the `krb5.conf` file in the following format:

```
[libdefaults]
  default_realm = <Realm name>
  forwardable = true
  ticket_lifetime = 24h
```

```

[realms]
<REALM NAME> = {
kdc = <Location where KDC is installed>
admin_server = <Location where KDC is installed>
}

[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>

```

3. Set the environment variables on the Secure Agent machine.
4. Restart the Secure Agent.
5. To generate the credential cache file on the Secure Agent machine and use Kerberos authentication to connect to Greenplum, perform the following tasks:
  - a. From the command line on the Secure Agent machine, run the following command and specify the Greenplum user name and realm name:

```
Kinit <user name>@<realm_name>
```
  - b. When prompted, enter the password for the Kerberos principal user.

## Setting environment variables

To use Kerberos authentication to connect to Greenplum, you need to set the required environment variables on the Secure Agent machine.

Run the following commands to set the environment variables:

- `setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>`
- `setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf`
- `setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf`

After you set the environmental variables, you need to restart the Secure Agent.

Alternatively, you can add the `KRB5_CONFIG` and `JAASCONFIG` environment variables when you create a Greenplum connection.

To add the environment variables when you configure a connection with Kerberos authentication, you need to add the `KRB5_CONFIG` and `JAASCONFIG` properties in the **Kerberos Connection Properties** field in a Greenplum connection.

For example, add the properties in the following format:

```

KRB5_CONFIG=<Absolute path of the Kerberos configuration file>
\krb5.conf;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf

```

**Note:** Ensure that you separate each key-value pair with a semicolon.

# Connect to Greenplum

Let's configure the Greenplum connection properties to connect to Greenplum.

## Before you begin

Before you get started, be sure to complete the prerequisites.

Check out ["Prerequisites" on page 287](#) to learn more about the authentication prerequisites and other tasks that you must perform.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Greenplum
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Host Name	Host name or IP address of the Greenplum server.
Port	Greenplum server port number. If you enter 0, the gpload utility reads from the environment variable \$PGPORT. Default is 5432.
Database	Name of the Greenplum database.
Schema	Name of the schema that contains the metadata for Greenplum sources or targets. Default is public.

## Authentication types

You can configure Database or Kerberos authentication types to connect to the Greenplum database.

Select the required authentication type and then configure the authentication-specific parameters.

### Database authentication

To configure Database authentication, you need the user name and password from your Greenplum account.

The following table describes the basic connection properties for database authentication:

Property	Description
Username	User name with permissions to access the Greenplum database.
Password	Password to connect to the Greenplum database.

The following table describes the advanced connection properties for Database authentication:

Property	Description
Certificates Path	<p>Path where the SSL certificates for the Greenplum server are stored.</p> <p>Specify the path if you want to establish secure communication between the gpload utility and the Greenplum server over SSL.</p> <p>For information about the files that need to be available in the certificates path, see the gpload documentation.</p> <p><b>Note:</b> You can use the SSL-based connection only in a Target transformation in a mapping to write to Greenplum.</p>
Metadata Additional Connection Configuration	<p>Additional connection properties that you want to set to fetch the metadata from Greenplum.</p> <p>Enter the properties in the following format:</p> <pre>&lt;parameter name1&gt;=&lt;value1&gt;, &lt;parameter name2&gt;=&lt;value2&gt;</pre>
Driver Name	<p>The driver name.</p> <p>Specify DataDirect 7.1 Greenplum Wire Protocol.</p>

## Kerberos authentication

To configure Kerberos authentication, you need the Kerberos connection properties, service principal name, host name, port, database name, and your Greenplum account details from your Greenplum account.

The following table describes the basic connection properties for Kerberos authentication:

Property	Description
Host Name	Host name or IP address of the Greenplum server.
Port	<p>Greenplum server port number.</p> <p>If you enter 0, the gpload utility reads from the environment variable \$PGPORT.</p> <p>Default is 5432.</p>
Database	Name of the Greenplum database.



The following table describes the advanced connection property for Kerberos authentication:

Property	Description
Kerberos Connection Properties	<p>Additional connection properties to use Kerberos authentication to connect to the Greenplum database.</p> <p>Enter properties in the following format:</p> <p>&lt;parameter name&gt;=&lt;parameter value&gt;</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p>
Service Principal Name	<p>Service principal name that you want to use for Kerberos authentication.</p> <p>Specify the service principal name in the following format:</p> <p>&lt;Service Name&gt;/&lt;Fully Qualified Domain Name&gt;@&lt;REALM.COM&gt;</p> <ul style="list-style-type: none"><li>- Service Name is the name of the service hosting the instance.</li><li>- Fully Qualified Domain Name is the fully qualified domain name of the host machine.</li><li>- REALM.COM is the domain name of the host machine. This value is optional. If you do not specify the realm name, the default realm is used.</li></ul>

## CHAPTER 90

# Hadoop connection properties

To use Hadoop Connector in a synchronization task, you must configure the connection properties.

**Important:** Hadoop Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Hive Connector to access the Hadoop clusters.

The following table describes the Hadoop connection properties:

Connection property	Description
Username	The username of schema of Hadoop component.
Password	The password of schema of Hadoop component.
JDBC Connection URL	The JDBC URL to connect to the Hadoop Component. Refer <a href="#">"JDBC URL" on page 295</a>
Driver	The JDBC driver class to connect to the Hadoop Component. For more information, see the Setting Hadoop Classpath for various Hadoop Distributions topic.
Commit Interval	The Batch size, in rows, to load data to hive.
Hadoop Installation Path	The Installation path of the Hadoop component. Not applicable to a kerberos cluster.
Hive Installation Path	Hive Installation Path Not applicable to a kerberos cluster.
HDFS Installation Path	The HDFS Installation Path. Not applicable to a kerberos cluster.
HBase Installation Path	The HBase Installation Path. Not applicable to a kerberos cluster.
Impala Installation Path	The Impala Installation Path. Not applicable to a kerberos cluster.
Miscellaneous Library Path	The library that communicates with Hadoop. Not applicable to a kerberos cluster.

Connection property	Description
Enable Logging	Enable logging enables the log messages. <b>Note:</b> The Enable Logging connection parameter is place-holder for a future release, and its state has no impact on connector functionality.
Hadoop Distribution	The Hadoop distributions for which you can use Kerberos Authentication. You can use Kerberos authentication for the Cloudera and HDP Hadoop distributions.
Authentication Type	You can select native or Kerberos authentication.
Key Tab File	The file that contains encrypted keys and Kerberos principals to authenticate the machine.
Hive Site XML	The directory where the core-site.xml, hive-site.xml and hdfs-site.xml are located. The three XML files must locate in the same location.
Superuser Principle Name	Users assigned to the superuser privilege can perform all the tasks that a user with the administrator privilege can perform.
Impersonation Username	You can enable different users to run mappings in a Hadoop cluster that uses Kerberos authentication or connect to sources and targets that use Kerberos authentication. To enable different users to run mappings or connect to big data sources and targets, you must configure user impersonation.

**Note:** Installation paths are the paths where you place the Hadoop jar. Hadoop Connector loads the libraries from installation paths before it sends instructions to Hadoop. When you use Kerberos Authentication type, you need not specify the Hadoop installation path, Hive installation path, HDFS installation path, HBase Installation path, Impala installation path, and Miscellaneous Library path.

If you do not use Kerberos Authentication and do not mention the installation path, you can set the Hadoop classpath for Amazon EMR, HortonWorks, MapR and Cloudera.

When you perform an insert operation on non-Kerberos clusters, the Secure Agent uses the `hadoop fs -put <FS> <HDFS>` command to upload the file to the HDFS and uses the `hadoop fs -rm -r <HDFS>` command to delete the file from the HDFS. When you enable Kerberos authentication, the Secure Agent does not use the Hadoop commands to write data to or delete data from the HDFS.

## JDBC URL

The connector connects to different components of Hadoop with JDBC. The URL format and parameters differ from components to components.

The Hive uses following JDBC URL format:

```
jdbc:<hive/hive2>://<server>:<port>/<schema>
```

The significance of URL parameters is discussed below:

- `hive/hive2` : Contains the protocol information. The version of the Thrift Server, that is, `hive` for HiveServer and `hive2` for HiveServer2.
- `Server, port` – server and port information of the Thrift Server.
- `Schema` – The hive schema which the connector needs to access.

For example, `jdbc:hive2://invrlx63iso7:10000/default` connects the default schema of Hive, uses a Hive Thrift server `HiveServer2` that starts on the server `invrlx63iso7` on port 10000.

Hadoop Connector uses the Hive thrift server to communicate with Hive.

The command to start the Thrift server is `-hive -service hiveserver2`.

Cloudera Impala uses the JDBC URL in the following format:

```
jdbc:hive2://<server>:<port>/;auth=<auth mechanism>
```

## JDBC Driver Class

The JDBC Driver class varies among Hadoop components. For example, `org.apache.hive.jdbc.HiveDriver` for Hive and Impala.

## CHAPTER 91

# Hadoop Files connection properties

When you set up a Hadoop Files connection, you must configure the connection properties.

**Important:** Hadoop Files Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Hadoop Files V2 Connector to access Hadoop Distributed File System (HDFS).

The following table describes the Hadoop Files connection properties:

Connection property	Description
Connection Name	Name of the Hadoop Files connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select Hadoop Files.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
User Name	Required to read data from HDFS. Enter a user name that has access to the single-node HDFS location to read data from or write data to.

Connection property	Description
NameNode URI	<p>The URI to access HDFS.</p> <p>Use the following format to specify the name node URI in Cloudera, Amazon EMR, and Hortonworks distributions:  <code>hdfs://&lt;namenode&gt;:&lt;port&gt;/</code></p> <p><b>Where</b></p> <ul style="list-style-type: none"> <li>- <code>&lt;namenode&gt;</code> is the host name or IP address of the name node.</li> <li>- <code>&lt;port&gt;</code> is the port that the name node listens for remote procedure calls (RPC).</li> </ul> <p>If the Hadoop cluster is configured for high availability, you must copy the <code>fs.defaultFS</code> value in the <code>core-site.xml</code> file and append <code>/</code> to specify the name node URI.</p> <p>For example, the following snippet shows the <code>fs.defaultFS</code> value in a sample <code>core-site.xml</code> file:</p> <pre>&lt;property&gt;   &lt;name&gt;fs.defaultFS&lt;/name&gt;   &lt;value&gt;hdfs://nameservice1&lt;/value&gt;   &lt;source&gt;core-site.xml&lt;/source&gt; &lt;/property&gt;</pre> <p>In the above snippet, the <code>fs.defaultFS</code> value is  <code>hdfs://nameservice1</code>  and the corresponding name node URI is  <code>hdfs://nameservice1/</code></p> <p><b>Note:</b> Specify either the name node URI or the local path. Do not specify the name node URI if you want to read data from or write data to a local file system path.</p>
Local Path	<p>A local file system path to read data from or write data to. Do not specify local path if you want to read data from or write data to HDFS. Read the following conditions to specify the local path:</p> <ul style="list-style-type: none"> <li>- You must enter <b>NA</b> in local path if you specify the name node URI. If the local path does not contain <b>NA</b>, the name node URI does not work.</li> <li>- If you specify the name node URI and local path, the local path takes the preference. The connection uses the local path to run all tasks.</li> <li>- If you leave the local path blank, the agent configures the root directory (<code>/</code>) in the connection. The connection uses the local path to run all tasks.</li> </ul>
Hadoop Distribution	<p>Hadoop distribution name. Enter <b>CLOUDERA</b>, <b>EMR</b>, or <b>HDP</b> based on the HDFS instance you want to use for the connection.</p> <p>You can use Kerberos authentication for the Cloudera CDH and Hortonworks HDP Hadoop distributions.</p> <p><b>Note:</b> Use all uppercase letters to specify the Hadoop distribution name.</p>
Keytab File	The file that contains encrypted keys and Kerberos principals to authenticate the machine.
Principle Name	Users assigned to the superuser privilege can perform all the tasks that a user with the administrator privilege can perform.
Impersonation Username	You can enable different users to run mappings in a Hadoop cluster that uses Kerberos authentication or connect to sources and targets that use Kerberos authentication. To enable different users to run mappings or connect to big data sources and targets, you must configure user impersonation.

## CHAPTER 92

# Hadoop Files V2 connection properties

When you set up a Hadoop Files V2 connection, you must configure the connection properties.

The following table describes the Hadoop Files V2 connection properties:

Connection property	Description
Connection Name	Name of the Hadoop Files V2 connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select <b>Hadoop Files V2</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
User Name	Required to read data from HDFS. Enter a user name that has access to the single-node HDFS location to read data from or write data to.

Connection property	Description
NameNode URI	<p>The URI to access HDFS.</p> <p>Use the following format to specify the name node URI in Cloudera, Amazon EMR, and Hortonworks distributions:</p> <pre>hdfs://&lt;namenode&gt;:&lt;port&gt;/</pre> <p>where,</p> <ul style="list-style-type: none"> <li>- &lt;namenode&gt; is the host name or IP address of the name node.</li> <li>- &lt;port&gt; is the port that the name node listens for remote procedure calls (RPC).</li> </ul> <p>To connect to the Hadoop cluster, specify the name node port <code>fs.defaultFS</code>.</p> <p>If the Hadoop cluster is configured for high availability, you must copy the <code>fs.defaultFS</code> value in the <code>core-site.xml</code> file and append <code>/</code> to specify the name node URI.</p> <p>For example, the following snippet shows the <code>fs.defaultFS</code> value in a sample <code>core-site.xml</code> file:</p> <pre>&lt;property&gt;   &lt;name&gt;fs.defaultFS&lt;/name&gt;   &lt;value&gt;hdfs://nameservice1&lt;/value&gt;   &lt;source&gt;core-site.xml&lt;/source&gt; &lt;/property&gt;</pre> <p>In the above snippet, the <code>fs.defaultFS</code> value is</p> <pre>hdfs://nameservice1</pre> <p>and the corresponding name node URI is</p> <pre>hdfs://nameservice1/</pre> <p><b>Note:</b> Specify either the name node URI or the local path. Do not specify the name node URI if you want to read data from or write data to a local file system path.</p>
Local Path	<p>A local file system path to read and write data. Read the following conditions to specify the local path:</p> <ul style="list-style-type: none"> <li>- You must enter <b>NA</b> in local path if you specify the name node URI. If the local path does not contain <b>NA</b>, the name node URI does not work.</li> <li>- If you specify the name node URI and local path, the local path takes the preference. The connection uses the local path to run all tasks.</li> <li>- If you leave the local path blank, the agent configures the root directory (<code>/</code>) in the connection. The connection uses the local path to run all tasks.</li> <li>- If the file or directory is in the local system, enter the fully qualified path of the file or directory.</li> </ul> <p>For example, <code>/user/testdir</code> specifies the location of a directory in the local system.</p> <p>Default value for Local Path is NA.</p>
Configuration Files Path	<p>The directory that contains the Hadoop configuration files.</p> <p><b>Note:</b> Copy the <code>core-site.xml</code>, <code>hdfs-site.xml</code>, and <code>hive-site.xml</code> from the Hadoop cluster and add them to a folder in Linux Box.</p>
Keytab File	<p>The file that contains encrypted keys and Kerberos principals to authenticate the machine.</p>
Principal Name	<p>Users assigned to the superuser privilege can perform all the tasks that a user with the administrator privilege can perform.</p>
Impersonation Username	<p>You can enable different users to run mappings in a Hadoop cluster that uses Kerberos authentication or connect to sources and targets that use Kerberos authentication. To enable different users to run mappings or connect to big data sources and targets, you must configure user impersonation.</p>



**Note:** When you read from or write to remote files, the **NameNode URI** and **Configuration Files Path** fields are mandatory. When you read from or write to local files, you require only the **Local Path** field.

## CHAPTER 93

# Hive connection properties

To use Hive Connector in a mapping task, you must create a connection in Data Integration.

When you set up a Hive connection, you must configure the connection properties.

The following table describes the Hive connection properties:

Connection property	Description
Authentication Type	<p>You can select one of the following authentication types:</p> <ul style="list-style-type: none"><li>- Kerberos. Select <b>Kerberos</b> for a Kerberos cluster.</li><li>- LDAP. Select <b>LDAP</b> for an LDAP-enabled cluster.</li></ul> <p><b>Note:</b> LDAP is not applicable to mappings in advanced mode.</p> <ul style="list-style-type: none"><li>- None. Select <b>None</b> for a Hadoop cluster that is not secure or not LDAP-enabled.</li></ul>
JDBC URL *	<p>The JDBC URL to connect to Hive.</p> <p>Specify the following format based on your requirement:</p> <ul style="list-style-type: none"><li>- To view and import tables from a single database, use the following format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/&lt;database name&gt;</code></li><li>- To view and import tables from multiple databases, do not enter the database name. Use the following JDBC URL format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/</code></li></ul> <p><b>Note:</b> After the port number, enter a slash.</p> <ul style="list-style-type: none"><li>- To access Hive on a Hadoop cluster enabled for TLS, specify the details in the JDBC URL in the following format: <code>jdbc:hive2://&lt;host&gt;:&lt;port&gt;/&lt;database name&gt;;ssl=true;sslTrustStore=&lt;TrustStore_path&gt;;trustStorePassword=&lt;TrustStore_password&gt;</code>, where the truststore path is the directory path of the truststore file that contains the TLS certificate on the agent machine.</li></ul>
JDBC Driver *	The JDBC driver class to connect to Hive.
Username	The user name to connect to Hive in LDAP or None mode.
Password	The password to connect to Hive in LDAP or None mode.
Principal Name	The principal name to connect to Hive through Kerberos authentication.
Impersonation Name	The user name of the user that the Secure Agent impersonates to run mappings on a Hadoop cluster. You can configure user impersonation to enable different users to run mappings or connect to Hive. The impersonation name is required for the Hadoop connection if the Hadoop cluster uses Kerberos authentication.
Keytab Location	The path and file name to the Keytab file for Kerberos login.

Connection property	Description
Configuration Files Path *	<p>The directory that contains the Hadoop configuration files for the client.</p> <p>Copy the site.xml files from the Hadoop cluster and add them to a folder in the Linux box. Specify the path in this field before you use the connection in a mapping to access Hive on a Hadoop cluster:</p> <ul style="list-style-type: none"> <li>- For mappings, you require the core-site.xml, hdfs-site.xml, and hive-site.xml files.</li> <li>- For mappings in advanced mode, you require the core-site.xml, hdfs-site.xml, hive-site.xml, mapred-site.xml, and yarn-site.xml files.</li> </ul>
DFS URI *	<p>The URI to access the Distributed File System (DFS), such as Amazon S3, Microsoft Azure Data Lake Storage, and HDFS.</p> <p><b>Note:</b> For mappings in advanced mode that run on the advanced cluster, Azure Data Lake Storage Gen2 is supported on the Azure HDinsight cluster.</p> <p>Based on the DFS you want to access, specify the required storage and bucket name.</p> <p>For example, for HDFS, refer to the value of the <b>fs.defaultFS</b> property in the <b>core-site.xml</b> file of the Hadoop cluster and enter the same value in the <b>DFS URI</b> field.</p>
DFS Staging Directory	<p>The staging directory in the Hadoop cluster where the Secure Agent stages the data. You must have full permissions for the DFS staging directory.</p> <p>Specify a transparent encrypted folder as the staging directory.</p>
Hive Staging Database	<p>The Hive database where external or temporary tables are created. You must have full permissions for the Hive staging database.</p>
Additional Properties	<p>Applies to mappings in advanced mode.</p> <p>The additional properties required to access the DFS.</p> <p>Configure the property as follows:</p> <p>&lt;DFS property name&gt;=&lt;value&gt;;&lt;DFS property name&gt;=&lt;value&gt;</p> <p>For example:</p> <p>To access the Amazon S3 file system, specify the access key, secret key, and the Amazon S3 property name, each separated by a semicolon:</p> <pre>fs.s3a.&lt;bucket_name&gt;.access.key=&lt;access key value&gt;; fs.s3a.&lt;bucket_name&gt;.secret.key=&lt;secret key value&gt;; fs.s3a.impl=org.apache.hadoop.fs.s3a.S3AFileSystem;</pre> <p>To access the Azure Data Lake Storage Gen2 file system, specify the authentication type, authentication provider, client ID, client secret, and the client endpoint, each separated with a semicolon:</p> <pre>fs.azure.account.auth.type=&lt;Authentication type&gt;; fs.azure.account.oauth.provider.type=&lt;Authentication_provider&gt;; fs.azure.account.oauth2.client.id=&lt;Client_ID&gt;; fs.azure.account.oauth2.client.secret=&lt;Client-secret&gt;; fs.azure.account.oauth2.client.endpoint=&lt;ADLS Gen2 endpoint&gt;</pre>
<p>* These fields are mandatory parameters.</p>	

## CHAPTER 94

# HubSpot connection properties

When you set up a HubSpot connection, you must configure the connection properties.

The following table describes the HubSpot connection properties:

Connection property	Description
Connection Name	The name of the HubSpot connection.
Description	The description of the connection.
Type	The type of connection. Select the HubSpot connection.
Client Id	The ID of your application to authenticate access to HubSpot. You can get the client ID value from the HubSpot applications.
Client Secret	The client secret key to authenticate access to HubSpot. You can get the client secret value from the HubSpot applications.
RefreshToken	The refresh token that you need to authenticate access to HubSpot.

## CHAPTER 95

# IBM MQ connection properties

When you set up an IBM MQ connection, configure the connection properties.

The following table describes the IBM MQ connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The IBM MQ connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select the Secure Agent from the list as the runtime environment.
Host	The machine that hosts the Queue Manager component.
Port	The port number that connects to the Queue Manager component.
User Name	The user name to connect to the connection channel of the Queue Manager component. Don't specify the user name when the channel authentication of the Queue Manager component is not enabled.
Password	The password to connect to the connection channel of the Queue Manager component. Don't specify the password when the channel authentication of the Queue Manager component is not enabled.
Queue Manager	The Queue Manager component from which queues need to be listed to send or receive messages.
Channel	The server-connection channel that connects to a queue in the Queue Manager. If you don't enable the channel authentication of the Queue Manager component, the default user account for the IBM MQ service writes data to the target.

Property	Description
Code Page	<p>The code page of the Queue Manager component that the Secure Agent uses to read from or write to IBM MQ.</p> <p>Select one of the following code pages from the list:</p> <ul style="list-style-type: none"> <li>- UTF-8</li> <li>- UTF-16</li> <li>- MS Windows Latin 1</li> </ul> <p>Default is UTF-8.</p>
SSL	<p>Specifies whether the connection uses an SSL socket to connect to IBM MQ.</p> <p>Default is disabled.</p>
Truststore File Path	<p>The path and file name of the truststore file that contains the SSL certificate to connect to IBM MQ.</p> <p>Specify both the directory and file name in the following format:</p> <pre>/root/&lt;folder name&gt;/&lt;truststore file name&gt;.jks</pre>
Truststore Password	<p>The password to access the truststore file that contains the SSL certificate.</p>
Keystore File Path	<p>The path and file name of the SSL keystore file that contains private keys and SSL certificates to establish a two-way secure communication with IBM MQ.</p> <p>Specify both the directory and file name in the following format:</p> <pre>/root/&lt;folder name&gt;/&lt;keystore file name&gt;.jks</pre> <p><b>Note:</b> To establish a two-way secure communication with IBM MQ, you also need to enter values in the <b>Truststore File Path</b>, <b>Truststore Password</b>, and <b>Keystore Password</b> fields.</p>
Keystore Password	<p>The password to access the keystore file that contains the SSL certificate.</p>
Skip Metadata Fetch	<p>Determines whether Data Integration bypasses retrieving and listing the IBM MQ queue names when you configure the source or target:</p> <ul style="list-style-type: none"> <li>- If you enable the option, Data Integration bypasses retrieving and listing the IBM MQ queue names. Instead, a placeholder queue name displays in the object list when you configure the source or target, and requires you to specify the queue name for the source or target in the advanced runtime properties in the mapping.</li> <li>- If you don't enable the option, Data Integration retrieves and displays all available IBM MQ queue names in the object list when you configure the source or target in the mapping.</li> </ul> <p>Default is disabled.</p>

## CHAPTER 96

# IDMS CDC connection properties

When you configure an IDMS CDC connection, you must set the connection properties.

The following table describes IDMS CDC connection properties:

Property	Description
Connection Name	A name for the IDMS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IDMS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For IDMS CDC, the type must be <b>IDMS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for IDMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains the capture registrations for the IDMS data sources. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.

Property	Description
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.  Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  CDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The IDMS event table must reside on the CDC source system.



Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="509 590 964 617">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPCC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="509 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 97

# IDMS connection properties

When you configure an IDMS connection, you must set the connection properties.

The following table describes IDMS connection properties:

Property	Description
Connection Name	A name for the IDMS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IDMS connection. Maximum length is 4000 characters.
Type	Type of connection. For IDMS, the type must be <b>IDMS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for IDMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  PWXMLSNR:14673
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the IDMS source.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.

Property	Description
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection property for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For IDMS data sources and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> property specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre data-bbox="500 1165 954 1192">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="500 1480 1396 1585" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the “Connection overrides reference” chapter.</p>
Write Properties > Write Mode	<p>Options are:</p> <ul data-bbox="500 1680 1404 1816" style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> <p>Default is <b>Confirm Write On</b>.</p>

## CHAPTER 98

# IMS CDC Connection Properties

When you configure an IMS CDC connection, you must set the connection properties.

The following table describes IMS CDC connection properties:

Property	Description
Connection Name	A name for the IMS CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IMS CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For IMS CDC, the type must be <b>IMS CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for IMS change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ADACDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The IMS instance that is specified in the <b>Database Instance</b> field of the registration group that contains the capture registrations for the IMS source. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.

Property	Description
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.  Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ADACDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an IMS table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 963 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXP) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 99

# IMS connection properties

When you configure an IMS connection, you must set the connection properties.

The following table describes the IMS connection properties:

Property	Description
Connection Name	A name for the IMS connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the IMS connection. Maximum length is 4000 characters.
Type	Type of connection. For IMS, the type must be <b>IMS</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for IMS runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example:  <code>PWXMLSNR:14673</code>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the IMS source.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source database.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.

Property	Description
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For IMS data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre>&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>
Write Properties	<p>Write Mode. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul> <p>Default is <b>Confirm Write On</b>.</p>



## CHAPTER 100

# JD Edwards EnterpriseOne connection properties

When you set up a JD Edwards EnterpriseOne connection, you must configure the connection properties.

The following table describes the JD Edwards EnterpriseOne connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Host Name	JD Edwards EnterpriseOne server host name.
Enterprise Port	JD Edwards EnterpriseOne server port number. Default is 6016.
User Name	The JD Edwards EnterpriseOne database user name.
Password	The password for the JD Edwards EnterpriseOne database user.
Environment	Name of the JD Edwards EnterpriseOne environment you want to connect to.
Role	Role of the JD Edwards EnterpriseOne user. Default is *ALL.
User Name	The JD Edwards EnterpriseOne database user name.
Password	Password for the database user.
Driver Class Name	<p>The driver class name that you can enter for the applicable database type. Required to write data in bulk with the interface table write option. Use the following JDBC driver class name:</p> <ul style="list-style-type: none"><li>- DataDirect JDBC driver class name for Oracle: <code>com.informatica.jdbc.oracle.OracleDriver</code></li><li>- DataDirect JDBC driver class name for IBM DB2: <code>com.informatica.jdbc.db2.DB2Driver</code></li><li>- DataDirect JDBC driver class name for Microsoft SQL Server: <code>com.informatica.jdbc.sqlserver.SQLServerDriver</code></li></ul> <p>For more information about which driver class to use with specific databases, see the vendor documentation.</p>

Property	Description
Connection String	<p>The connection string to connect to the database. Required to write data in bulk with the interface table write option.</p> <p>The JDBC connection string uses the following syntax:</p> <ul style="list-style-type: none"> <li>- For Oracle: jdbc:informatica:oracle://&lt;host name&gt;:&lt;port&gt;,ServiceName=&lt;db service name&gt;</li> <li>- For DB2: jdbc:informatica:db2://&lt;host name&gt;:&lt;port&gt;;databaseName=&lt;db name&gt;</li> <li>- For Microsoft SQL: jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port&gt;;databaseName=&lt;db name&gt;</li> </ul>
JDE Product Code	<p>The product code for the tables and views in JD Edwards EnterpriseOne.</p> <p><b>Note:</b> You must specify only the product code without the description. If you specify a schema that is not valid, a java exception appears.</p>

# CHAPTER 101

## JDBC connection properties

When you set up a JDBC connection, you must configure the connection properties.

**Important:** JDBC Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use JDBC V2 Connector to access data from a database with a JDBC type 4 driver.

The following table describes JDBC connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
JDBC Connection URL	The JDBC URL string to connect to the database. The format of the JDBC URL is: <code>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</code> , where subprotocol defines the database connectivity mechanism that one or more drivers might support. The contents and syntax of the subname depends on the subprotocol. For information about the formatting requirements for the JDBC URL connection string, see the JDBC driver vendor specific documentation.
JDBC Jar Directory	Optional. The path to the JDBC driver jar file. For example, you can enter the following directory: <code>C:/jdbc</code> . When you do not specify a directory path, the Secure Agent obtains the jar file from the directory that is specified in the CLASSPATH system variable. To use the serverless runtime environment for the JDBC connection, specify the following location: <code>/home/cldagnt/SystemAgent/serverless/configurations/jdbc</code>
JDBC Driver Class Name	Optional. Specify the JDBC driver class name if you are using a JDBC driver without auto class load feature. If you do not specify this property, the Secure Agent loads the driver class name from the JDBC jar file.
Schema	Schema name, which varies by database. For example, - Informix. Optional. The schema name is the database name. You must enter a schema name to fetch metadata if the JDBC connection URL does not provide enough context.
Username	User name to connect to the database.
Password	Password to connect to the database.

## CHAPTER 102

# JDBC V2 connection properties

Create a JDBC V2 connection to access data from Aurora PostgreSQL or any database that supports the Type 4 JDBC driver.

## Prerequisites

Before you create a JDBC V2 connection to read from or write to databases that support the JDBC Type 4 driver, complete the prerequisites.

### Install the Type 4 JDBC driver

To read from or write to JDBC V2 objects, you need to install the Type 4 JDBC driver on the Secure Agent machine.

1. Download the latest Type 4 JDBC driver version that your database supports from the third-party vendor site.  
If you want to use JDBC V2 Connector to connect to Aurora PostgreSQL, download the Aurora PostgreSQL driver. Informatica has certified Aurora PostgreSQL driver 42.2.6 for JDBC V2 Connector.
2. Install the Type 4 JDBC driver for the database on the Secure Agent machine and perform the following tasks:
  - a. Navigate to the following directory on the Secure Agent machine:  
`<Secure Agent installation directory>/ext/connectors/thirdparty/`
  - b. Create a folder and add the driver based on the type of mapping that you want to configure.  
For mappings, add the driver in the following folder:  
`informatica.jdbc_v2/common`  
For mappings in advanced mode, add the driver in the following folders:  
`informatica.jdbc_v2/common`  
`informatica.jdbc_v2/spark`
3. Restart the Secure Agent.  
If you update the driver on the Secure Agent machine while the mapping in advanced mode runs, you need to restart the Secure Agent.

# Connect to JDBC V2

Let's configure the JDBC V2 connection properties to connect to JDBC-compliant databases.

## Before you begin

Before you get started, you'll need to install the Type 4 JDBC driver on the Secure Agent machine to establish a JDBC V2 connection.

Check out ["Prerequisites" on page 320](#) to learn more about the configuration prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - ; Maximum length is 255 characters.
Description	
Type	JDBC V2
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment. Select a Secure Agent. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 324</a> .
JDBC Driver Class Name	Name of the JDBC driver class. For example, to connect to Aurora PostgreSQL, specify the following driver class name: org.postgresql.Driver For more information about which driver class to use with specific databases, see the corresponding third-party vendor documentation.

Property	Description
Connection String	<p>Connection string to connect to the database.</p> <p>Use the following format to specify the connection string: <code>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</code></p> <p>For example, the connection string for the Aurora PostgreSQL database type is <code>jdbc:postgresql://&lt;host&gt;:&lt;port&gt;[/dbname]</code>.</p> <p>For more information about the connection string to use with specific drivers, see the corresponding third-party vendor documentation.</p> <p>You can also connect to SSL-enabled Aurora PostgreSQL databases in mappings in advanced mode.</p> <p>For more information, see <a href="#">"Connect to SSL-enabled databases for mappings in advanced mode" on page 323</a>.</p>
User Name	The user name to connect to the database.
Password	The password to connect to the database.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Database Type	<p>The database type to which you want to connect.</p> <p>Select one of the following database types:</p> <ul style="list-style-type: none"> <li>- PostgreSQL. Connect to the Aurora PostgreSQL database hosted in the Amazon Web Services or the Microsoft Azure environment.</li> <li>- Azure SQL Database. Connect to Azure SQL Database hosted in the Microsoft Azure environment.</li> <li>- Others. Connect to any database that supports the Type 4 JDBC driver, such as Salesforce Data Cloud.</li> </ul> <p>Default is Others.</p>
Schema Name	<p>The schema name used for the JDBC object.</p> <p>If you don't specify the schema name, all the schemas available in the database are listed.</p> <p>To read from or write to Oracle public synonyms, enter PUBLIC.</p>
Connection Environment SQL	<p>The SQL statement to set up the database environment when you connect to a PostgreSQL database. The database environment applies for the entire session that uses this connection.</p> <p>For example, you can enter this statement to set the time zone:</p> <pre>SET timezone to 'America/New_York';</pre>
Additional Security Properties	<p>Masks sensitive and confidential data of the connection string that you don't want to display in the session log.</p> <p>Specify the part of the connection string that you want to mask.</p> <p>When you create a connection, the string you enter in this field appends to the string that you specified in the <b>Connection String</b> field.</p>
Enable Auto Commit <sup>1</sup>	<p>Specifies whether the driver supports connections to automatically commit data to the database when you run an SQL statement.</p> <p>When disabled, the driver does not support connections to automatically commit data even if the auto-commit mode is enabled in the JDBC driver.</p> <p>Default is disabled.</p>

Property	Description
Support Mixed-Case Identifiers	Indicates whether the database supports case-sensitive identifiers. When enabled, the Secure Agent encloses all identifiers within the character selected for the SQL Identifier Character property. Default is disabled.
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select <b>None</b> if the database uses regular identifiers. When the Secure Agent generates SQL queries, it does not place delimited characters around any identifiers. Select a character from the list based on what delimiter the database uses for identifiers. When the Secure Agent generates SQL queries, it encloses delimited identifiers within this character.
<sup>1</sup> Doesn't apply to mappings in advanced mode.	

## Connect to SSL-enabled databases for mappings in advanced mode

You can use JDBC V2 connection in mappings in advanced mode to connect to an SSL-enabled JDBC-complaint database. To run mappings in advanced mode with SSL-enabled JDBC-complaint databases, you need to download the SSL certificates to the Secure Agent machine, and then perform certain prerequisite tasks.

1. Specify the JDBC URL in the JDBC V2 connection properties.

To connect to an SSL-enabled Aurora PostgreSQL database, specify the following JDBC URL:

```
jdbc:postgresql://<host>:<port>/dbname?sslmode=verify-ca&sslrootcert=<Location of the SSL certificate on the Secure Agent machine>, where the values for sslmode supports verify-ca and verify-ca.
```

For example, `jdbc:postgresql://aurorapostgres-appsdk.abc.ap-south-1.rds.amazonaws.com:5432/JDBC_V2?sslmode=verify-full&sslrootcert=/data/home/qamercury/cloud_td/Aurora_cert/rds-combined-ca-bundle.pem`.

2. After you specify the JDBC URL in the JDBC V2 connection properties, in the advanced session properties of the mapping task, select **advanced.custom.property** as the session property name.
3. In the session property value, specify the following value:

```
Spark.NeedUserCredentialFileForAdapter=true&Spark.UserCredentialDirOnDIS=<Location of the SSL certificate on the Secure Agent machine>
```

- `Spark.NeedUserCredentialFileForAdapter`. When you set this property to true, the Secure Agent copies the SSL certificate from the Secure Agent machine to the advanced cluster.
- `Spark.UserCredentialDirOnDIS`. When you set this property to the location of the SSL certificates, the Secure Agent uses the specified location to get the SSL certificate.  
This property is optional. If you do not specify this property, the Secure Agent considers the following default location: `/infa/user/credentials`

# Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS or Azure to connect to JDBC-compliant databases.

Before you configure a JDBC V2 connection using the serverless runtime environment, perform the following tasks:

- Add the JDBC driver JAR files in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the .yml serverless configuration file.

## Add the JDBC driver JAR files in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to configure a JDBC V2 connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the JDBC driver files in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account:  
<Supplementary file location>/serverless\_agent\_config/common
3. For mappings in advanced mode, additionally add the JDBC driver files in the following location in the Amazon S3 bucket or Azure container:  
<Supplementary file location>/serverless\_agent\_config/spark

## Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment:

1. Copy the following code snippet to a text editor based on the mappings that you want to run in a serverless environment:

- For mappings that do not apply in advanced mode, add the following code snippet:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: common/<Driver_filename>
          - fileCopy:
              sourcePath: common/<Driver_filename>
```

- For mappings in advanced mode, add the following code snippet:

```
version: 1
agent:
  elasticServer:
    autoApply:
      jdbcv2:
        common:
          - fileCopy:
              sourcePath: common/<Driver_filename>
          - fileCopy:
              sourcePath: common/<Driver_filename>
        spark:
          - fileCopy:
              sourcePath: spark/<Driver_filename>
          - fileCopy:
              sourcePath: spark/<Driver_filename>
```

where the source path is the directory path of the driver files in AWS or Azure.



2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`  
When the `.yml` file runs, the JDBC driver files are copied from the AWS or Azure location to the serverless agent directory.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 103

# JIRA Cloud connection properties

When you set up a JIRA Cloud connection, you must configure the connection properties.

The following table describes the JIRA Cloud connection properties:

Connection property	Description
Connection Name	Name of the JIRA Cloud connection.
Description	Description of the JIRA Cloud connection.
Type	Type of connection. Select JiraCloud (Informatica) from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent.
Authentication	Authentication type for the connection. Select JiraCloud.
URI	The base JIRA URI of JIRA instance to connect. For example, <code>https://abcd.atlassian.net</code> .
Username	User name for the JIRA account.
Password	The API token for the JIRA account. For more information on how to create an API token, see <a href="https://kb.informatica.com/solution/23/Pages/70/576517.aspx">https://kb.informatica.com/solution/23/Pages/70/576517.aspx</a> .

# CHAPTER 104

## Jira connection properties

Create a JIRA connection to connect to JIRA so that you can read data from and write data to JIRA. You can use the JIRA connection to specify source or target objects in synchronization tasks, mappings, and mapping tasks.

### Connect to Jira

Let's configure the JIRA connection properties to connect to JIRA.

#### Before you begin

Before you configure a connection, you'll need to get the user name, password, and the base URL from your Jira account.

The following video shows you how to get the information you need:



#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Jira

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Hosted Agent doesn't apply to mappings in advanced mode.</p> <p>You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.</p>
Username	User name of the JIRA account.
Password	Password of the JIRA account.
URI	<p>The base URL of your Jira instance.</p> <p>For example, if your JIRA instance is hosted at mycompany.atlassian.net, the URI is https://mycompany.atlassian.net/.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
UTC Offset	<p>Appends the Coordinated Universal Time (UTC) to your datetime field to represent the time in your time zone.</p> <p>Select the UTC offset from the list based on your time zone.</p> <p>The adjustment to UTC yields the local time based on your region. UTC is expressed as UTC±, with a plus sign (+) that indicates time ahead of UTC and a minus sign (-) indicates time behind UTC. For instance, if your location is 5 hours ahead of UTC, select UTC+5. If your location is 3 hours behind UTC, select UTC-3.</p> <p>Default is UTC.</p>
Enable Logging	<p>Enables logging for the connector.</p> <p>Select the checkbox to enable logging when you create a connection, and use the connection to import metadata and run tasks.</p> <p>You can access the connection and design time logs in the Tomcat in the following location: &lt;Secure Agent installation directory&gt;\apps\Data_Integration_Server\logs\tomcat</p> <p>For the runtime logs, see the session log in the <b>My Jobs</b> page.</p>

## CHAPTER 105

# JMS connection properties

When you set up a JMS connection, you must configure the connection properties.

The following table describes the connection properties for the JMS connection:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identify the connection. The description cannot exceed 4,000 characters.
Type	The JMS connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Connection URL	URL of the JNDI naming provider. For example, in IBM MQ it is the directory location that contains the .bindings file.
JNDI User Name	Optional. User name to connect to the JNDI context factory.
JNDI Password	Optional. The password of the user account that you use to connect to the JNDI context factory.
JNDI Context Factory	The JMS provider specific initial JNDI context factory implementation for connecting to the JNDI service. This value is a fully qualified class name of the Initial Context Factory. For example, the class name of the Initial Context Factory for ActiveMQ is <code>org.apache.activemq.jndi.ActiveMQInitialContextFactory</code> For more information, see the documentation of the JMS provider.
JNDI Package Prefixes	A colon-delimited list of package prefixes to use when loading URL context factories. These are the package prefixes for the name of the factory class that will create a URL context factory. For more information about the values, see the documentation of the JMS provider.
JMS Connection Factory	The name of the object in the JNDI server that enables the JMS Client to create JMS connections. For example, <code>jms/QCF</code> or <code>jmsSalesSystem</code> .

Property	Description
JMS Connection User Name	Optional. User name to connect to the JMS connection factory.
JMS Connection Password	Optional. The password of the user account that you use to connect to the JMS connection factory.

**Note:** Ensure to copy the external JMS JAR files to the following location:

`<Secure_Agent_home>/ext/connectors/thirdparty/infa.jms`

After copying the external JMS JAR files, restart the Secure Agent.

## CHAPTER 106

# JSON Target connection properties

When you create a JSON Target connection, you must configure the connection properties.

**Important:** JSON Target Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the JSON Target connection properties:

Connection property	Description
Secure Agent	Select the appropriate Secure Agent from the list.
Sample JSON Schema Name	Enter sample JSON file path. For example, ABCD.JSON.
JSON Working Directory	Enter the folder path for JSON working directory.
Final JSON File Name	Enter final JSON file path with the file name.
Requires JSON Customization	Allows JSON customization. Default is <b>NO</b> .
Final Customized JSON File Name	Enter final customized JSON file path with the file name.

## CHAPTER 107

# Kafka connection properties

When you set up a Kafka connection, configure the connection properties.

The following table describes the Kafka connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive. It must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you use to identify the connection. The description cannot exceed 4,000 characters.
Type	The Kafka connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page in Administrator to install the connector.
Runtime Environment	Name of the runtime environment where you want to run tasks. Specify a Secure Agent or a serverless runtime environment for a mapping that runs on the advanced cluster.
Kafka Broker List	Comma-separated list of the Kafka brokers. To list a Kafka broker, use the following format: <code>&lt;HostName&gt;:&lt;PortNumber&gt;</code> <b>Note:</b> When you connect to a Kafka broker over SSL, you must specify the fully qualified domain name for the host name. Otherwise, the test connection fails with SSL handshake error.
Retry Timeout	Optional. Number of seconds after which the Secure Agent attempts to reconnect to the Kafka broker to read or write data. Default is 180 seconds. This property is not used by Database Ingestion and Replication. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b> .
Kafka Broker Version	Kafka message broker version. The only valid value is Apache 0.10.1.1 and above. Optional for a streaming ingestion and replication task.



Property	Description
Additional Connection Properties	<p>Optional. Comma-separated list of additional configuration properties of the Kafka producer or consumer.</p> <p>For a streaming ingestion and replication task, ensure that you set the <code>&lt;kerberos name&gt;</code> property if you configure <code>&lt;Security Protocol&gt;</code> as <code>SASL_PLAINTEXT</code> or <code>SASL_SSL</code>.</p> <p>For a database ingestion and replication task, if you want to specify a security protocol and properties, specify them here instead of in the <b>Additional Security Properties</b> property. For example: <code>security.protocol=SSL,ssl.truststore.location=/opt/kafka/config/kafka.truststore.jks,ssl.truststore.password=&lt;trustore_password&gt;</code>.</p>
Confluent Schema Registry URL	<p>Location and port of the Confluent schema registry service to access Avro sources and targets in Kafka.</p> <p>To list a schema registry URL, use the following format:</p> <pre>&lt;https&gt;://&lt;HostName or IP&gt;:&lt;PortNumber&gt;</pre> <p>or</p> <pre>&lt;http&gt;://&lt;HostName or IP&gt;:&lt;PortNumber&gt;</pre> <p>Example for the schema registry URL:</p> <pre>https://kafkarnd.informatica.com:8082</pre> <p>or</p> <pre>http://10.65.146.181:8084</pre> <p>Applies only when you import a Kafka topic in Avro format that uses the Confluent schema registry to store the metadata.</p> <p>This property is not used by Database Ingestion and Replication. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
SSL Mode	<p>Required. Determines the encryption type to use for the connection.</p> <p>You can choose a mode from the following SSL modes:</p> <ul style="list-style-type: none"> <li>- Disabled. Establishes an unencrypted connection to the Kafka broker.</li> <li>- One-way. Establishes an encrypted connection to the Kafka broker using truststore file and truststore password.</li> <li>- Two-way. Establishes an encrypted connection to the Kafka broker using truststore file, truststore password, keystore file, and keystore password.</li> </ul> <p>This property is not used by Database Ingestion and Replication. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b>.</p>
SSL TrustStore File Path	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Absolute path and file name of the SSL truststore file that contains the SSL certificate to connect to the Kafka broker.</p>
SSL TrustStore Password	<p>Required when you use the one-way or two-way SSL mode.</p> <p>Password for the SSL truststore.</p>
SSL KeyStore File Path	<p>Required when you use the two-way SSL mode.</p> <p>Absolute path and file name of the SSL keystore file that contains private keys and certificates to connect to the Kafka broker.</p>

Property	Description
SSL KeyStore Password	Required when you use the two-way SSL mode. Password for the SSL keystore.
Additional Security Properties	Optional. Comma-separated list of additional configuration properties to connect to the Kafka broker in a secure way. If you specify two different values for the same property in <b>Additional Connection Properties</b> and <b>Additional Security Properties</b> , the value in <b>Additional Security Properties</b> overrides the value in <b>Additional Connection Properties</b> . This property is not used by Database Ingestion and Replication. You can specify a security protocol and properties in <b>Additional Connection Properties</b> .

### Schema Registry Security Configuration Properties

When you configure the **Schema Registry URL** connection property, you can configure the schema registry security configuration properties. These properties apply only to mappings in advanced mode. You can configure one-way SSL, two-way SSL, and basic authentication to connect to the Confluent schema registry in a secure way.

The following table describes the security properties for the Kafka connection when you use the Confluent schema registry:

Property	Description
SSL Mode Schema Registry <sup>1</sup>	Required. Determines the encryption type to use for the connection. You can choose a mode from the following SSL modes: <ul style="list-style-type: none"> <li>- Disabled. Establishes an unencrypted connection to the Confluent schema registry.</li> <li>- One-way. Establishes an encrypted connection to the Confluent schema registry using truststore file and truststore password.</li> <li>- Two-way. Establishes an encrypted connection to the Confluent schema registry using truststore file, truststore password, keystore file, and keystore password.</li> </ul> This property is not used by Database Ingestion and Replication. You can specify an equivalent Kafka property in <b>Additional Connection Properties</b> .
SSL TrustStore File Path Schema Registry <sup>1</sup>	Required when you use the one-way or two-way SSL mode. Absolute path and file name of the SSL truststore file that contains the SSL certificate to connect to the Confluent schema registry.
SSL TrustStore Password Schema Registry <sup>1</sup>	Required when you use the one-way or two-way SSL mode. Password for the SSL truststore.
SSL KeyStore File Path Schema Registry <sup>1</sup>	Required when you use the two-way SSL mode. Absolute path and file name of the SSL keystore file that contains private keys and certificates to connect to the Confluent schema registry.

Property	Description
SSL KeyStore Password Schema Registry <sup>1</sup>	<p>Required when you use the two-way SSL mode.</p> <p>Password for the SSL keystore.</p>
Additional Security Properties Schema Registry <sup>2</sup>	<p>Optional. Comma-separated list of additional security properties to connect to the Confluent schema registry in a secure way.</p> <p>For example, when you configure basic authentication to establish a secure communication with Confluent schema registry, specify the following value:</p> <pre data-bbox="456 611 1463 636">basic.auth.credentials.source=USER_INFO,basic.auth.user.info=&lt;username&gt;:&lt;password&gt;</pre> <p>If you specify two different values for the same property in <b>Additional Connection Properties</b> and <b>Additional Security Properties Schema Registry</b>, the value in <b>Additional Security Properties Schema Registry</b> overrides the value in <b>Additional Connection Properties</b>.</p> <p>This property is not used by Database Ingestion and Replication.</p>
<p><sup>1</sup> Applies only to mappings in advanced mode.</p> <p><sup>2</sup> Applies to both mappings and mappings in advanced mode.</p>	

## CHAPTER 108

# Klaviyo connection properties

When you create a Klaviyo connection, configure the connection properties.

**Important:** Effective in the November 2024 release, Klaviyo Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Klaviyo connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Klaviyo
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent or a Hosted Agent.
Private API Key	Klaviyo private API key to authenticate access to the Klaviyo account. For more information about the private key, see the Klaviyo documentation.

## CHAPTER 109

# LDAP connection properties

When you set up an LDAP connection, you must configure the connection properties.

The following table describes the LDAP connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks. <b>Note:</b> You can specify only the Secure Agent as the run-time environment for an LDAP connection.
Host Name	Required. LDAP directory server host name. You can use the LDAP or LDAPS protocol to connect to LDAP Server. - To use the LDAP protocol, use one of the following formats: - ldap://<hostname> - <hostname> - To use the LDAPS protocol, use the ldaps://<hostname> format. <b>Note:</b> If you use SSL, use the host name that you specify in the SSL certificate.
Port	Required. LDAP directory server port number. Default is 389.
Anonymous Connection	Establishes an anonymous connection with the LDAP directory server. Select anonymous connection to access a directory server as an anonymous user without authentication. <b>Note:</b> You cannot establish an anonymous connection with Active Directory.
User Name	The LDAP user name to connect to the LDAP directory server. Required if you want to connect to Active Directory.
Password	The password to connect to the LDAP directory server. If you do not enter the password, the Client establishes an anonymous connection. Required if you want to connect to Active Directory.
Secure Connection	Establishes a secure connection with the LDAP directory server through the TLS protocol.
TrustStore File Name	The file name of the truststore that contains the TLS certificate to establish a one-way secure connection with the LDAP directory server. Contact the LDAP Administrator for the truststore file name and password.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Name	The file name of the keystore that contains the keys and certificates required to establish a two-way secure communication with the LDAP directory server. Contact the LDAP Administrator for the keystore file name and password.

<b>Property</b>	<b>Description</b>
KeyStore Password	The password for the keystore file required for secure communication.
Base DN	<p>Required. The distinguished name (DN) of the root directory in the LDAP directory server.</p> <p>For example, use the following base DN to connect to the Informatica domain: dc=informatica-connector,dc=com</p> <p>If you do not specify the base DN, the Secure Agent fails to fetch the metadata.</p>

## CHAPTER 110

# Magento V1 connection properties

When you create a Magento V1 connection, configure the connection properties.

You can use the following authentication methods to connect to Magento:

- Token. Uses the Magento account user name, password, and store URL to connect to Magento.
- OAuth 1.0. Uses the OAuth 1.0 protocol with the store URL, consumer key, consumer secret, access token, and token secret to connect to Magento.

## CHAPTER 111

# Mailchimp connection properties

When you create a Mailchimp connection, configure the connection properties.

The following table describes the Mailchimp connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Mailchimp
Runtime Environment	The name of the runtime environment where you want to run tasks. You can specify a Secure Agent or a Hosted Agent.
Server Prefix	The server parameter in the URL that corresponds to the data center for the Mailchimp account. For example, in <https://us19.admin.mailchimp.com>, us19 is the server prefix.
API Key	Mailchimp API key to authenticate access to the account. The role of the user who generates the API key determines the access to each Mailchimp endpoint.



# CHAPTER 112

## Marketo V3 connection properties

Create a Marketo V3 connection to securely read data from or write data to Marketo.

### Connect to Marketo

Let's configure the Marketo V3 connection properties to connect to Marketo.

#### Before you begin

Before you configure a connection, create an API user and associate it with an API role to grant access permissions for the Marketo REST APIs. You also need to get the client ID, client secret, and REST API URL from your Marketo account to authenticate the Marketo custom service.

For more information on how to create an API user and generate the client ID and client secret, see [Custom Services](#) in the Marketo documentation.

The following video shows you how to get the information you need:



#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Marketo V3

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure agent, Hosted Agent, or serverless runtime environment.</p>
Client ID	<p>The client ID of the Marketo service.</p> <p>You need the client ID to generate an access token to authenticate access to the Marketo service.</p>
Client Secret	<p>The client secret of the Marketo service.</p>
REST API URL	<p>The URL to connect to the Marketo REST APIs.</p> <p>Enter the URL in the following format: https://&lt;Host name of the Marketo Rest API Server&gt;</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
grant_type	<p>The access permissions for an administrator to invoke the Marketo REST APIs to read from and write to Marketo.</p> <p>Enter client_credentials as the grant type. If you don't specify the grant type, an error occurs and the connection fails.</p>
Bypass Proxy	<p>Determines if the Secure Agent uses the proxy server settings defined in the proxy.ini file or the Secure Agent Manager to connect to Marketo.</p> <p>When you select Bypass Proxy, you connect to Marketo using the Secure Agent Manager. If you don't select Bypass Proxy, you connect to Marketo using the proxy server.</p> <p>Default is enabled.</p> <p><b>Note:</b> This property doesn't apply to connections configured for application ingestion tasks.</p>

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux.

You can use the unauthenticated or authenticated proxy server. You can configure proxy for connections used both in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To bypass the proxy server settings defined for the Secure Agent, select Bypass Proxy in the advanced settings for the connection.

## CHAPTER 113

# Microsoft Access connection properties

When you set up a Microsoft Access connection, you must configure the connection properties.

The following table describes the connection properties:

Connection property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Data Source Name	System DSN name.
Code Page	The code page compatible with the Microsoft Access source. Select one of the following code pages: <ul style="list-style-type: none"><li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li><li>- UTF-8. Select for Unicode and non-Unicode data.</li><li>- Shift-JIS. Select for double-byte character data.</li><li>- ISO 8859-15 Latin 9 (Western European).</li><li>- ISO 8859-2 Eastern European.</li><li>- ISO 8859-3 Southeast European.</li><li>- ISO 8859-5 Cyrillic.</li><li>- ISO 8859-9 Latin 5 (Turkish).</li><li>- IBM EBCDIC International Latin-1.</li></ul>

## CHAPTER 114

# Microsoft Azure Blob Storage connection properties

When you create a Microsoft Azure Blob Storage connection, you must configure the connection properties.

**Important:** Microsoft Azure Blob Storage Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Microsoft Azure Blob Storage V3 Connector to access Microsoft Azure Blob Storage.

The following table describes Microsoft Azure Blob Storage connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Account Name	Microsoft Azure Blob Storage account name.
Account Key	Microsoft Azure Blob Storage access key.
Container Name	Microsoft Azure Blob Storage container name.
File Delimiter	Character used to separate fields in the file. Default is a comma (,).

# Microsoft Azure Blob Storage V2 connection properties

When you create a Microsoft Azure Blob Storage V2 connection, you must configure the connection properties.

**Important:** Microsoft Azure Blob Storage V2 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Microsoft Azure Blob Storage V3 Connector to access Microsoft Azure Blob Storage.

The following table describes Microsoft Azure Blob Storage V2 connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Account Name	Microsoft Azure Blob Storage account name.
Account Key	Microsoft Azure Blob Storage access key.
Container Name	Microsoft Azure Blob Storage container name.

## CHAPTER 116

# Microsoft Azure Blob Storage V3 connection properties

Create a Microsoft Azure Blob Storage V3 connection to securely read data from or write data to Microsoft Azure Blob Storage.

## Prepare for authentication

You can use shared key authentication or shared access signature authentication in the Microsoft Azure Blob Storage V3 connection to connect to Microsoft Azure Blob Storage.

Before you configure authentication, create a storage account to use with Microsoft Azure Blob Storage and create a blob container in the storage account. For more information on how to create a storage account and a blob container, see the [Prerequisites to create a Microsoft Azure Blob Storage V3 connection](#) Informatica How-To Library article.

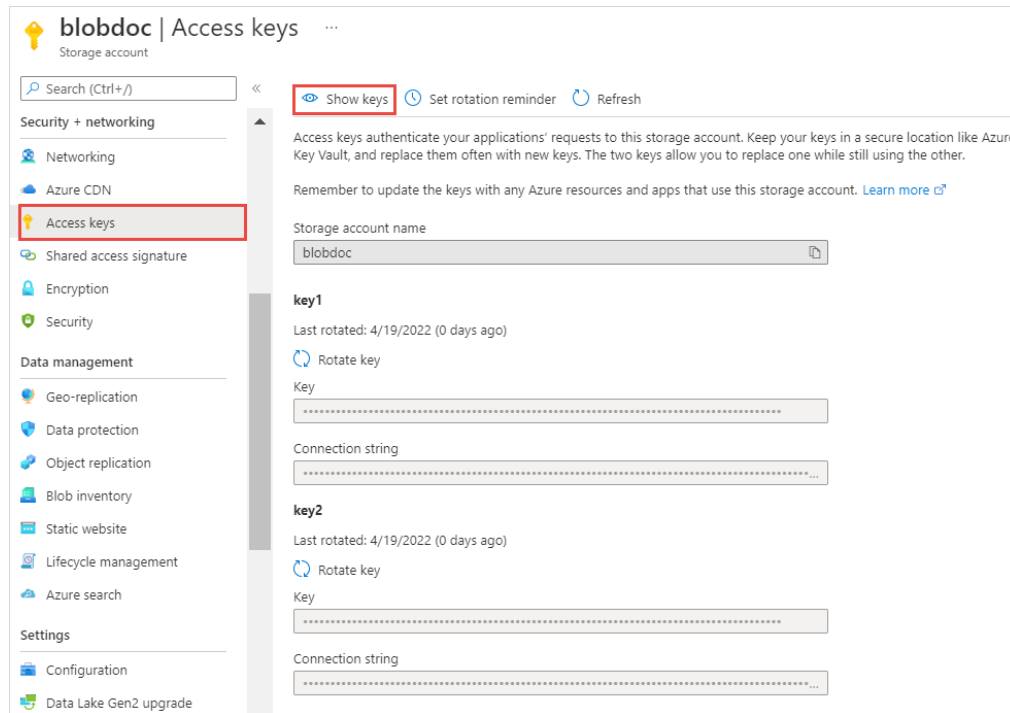
Before you configure the connection properties, you also need to keep the authentication details handy based on the authentication type that you want to use.

## Shared key authentication

To connect to Microsoft Azure Blob Storage using shared key authentication, you need the storage account name and account key.

1. Open the storage account.
2. Under **Security + Networking**, click **Access keys**.

3. Click **Show keys**.



4. Make a note of the storage account name and account key. You can use key1 or key2.

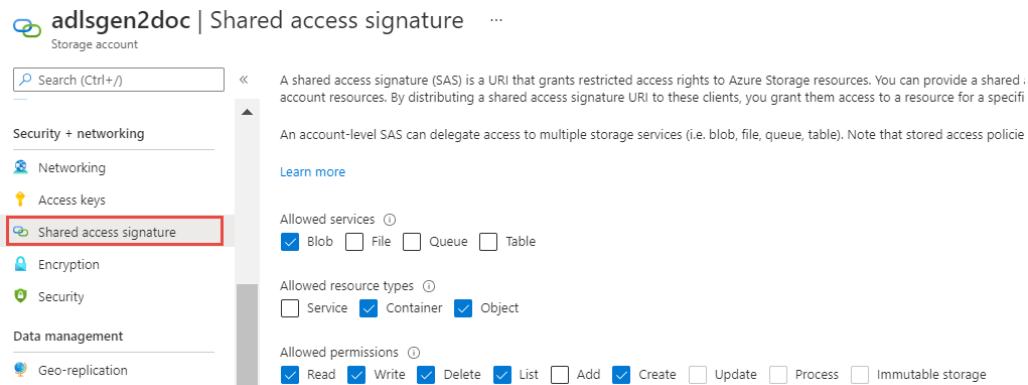
## Shared access signature

To connect to Microsoft Azure Blob Storage using shared access signature, you need to configure the minimum permissions for shared access signature authentication and generate the SAS token in the Azure portal.

You can generate the SAS token for the storage account or for the container.

- To generate the SAS token for the storage account, on the Azure portal, go to **Security + Networking**, and click **Shared access signature**.

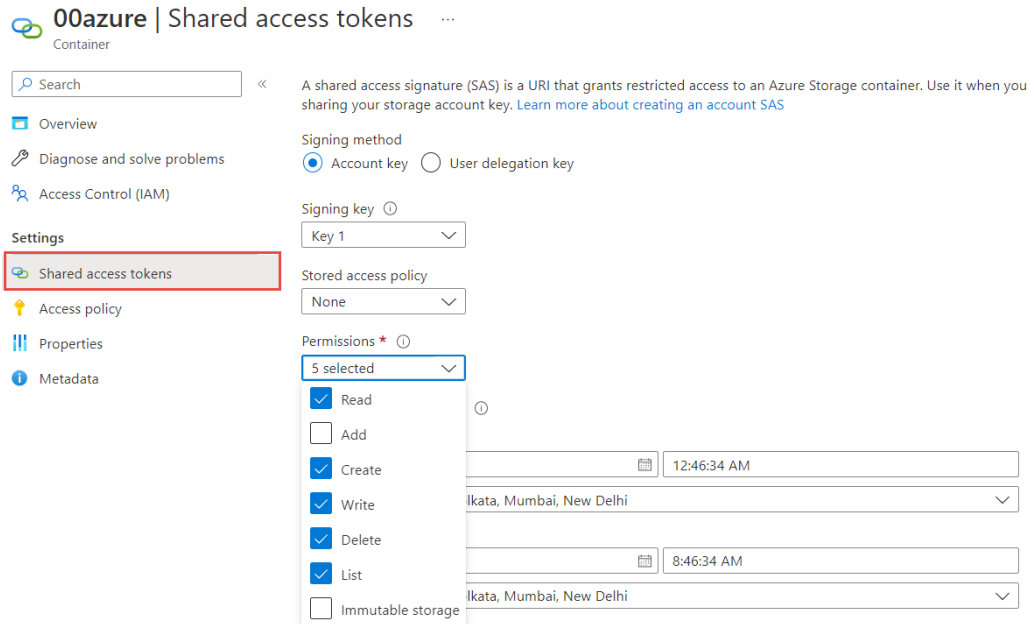
Select the minimum permissions required for shared access signature authentication, as shown in the following image:





- To generate the SAS token for the Blob container, go to **Settings** of the container, and click **Shared access tokens**. You can use either the Account key or User delegation key signing method. If you use the User delegation key signing method, ensure that you have the **Storage Blob Data Owner** role for the container or the storage account.

Select the minimum permissions required for shared access signature authentication, as shown in the following image:



## Connect to Microsoft Azure Blob Storage V3

Let's configure the Microsoft Azure Blob Storage V3 connection properties to connect to Microsoft Azure Blob Storage.

### Before you begin

Before you get started, you'll need to get the blob container name and type of Azure endpoint from your storage account. You also need to get information from your Microsoft Azure Blob Storage account based on the authentication type that you want to configure.

To use shared key authentication, you need the storage account name and account key. To use shared access signature authentication, you need the shared access signature token from the Azure portal.

Check out [“Prepare for authentication” on page 347](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Azure Blob Storage V3
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Account Name	Microsoft Azure Blob Storage account name.

## Authentication types

You can configure shared key authentication and shared access signature authentication types to access Microsoft Azure Blob Storage.

Select the required authentication method and then configure the authentication-specific parameters.

### Shared key authentication

Shared key authentication uses the storage account name and account key to connect to Microsoft Azure Blob Storage.

The following table describes the connection properties for shared key authentication:

Property	Description
Account Key	The account key for the Microsoft Azure Blob Storage account.
Container Name	The name of the blob container in the Microsoft Azure Blob Storage account.
Endpoint Suffix	Types of Microsoft Azure endpoints. Select one of the following options: <ul style="list-style-type: none"><li>- core.windows.net. Connects to Azure endpoints.</li><li>- core.usgovcloudapi.net. Connects to Azure Government endpoints.</li><li>- core.chinacloudapi.cn. Not applicable.</li></ul> Default is core.windows.net.

## Shared access signature authentication

Shared access signature authentication uses the SAS token to connect to Microsoft Azure Blob Storage. Use the SAS token to grant access to the resources in the storage account or container for a specific time range without sharing the account key.

**Note:** The file ingestion task fails if this option is on a container level and if you use a different container.

The following table describes the connection properties for shared access signature authentication:

Property	Description
SAS Token	The shared access signature token generated in the Azure portal to authenticate successfully and gain access to the Microsoft Azure Blob Storage resources.
Container Name	The name of the blob container in the Microsoft Azure Blob Storage account.
Endpoint Suffix	Types of Microsoft Azure endpoints. Select one of the following options: <ul style="list-style-type: none"><li>- core.windows.net. Connects to Azure endpoints.</li><li>- core.usgovcloudapi.net. Connects to Azure Government endpoints.</li><li>- core.chinacloudapi.cn. Not applicable.</li></ul> Default is core.windows.net.

## Proxy Server Settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated proxy server that requires only the host and port address for configuration.

To configure proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.  
For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure proxy server through the JVM options. To do this, perform the following steps:
  1. Log in to Informatica Intelligent Cloud Services.
  2. Open Administrator and select **Runtime Environments**.
  3. Select the Secure Agent for which you want to configure the proxy server.
  4. On the upper-right corner of the page, click **Edit**.
  5. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Service.
  6. Add the following parameters in any **JVMOption** field and specify appropriate values for each parameter:

Parameter	Description
-DproxyEnabled=	Required. Set the value to true to enable proxy server.
-Dhttp.proxyHost=	Required. Host name of the outgoing HTTP proxy server.
-Dhttp.proxyPort=	Required. Port number of the outgoing HTTP proxy server.

Example for HTTP:

```
JVMOption1=-DproxyEnabled=true
```

```
JVMOption2=-Dhttp.proxyHost=<proxy_server_hostname>
```

```
JVMOption3=-Dhttp.proxyPort=8081
```

7. Click **Save**.  
The Secure Agent restarts to apply the settings.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 117

# Microsoft Azure Cosmos DB SQL API connection properties

Create a Microsoft Azure Cosmos DB SQL API connection to securely read data from or write data to Microsoft Azure Cosmos DB SQL API.

## Connect to Microsoft Azure Cosmos DB SQL API

Let's configure the Microsoft Azure Cosmos DB SQL API connection properties to connect to Microsoft Azure Cosmos DB SQL API.

### Before you begin

Before you configure the connection properties, you'll need to get the Cosmos DB URI, database name, and key values from your Microsoft Azure Cosmos DB SQL API account. You can find the key details on the **Keys** tab of your Microsoft Azure Cosmos DB SQL API settings.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Microsoft Azure Cosmos DB SQL API

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Do not use a Hosted Agent if you use the connection in mappings in advanced mode.</p>
Cosmos DB URI	<p>The URI to access the Microsoft Azure Cosmos DB account.</p>
Key	<p>The primary or secondary key that grants you complete administrative access to the resources in the Microsoft Azure Cosmos DB account.</p>
Database	<p>Name of the database that contains the container from which you want to read or write JSON documents.</p>

## CHAPTER 118

# Microsoft Azure Data Lake Storage Gen2 connection properties

Create a Microsoft Azure Data Lake Storage Gen2 connection to securely read data from or write to Microsoft Azure Data Lake Storage Gen2.

## Prepare for authentication

You can configure Shared Key, Managed Identity, and Service Principal authentication types to access Microsoft Azure Data Lake Storage Gen2.

Before you configure the authentication, you must create a storage account to use with Microsoft Azure Data Lake Storage Gen2 and create a blob container in the storage account. You can use role-based access control or access control lists to authorize the users to access the resources in the storage account.

You must also register an application in Azure Active Directory to authenticate users to access the Microsoft Azure Data Lake Storage Gen2 account. You can use role-based access control or access control lists to authorize the application.

You must also create an Azure Active Directory web application for service-to-service authentication with Microsoft Azure Data Lake Storage Gen2 and ensure that you have superuser privileges to access the folders or files created in the application.

For more information about these prerequisite tasks, see the Informatica How-To Library article, [Prerequisites to create a Microsoft Azure Data Lake Storage Gen2 connection](#).

After you complete the prerequisite tasks, you need to keep the authentication details handy based on the authentication type that you want to use:

- To use service principal authentication, you need the client ID, client secret, and tenant ID for your application registered in the Azure Active Directory.
- To use shared key authentication, you need the account key for the Microsoft Azure Data Lake Storage Gen2 account.
- To use managed identity authentication, you need the client ID or application ID for your application registered in the Azure Active Directory. Before you get the client ID or application ID, be sure to complete certain prerequisites.

## Managed identity authentication

Managed Identity authentication uses managed identities in Azure Active Directory to authenticate and authorize access to Azure resources securely.

Before you use managed identity authentication to connect to Microsoft Azure Data Lake Storage Gen2, be sure to complete certain prerequisites.

1. Create an Azure virtual machine.
2. Install the Secure Agent on the Azure virtual machine.
3. Enable system assigned identity or user assigned identity for the Azure virtual machine.  
If you enable both and do not specify the client ID, the system assigned identity is used for authentication.
4. After you add or remove a managed identity, restart the Azure virtual machine.

## Connect to Microsoft Azure Data Lake Storage Gen2

Let's configure the Microsoft Azure Data Lake Storage Gen2 connection properties to connect to Microsoft Azure Data Lake Storage Gen2.

### Before you begin

Before you get started, you'll need to get information from your Microsoft Azure Data Lake Storage Gen2 account based on the authentication type that you want to configure.

Check out ["Prepare for authentication" on page 355](#) to learn more about the authentication prerequisites.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Azure Data Lake Storage Gen2



Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Do not use a Hosted Agent if you use the connection in mappings in advanced mode.</p> <p>You cannot run a database ingestion or streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>
Account Name	Microsoft Azure Data Lake Storage Gen2 account name or the service name.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.
Directory Path	<p>The path of a directory without the file system name.</p> <p>You can select from the following directory structures:</p> <ul style="list-style-type: none"> <li>- / for root directory</li> <li>- /dir1</li> <li>- dir1/dir2</li> </ul> <p>Default is /.</p>

## Authentication types

You can select service principal authentication, shared key authentication, and managed identity authentication to access the Microsoft Azure Data Lake Storage Gen2 account.

**Note:** Data Ingestion and Replication supports managed identity authentication. However, Streaming Ingestion and Replication does not support shared key authentication or managed identity authentication.

Select your preferred authentication type and then configure the authentication-specific parameters.

### Service principal authentication

Service principal authentication uses the client ID, client secret, and tenant ID to connect to Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for service principal authentication:

Property	Description
Client ID	The client ID of your application. Specify the client ID for your application registered in the Azure Active Directory.
Client Secret	The client secret key generated for the client ID. Specify the client secret key to complete the OAuth authentication in the Azure Active Directory.
Tenant ID	The directory ID of the Azure Active Directory.
Endpoint Suffix	The type of Microsoft Azure endpoints. Select one of the following endpoints: <ul style="list-style-type: none"> <li>- core.windows.net. Connects to Azure endpoints.</li> <li>- core.usgovcloudapi.net. Connects to US government Microsoft Azure Data Lake storage Gen2 endpoints.</li> <li>- core.chinacloudapi.cn. Connects to Microsoft Azure Data Lake storage Gen2 endpoints in the China region.</li> </ul> Default is core.windows.net. <b>Note:</b> You cannot configure the Azure Government endpoints for mappings in advanced mode.

## Shared key authentication

Shared key authentication uses the account key to connect to Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for shared key authentication:

Property	Description
Account Key	The account key for the Microsoft Azure Data Lake Storage Gen2 account.
Endpoint Suffix	The type of Microsoft Azure endpoints. Select one of the following endpoints: <ul style="list-style-type: none"> <li>- core.windows.net. Connects to Azure endpoints.</li> <li>- core.usgovcloudapi.net. Connects to US government Microsoft Azure Data Lake storage Gen2 endpoints.</li> <li>- core.chinacloudapi.cn. Connects to Microsoft Azure Data Lake storage Gen2 endpoints in the China region.</li> </ul> Default is core.windows.net. <b>Note:</b> You cannot configure the Azure Government endpoints for mappings in advanced mode.

## Managed identity authentication

Managed identity authentication authenticates using identities that are assigned to applications in Azure to access Azure resources in Microsoft Azure Data Lake Storage Gen2.

When you create a Microsoft Azure Data Lake Storage Gen2 connection, select the Azure virtual machine on which you have installed the Secure Agent. If you enable system assigned identity, assign the required role or permissions to the Azure virtual machine to run the mappings and tasks. If you enable user assigned identity, assign the required role or permissions to the user assigned identity. For example, if you use role-based access control, assign the Storage Blob Data Contributor role and if you use access control lists, assign the read, write, and execute permissions.

The following table describes the basic connection properties for managed identity authentication:

Property	Description
Client ID	The client ID of your application. To use managed identity authentication, specify the client ID for the user-assigned managed identity. Leave the field blank in the following scenarios: <ul style="list-style-type: none"><li>- If the permission is provided by system-assigned managed identity.</li><li>- If there is no system-assigned identity but only a single user-assigned managed identity.</li></ul>
Endpoint Suffix	The type of Microsoft Azure endpoints. Select one of the following endpoints: <ul style="list-style-type: none"><li>- core.windows.net. Connects to Azure endpoints.</li><li>- core.usgovcloudapi.net. Connects to US government Microsoft Azure Data Lake storage Gen2 endpoints.</li><li>- core.chinacloudapi.cn. Connects to Microsoft Azure Data Lake storage Gen2 endpoints in the China region.</li></ul> Default is core.windows.net. <b>Note:</b> You cannot configure the Azure Government endpoints for mappings in advanced mode.

## Proxy Server Settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server.

**Note:** You cannot use a proxy server with managed identity authentication.

You can use one of the following types of proxy servers:

- Unauthenticated proxy - Requires only the host and port address for configuration.
- Authenticated proxy - Requires the host address, port address, user name, and password for configuration.

To configure proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.  
For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Bypass the proxy server

You can bypass the proxy server settings configured for the Secure Agent.

Perform the following steps to bypass the proxy server:

1. Navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

2. Specify the following command in the `proxy.ini` file:

```
InfaAgent.NonProxyHost=localhost|{*}core.windows.net|127.0.0.1|[\:\<:1]*
```

To bypass proxy server for service principal authentication, append `login.microsoftonline.com` to the command.

To bypass proxy server for managed identity authentication, append `169.254.169.254` to the command.

For example,

```
InfaAgent.NonProxyHost=localhost|127.0.0.1|[\:\<:1]|<accountname>.blob.core.windows.net|  
<accountname>.dfs.core.windows.net|<accountname>.blob.core.windows.net|  
login.microsoftonline.com|169.254.169.254
```

3. Restart the Secure Agent.

## CHAPTER 119

# Microsoft Azure DocumentDB Connection Properties

When you set up a Microsoft Azure DocumentDB connection, you must configure the connection properties.

**Important:** Microsoft Azure DocumentDB is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Microsoft Azure Cosmos DB SQL API Connector to access Microsoft Azure DocumentDB.

The following table describes Microsoft Azure DocumentDB connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
DocumentDB URI	The URI of Microsoft Azure DocumentDB account.
Key	The primary and secondary key to which provides you complete administrative access to the resources within Microsoft Azure DocumentDB account.
Database	Name of the database that contains the collections from which you want to read or write JSON documents.

## CHAPTER 120

# Microsoft Azure Event Hub connection properties

When you set up an Azure Event Hub connection, you must configure the connection properties.

The following table describes the Azure Event Hub connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive. It must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you use to identify the connection. The description cannot exceed 4,000 characters.
Type	The Azure Event Hub connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page in Administrator to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Tenant ID	The ID of the tenant that the data belongs to. This ID is the Directory ID of the Azure Active Directory.
Subscription ID	The ID of the Azure subscription.
Resource Group Name	The name of the Azure resource group associated with the Event Hub namespace.
Client Application ID	The ID of the application created under the Azure Active Directory.
Client Secret Key	The secret key generated for the application.
Event Hub Namespace	The name of the Event Hub namespace that is associated with the resource group name.

<b>Property</b>	<b>Description</b>
Shared Access Policy Name	Optional. The name of the Event Hub Namespace Shared Access Policy. The policy must apply to all data objects that are associated with this connection. To read from Event Hubs, you must have Listen permission. To write to an Event Hub, the policy must have Send permission.
Shared Access Policy Primary Key	Optional. The primary key of the Event Hub Namespace Shared Access Policy.

## CHAPTER 121

# Microsoft Azure SQL Data Warehouse - Database Ingestion connection properties

When you define a Microsoft Azure SQL Data Warehouse Database Ingestion connection, you must configure connection properties. You can use this connection type in database ingestion tasks, which you configure in the Mass Ingestion service.

**Note:** Some properties are for Microsoft Azure Data Lake Storage Gen1. Database Ingestion and Replication uses Microsoft Azure Data Lake Storage Gen1 to stage data in files before sending the data to the Microsoft Azure SQL Database Warehouse target tables.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that you select the type for Microsoft Azure SQL Data Warehouse - Database Ingestion.
Runtime Environment	The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.
Azure DW JDBC URL	The Microsoft Azure SQL Data Warehouse JDBC connection string. Example connection string for Microsoft SQL Server authentication: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database</code> Example connection string for Azure Active Directory (AAD) authentication: <code>jdbc:sqlserver://server.database.windows.net:1433; database=database;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</code> <b>Note:</b> The default authentication type is Microsoft SQL Server authentication.



Property	Description
Azure DW JDBC Username	The user name to use for connecting to the Microsoft Azure SQL Data Warehouse account. Provide the AAD user name for AAD authentication.
Azure DW JDBC Password	The password to use for connecting to the Microsoft Azure SQL Data Warehouse account.
Azure DW Schema Name	The name of the schema in the Microsoft Azure SQL Data Warehouse target.
ADLS Account Name	The name of the Microsoft Azure Data Lake Storage Gen1 account.
Client Id	The ID of your client application for completing the OAuth Authentication in the Active Directory.
Client Secret	The client secret key for completing the OAuth Authentication in the Active Directory.
Directory	A Microsoft Azure Data Lake Storage Gen1 directory that Mass Ingestion Databases uses to stage data in files. The default is the root directory.
AuthEndpoint	The OAuth 2.0 token endpoint from where authentication based on the client ID and Client secret is completed.

## CHAPTER 122

# Microsoft Azure SQL Data Warehouse connection properties

The following table describes Microsoft Azure SQL Data Warehouse connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Azure DW JDBC URL	Microsoft Azure Data Warehouse JDBC connection string. For example, you can enter the following connection string: <code>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433;database=&lt;Database&gt;</code>
Azure DW JDBC Username	User name to connect to the Microsoft Azure SQL Data Warehouse account.
Azure DW JDBC Password	Password to connect to the Microsoft Azure SQL Data Warehouse account.
Azure DW Schema Name	Name of the schema in Microsoft Azure SQL Data Warehouse.
Azure Blob Account Name	Name of the Microsoft Azure Storage account to stage the files.
Azure Blob Account Key	Microsoft Azure Storage access key to stage the files.

## CHAPTER 123

# Microsoft Azure SQL Data Warehouse V2 connection properties

The following table describes Microsoft Azure SQL Data Warehouse V2 connection properties:

**Important:** Microsoft Azure SQL Data Warehouse V2 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Microsoft Azure Synapse SQL Connector to access Microsoft Azure SQL Data Warehouse.

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Azure DW JDBC URL	Microsoft Azure Data Warehouse JDBC connection string. Example for Microsoft SQL Server authentication: <code>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433;database=&lt;Database&gt;</code> Example for Azure Active Directory (AAD) authentication: <code>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433;database=&lt;Database&gt;;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;</code> The default authentication is Microsoft SQL Server authentication.
Azure DW JDBC Username	User name to connect to the Microsoft Azure SQL Data Warehouse account. Provide AAD user name for AAD authentication.
Azure DW JDBC Password	Password to connect to the Microsoft Azure SQL Data Warehouse account.
Azure DW Schema Name	Name of the schema in Microsoft Azure SQL Data Warehouse.
Azure Blob Account Name	Name of the Microsoft Azure Storage account to stage the files.
Azure Blob Account Key	Microsoft Azure Storage access key to stage the files.

## CHAPTER 124

# Microsoft Azure Synapse Analytics Database Ingestion connection properties

When you define a Microsoft Azure Synapse Analytics Database Ingestion connection, you must configure connection properties. You can use this connection type in application ingestion and replication tasks and database ingestion and replication tasks, which you configure in the Data Ingestion and Replication service.

**Note:** Some properties are for Microsoft Azure Data Lake Storage Gen2. Application Ingestion and Replication and Database Ingestion and Replication use Microsoft Azure Data Lake Storage Gen2 to stage data in files before sending the data to the Microsoft Azure Synapse Analytics target tables.

The following table describes the connection properties:

Property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Ensure that the type is <b>Microsoft Azure Synapse Analytics Database Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run the application ingestion and replication tasks or database ingestion and replication tasks. You define runtime environments in Administrator. <b>Note:</b> You cannot run application ingestion and replication tasks or database ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Azure Synapse Analytics JDBC URL	The Microsoft Azure Synapse Analytics (formerly SQL Data Warehouse) JDBC connection string. Example connection string for Microsoft SQL Server authentication: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database</code> Example connection string for Azure Active Directory (AAD) authentication: <code>jdbc:sqlserver://server.database.windows.net:1433;database=database;encrypt=true;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=30;Authentication=ActiveDirectoryPassword;</code> <b>Note:</b> The default authentication type is Microsoft SQL Server authentication.

<b>Property</b>	<b>Description</b>
Azure Synapse Analytics JDBC Username	The user name to use for connecting to the Microsoft Azure Synapse Analytics account. Provide the AAD user name for AAD authentication.
Azure Synapse Analytics JDBC Password	The password to use for connecting to the Microsoft Azure Synapse Analytics account.
Azure Synapse Analytics Schema Name	The name of the schema in the Microsoft Azure Synapse Analytics target.
ADLS Gen2 Account Name	The name of the Microsoft Azure Data Lake Storage Gen2 account.
Client Id	The ID of your client application for completing the OAuth Authentication in the Active Directory.
Client Secret	The client secret key for completing the OAuth Authentication in the Active Directory.
Directory	The Microsoft Azure Data Lake Storage Gen2 directory that Application Ingestion and Replication and Database Ingestion and Replication use to stage data in files. The default is the root directory.
Filesystem Name	The name of an existing file system in the Microsoft Azure Data Lake Storage Gen2 account.
Tenant ID	The Directory ID of the Azure Active Directory.

## CHAPTER 125

# Microsoft Azure Synapse SQL connection properties

Create a Microsoft Azure Synapse SQL connection to securely read data from or write data to Microsoft Azure Synapse SQL.

## Prerequisites

You can configure Microsoft SQL Server, Azure Active Directory, Managed Identity, and Service Principal authentication types to access Microsoft Azure Synapse SQL.

You can also connect to a serverless SQL pool when you read data from Microsoft Azure Synapse SQL. When you connect to a serverless SQL pool, you can configure Microsoft SQL Server, Azure Active Directory, and Managed Identity authentication types to access Microsoft Azure Synapse SQL. For more information on the authentication details, see the Informatica How-To Library article, [Prerequisites to connect to a serverless SQL pool](#).

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

## Azure Active Directory authentication

To connect to Microsoft Azure Synapse SQL using Azure Active Directory (AAD) authentication, you need to create an Azure Active Directory administrator and an Azure Active Directory user.

### Import a server certificate

If a trust store file isn't configured for your organization and you want to use AAD authentication with Active Directory Federation Services in Azure, you need to import the server certificate. For more information, contact your organization administrator.

Import the server certificate to the following location:

```
<Secure Agent installation directory>\jdk\jre\lib\security\cacerts
```

Use the following command to import the certificate:

```
keytool -import -trustcacerts -alias <alias name of the certificate> -file <certificate file path> -keystore
```

```
<Secure Agent installation directory>\jdk\jre\lib\security\cacerts
```

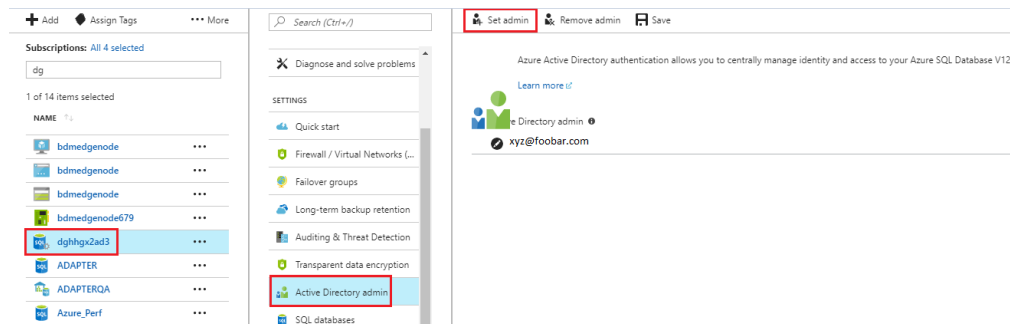
```
-storepass <password for the truststore>
```

## Create an Azure Active Directory administrator

To add new users to your Azure Active Directory, you must have an administrator role.

To set up an Azure Active Directory administrator for AAD and Microsoft SQL Server that hosts your Microsoft Azure Synapse SQL, perform the following steps:

1. Log on to the Microsoft Azure portal using your credentials.  
The Dashboard page appears.
2. From the All Resources page, select the Microsoft SQL Server that hosts Microsoft Azure Synapse SQL.
3. Under Settings displayed for Microsoft SQL Server, select the **Active Directory admin** option.  
The image shows the Active Directory admin settings:



4. Click **Set admin**.  
The Add admin page appears.
5. Enter the email ID that you want to use as admin, and then click **Select**.
6. Click **Save**.

## Create an Azure Active Directory user

Create an AAD user and use the AAD user credentials when you configure a Microsoft Azure Synapse SQL connection with AAD authentication.

Perform the following steps to create an AAD user:

1. Connect to Microsoft Azure Synapse SQL using the Azure Active Directory administrator created in the previous steps.  
You can use Microsoft SQL Server Management Studio to connect to the Microsoft Azure Synapse SQL.
2. In a new query window in Microsoft SQL Server Management Studio, run the following command to create an AAD user:  

```
create user [user@foobar.com] from external provider;
```

3. Assign the following privileges to the user:

```
CREATE USER [username] FROM EXTERNAL PROVIDER;
ALTER ROLE db_datareader ADD MEMBER [username]
ALTER ROLE db_datawriter ADD MEMBER [username]
GRANT EXECUTE TO [username]
grant ALTER ANY EXTERNAL DATA SOURCE to [username];
grant create table to [username];
grant create schema to [username];
grant select to [username];
grant update to [username];
grant insert to [username];
grant delete to [username];
grant create view to [username];
grant select on schema :: sys to [username];
grant control to [username];
EXEC sp_addrolemember 'db_owner','[username]';
ALTER ROLE db_owner ADD MEMBER [username]
```

## Service principal authentication

Service Principal authentication involves the use of a service principal identity to authenticate and authorize access to Azure resources. Before you use service principal authentication to connect to Microsoft Azure Synapse SQL, be sure to complete certain prerequisites.

1. Register a service principal application.
2. Configure a service principal user for a serverless SQL pool.
3. Configure a service principal user for a dedicated SQL pool.

For more information, see [Prerequisites to use service principal authentication](#) Informatica How-To Library article.

## Managed Identity authentication

Managed Identity authentication uses managed identities in Azure Active Directory to authenticate and authorize access to Azure resources securely.

When you use managed identity authentication to connect to Microsoft Azure Synapse SQL, the user for the system assigned identity is the virtual machine for which you enable the identity. The user for the user assigned identity is the user identity that you create in the Azure portal.

Before you use managed identity authentication to connect to Microsoft Azure Synapse SQL or Microsoft Azure Data Lake Storage Gen2, be sure to complete certain prerequisites.

1. Create an Azure virtual machine.
2. Install the Secure Agent on the Azure virtual machine.
3. Enable system assigned identity or user assigned identity for the Azure virtual machine.  
If you enable both and do not specify the client ID, the system assigned identity is used for authentication.



4. After you add or remove a managed identity, restart the Azure virtual machine.

## Serverless SQL pool

You can configure a Microsoft Azure Synapse SQL connection to connect to a serverless SQL pool. A serverless SQL pool does not store data or require any preconfigured infrastructure. You can connect to a serverless SQL pool when you want to query external tables that reference data stored in Microsoft Azure Data Lake Storage Gen2 or when you want to use queries with the OPENROWSET function.

To connect to a serverless SQL pool, specify the Azure DW JDBC URL connection string for a serverless SQL pool in the Microsoft Azure Synapse SQL connection.

Before you connect to a serverless SQL pool to read from Microsoft Azure SQL Data Warehouse, be sure to complete the following prerequisites:

1. Configure an Azure Analytics serverless pool workspace.
2. Create an SQL database in the serverless pool workspace.
3. Get the JDBC URL for the following authentication types:
  - Microsoft SQL Server authentication
  - Azure Active Directory (AAD) authentication
  - Managed Identity authentication
4. To use Service Principal authentication to connect to Microsoft Azure Data Lake Storage Gen2 to stage the files, get credentials for Service Principal.
5. Configure steps to read data from a file using the OPENROWSET query or by creating an external table.

For more information, see [Prerequisites to connect to a serverless SQL pool](#) Informatica How-To Library article.

# Connect to Microsoft Azure Synapse SQL

Let's configure the Microsoft Azure Synapse SQL connection properties to connect to Microsoft Azure Synapse SQL.

## Before you begin

Before you get started, you'll need to get information from your Microsoft Azure Synapse SQL account based on the authentication type that you want to configure.

Check out [Azure Active Directory authentication](#), [Managed Identity authentication](#), and ["Service principal authentication" on page 372](#) for the information you need from Microsoft Azure Synapse SQL.

To get the JDBC URL from your Azure account, see [Obtaining the JDBC URL](#) How-To Library article.

Check out [serverless SQL pool](#) for the information you need to connect to a serverless SQL pool.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Azure Synapse SQL
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. Hosted Agent doesn't apply to mappings in advanced mode.

Property	Description
Azure DW JDBC URL	<p>The Microsoft Azure Synapse SQL JDBC connection string.</p> <p>Use the following string to connect to Microsoft Azure Synapse SQL:</p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;</pre> <p>You can include an authentication parameter in the connection string to specify the authentication type. You can configure the following authentication types to connect to Microsoft Azure Synapse SQL:</p> <ul style="list-style-type: none"> <li>- Microsoft SQL Server</li> <li>- Azure Active Directory</li> <li>- Managed Identity</li> <li>- Service Principal</li> </ul> <p>If you don't include an authentication parameter in the connection string, the Secure Agent uses Microsoft SQL Server authentication as the authentication type.</p> <p><b>Use the following string to connect to a serverless SQL pool in Microsoft Azure Synapse SQL:</b></p> <pre>jdbc:sqlserver://&lt;Serverless SQL endpoint&gt;:1433; database=&lt;Database&gt;;Authentication=ActiveDi rectoryMsi;</pre> <p><b>Connection string format for Microsoft SQL Server authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;</pre> <p><b>Connection string format for Azure Active Directory (AAD) authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServe rCertificate=false; hostNameInCertificate=*.database.windows.ne t;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p><b>Connection string format for Service Principal authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServe rCertificate=false; hostNameInCertificate=*.database.windows.ne t;loginTimeout=30; Authentication= ActiveDirectoryServicePrincipal;</pre> <p><b>Connection string format for Managed Identity authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;Authentication=ActiveDi rectoryMsi;</pre>

Property	Description
Azure DW JDBC Username	User name to connect to the Microsoft Azure Synapse SQL account. <ul style="list-style-type: none"> <li>- For AAD authentication, provide your AAD user name.</li> <li>- For Microsoft SQL server authentication, provide your SQL auth user name.</li> <li>- For service principal authentication, provide the application ID or client ID for your application registered in Azure Active Directory.</li> </ul> This property doesn't apply to Managed Identity authentication.
Azure DW JDBC Password	Password to connect to the Microsoft Azure Synapse SQL account. <ul style="list-style-type: none"> <li>- For AAD authentication, provide the password of the AAD user.</li> <li>- For Microsoft SQL server authentication, provide the password of SQL auth user.</li> <li>- For service principal authentication, provide the client secret for your application registered in the Azure Active Directory.</li> </ul> This property doesn't apply to Managed Identity authentication.
Azure DW Client ID	Required if you want to use the user-assigned managed identity for Managed Identity Authentication to connect to Microsoft Azure Synapse SQL. The client ID of the user-assigned managed identity. If you use system-assigned managed identity, leave the field empty.
Azure DW Schema Name	Name of the schema in Microsoft Azure Synapse SQL.

## Azure storage types

You can select Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2 as the Azure storage type to stage the data files. Default is Azure Blob.

Select your preferred storage type and then configure the storage-specific parameters.

To get credentials for shared key authentication when you connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2 to stage files, see [Get credentials for shared key authentication](#) How-To Library article.

To get credentials for service principal authentication when you connect to Microsoft Azure Data Lake Storage Gen2 to stage files, see [Get credentials for service principal authentication](#) How-To Library article.

### Azure Blob storage

When you select Microsoft Azure Blob as the storage type, you can configure Shared Key Authentication as the authentication type to stage the files.

**Note:** If you connect to a serverless SQL pool, you must configure Microsoft Azure Data Lake Storage Gen2 as the storage type.

The following table describes the authentication type that you can configure for Microsoft Azure Blob storage:

Property	Description
Authentication Type	Authentication type to connect to Microsoft Azure Blob storage to stage the files. You can configure Shared Key Authentication as the authentication type to stage the files.

### Shared Key Authentication

Uses the storage account name and account key to connect to Microsoft Azure Blob storage.

The following table describes the basic connection properties for shared key authentication:

Property	Description
Azure Blob Account Name	Name of the Microsoft Azure Blob Storage account to stage the files.
Azure Blob Account Key	The Microsoft Azure Blob Storage access key to stage the files.
Container Name	The name of the container in the Azure Blob Storage account.

### ADLS Gen2 storage

When you select Microsoft Azure Data Lake Storage Gen2 as the storage type, you can configure various authentication types to stage the files.

The following table describes authentication types that you can configure for Microsoft Azure Data Lake Storage Gen2 storage:

Property	Description
Authentication Type	Authentication type to connect to Azure storage to stage the files. Select one of the following options: <ul style="list-style-type: none"> <li>- Shared Key Authentication</li> <li>- Service Principal Authentication</li> <li>- Managed Identity Authentication</li> </ul> For more information on how to configure the authentication types, see <a href="#">Setting up authentication to connect to Microsoft Azure Synapse SQL</a> .

### Shared Key Authentication

Uses the storage account name and account key to connect to Microsoft Azure Data Lake Storage Gen2.

**Note:** You cannot select shared key authentication type when you connect to a serverless SQL pool.

The following table describes the basic connection properties for shared key authentication:

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
ADLS Gen2 Account Key	The Microsoft Azure Data Lake Storage Gen2 access key to stage the files.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

### Service Principal Authentication

Uses the account name, client ID, client secret, and tenant ID to connect to Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for service principal authentication:

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
Client ID	The client ID of your application. Enter the application ID or client ID for your application registered in the Azure Active Directory.
Client Secret	The client secret for your application.
Tenant ID	The directory ID or tenant ID for your application.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

### Managed Identity Authentication

Select this authentication type to authenticate using system-assigned or user-assigned identities that are assigned to applications in Azure to access Azure resources in Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for managed identity authentication:

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
Client ID	The client ID of your application. Enter the client ID for the user-assigned managed identity. If the managed identity is system-assigned, leave the field empty.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

In a file ingestion task, if you select Microsoft Azure Synapse SQL with Managed Identity authentication type as the target, then you must select Microsoft Azure Data Lake Storage Gen2 as the source.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
External Data Source	The data source to create the external table. Ensure that the external data source exists in Microsoft Azure Synapse SQL and you have the permission to access the external data source. When you use the copy command method to load data from the staging location to Microsoft Azure Synapse SQL, you don't need to specify an external data source.
Staging Schema Name	The name of the schema that the Secure Agent uses to create external tables for staging data files. If you do not specify the staging schema name, the Secure Agent considers the configured Azure DW Schema Name.
Blob End-point	Type of Microsoft Azure endpoint. Select one of the following endpoints: - core.windows.net. Connects to Azure endpoints. Use this endpoint when you connect to a serverless SQL pool. - core.usgovcloudapi.net. Connects to US Government Microsoft Azure Synapse SQL endpoints. - core.chinacloudapi.cn. Connects to Microsoft Azure Synapse SQL endpoints in the China region. Default is core.windows.net.
VNet Rule	Enable to connect to a Microsoft Azure Synapse SQL endpoint residing in a virtual network (VNet). This property doesn't apply to a serverless runtime environment.

## Verify permissions

Permissions define the level of access for the operations that you can perform in Microsoft Azure Synapse SQL.

You must verify the following permissions:

- Ensure that a default schema is present at the account level or user or group level in Microsoft Azure SQL Data Warehouse.
- Verify that either the `db_owner` privilege or the following more granular privileges are granted to the user to connect to Microsoft Azure SQL Data Warehouse and perform operations successfully:

```
- EXEC sp_addrolemember 'db_datareader', '<user>'; // Alternately assign permission to the individual table.
```

```
- EXEC sp_addrolemember 'db_datawriter', '<user>'; // Alternately assign permission to the individual table.
```

```
- GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;
```

```
- GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;
```

```
- GRANT CONTROL TO <user>; // To grant all permissions on the database.
```

or

```
GRANT ALTER ANY SCHEMA TO <user>; // To grant permissions only on the schema.
```

```
- GRANT CREATE TABLE TO <user>;
```

- Assign required privileges for tasks performed through Pre-SQL and Post-SQL commands.
- If you configure the staging schema name in the connection properties, ensure the following additional privileges are granted to the user:
  - ALTER ROLE db\_datareader ADD MEMBER <user>;
  - GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;
  - GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;
  - GRANT CREATE TABLE TO <user>;
  - GRANT ALTER ON SCHEMA::  - GRANT REFERENCES ON DATABASE SCOPED CREDENTIAL::For example, GRANT REFERENCES ON DATABASE SCOPED CREDENTIAL::db\_creds1 TO srvls;
- If you have the ALTER ANY SCHEMA permissions, you must create the Master Key, Database Scoped Credential, and External Data Source in Microsoft Azure Synapse SQL that require the CONTROL permission on the database and specify the external data source when you create a connection. Also, Microsoft Azure Synapse SQL Connector does not delete the Database Scoped Credential and External Data Source. You must manually delete the Database Scoped Credential and External Data Source.
- When you use managed identity authentication to connect to Microsoft Azure Synapse SQL, grant permissions to the virtual machine and user identity. For example, GRANT CONTROL TO <virtual machine name>; and GRANT CONTROL TO <user identity name>;



## CHAPTER 126

# Microsoft CDM Folders V2 connection properties

When you set up a Microsoft CDM Folders V2 connection, configure the connection properties.

**Important:** Microsoft CDM Folders V2 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Microsoft CDM Folders V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Microsoft CDM Folders V2 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
ADLSGen2 Storage Account Name	Name of the ADLS Gen2 storage account.
Azure AD App Client ID	The client ID of the Azure Active Directory account to authenticate user access to the storage account. You can get the application ID from the Microsoft Azure Active Directory administrator.
Azure AD App Client Secret	The client secret key of the Azure Active Directory application to authenticate access to the storage account. You can get the key value from the Microsoft Azure Active Directory administrator.
Azure Tenant ID	The tenant ID of the Azure Active Directory account to authenticate user access to the storage account. You can get the directory ID from the Microsoft Azure Active Directory administrator.
ADLSGen2 File System Name	The name of the file system that you create in the Azure Storage Explorer application. A file system can contain more than one common data model folders.

Property	Description
CDM Folder Path	<p>The path of the common data model folder that you create within the file system.</p> <p>You can use the following values for CDM folder path:</p> <ul style="list-style-type: none"><li>- /</li><li>- /folder1</li><li>- /folder1/folder2</li></ul> <p>The recommended CDM folder path is /folder1.</p> <p>Default is empty.</p>
Adls Gen2 End-point	The ADLS Gen2 endpoint core.windows.net.

## CHAPTER 127

# Microsoft Dynamics 365 for Operations connection properties

Create a Microsoft Dynamics 365 for Operations connection to securely read data from and write data to Microsoft Dynamics 365 for Operations.

## Prepare for authentication

You can configure OAuth 2.0 and OAuth 2.0 client secret grant authentication types to connect to Microsoft Dynamics 365 for Operations.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

You also need to add the required domains to the list of approved IP addresses to connect to Microsoft Dynamics 365 for Operations.

For more information about the domains that you need to add to the list of approved IP addresses, see the [List of domains](#) knowledge article.

**Note:** You cannot use OAuth 2.0 client certificate grant authentication to access Microsoft Dynamics 365 for Operations.

## OAuth 2.0 authentication

You need the Microsoft Dynamics 365 for Operations user name and password to configure OAuth 2.0 authentication to access Microsoft Dynamics 365 for Operations.

Additionally, you need the service URL and application ID for OAuth 2.0 authentication.

To get these details, the organization administrator needs to register your Microsoft Dynamics 365 for Operations application with Azure Active Directory.

For more information about the registration steps with Azure Active Directory, see [Register your application](#).

## OAuth 2.0 client secret grant authentication

You need the tenant ID and client secret and to use OAuth 2.0 client secret grant authentication to access Microsoft Dynamics 365 for Operations.

To get the tenant ID and client secret, you need to register your Microsoft Dynamics 365 for Operations application with the Azure Active Directory.

Additionally, you need the service URL and application ID for OAuth 2.0 client secret grant authentication.

## Set the -Dlog4j.configuration property

1. Copy the `log4j.properties` file from `<Secure Agent installation directory>\downloads\package-MSDAX7.<version>\package\plugins\449700` directory and place it in a location in the Secure Agent machine.
2. Set the JVM option for type DTM to `-Dlog4j.configuration=<log4j.propertyfile location>\log4j.properties` in the system configuration details of the Secure Agent.
3. Restart the Secure Agent.

# Connect to Microsoft 365 for Operations

Let's configure the Microsoft Dynamics 365 for Operations connection properties to connect to Microsoft Dynamics 365 for Operations.

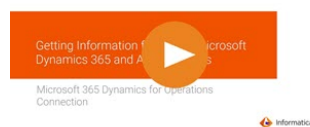
## Before you begin

Before you get started, you'll need to get information from your Microsoft Dynamics 365 for Operations and AAD account based on the authentication type that you want to configure.

To configure OAuth 2.0 authentication, get the Microsoft Dynamics 365 for Operations user name and password.

To configure OAuth 2.0 client secret grant authentication, get the tenant ID and client secret from your Azure Active Directory (AAD) account.

The following video shows you how to get information from your Microsoft Dynamics 365 and AAD account:



Check out [“Prepare for authentication” on page 383](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + ,</code> . Maximum length is 255 characters.
Description	

Property	Description
Type	Microsoft Dynamics 365 for Operations
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p>

## Authentication types

You can configure OAuth 2.0 and OAuth 2.0 Client Secret Grant authentication types to access Microsoft Dynamics 365 for Operations.

Select the required authentication method and then configure the authentication-specific parameters.

**Note:** You cannot use OAuth 2.0 client certificate grant authentication to access Microsoft Dynamics 365 for Operations. The keystore file, keystore password, key alias, and key password properties that display for the client certificate grant authentication are not applicable to a Microsoft Dynamics 365 for Operations connection.

### OAuth 2.0 authentication

OAuth 2.0 authentication requires the user name, password, service URL, and AAD application ID of your Microsoft Dynamics 365 for Operations account.

The following table describes the basic connection properties for OAuth 2.0 authentication:

Property	Description
Service URL	<p>The URL of the Microsoft Dynamics 365 for Operations service.</p> <p>Enter the URL in the following format:</p> <pre>https:&lt;server name&gt;:&lt;port number&gt;</pre> <p>If you don't specify the port number in the URL, the agent uses port number 443 in the query.</p>
Username	The user name to connect to Microsoft Dynamics 365 for Operations account.
Password	The password to connect to Microsoft Dynamics 365 for Operations account.
Application ID	The AAD application ID for Microsoft Dynamics 365 for Operations.

## OAuth 2.0 client secret grant authentication

OAuth 2.0 client secret grant authentication requires the tenant ID, client secret, service URL, and AAD application ID of your Microsoft Dynamics 365 for Operations account.

The following table describes the basic connection properties for OAuth 2.0 client secret grant authentication:

Property	Description
Service URL	The URL of the Microsoft Dynamics 365 for Operations service. Enter the URL in the following format: <code>https:&lt;server name&gt;:&lt;port number&gt;</code> If you don't specify the port number in the URL, the agent uses port number 443 in the query.
Application ID	The AAD application ID for Microsoft Dynamics 365 for Operations.
Tenant ID	The directory ID for Azure Active Directory.
Client Secret	The client secret for the Microsoft Dynamics 365 for Operations account.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Retry Error Codes	HTTP error codes for temporary issues or failures in network requests or operations for which the Microsoft Dynamics 365 for Sales connection attempts retries. You can enter HTTP error codes, each separated by a comma.
Retry Count	The total number of retries to get the response from the Microsoft Dynamics 365 for Operations endpoint, determined by the retry interval you specify. Default is 0. If you enable the retry count and run a task, the task stops responding when the Microsoft Dynamics 365 for Operations server is down or not reachable from the Secure Agent.
Retry Interval	The time in seconds to wait before the Microsoft Dynamics 365 for Operations connection makes another attempt to receive a response. Default is 60 seconds.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, you can use the serverless runtime environment to connect to Informatica Intelligent Cloud Services through the proxy server.

You can use the unauthenticated or authenticated proxy server. You can configure proxy both in mappings and in mappings in advanced mode.

To configure the proxy settings for the serverless runtime environment, see *Runtime Environments* in the Administrator help.

## CHAPTER 128

# Microsoft Dynamics 365 for Sales connections

Create a Microsoft Dynamics 365 for Sales connection to securely read data from and write data to Microsoft Dynamics 365 for Sales.

## Prepare for authentication

You can configure OAuth 2.0 password grant, OAuth 2.0 client certificate grant, and OAuth 2.0 client secret grant authentications to connect to Microsoft Dynamics 365 for Sales deployed online or on-premises.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

### OAuth 2.0 password grant

You need the Microsoft Dynamics 365 for Sales user name and password to configure OAuth 2.0 password grant authentication to access Microsoft Dynamics 365 for Sales deployed online or on-premises. You additionally need the security token service URL to access the instance deployed on-premises.

To get these details, the organization administrator needs to register your on-premises Microsoft Dynamics 365 for Sales application with Azure Active Directory.

For more information about the registration steps with Azure Active Directory, see [Register your application](#).

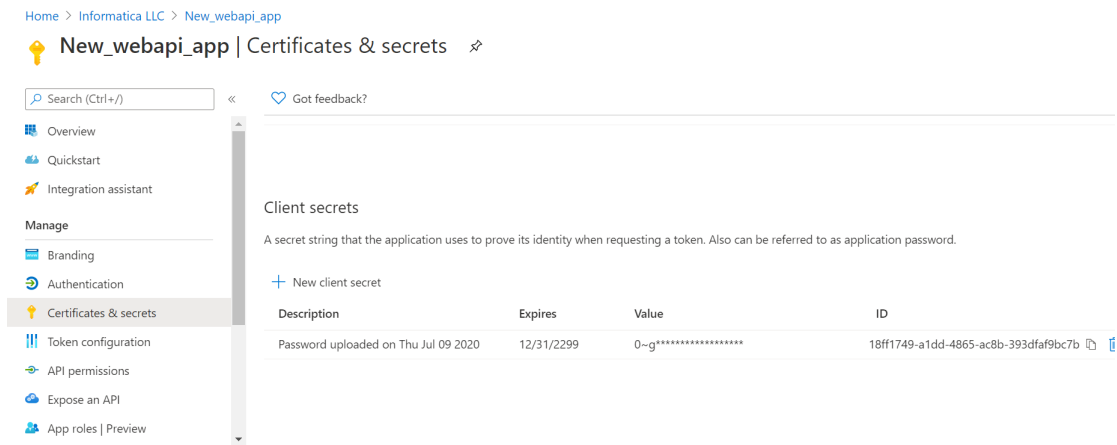
### OAuth 2.0 client secret grant

You need the client secret to use OAuth 2.0 client secret grant authentication to access Microsoft Dynamics 365 for Sales.

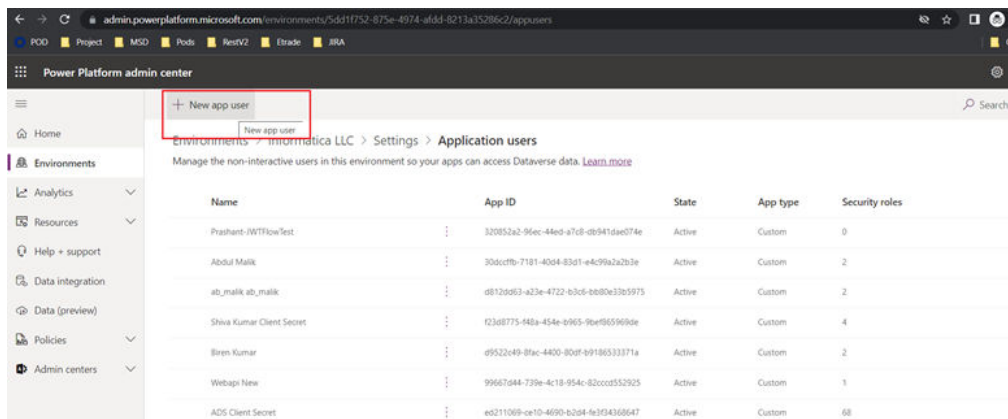
To get the client secret, you need to register your Microsoft Dynamics 365 for Sales web application and create a new application user for the registered application.

Perform the following tasks to create a new application user for the registered application.

1. Go to the Azure registered applications page in Azure Active Directory.
2. Select your application.



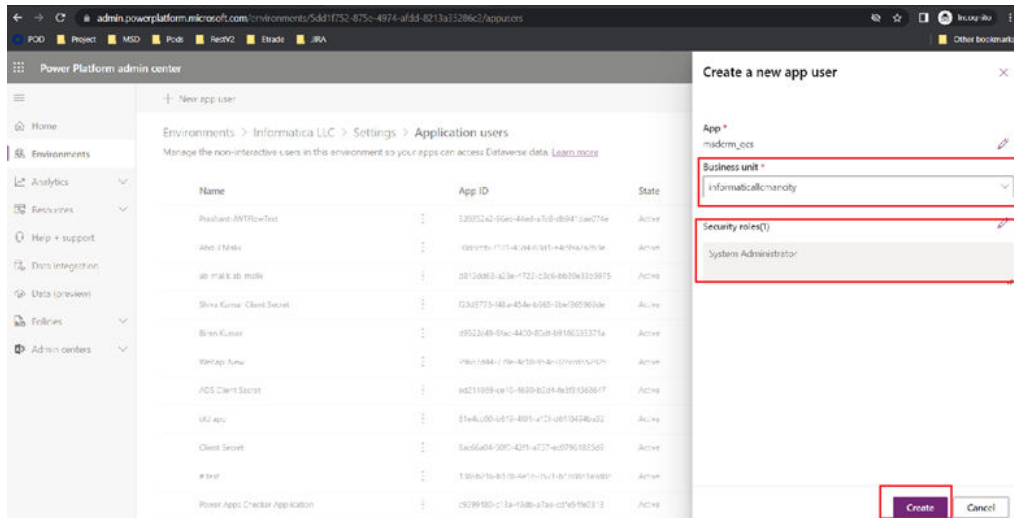
3. Click **New client secret** to generate a client secret.
4. Log in to <https://admin.powerplatform.microsoft.com/> to create a new application user for the registered application.
5. Navigate to **Environments** and select the required environment.
6. In the **Settings** option for the environment, click **Users+permissions**.
7. Select the **Applications users** option.
8. Click **+New app user**.



A tab opens on the right requesting for App and User details.

9. Create a new application user and enter the details shown in the following image:





You can choose an App, a Business Unit, and Security role for the new application user.

10. Click **Create**.

Keep the generated application ID and client secret handy to use in a Microsoft Dynamics 365 for Sales connection.

## OAuth 2.0 client certificate grant

You need a valid client certificate to use the client certificate grant authentication type.

To get the client certificate, register your Microsoft Dynamics 365 for Sales web application and create a new application user for the registered application.

From the command line, run the following commands from any machine and use the certificates in the Azure Active Directory application.

1. To create a public-private key pair, run the following command:

```
keytool -genkey -alias <keypair_name1> -keyalg <key_algorithm> -validity <number_days> -
keystore <path and file name of the generated certificate> -storetype <store_type> -
keypass <key_password> -storepass <store_password>
```

For example, `keytool -genkey -alias keyalias -keyalg RSA -validity 1825 -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks" -storetype JKS -keypass keypassword -storepass changeit`

2. To import the root CA certificate(s) followed by the user's signed certificate to the keystore, run the following commands:

```
a. keytool -import -trustcacerts -alias <keypair_name2> -file <CA_certificate_name> -
keystore <path and file name of the generated certificate>
keytool -import -trustcacerts -alias <keypair_name2> -file <CA_certificate_name> -
keystore <path and file name of the generated certificate>
```

- b. `keytool -import -trustcacerts -alias <keypair_name1> -file <user's_signed_certificate_name> -keystore <path and file name of the generated certificate>`

**For example,** `keytool -import -trustcacerts -alias keyalias -file b2024001944cdb12.crt -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks"`

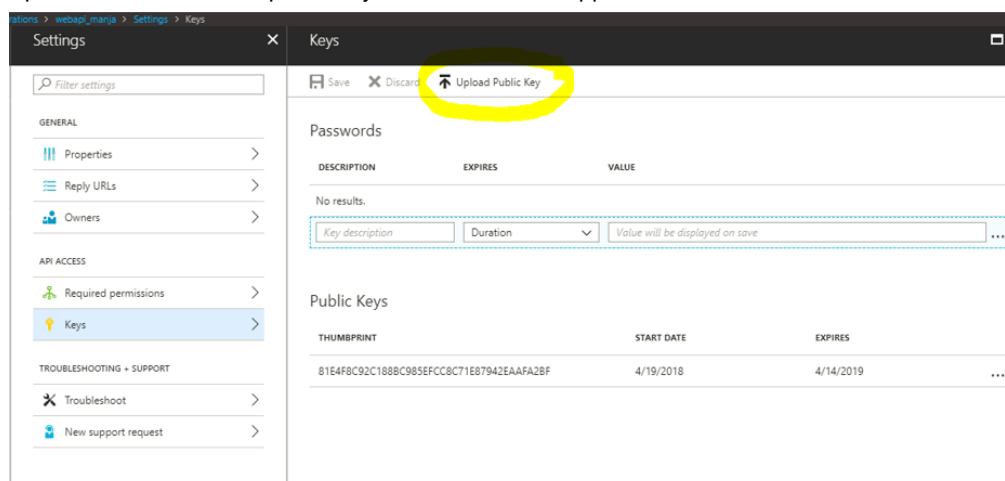
**Note:** These steps might vary depending on the types of files you receive from the CA. If you receive a single file with all the certificates, perform only step b. Do not perform these steps for self-signed certificates.

3. To export the certificate from the keystore, run the following command:

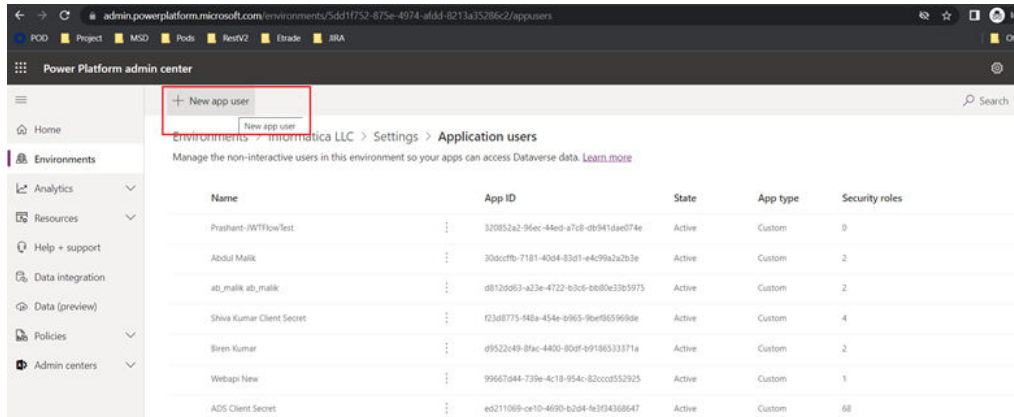
`keytool -export -alias <keypair_name1> -file <certificate_name> -keystore <path and file name of the generated certificate>`

**For example,** `keytool -export -alias keyalias -file keyalias.crt -keystore "C:\Cdrive\Cloud\R27\MSDCRM_WebAPI\MSDCRM_WebAPI\certificate\iicsdummy.com\federated.jks"`

4. Upload the certificate or public key under a new Web application.

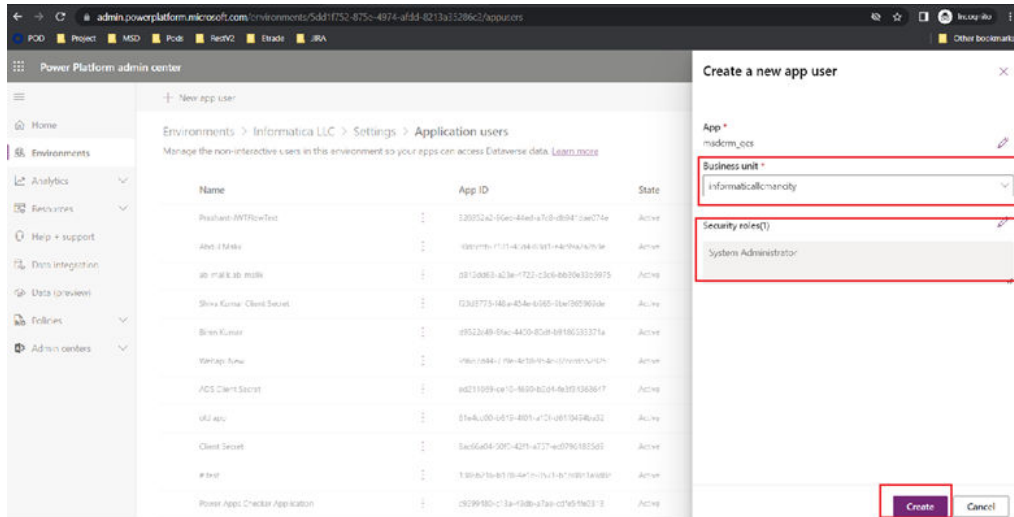


5. Log in to <https://admin.powerplatform.microsoft.com/> to create a new application user for the registered application.
6. Navigate to **Environments** and select the required environment.
7. In the **Settings** option for the environment, click **Users+permissions**.
8. Select the **Applications users** option.
9. Click **+New app user**.



A tab opens on the right requesting for App and User details.

10. Create a new application user and enter the details shown in the following image:



You can choose an App, a Business Unit, and Security role for the new application user.

11. Click **Create**.

Keep the generated application ID, keystore file, keystore password, key alias, and key password handy to use in a Microsoft Dynamics 365 for Sales connection.

## Connect to Microsoft Dynamics 365 for Sales

Let's configure the Microsoft Dynamics 365 for Sales connection properties to connect to Microsoft Dynamics 365 for Sales.

### Before you begin

Before you get started, your organization administrator needs to register your Microsoft Dynamics 365 for Sales application deployed online or on-premises with Azure Active Directory.

You'll need to get information from your Microsoft Dynamics 365 for Sales and Azure Active Directory (AAD) account based on the authentication type that you want to configure to access Microsoft Dynamics 365 for Sales.

Check out ["Prepare for authentication" on page 387](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Dynamics 365 for Sales
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in Runtime Environments in the Administrator help. If you want to use the Hosted Agent to access Microsoft Dynamics 365 for Sales, the connection must use OAuth 2.0 Password Grant authentication.

## Authentication types

You can select the Microsoft Dynamics 365 for Sales server type as on-premise or online based on where your instance is deployed and the applicable authentication type in the Microsoft Dynamics 365 for Sales connection properties to access Microsoft Dynamics 365 for Sales from Data Integration.

**Note:** For enhanced security, consider using OAuth 2.0 Secret Grant or OAuth 2.0 Certificate Grant authentication type to establish a connection.

### OAuth 2.0 password grant authentication

You can configure the OAuth 2.0 Password Grant authentication to connect to Microsoft Dynamics 365 for Sales deployed online or on-premises.

The following table describes the basic connection properties for OAuth 2.0 password grant authentication:

Property	Description
Web API url	The URL of the Microsoft Dynamics 365 for Sales endpoint.
Username	The user name to connect to the Microsoft Dynamics 365 for Sales account.
Password	The password to connect to the Microsoft Dynamics 365 for Sales account.
Application ID	The application ID for Microsoft Dynamics 365 for Sales registered in Azure Active Directory.
Server Type	The Microsoft Dynamics 365 for Sales server that you want to access. You can select the server type from the following list: <ul style="list-style-type: none"> <li>- Microsoft Dynamics Online. Connects to Microsoft Dynamics 365 for Sales deployed online.</li> <li>- Microsoft Dynamics On-premise. Connects to Microsoft Dynamics 365 for Sales deployed on-premises.</li> </ul>
Security Token Service URL	The Microsoft Dynamics 365 for Sales security token service URL. This URL is required when you access Microsoft Dynamics 365 for Sales on-premises. Specify the security token service URL in the following format: <code>https://sts1.&lt;company&gt;.com/adfs/oauth2/token</code>

## OAuth 2.0 client secret grant authentication

You can configure OAuth 2.0 client secret grant authentication when you connect to Microsoft Dynamics 365 for Sales online.

The following table describes the basic connection properties for OAuth 2.0 client secret grant authentication:

Property	Description
Web API url	The URL of the Microsoft Dynamics 365 for Sales endpoint.
Application ID	The application ID for Microsoft Dynamics 365 for Sales registered in Azure Active Directory.
Tenant ID	The directory ID in Azure Active Directory.
Client Secret	The client secret key to connect to Microsoft Dynamics 365 for Sales account.
Server Type	The Microsoft Dynamics 365 for Sales server that you want to access. Select the Microsoft Dynamics Online server type to connect to Microsoft Dynamics 365 for Sales deployed online.

## OAuth 2.0 client certificate grant authentication

You can configure OAuth 2.0 client certificate grant authentication to connect to Microsoft Dynamics 365 for Sales online.

The following table describes the basic connection properties for OAuth 2.0 client certificate grant authentication:

Property	Description
Web API url	The URL of the Microsoft Dynamics 365 for Sales endpoint.
Application ID	The application ID for Microsoft Dynamics 365 for Sales registered in Azure Active Directory.
Tenant ID	The directory ID in Azure Active Directory.
Keystore File	The location and the file name of the key store. This property doesn't apply if you use the Hosted Agent. For the serverless runtime environment, specify the following keystore file path in the serverless agent directory: For example: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;certificate file&gt;</code>
Keystore Password	The password for the keystore file required for secure communication.
Key Alias	The alias name for the individual key in the keystore file.
Key Password	The password for the individual key in the keystore file used for enhanced secure communication. This property doesn't apply if you use the Hosted Agent.
Server Type	The Microsoft Dynamics 365 for Sales server that you want to access. Select the Microsoft Dynamics Online server type to connect to Microsoft Dynamics 365 for Sales deployed online.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Retry Error Codes	HTTP error codes for temporary issues or failures in network requests or operations for which the Microsoft Dynamics 365 for Sales connection attempts retries. You can enter HTTP error codes, each separated by a comma.
Retry Count	The total number of retries to get the response from the Microsoft Dynamics 365 for Sales endpoint, determined by the retry interval you specify. Default is 5.
Retry Interval	The wait time in seconds to wait before the Microsoft Dynamics 365 for Sales connection makes another attempt to receive a response. Default is 60 seconds.

# Configure the serverless runtime environment

You can choose to use the serverless runtime environment when you connect to Microsoft Dynamics 365 for Sales.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in Runtime Environments in the Administrator help.

When you use the serverless runtime environment, you cannot use a proxy server to connect to Informatica Intelligent Cloud Services.

To use the serverless runtime environment with client certificate grant authentication, you require the client certificates in the serverless runtime location.

Perform the following tasks to configure a serverless runtime environment to use with client certificate grant authentication:

1. Create the following structure for the serverless agent configuration in AWS or Azure: <Supplementary file location>/serverless\_agent\_config
2. Add the certificates in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/SSL
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<certificate_file_name>
```

where the source path is the directory path of the certificate files in AWS or Azure.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the SSL certificates are copied from the AWS or Azure location to the serverless agent directory.
5. In the Microsoft Dynamics 365 for Sales connection properties, specify the following certificate path in the serverless agent directory in the **Trust Store** and **Key Store** fields:  
`/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert.p12>`

## Troubleshooting a Microsoft Dynamics 365 for Sales connection

If the test connection takes a long time, ensure that the `vocabularies.odata.org` and `login.microsoftonline.com` domains have access in the network firewall of the agent server and then retest the connection.

For more information, you can see [Domain access in firewall](#) Knowledge base article.

## Microsoft Dynamics 365 Mass Ingestion connection properties

When you set up a Microsoft Dynamics 365 Mass Ingestion connection, you must configure the connection properties.

The Microsoft Dynamics 365 Mass Ingestion connection requires a native application that is registered in Azure Active Directory (Azure AD) to access the Microsoft Dynamics 365 data. Before you configure the connection, you must register an application in Azure AD to allow the connection to access the Microsoft Dynamics 365 data. For more information about registering an application in Azure AD, see the [Microsoft documentation](#).

The properties of a Microsoft Dynamics 365 Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0 Username-Password Flow:** Authenticates the connection by using the Microsoft Dynamics 365 account login credentials and the client ID of the application registered in Azure AD.
- **OAuth 2.0 Client Secret Flow:** Authenticates the connection by using the client ID and client secret of the application registered in Azure AD.
- **OAuth 2.0 JWT Bearer Flow:** Authenticates the connection by using a X509 Public Key Infrastructure (PKI) certificate and a JSON Web Token (JWT). Use this authentication method to gain secured access to Microsoft Dynamics 365 without sharing sensitive information, such as client secret and Microsoft Dynamics 365 account login credentials.

### Connection properties for OAuth 2.0 Username-Password Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 Username-Password Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Microsoft Dynamics 365 Mass Ingestion</b> connection type.



Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Microsoft Dynamics 365 account.
Password	Password for the Microsoft Dynamics 365 account.
Client ID	Client ID of the application registered in Azure AD.
Resource URL	URL of the Microsoft Dynamics 365 organization. You must enter the resource URL in the following format: <code>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</code>
OAuth Token URL	OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint. You must enter the following value in this field: <code>https://login.windows.net/common/oauth2/token</code>

**Note:** For more information about the OAuth 2.0 Username-Password Flow authentication method, see the Microsoft Dynamics 365 documentation.

### Connection properties for OAuth 2.0 Client Secret Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 Client Secret Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Microsoft Dynamics 365 Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the application registered in Azure AD.
Client Secret	Client secret of the application registered in Azure AD.

Connection property	Description
Resource URL	URL of the Microsoft Dynamics 365 organization. You must enter the resource URL in the following format: <code>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</code>
OAuth Token URL	OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint. You must enter the following value in this field: <code>https://login.microsoftonline.com/&lt;tentant_id&gt;/oauth2/token</code>

**Note:** For more information about the OAuth 2.0 Client Secret Flow authentication method, see the Microsoft Dynamics 365 documentation.

### Connection properties for OAuth 2.0 JWT Bearer Flow authentication

The following table describes the connection properties for a Microsoft Dynamics 365 Mass Ingestion connection configured with OAuth 2.0 JWT Bearer Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Microsoft Dynamics 365 Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Client ID	Client ID of the application registered in Azure AD.
Certificate Signature	Base64URL string that encodes the hexadecimal value which represents the SHA-1 thumbprint of the X509 certificate.
Keystore Path	Absolute path to the keystore file that contains the X509 certificate required to validate a JSON Web Token (JWT) and establish a secure connection with Microsoft Dynamics 365. The keystore file must be in the Java KeyStore (JKS) format.
Keystore Password	Password for the keystore file.
Private Key Alias	Alias name of the private key used to sign the JWT.
Private Key Password	Password for the private key.

Connection property	Description
Audience for JWT	<p>URL of the Microsoft Dynamics 365 resource server to which the application that is registered in Azure AD sends the JWT for validation.</p> <p>You must enter the address in the following format:</p> <pre>https://login.microsoftonline.com/&lt;tenant_id&gt;/oauth2/token</pre>
Resource URL	<p>URL of the Microsoft Dynamics 365 organization.</p> <p>You must enter the resource URL in the following format:</p> <pre>https://&lt;Microsoft_Dynamics_365_org_name&gt;.api.crm8.dynamics.com</pre>
OAuth Token URL	<p>OAuth 2.0 token endpoint of the Microsoft Dynamics 365 organization. The application that is registered in Azure AD sends the access token requests to this endpoint.</p> <p>You must enter the following value in this field:</p> <pre>https://login.microsoftonline.com/&lt;tenant_id&gt;/oauth2/token</pre>

**Note:** For more information about the OAuth 2.0 Client Secret Flow authentication method, see the Microsoft Dynamics 365 documentation.

## CHAPTER 130

# Microsoft Dynamics AX V3 connection properties

When you set up a Microsoft Dynamics AX V3 connection, you must configure the connection properties.

The following table describes the Microsoft Dynamics AX V3 connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Optional. Provide a relevant description for the connection.
Type	Select Microsoft Dynamics AX V3 from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication	Authenticates users who want to access Microsoft Dynamics AX 2012. Microsoft Dynamics AX V3 Connector supports Basic and NTLM authentication.
WSDL URI	Enter the required WSDL file path. <b>Note:</b> To find the WSDL URI, go to <b>System Administration &gt; Inbound Ports</b> in the Microsoft Dynamics AX 2012 instance. For example, the format of WSDL URI is <code>http://&lt;Hostname&gt;:&lt;Port&gt;/&lt;App_Pool_Name&gt;/&lt;Port name&gt;/xppservice.svc</code> .
Username	The user name to login to the Microsoft Dynamics AX 2012 web page.
Password	The password associated with the NT login user.
Company Name	Optional. Enter your company name. You can enter multiple company names separated by semi-colons. For example, <code>ceu;ceed</code> .
Language	Optional. Localizes the data you read from or write to Microsoft Dynamics AX 2012. Specify the language code.

## CHAPTER 131

# Microsoft Dynamics CRM connection properties

Use a Microsoft Dynamics CRM connection to connect to a Microsoft Dynamics CRM object.

**Important:** Microsoft Dynamics CRM Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use REST V2 Connector to access Microsoft Dynamics CRM.

The following table describes the Microsoft Dynamics CRM connection properties:

Connection property	Description
Authentication Type	Authentication type for the connection. Select a valid authentication type. Use one of the following authentication types: <ul style="list-style-type: none"><li>- Active Directory</li><li>- Internet Facing Deployment (IFD)</li><li>- Microsoft Live Authentication using OAuth Authentication</li></ul> <b>Note:</b> When you use a serverless runtime environment, you cannot configure Active Directory and IFD authentication.
User Name	The user name to connect to Microsoft Dynamics CRM account. For Microsoft Live authentication using OAuth, use the Application ID as user name.
Password	The password to connect to Microsoft Dynamics CRM account. For Microsoft Live authentication using OAuth, use the Client Secret as password.
Organization Name	Microsoft Dynamics CRM organization name. Organization names are case sensitive. For Microsoft Live Authentication using OAuth, use the Tenant ID registered with the Organization.
Domain	Microsoft Dynamics CRM domain name. You can use the domain specified in the connection property for IFD and Active Directory authentication.

Connection property	Description
Service URL	<p>URL of the Microsoft Dynamics CRM service.</p> <p>For Active Directory authentication, use one of the following formats:  <code>http://&lt;server.company.com&gt;:&lt;port&gt;</code> or <code>https://&lt;server.company.com&gt;:&lt;port&gt;</code></p> <p>For IFD authentication, use the following format:  <code>https://&lt;server.company.com&gt;:&lt;port&gt;</code></p> <p>For Microsoft Live authentication using OAuth, specify the CRM Organization Service web service URL.</p>
Security Token Service URL	<p>Microsoft Dynamics CRM security token service URL. For example, <code>sts1.company.com</code>.</p> <p>IFD authentication only.</p>

## CHAPTER 132

# Microsoft Dynamics NAV connection properties

When you set up a Microsoft Dynamics NAV connection, you must configure the connection properties.

**Important:** Microsoft Dynamics NAV Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Microsoft Dynamics NAV connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	User name of the NAV account.
Password	Password for the NAV account.
Host Name	Name of the NAV Server host.
Port	NAV web service port number.
Service Instance	Name of the Microsoft Dynamics NAV Server instance for web service.
Company Name	Name of the company in NAV to which the user belongs.
Domain_Name	Domain name.

## CHAPTER 133

# Microsoft Excel connection properties

When you set up a Microsoft Excel connection, you must configure the connection properties.

The following table describes the Microsoft Excel connection properties:

Connection property	Description
Connection Name	Name of the Microsoft Excel connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select <b>Microsoft Excel</b> source from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Folder URI	The directory that contains the Microsoft Excel file. The Microsoft Excel file must be located on the same machine on which the Secure Agent runs.
TreatFirstRowAsHeader	Specifies whether the first row in the file is a header row.
Filename	The name of the Microsoft Excel file. <b>Note:</b> You must add the <code>.xlsx</code> extension to the file name.



## CHAPTER 134

# Microsoft Fabric Data Warehouse connection properties

When you set up a Microsoft Fabric Data Warehouse connection, configure the connection properties.

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Fabric Data Warehouse
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
SQL Connection String	The SQL connection string to connect to Microsoft Fabric Data Warehouse. Specify the connection string in the following format: <code>&lt;Server&gt;.datawarehouse.pbidedicated.windows.net</code>
Client ID	The application ID or client ID of your application registered in Azure Active Directory for service principal authentication.
Client Secret	The client secret for your application registered in Azure Active Directory.
Tenant ID	The tenant ID of your application registered in Azure Active Directory.
Workspace	The name of the workspace in Microsoft Fabric Data Warehouse that you want to connect.
Database	The name of the database in Microsoft Fabric Data Warehouse that you want to connect.

The following table describes the advanced connection property:

Property	Description
Schema Name	The name of the schema in Microsoft Fabric Data Warehouse where the tables are stored.

## CHAPTER 135

# Microsoft Fabric Lakehouse connection properties

When you set up a Microsoft Fabric Lakehouse connection, configure the connection properties.

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Microsoft Fabric Lakehouse
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
SQL Connection String	The SQL connection string to connect to Microsoft Fabric Lakehouse. Specify the connection string in the following format: <code>&lt;Server&gt;.lakehouse.pbidedicated.windows.net</code>
Client ID	The application ID or client ID of your application registered in Azure Active Directory for service principal authentication.
Client Secret	The client secret for your application registered in Azure Active Directory.
Tenant ID	The tenant ID of your application registered in Azure Active Directory.
Workspace	The name of the workspace in Microsoft Fabric Lakehouse that you want to connect.
Database	The name of the database in Microsoft Fabric Lakehouse that you want to connect.

## CHAPTER 136

# Microsoft Fabric OneLake connection properties

When you set up a Microsoft Fabric OneLake connection, configure the connection properties.

The following table describes the Microsoft Fabric OneLake connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Microsoft Fabric OneLake connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. <b>Note:</b> The Hosted Agent and serverless runtime environments are not supported by application ingestion and replication, database ingestion and replication, and file ingestion and replication tasks.
Workspace Name	Name of the workspace in Microsoft Fabric OneLake. Workspace name cannot contain special characters or spaces.
Lakehouse Path	Path or name of the lakehouse present in the workspace. You can specify the path in one of the following ways: - <i>root directory (/)</i> to access the files in the workspace. - <i>lakehouse name/Files</i> to access the files present in the lakehouse.
Authentication Type	Authentication type to access Microsoft Fabric OneLake. Service Principal Authentication uses the client ID, client secret, and tenant ID to connect to Microsoft Fabric OneLake.
Client ID	The application ID or client ID of your application registered in the Azure Active Directory.
Client Secret	The client secret of your application registered in the Azure Active Directory.

Property	Description
Tenant ID	The ID of the Azure Active Directory instance in which you created the application.
Microsoft Fabric OneLake Endpoint	The type of Microsoft Fabric OneLake endpoint that you want to connect to. Default is <b>fabric.microsoft.com</b> .

## CHAPTER 137

# Microsoft Power BI Connection Properties

When you set up a Microsoft Power BI connection, you must configure the connection properties.

The following table describes the Microsoft Power BI connection properties in the Connection Details area in Administrator:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Type of the connection. Select Microsoft Power BI.

The following table describes the Microsoft Power BI connection properties in the Microsoft Power BI Properties area in Administrator:

Property	Description
Runtime Environment	The execution platform that runs tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.

The following table describes the Microsoft Power BI connection properties in the Connection Section area in Administrator:

Property	Description
PowerBI Cloud Connection Mode	The Connection Mode. Choose to connect using the Administrator user option or the Service Principal option.
PowerBI Cloud URL	The URL to access the Microsoft Power BI cloud host.

### Administrator User option

Specify the following properties:

Property	Description
PowerBI Cloud Client ID	The ID to connect to the Microsoft Power BI cloud host.
PowerBI Cloud Username	User name of the administrator to connect to the Microsoft Power BI cloud host.
PowerBI Cloud Password	The password of the administrator account to connect to the Microsoft Power BI cloud host.
Proxy host	Host name of the outgoing proxy server.
Proxy port	Port number of the outgoing proxy server.
Proxy username	Name of the authenticated user of the proxy server. This is required if the proxy server requires authentication.
Proxy password	Password for the authenticated user. This is required if the proxy server requires authentication.

### Service Principal option

Use the service principal authentication method for national clouds in the United States. If you use other national clouds, see [Tutorial: Embed Power BI content into your application for national clouds](#).

Specify the following properties:

Property	Description
PowerBI Cloud Auth URL	URL for user authentication.
PowerBI Cloud Scope	Parameter that the endpoint uses to authenticate the user.
PowerBI Cloud Client ID	The ID to connect to the Microsoft Power BI cloud host.
PowerBI Cloud Tenant ID	Name of the Azure Active Directory tenant.
PowerBI Cloud Client Secret	The client secret key to complete OAuth Authentication in the Azure Active Directory.
Proxy host	Host name of the outgoing proxy server.
Proxy port	Port number of the outgoing proxy server.
Proxy username	Name of the authenticated user of the proxy server. Required if the proxy server requires authentication.
Proxy password	Password for the authenticated user. Required if the proxy server requires authentication.

## CHAPTER 138

# Microsoft SharePoint connection properties

When you create a Microsoft SharePoint connection, you must configure the connection properties.

The following table describes the Microsoft SharePoint connection properties:

Property	Description
Connection Name	Enter the Microsoft SharePoint connection.
Description	Provide a relevant description for the connection.
Type	Select the type of connection as Microsoft SharePoint connection.
Runtime Environment	Runtime environment that contains the Secure Agent used to access Microsoft SharePoint.
Username	Enter the Microsoft SharePoint account username.
Password	Enter the Microsoft SharePoint account password.
SharePoint URL	Enter the URI for the data source exposed via OData protocol layer. All requests are extensions of this URI. For example, <a href="https://infasharepoint.abcd.com/Site/_vti_bin/Data.svc">https://infasharepoint.abcd.com/Site/_vti_bin/Data.svc</a>
UTC Offset	Select the UTC time offset to be appended with datetime field. The default value is UTC. When you use the \$LastRuntime variable in a data filter, use the time zone to offset the \$LastRuntime variable.
Attachment File Path	Optional. Specify the folder path where you want to download and attach the file to Microsoft SharePoint.
Batch Size	Defines the number of rows to be fetched from Microsoft SharePoint server.
Enable Logging	Select the checkbox to enable logging.

## CHAPTER 139

# Microsoft Sharepoint Online connection properties

Create a Microsoft SharePoint Online connection to connect to Microsoft SharePoint Online and read data from or write data to Microsoft SharePoint Online. You can use Microsoft SharePoint Online connections in synchronization tasks, mappings, and mapping tasks.

You can create a subsite account in the Microsoft SharePoint Online application and specify the URL of the subsite account in the connection properties. Subsites enable you to categorize data as per your requirements.

For more information about how to create a subsite Microsoft SharePoint Online account, see <https://support.office.com/en-us/article/Create-sites-and-subsites-FD5031E1-162F-436E-95C7-3946F034D350>

## Prepare for authentication

You can configure Access Control Service and Microsoft Entra ID authentication types to access Microsoft SharePoint Online. Consider using Microsoft Entra ID authentication to connect more securely to Microsoft SharePoint Online.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

### Access Control Service

In Microsoft SharePoint Online, you can register applications in Access Control Service for app-only access, and the admin can restrict site access through the SharePoint admin center.

#### Generate the client ID and client secret

The client ID and client secret are required to generate a valid access token.

1. Log in to the Microsoft SharePoint Online account.
2. Enter the following site or subsite URL:

**Site:** `https://<sitename.com>/_layouts/15/appregnew.aspx`

**Subsite:** `https://<sitename.com>/<subsitelocation>/_layouts/15/appregnew.aspx`

The **App Information** page appears.



3. Click **Generate** next to the **Client Id** field.

The value of the client ID is displayed in the **Client Id** field. The following image shows the **App Information** page where you can generate the values of the client ID and client secret:

The screenshot shows a form with the following fields and values:

- Client Id:** f30abc2c-3971-4608-ac48-b02ee513c! (with a Generate button)
- Client Secret:** meeBciu+DR+KQo43itrAkoykKTU1Wa (with a Generate button)
- Title:** SharePoint
- App Domain:** www.app\_domain.com (with an example: "www.contoso.com")
- Redirect URL:** https://informaticaone.sharepoint.com (with an example: "https://www.contoso.com/default.aspx")

4. Click **Generate** next to the **Client Secret** field.  
The value of the client secret is displayed in the **Client Secret** field.
5. Enter an appropriate title for the App in the **Title** field.
6. Enter an app domain name in the **App Domain** field.  
For example, `www.google.com`
7. Enter a URL in the **Redirect URL** field.  
For example, `https://localhost/`. You must enter the same redirect URL in the connection property.
8. Click **Create**.

The page redirects to the Microsoft SharePoint Online page and the following message appears:

The app identifier has been successfully created.

The values of the client ID, client secret, title, and redirect URL are displayed.

## Generate the bearer realm

A bearer realm is a unique ID provided for each user. Generate the bearer realm to obtain the authorization code.

1. Open the Google PostMan application.
2. Enter the following site or subsite URL in the Google PostMan application:

**Site:** `https://<sitename.com>/_layouts/15/appregnew.aspx`

**Subsite:** `https://<sitename.com>/<subsitename.com>/_layouts/15/appregnew.aspx`

The following image shows the **BearerToken** page where you can generate the value of the bearer realm:

The screenshot shows the BearerToken page in Google PostMan. The URL is `https://informaticaone.sharepoint.com/_vti_bin/client.svc`. The Headers tab is selected, and the Authorization header is configured as follows:

Key	Value	Description
<input checked="" type="checkbox"/> Authorization	Bearer	
<input type="checkbox"/> New key	Value	Description

3. Select the **GET** method.
4. On the **Headers** tab, enter **Authorization** in the **Key** field and **Bearer** in the **Value** field.

5. Click **Send**.
6. Select the **Headers** tab in the **Response** header.

The bearer realm value appears in the **WWW-Authenticate** section. For example:

```
Bearer realm="77baf95d-f3e0-42b-aa08-9b798b8c177b"
```

## Generate the authorization code

Generate the authorization code to gain access to the current site and to generate a valid refresh token.

Perform the following steps to generate the authorization code:

1. Enter the following site or subsite URL in the Google chrome browser:

**Site:** `https://<site.sharepoint.com>/_layouts/15/OAuthAuthorize.aspx?`

`client_id=<client_GUID>&scope=<app_permissions_list>&response_type=code&redirect_uri=<redirect_uri>`

**For example,** `https://icloudconnectivitydev.sharepoint.com/_layouts/15/oauthauthorize.aspx?`

`client_id=ecea5b1b-80e4-4f3e-a269-48b85c1797a8&`

`scope=AllSites.Manage&response_type=code&redirect_uri=https%3A%2F%2Flocalhost%2F`

**Subsite:** `https://<site.sharepoint.com>/<subsiteid>/_layouts/15/OAuthAuthorize.aspx?`

`client_id=<client_GUID>&scope=<app_permissions_list>&response_type=code&redirect_uri=<redirect_uri>`

**For example,** `//informaticaone.sharepoint.com/sites/TEST/_layouts/15/oauthauthorize.aspx?`

`client_id=ecea5b1b-80e4-4f3e-a269-48b85c1797a8&`

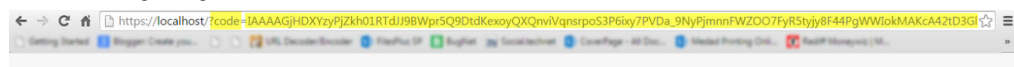
`scope=AllSites.Manage&response_type=code&redirect_uri=https%3A%2F%2Flocalhost%2F`

2. Click **Trust it** to grant the application read access to the current site after the page redirects to the redirect URL page that you specify in the connection property.

The redirect URL page includes the authorization code as a query string in the following format:

`https://<redirect_url>/?code=<authcode>`

The following image shows the authorization code in the URI:



**Note:** The authorization code generated is valid only for five minutes.

## Generate the Refresh Token

You need a refresh token to perform the POST and GET methods in the PostMan application. After you generate a refresh token, it remains valid for six months.



3. Click **New Registration**.
4. Specify a display name for your application and supported account type, enter the redirect URI and then click **Register**.  
 Ensure that you select either the Single tenant or Multitenant account type. You can't use the personal Microsoft account type.  
 A client ID is generated. Ensure that you copy the client ID and keep it handy to use when you configure a Microsoft SharePoint connection.
5. Click **Add a Certificate or Secret**.
6. Click **New client secret**, and then add the description and the expiry time.  
 A client secret value is generated. Ensure that you copy the secret value and keep it handy to use when you configure a Microsoft SharePoint connection.
7. Now, click **API permissions** in the left pane.
8. Click **Add a permission**.
9. Click **SharePoint**, and then click **Delegated permission** on the Request API permissions page.
10. Select the permissions that the client application must have on behalf of the signed-in user.  
 The following list outlines the permissions and the levels of access each permission provides:
  - **AllSites.FullControl**. Full Control access.
  - **AllSites.Manage**. Read and write access.
  - **AllSites.Read**. Read access.
  - **AllSites.Write**. Write access
 Consider selecting the AllSites.Manage permission to ensure appropriate access to SharePoint Online.
11. Click **Add Permissions**.

## Generate the authorization code for Entra ID

You can use the tenant ID to generate the authorization code.

1. Open the PostMan application.
2. In Postman, enter one of the following URLs based on your account type:
  - For a single tenant account, enter the following URL: `https://login.microsoftonline.com/<Single_Tenant_Id_value>/oauth2/v2.0/authorize`
  - For a multi-tenant account, enter the following URL: `https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize`

Replace `<Single_Tenant_Id_value>` with the tenant ID found in the overview section of your registered application if you are working with a single tenant account. For multi-tenant accounts, use the organizations endpoint.

3. Select the **GET** method.
4. On the **Params** tab, enter the name and value.

To authenticate and verify access permissions, enter the following query parameters:

```
client_id=<client_id> &response_type=code &redirect_uri=<redirect_URI>
&scope=<sharepoint_url>/<delegated permission> offline_access
&client_secret=<client_secret>
```

The scope query contains delegated permissions for your Azure application. If you selected **AllSites.Manage** as the delegated permission when you registered the Azure application with Azure

Active Directory, specify the permission in the scope query parameter as shown in the following example:

```
client_id=<client_id> &response_type=code &redirect_uri=<redirect_URI>
&scope=<sharepoint_url>/AllSites.Manage offline_access &client_secret=<client_secret>.
```

5. Copy the URL and paste it in the browser.
6. Enter the SharePoint Online log in credentials.
7. Verify and click **Accept** on the consent screen.

The redirect URL page includes the authorization code as a query string in the following format:

```
https://<redirect_url>/?code=<authcode>
```

Ensure that you copy the authorization code and keep it handy to use when you generate a refresh token.

## Generate refresh token for Entra ID

Generate the refresh token in the PostMan application.

1. In Postman, enter one of the following URLs based on your account type:
  - For a single tenant account, enter the following URL: `https://login.microsoftonline.com/<Single_Tenant_Id_value>/oauth2/v2.0/token`
  - For a multi-tenant account, enter the following URL: `https://login.microsoftonline.com/organizations/oauth2/v2.0/token`

Replace `<Single_Tenant_Id_value>` with the tenant ID found in the overview section of your registered application if you are working with a single tenant account. For multi-tenant accounts, use the organizations endpoint.

2. Select the **POST** method.
3. On the **Header** tab, enter **Content-Type** in the **Key Name** field and **application/x-www-form-urlencoded** in the **Value** field.
4. On the **Body** tab, enter the xml request in the following format:

```
grant_type=authorization_code &client_id=<client_id>&client_secret=<client_secret>
&code=<auth_code> &redirect_uri=<redirect_url>
```

You must use the client ID and client secret that you generated when you registered the Azure application with Azure Active Directory.

5. Click **Send**.

The refresh token is generated in the **Response** tab.

A refresh token is generated. Ensure that you copy the refresh token and keep it handy to use when you configure a Microsoft SharePoint connection.

# Connect to Microsoft Sharepoint Online

Let's configure the Microsoft SharePoint Online connection properties to connect to Microsoft SharePoint Online.

## Before you begin

Before you get started, you'll need to get information from your SharePoint Online account based on the authentication type that you want to configure.

To configure Access Control Service authentication, generate the client ID, client secret, bearer realm, authorization code, and refresh code from your Microsoft SharePoint Online account.

To configure Microsoft Entra ID authentication, get the client ID, client secret and the refresh token from your Microsoft SharePoint Online account.

Check out ["Prepare for authentication" on page 412](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Sharepoint Online
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.

## SharePoint Online authentication types

You can configure Access Control Service and Microsoft Entra ID authentication types to access SharePoint Online.

Select the required connection type and then configure the connection-specific parameters.

### Access Control Service

You can use the Access Control Service authentication to access the SharePoint API.

The following table describes the basic connection properties for Access Control Service authentication:

Property	Description
Client_Id	Client ID of Microsoft SharePoint Online required to generate a valid access token.
Client_Secret	Client secret of Microsoft SharePoint Online required to generate a valid access token.
Refresh-Token	Refresh token of Microsoft SharePoint Online.
Redirect_URL	URL where you want to redirect from the Microsoft SharePoint Online account.
URL	URL to the Microsoft SharePoint Online account.
Attachment_File_Path	Directory on the Secure Agent machine where you want to download or attach files to Microsoft SharePoint Online.

The following table describes the advanced connection properties for Access Control Service authentication:

Property	Description
Subsite_URL	URL of the Microsoft SharePoint Online account within the Microsoft SharePoint site. If you do not enter a subsite URL, the Microsoft SharePoint Online Connector reads the files from the URL that you specify in the <b>URL</b> property.

## Microsoft Entra ID

You can use the Microsoft Entra ID authentication to access Microsoft SharePoint resources securely.

The following table describes the basic connection properties for Microsoft Entra ID authentication:

Property	Description
Account types	The tenant that you want to use to access the application. Select from the following options: <ul style="list-style-type: none"> <li>- Single tenant. Select if your target audience is inside your organization.</li> <li>- Multi tenant. Select if your target audience includes businesses or educational customers and requires multi-tenancy support.</li> <li>- Default is None.</li> </ul>
Single tenant id	Required only when you select the Single tenant account type. The unique ID of the organization to manage and control access to resources, applications, devices, and services.
Client_Id	Client ID of Microsoft SharePoint Online required to generate a valid access token.
Client_Secret	Client secret of Microsoft SharePoint Online required to generate a valid access token.
Refresh-Token	Refresh token of Microsoft SharePoint Online.
Redirect_URL	URL where you want to redirect from the Microsoft SharePoint Online account.

Property	Description
URL	URL to the Microsoft SharePoint Online account.
Attachment_File_Path	Directory on the Secure Agent machine where you want to download or attach files to Microsoft SharePoint Online.

The following table describes the advanced connection properties for Microsoft Entra ID authentication:

Property	Description
Subsite_URL	Enter the subsite URL of the Microsoft SharePoint Online account. If you do not enter a subsite URL, the Microsoft SharePoint Online Connector reads the files from the URL that you specify in the <b>URL</b> property.



## CHAPTER 140

# Microsoft SQL Server CDC connection properties

When you configure a SQL Server CDC connection, you must set the connection properties.

The following table describes SQL Server CDC connection properties:

Property	Description
Connection Name	A name for the SQL Server CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the SQL Server CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For SQL Server CDC, the type must be <b>SQL Server CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for SQL Server change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  MSSCDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The SQL Server instance name that is specified in the <b>Instance</b> field of the registration group that contains the registrations for the SQL Server source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Logger DBID	The DBID parameter value that is specified in the PowerExchange Logger for Linux, UNIX, and Windows configuration file, pwxocl.cfg. This value is required only if the PowerExchange Logger extracts change data for articles in multiple publication databases. In this case, you must also set the MULTIPUB parameter to Y in the MSQL CAPI_CONNECTION statement in the PowerExchange dbmover.cfg configuration file. Otherwise, the extraction fails.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code> For example: <code>MSSCDC2B:25100</code> <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.

Property	Description
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a SQL Server table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="505 785 959 810">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="505 1100 1403 1205" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 141

# Microsoft SQL Server connection properties

Create a Microsoft SQL Server connection to read from or write data to Microsoft SQL Server.

## Prepare for authentication

You can configure Database or Kerberos authentication method to connect to Microsoft SQL Server. Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use. For Kerberos authentication, you need to configure certain prerequisites.

### Prepare for Kerberos authentication

You can use Kerberos authentication to connect to Microsoft SQL Server databases by placing the required configuration files on the Secure Agent machine. You can also use Kerberos authentication to connect to SSL-enabled Microsoft SQL Server databases.

**Note:** Data Ingestion and Replication does not support Kerberos authentication.

When you configure Kerberos authentication to connect to Microsoft SQL Server, consider the following guidelines:

- You can't use the Hosted Agent or serverless runtime environment.
- Ensure that the Secure Agent and database server that you use are registered in the KDC server.
- You can't add more than one KDC to a krb5.conf file.
- You can't generate a credential cache file for more than one Kerberos principal user.

### Configuring Kerberos authentication

Before you use Kerberos authentication to connect to Microsoft SQL Server on Linux or Windows, the organization administrator needs to perform the prerequisite tasks.

1. To configure the Java Authentication and Authorization Service configuration file (JAAS), perform the following tasks:
  - a. Create a JAAS configuration file on the Secure Agent machine.

- b. Add the following entries to the JAAS configuration file:

```
JDBC_DRIVER_01 {
  com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;
};
```

2. To configure the `krb5.conf` file, perform the following tasks:

- a. Create a `krb5.conf` file on the Secure Agent machine.
- b. Add the details of the Key Distribution Center (KDC) and admin server to the `krb5.conf` file in the following format:

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
<REALM NAME> = {
  kdc = <Location where KDC is installed>
  admin_server = <Location where KDC is installed>
}

[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>
```

3. Set the following environment variables on the Secure Agent machine.  
For more information about the required environment variables, see [“Setting environment variables” on page 425](#).
4. Restart the Secure Agent.
5. To generate the credential cache file on the Secure Agent machine and use Kerberos authentication to connect to Microsoft SQL Server, perform the following tasks:
  - a. On the Secure Agent machine, run the following command and specify the Microsoft SQL Server user name and realm name:

```
Kinit <user name>@<realm_name>
```
  - b. When prompted, enter the password for the Kerberos principal user.

## Setting environment variables

To use Kerberos authentication to connect to Microsoft SQL Server, you need to set the required environment variables on the Secure Agent machine.

Set the following environment variables:

- `setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>`
- `setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf`
- `setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf`

After you set the environmental variables, you need to restart the Secure Agent.

Alternatively, you can add the environment variables when you create a Microsoft SQL Server connection.

To add the environment variables when you configure a connection and use Kerberos authentication, you need to add the `KRB5_CONFIG`, `KRB5CCNAME`, and `JAASCONFIG` properties in the **Metadata Advanced Connection Properties** field in a Microsoft SQL Server connection.

For example, add the properties in the following format:

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>
\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File
name>;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf
```

**Note:** Ensure that you separate each key-value pair with a semicolon.

## Connect to Microsoft SQL Server

Let's configure the Microsoft SQL Server connection properties to connect to Microsoft SQL Server databases.

### Before you begin

Before you get started, you'll need to get information from your SQL Server DB account based on the authentication method and the type of SQL server DB to which you want to connect.

Check out ["Prepare for authentication" on page 424](#) to learn more about the authentication prerequisites.

### Connection details

The following table describes the Microsoft SQL Server connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Type of connection. Select SQL Server from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or serverless runtime environment.
SQL Server Version	Microsoft SQL Server database version.

### Authentication types

You can configure one of the following authentication modes to connect to Microsoft SQL Server databases:

- **SQL Server Authentication.** Uses your Microsoft SQL Server user name and password to access Microsoft SQL Server.
- **Windows Authentication (Deprecated).** Uses the Microsoft Windows authentication to access Microsoft SQL Server. This option is available when you access Data Integration by using Microsoft Windows.

When you choose this option, you don't need to enter credentials to access Microsoft SQL Server and ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database.

**Note:** Windows authentication is not certified for Microsoft SQL Server 2017 version hosted on Linux. You can't configure Windows Authentication when you use a serverless runtime environment.

- Active Directory Password. Uses the Azure Active Directory user name and password to authenticate and access the Microsoft Azure SQL Database.

**Note:** Database Ingestion and Replication supports this authentication mode for initial load jobs and for incremental load and combined initial and incremental load jobs that use the **CDC Tables** or **Log-based** capture method. If you use this option for these jobs, verify that the **Validate Server Certificate** value is False.

- Windows Authentication v2. Uses this authentication method to access Microsoft SQL Server from Data Integration or Data Ingestion and Replication using an agent hosted on a Linux or Windows machine. When you choose this option on Linux, enter your domain name and Microsoft Windows credentials to access Microsoft SQL Server.

When you choose this option on Windows, the agent uses the user credentials specified in the connection only to test the connection. During runtime, the agent uses the credentials of the user who started the Secure Agent service. Ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database.

**Note:** You can't configure Windows Authentication when you use a serverless runtime environment.

- Kerberos. Uses Kerberos authentication to connect to Microsoft SQL Server. Data Ingestion and Replication does not support this authentication type. When you choose this option on Windows, ensure that the user account that starts the Secure Agent service is available in the Microsoft SQL Server database. You don't need to enter your credentials to access Microsoft SQL Server.

**Note:** You can't configure the Kerberos authentication when you use a Hosted Agent or serverless runtime environment.

Select the required authentication type and then configure the authentication-specific parameters.

Default is SQL Server Authentication.

## SQL Server authentication

The following table describes the basic connection properties for SQL Server authentication:

Property	Description
Domain	Applies to Windows Authentication v2. The domain name of the Windows user.
User Name	User name for the database login. The user name can't contain a semicolon. To connect to Microsoft Azure SQL Database, specify the user name in the following format: <code>username@host</code> If you use Windows Authentication v2 on Windows, the user name is used as follows: <ul style="list-style-type: none"><li>- During design time, the agent uses the user name specified here to test the connection.</li><li>- During runtime, the Microsoft SQL server driver ignores the user name specified in this field and uses the credentials of the user who started the Secure Agent service.</li></ul> If you use Windows Authentication v2 on Linux, the user name specified here is used both during design time and runtime. <b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.

Property	Description
Password	<p>Password for the database login. The password can't contain a semicolon.</p> <p>If you use Windows Authentication v2 on Windows, the password is used as follows:</p> <ul style="list-style-type: none"> <li>- During design time, the agent uses the password specified here to test the connection.</li> <li>- During runtime, the Microsoft SQL server driver ignores the password specified in this field and uses the credentials of the user who started the Secure Agent service.</li> </ul> <p>If you use Windows Authentication v2 on Linux, the password specified here is used both during design time and runtime.</p> <p><b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.</p>
Host	<p>Name of the machine hosting the database server.</p> <p>To connect to Microsoft Azure SQL Database, specify the fully qualified host name.</p> <p>For example, <code>vmjcmwxsfbheng.westus.cloudapp.azure.com</code>.</p>
Port	<p>Network port number used to connect to the database server.</p> <p>Default is 1433.</p>
Instance Name	<p>Instance name of the Microsoft SQL Server database.</p>
Database Name	<p>Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters.</p> <p>Database names can include alphanumeric and underscore characters.</p>
Schema	<p>Schema used for the target connection.</p>
Code Page	<p>The code page of the database server.</p>

## Windows authentication

The following table describes the basic connection properties for Windows authentication:

Property	Description
Domain	<p>Applies to Windows Authentication v2.</p> <p>The domain name of the Windows user.</p>
Host	<p>Name of the machine hosting the database server.</p> <p>To connect to Microsoft Azure SQL Database, specify the fully qualified host name.</p> <p>For example, <code>vmjcmwxsfbheng.westus.cloudapp.azure.com</code>.</p>
Port	<p>Network port number used to connect to the database server.</p> <p>Default is 1433.</p>
Instance Name	<p>Instance name of the Microsoft SQL Server database.</p>
Database Name	<p>Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters.</p> <p>Database names can include alphanumeric and underscore characters.</p>



Property	Description
Schema	Schema used for the target connection.
Code Page	The code page of the database server.

## Active Directory Password authentication

The following table describes the basic connection properties for Active Directory Password authentication:

**Note:** Database Ingestion and Replication supports this authentication mode for initial load jobs and for incremental load and combined initial and incremental load jobs that use the **CDC Tables** or **Log-based** capture method.

Property	Description
Domain	Applies to Windows Authentication v2. The domain name of the Windows user.
User Name	User name for the database login. The user name can't contain a semicolon. To connect to Microsoft Azure SQL Database, specify the user name in the following format: <code>username@host</code> If you use Windows Authentication v2 on Windows, the user name is used as follows: <ul style="list-style-type: none"> <li>- During design time, the agent uses the user name specified here to test the connection.</li> <li>- During runtime, the Microsoft SQL server driver ignores the user name specified in this field and uses the credentials of the user who started the Secure Agent service.</li> </ul> If you use Windows Authentication v2 on Linux, the user name specified here is used both during design time and runtime. <b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Password	Password for the database login. The password can't contain a semicolon. If you use Windows Authentication v2 on Windows, the password is used as follows: <ul style="list-style-type: none"> <li>- During design time, the agent uses the password specified here to test the connection.</li> <li>- During runtime, the Microsoft SQL server driver ignores the password specified in this field and uses the credentials of the user who started the Secure Agent service.</li> </ul> If you use Windows Authentication v2 on Linux, the password specified here is used both during design time and runtime. <b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Host	Name of the machine hosting the database server. To connect to Microsoft Azure SQL Database, specify the fully qualified host name. For example, <code>vmjcmwxsfbheng.westus.cloudapp.azure.com</code> .
Port	Network port number used to connect to the database server. Default is 1433.
Instance Name	Instance name of the Microsoft SQL Server database.
Database Name	Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters. Database names can include alphanumeric and underscore characters.

Property	Description
Schema	Schema used for the target connection.
Code Page	The code page of the database server.

## Windows Authentication V2

The following table describes the basic connection properties for Windows Authentication V2:

Property	Description
Domain	Applies to Windows Authentication v2. The domain name of the Windows user.
User Name	User name for the database login. The user name can't contain a semicolon. To connect to Microsoft Azure SQL Database, specify the user name in the following format: <code>username@host</code> If you use Windows Authentication v2 on Windows, the user name is used as follows: <ul style="list-style-type: none"> <li>- During design time, the agent uses the user name specified here to test the connection.</li> <li>- During runtime, the Microsoft SQL server driver ignores the user name specified in this field and uses the credentials of the user who started the Secure Agent service.</li> </ul> If you use Windows Authentication v2 on Linux, the user name specified here is used both during design time and runtime. <b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Password	Password for the database login. The password can't contain a semicolon. If you use Windows Authentication v2 on Windows, the password is used as follows: <ul style="list-style-type: none"> <li>- During design time, the agent uses the password specified here to test the connection.</li> <li>- During runtime, the Microsoft SQL server driver ignores the password specified in this field and uses the credentials of the user who started the Secure Agent service.</li> </ul> If you use Windows Authentication v2 on Linux, the password specified here is used both during design time and runtime. <b>Note:</b> This property is not applicable if you use the Windows Authentication mode to access Microsoft SQL Server.
Host	Name of the machine hosting the database server. To connect to Microsoft Azure SQL Database, specify the fully qualified host name. For example, <code>vmjcmwxsfbheng.westus.cloudapp.azure.com</code> .
Port	Network port number used to connect to the database server. Default is 1433.
Instance Name	Instance name of the Microsoft SQL Server database.
Database Name	Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters. Database names can include alphanumeric and underscore characters.

Property	Description
Schema	Schema used for the target connection.
Code Page	The code page of the database server.

## Kerberos authentication

The following table describes the basic connection properties for Kerberos authentication:

**Note:** Data Ingestion and Replication does not support Kerberos authentication.

Property	Description
Domain	Applies to Windows Authentication v2. The domain name of the Windows user.
Host	Name of the machine hosting the database server. To connect to Microsoft Azure SQL Database, specify the fully qualified host name. For example, <code>vmjcmwxsfbheng.westus.cloudapp.azure.com</code> .
Port	Network port number used to connect to the database server. Default is 1433.
Instance Name	Instance name of the Microsoft SQL Server database.
Database Name	Database name for the Microsoft SQL Server target connection. Database name is case-sensitive if the database is case-sensitive. Maximum length is 100 characters. Database names can include alphanumeric and underscore characters.
Schema	Schema used for the target connection.
Code Page	The code page of the database server.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Encryption Method	The method that the Secure Agent uses to encrypt the data sent between the driver and the database server. You can use the encryption method to connect to Microsoft Azure SQL Database. Default is None.
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption.

Property	Description
Validate Server Certificate	<p>When set to True, Secure Agent validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Secure Agent also validates the host name in the certificate.</p> <p>When set to false, the Secure Agent doesn't validate the certificate that is sent by the database server.</p>
Trust Store	<p>The location and name of the truststore file. The truststore file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Trust Store Password	The password to access the contents of the truststore file.
Host Name in Certificate	Host name of the machine that hosts the secure database. If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata.</p> <p>Enter properties in the following format:</p> <pre>&lt;parameter name&gt;=&lt;parameter value&gt;</pre> <p>If you enter more than one property, separate each key-value pair with a semicolon.</p> <p>For example, enter the following property to configure the connection timeout when you test a connection:</p> <pre>LoginTimeout=&lt;value_in_seconds&gt;</pre> <p><b>Note:</b> The default connection timeout is 270 seconds.</p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver required at run time.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p>

## Configure SSL with the serverless runtime environment

You can use the serverless runtime environment with Microsoft SQL Server Connector to connect to an SSL-enabled Microsoft SQL Server database.

Before you configure a secure Microsoft SQL Server connection using the serverless runtime environment, complete the following prerequisite tasks to add the SSL certificates to the serverless runtime location:

1. Create the following structure for the serverless agent configuration in AWS or Azure: <Supplementary file location>/serverless\_agent\_config
2. Add the truststore certificate in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/SSL

3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<TrustStore_filename>
```

where the source path is the directory path of the certificate file in AWS or Azure.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`  
When the .yml file runs, the SSL certificate is copied from the AWS or Azure location to the serverless agent directory.
5. In the Microsoft SQL Server connection properties, specify the following certificate path in the serverless agent directory in the **Trust Store** field: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>`

## CHAPTER 142

# Mixpanel connection properties

When you create a Mixpanel connection, configure the connection properties.

The following table describes the Mixpanel connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Mixpanel
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent or a Hosted Agent.
User Name	The user name of the Mixpanel account.
Password	The password for the Mixpanel account.

## CHAPTER 143

# MLLP connection properties

When you configure a Minimal Lower Layer Protocol (MLLP) connection, you must configure the connection properties.

The following table describes the MLLP connection properties:

Property	Description
Connection Name	A name for the MLLP connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the MLLP connection. Maximum length is 4000 characters.
Type	Type of connection. For MLLP connection, the type must be <b>MLLP</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Host	Host name or IP address of the MLLP server.
Port	Port number for the MLLP server. Default is 2575.
Response Timeout	The wait time in seconds to receive a message from the specified MLLP server after sending the message. A timeout value of 0 is interpreted as infinite timeout. Default is 60 seconds.
Connection Timeout	Maximum number of seconds to wait when attempting to connect to the server. A timeout occurs if a successful connection does not occur in the specified amount of time. If the value is 0 or blank, the wait time is infinite. Default is 30 seconds.
Connection Retry Interval	Number of seconds to wait between each connection retry attempt. For example, to retry to connect up to 10 times with a five second delay between retries, set <b>Connection Retry Attempts</b> to 10 and <b>Connection Retry Interval</b> to 5. Default is 0.
Connection Retry Attempts	Number of times to retry connecting to the MLLP server if a successful connection does not occur. This setting applies to both the initial connection and any reconnect attempts due to lost connections. Default is 0. Specify 0 to disable the retry attempts.

Property	Description
Proxy Type	Type of proxy server to use for the connection. Select one of the following options: <ul style="list-style-type: none"> <li>- No Proxy. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- HTTP. Uses the HTTP proxy.</li> <li>- SOCKS. Uses the SOCKS (version 4 and 5) proxy.</li> <li>- Platform Proxy. Considers proxy configured at the agent level.</li> </ul> Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	Host name or IP address of the proxy server on your network.
Proxy Port	Port number of the proxy server on your network.
User	User name to use for login when connecting to the proxy server.
Password	Password for connecting to the proxy server.



## CHAPTER 144

# MongoDB Mass Ingestion connection properties

When you set up a MongoDB Mass Ingestion connection, you must configure the connection properties.

The following table describes MongoDB Mass Ingestion connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 255 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ ; : " ' < , > . ? /
Description	Optional. A description of the connection. The description cannot exceed 4,000 characters.
Type	Type of connection. You must select <b>MongoDB Mass Ingestion</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Host and Port	An SRV record or a comma-separated list of <i>host_name:port</i> pairs. <b>Note:</b> If you are using the MongoDB replica set mode, you can enter multiple host names for resilience. If one host is not available, another specified host will be used.
SRV	Select this check box if you specified an SRV record in <b>Host and Port</b> property.
Authentication	The authentication method for establishing a secure connection. Select one of the following authentication modes: <ul style="list-style-type: none"><li>- <b>Username and Password</b>. Uses the user name and password credentials to connect to the MongoDB server.</li><li>- <b>X.509</b>. Uses an X.509 certificate to connect to the MongoDB server.</li></ul> Default is <b>Username and Password</b> .
SSL KeyStore File Path	If you selected <b>X.509</b> authentication, the absolute path of the keystore file on the Secure Agent machine that contains the keys and certificates required for secure communication. The keystore file must be in JKS format. Ensure that you download the certificates and place them in the Secure Agent machine before you specify this property. To successfully test the connection, the Secure Agent must have access to the specified keystore and truststore files using the passwords provided. If you use a Secure Agent group, all agents must have access to these files. Place a copy of the files on every machine where a Secure Agent runs.

Connection property	Description
SSL KeyStore Password	If you selected <b>X.509</b> authentication, the password for the keystore file that is required for secure communication.
SSL TrustStore File Path	If you selected <b>X.509</b> authentication, the absolute path of the truststore file on the Secure Agent machine.
SSL TrustStore Password	If you selected <b>X.509</b> authentication, the password for the truststore file.
User Name	If you selected <b>Username and Password</b> authentication, enter the user name to use for logging in to the database.
Password	If you selected <b>Username and Password</b> authentication, enter the password for the specified database user.
Authentication Database	The name of the authentication database associated with the specified user.
Replica Set Name	The name of the replica set that is composed of the MongoDB servers with replicas of the source data. This field is relevant if you are using the MongoDB replica set mode.
Additional Connection Properties	<p>One or more additional MongoDB connection string options that you want to use. Specify the properties as key-value pairs. If you specify more than one property, separate them with the ampersand symbol (&amp;). The connection properties are case sensitive.</p> <p>Example:</p> <pre>authSource=admin&amp;replicaSet=rsprimary</pre> <p>For more information about the MongoDB connection string options, refer to:  <a href="https://www.mongodb.com/docs/v5.2/reference/connection-string/#connection-string-options">https://www.mongodb.com/docs/v5.2/reference/connection-string/#connection-string-options</a></p>

## CHAPTER 145

# MongoDB connection properties

When you set up a MongoDB connection, configure the connection properties.

**Important:** MongoDB Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the MongoDB connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The MongoDB connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Host Name*	Host name or IP address of the MongoDB server.
Port*	MongoDB server port number. Default is 27017.
User Name*	User name to access the MongoDB server.
Password*	Password corresponding to the user name to access the MongoDB server.
Database Name	Name of the MongoDB database to connect to.

Property	Description
Additional Connection Properties	<p>The JDBC connection parameters required in a MongoDB connection. Enter one or more JDBC connection parameters in the following format:</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;</pre> <p>Provide the JDBC parameters as ampersand-separated key-value pairs. Configure the following JDBC connection parameters in a MongoDB connection:</p> <ul style="list-style-type: none"> <li>- AuthSource</li> <li>- BatchSize</li> <li>- connectTimeoutMS</li> <li>- DefaultStringColumnLength</li> <li>- DmlBatchSize</li> <li>- EnableDoubleBuffer</li> <li>- EnableTransaction</li> <li>- LogLevel</li> <li>- LogPath</li> <li>- SamplingLimit</li> <li>- SamplingStepSize</li> <li>- SamplingStrategy</li> </ul> <p>For example,</p> <pre>DefaultStringColumnLength=512&amp;DmlBatchSize=1000&amp; EnableDoubleBuffer=false&amp;EnableTransaction=true&amp; SamplingLimit=200&amp;SamplingStepSize=2&amp;SamplingStrategy=Backwards</pre>
SSL Mode	<p>SSL mode indicates the encryption type to use for the connection. SSL is not applicable when you use the Hosted Agent. You can configure SSL when you use the Secure Agent or the serverless runtime environment.</p> <p><b>Note:</b> Set it to <b>Required</b> for connecting to MongoDB Atlas.</p>
SSL Truststore Path	Not applicable for MongoDB Connector.
SSL Truststore Password	Not applicable for MongoDB Connector.
<p>*If you specify the host name, port, user name, and password of the MongoDB server in the connection properties and also in the additional connection properties field, the values in the additional connection properties take precedence.</p>	

For more information about configuring the MongoDB JDBC connection parameters, see the Informatica How-To Library article, "Configuring the Simba MongoDB JDBC Driver Options for MongoDB Connector":

<https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/configuring-the-simba-mongodb-jdbc-driver-options-for-mongodb-co/abstract.html>

## CHAPTER 146

# MongoDB V2 connection properties

When you create a MongoDB V2 connection, you must configure the connection properties.

The following table describes the MongoDB V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	MongoDB V2
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	Name of the runtime environment where you want to run tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Node name or IP address of the primary shard in the MongoDB cluster.
Service Record Lookup Enabled	The connection format to indicate that the hostname corresponds to a DNS Service Record Lookup. It enables the connector to query the DNS to construct the available server list that runs MongoDB instances. Select this checkbox if the host name corresponds to a DNS SRV record. Port is not considered if this checkbox is selected.

Property	Description
Port	MongoDB server port number. Default is 27017.
Authentication	Authentication method to access the MongoDB resources. Choose one of the following authentication methods: <ul style="list-style-type: none"> <li>- Username and Password. Uses user name and password credentials to connect to the MongoDB server.</li> <li>- X.509. Uses X.509 certificate to connect to the MongoDB server.</li> </ul>
User Name	User name to access the MongoDB server.
Password	Password corresponding to the user name to access the MongoDB server.
SSL KeyStore File Path	The absolute path of the keystore file in the Secure Agent machine that contains the keys and certificates required to establish a secure communication. Ensure that you download the certificates and place them in the Secure Agent machine before you specify this parameter. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;keystore_filename&gt;</code> For more information, see the <a href="#">"Configure SSL for the serverless runtime environment" on page 444</a> chapter. Applicable if you select X.509 authentication type.
SSL KeyStore Password	The password for the keystore file required for secure communication. Applicable if you select X.509 authentication type.
Database Name	Name of the MongoDB database that you want to connect to.
Additional Properties	Optional properties that you can configure to read data from or write data to Amazon DocumentDB and other non-SSL MongoDB deployments. For information about the additional properties that you can configure, see the <a href="#">"Additional connection properties" on page 442</a> chapter. To specify more than one property, separate the key-value pairs with an ampersand. You can specify the properties in the following format: <code>propertyName1=&lt;value1&gt;&amp;propertyName2=&lt;value2&gt;</code>

## Additional connection properties

You can configure additional options in a MongoDB V2 connection.

### Amazon DocumentDB optional properties

Configure additional connection properties in the Additional Properties field to connect to Amazon DocumentDB:

### **ssltruststorefilepath**

The absolute path of the truststore file in the Secure Agent machine that contains the keys and certificates required to establish a secure communication.

For example, `ssltruststorefilepath= <path_of_truststore_file>`

For the serverless runtime environment, specify the following certificate path to the serverless agent directory:

```
/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<truststore_filename>
```

For more information, see [“Configure SSL for the serverless runtime environment” on page 444](#) chapter.

### **ssltruststorepassword**

The password for the truststore file required for secure communication.

For example, `ssltruststorepassword=<password>`.

## Sampling properties

Configure sampling properties in the Additional Properties field:

### **samplesize**

The number of documents to scan to infer the schema from the MongoDB source.

For example, `samplesize=100`.

Default is 100.

### **samplemethod**

The method to sample documents to infer the schema from the MongoDB source.

You can specify one of the following methods:

- `firstpage`. Scans first `n` documents from MongoDB where `n` indicates the sample size. MongoDB determines the ordering of rows for scanning.
- `random`. Scans `n` number of random documents from MongoDB.
- `all`. Scans the entire collection to infer schema.

## Other properties

Configure additional connection properties in the Additional Properties field to connect to non-SSL MongoDB deployments:

### **ssl**

Determines if the connection uses SSL or non-SSL.

Set this parameter to `false` in the connection properties to connect to MongoDB deployments that do not use SSL.

Default is `true`.

### **authsource**

Allows you to provide the database name against which you can authenticate user credentials.

For example, `authsource=testadmin`.

Default is `admin`.

# Configure SSL for the serverless runtime environment

You can use the serverless runtime environment with MongoDB V2 Connector to connect to an SSL-enabled MongoDB database.

Before you configure a secure MongoDB V2 connection using the serverless runtime environment, you need to perform certain prerequisites:

1. Ensure that the truststore and keystore certificate files are in .jks format.
2. Add the truststore and keystore certificates in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/SSL
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<cert_filename>
        - fileCopy:
            sourcePath: SSL/<cert_filename>
```

where the source path is the directory path of the certificate files in AWS or Azure.

**Note:** You can add multiple source paths of the certificate files by adding multiple *fileCopy* tags.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the SSL certificates are copied from the AWS or Azure location to the serverless agent directory.
5. Deploy the serverless agent.
6. Specify the following certificate path in the serverless agent directory for the truststore and keystore file path fields: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>`



## CHAPTER 147

# MQTT connection properties

When you set up an MQ Telemetry Transport (MQTT) connection, you must configure the connection properties.

The following table describes the MQTT connection properties:

Property	Description
Connection Name	Name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { [ ]   \ : ; " ' < , > . ? /
Description	Optional. Description that you can use to identify the connection. The description cannot exceed 4,000 characters.
Type	The MQTT connection type. If you do not see the connection type, go to the <b>Add-On Connectors</b> page to install the connector.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Broker URI	The connection URL of the MQTT broker. If specified, this value overrides the URL specified in the main portion of the URL. Sample URL: <code>tcp://&lt;IP Address&gt;:&lt;port&gt;</code>
Client Id	Client identifier of your MQTT client. If this value is left blank, the MQTT server assigns a unique value. This property value must be unique for each MQTT client connecting to a specific MQTT server. Sharing projects without changing the Client ID can lead to connection issues, including disconnections and missing updates.
Username	Username to use when connecting to the broker.
Password	Password to use when connecting to the broker.
Connection Timeout	Maximum time interval the client will wait for the connection to the MQTT server to be established. Default timeout is 30 seconds. A value of 0 disables timeout processing. That is, the client waits until the network connection is made successfully or fails.

Property	Description
Use SSL	Enable this option to use SSL for secure transmission. If you enable the SSL authentication, ensure to provide both keystore and truststore details for using the MQTT connection in a streaming ingestion and replication task.
Keystore Filename	Contains the keys and certificates required for secure communication.
Keystore Password	Password for the keystore filename.
Keystore Type	Type of keystore to use. Keystore type defines the storage and data format of the keystore information and the algorithms used to protect private keys in the keystore. Use one of the following types: <ul style="list-style-type: none"> <li>- JKS. Stores private keys and certificates.</li> <li>- PKCS12. Stores private keys, secret keys. and certificates.</li> </ul>
Truststore Filename	File name of the truststore file.
Truststore Password	Password for the truststore file name.
Truststore Type	Type of truststore to use. Use one of the following types: <ul style="list-style-type: none"> <li>- JKS</li> <li>- PKCS 12</li> </ul>
TLS Protocol	Transport protocols to use. Use one of the following types: <ul style="list-style-type: none"> <li>- SSL</li> <li>- SSLv3</li> <li>- TLS</li> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul>

## CHAPTER 148

# MRI Software connection properties

**Important:** Effective in the November 2024 release, MRI Software Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

When you set up an MRI Software connection, you must configure the connection properties.

The following table describes the MRI Software connection properties:

Property	Description
Connection Name	Enter a name for the connection.
Description	Optional. Enter a description for the connection.
Type	Type of connection. Select <b>MRI Software</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
URL	Endpoint URL of the MRI Software application.
Username	User name of the MRI Software application.
Password	Password for the MRI Software application.
Client ID	The client ID created in the MRI Software application.
Database Name	Name of the MRI database.
Partner Key	The partner key provided by MRI Software.
API Type	The type of MRI Software API that you want to connect to. Select one of the following options: <ul style="list-style-type: none"><li>- <b>Data Pipeline</b>. Select to connect to the Data Pipeline API to read large amount of data.</li><li>- <b>REST</b>. Select to connect to the REST API.</li></ul>

## CHAPTER 149

# MySQL CDC connection properties

When you configure a MySQL CDC connection, you must set the connection properties.

The following table describes MySQL CDC connection properties:

Property	Description
Connection Name	A name for the MySQL CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the MySQL CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For MySQL CDC, the type must be <b>MySQL CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for MySQL change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example:  <code>MYSCDC1A:1467</code>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	MySQL instance name that is specified in the <b>Instance</b> field of the registration group that contains capture registrations for the MySQL source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system that contains the extraction maps. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.  Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  MYSCDC2B:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a MySQL table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 963 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 150

# MySQL connection properties

When you set up a MySQL connection, configure the connection properties.

The following table describes the MySQL connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Type of connection. Select MySQL from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. <b>Note:</b> You cannot run a database ingestion and replication task on a Hosted Agent or serverless runtime environment.
User Name	User name for the database login. The user name can't contain a semicolon.
Password	Password for the database login. The password can't contain a semicolon.
Host	Name of the machine that hosts the database server. <b>Note:</b> The host name is auto populated with the port number if you have enabled the Secret Vault licenses in your Organization. You can remove the port number and enter the host name.
Port	Network port number used to connect to the database server. Default is 3306.
Database Name	Name of the MySQL database that you want to connect to. <b>Note:</b> The database name is case-sensitive. Maximum length is 64 characters. Database name can contain alphanumeric and underscore characters.
Code Page	The code page of the database server.

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata. Enter properties in the following format:</p> <pre>&lt;parameter name&gt;=&lt;parameter value&gt;</pre> <p>If you enter more than one property, separate each key-value pair with a semicolon.</p> <p>For example, enter the following property to configure the connection timeout when you test a connection:</p> <pre>connectTimeout=&lt;value_in_milliseconds&gt;</pre> <p><b>Note:</b> The default connection timeout is 270000 milliseconds.</p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver to run mappings ingestion and replication jobs.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p>

## SSL properties

You can configure a MySQL connection to use SSL to securely communicate with the MySQL database.

**Note:** You can enable SSL for a MySQL connection only when you use the 8.x MySQL JDBC and ODBC drivers. Ensure that both the MySQL JDBC and ODBC drivers are of 8.x version.

To configure SSL, you must first download and install the MySQL ODBC and JDBC drivers, version 8.x. For information about installing the MySQL ODBC and JDBC drivers, version 8.x, see the Knowledge Base article: [561573](#)

After you install the drivers, in the MySQL connection properties, enable SSL and specify the TLS protocols that you want to use for the secure communication.

When you enable SSL for the MySQL connection, you must configure the SSL properties for both the MySQL JDBC and ODBC drivers. Configure the required SSL properties for the JDBC driver, so that the Secure Agent can access metadata securely from MySQL. Also, configure the required SSL properties for the ODBC driver, so that the Secure Agent runs mappings to securely read from or write data to MySQL.

**Note:** SSL is not applicable when you use the Hosted Agent. You can configure SSL when you use the Secure Agent or the serverless runtime environment.



The following table describes the MySQL connection SSL properties:

Connection property	Description
Use SSL	<p>Determines whether the Secure Agent establishes a secure connection to the MySQL database.</p> <p>When you select this option and the database server supports SSL, the Secure Agent establishes an encrypted connection. If the MySQL database server cannot configure SSL, the connection either fails or the Secure Agent establishes an unencrypted connection depending on whether you enable or disable the <b>Require SSL</b> checkbox.</p> <p>If you do not select the <b>Use SSL</b> checkbox, the Secure Agent attempts to establish an unencrypted connection.</p>
Verify Server Certificate	<p>If you select <b>Use SSL</b> and select this option, the client validates the server certificate that is sent by the database server.</p>
Require SSL	<p>Applicable only if you select <b>Use SSL</b>.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database supports SSL, the Secure Agent establishes an SSL connection.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent attempts to establish an SSL connection but fails.</p> <p>If you clear the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent establishes an unencrypted connection.</p>
TLS Protocols	<p>The TLS protocols used for the secure communication when you select <b>Use SSL</b>.</p> <p>You can select from the following protocols:</p> <ul style="list-style-type: none"> <li>- TLSv1</li> <li>- TLSv1.1</li> <li>- TLSv1.2</li> </ul> <p>Default is TLSv1.2. The TLSv1 and TLSv1.1 protocols are not applicable.</p>

The following table describes the MySQL connection properties for the JDBC driver version 8.x when you enable **Use SSL**:

Connection property	Description
Trust Certificate Key Store	<p>The path and file name of the truststore file. You must prefix the file path with file colon (file:).</p> <p>For example, <code>file:C:\SSL\mysql_new\truststore</code></p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Trust Certificate Key Store Password	<p>The password for the truststore file.</p>

Connection property	Description
Client Certificate Key Store	The path and file name of the keystore file. You must prefix the file path with file colon (file:). For example, file:C:\SSL\mysql_new\keystore For the serverless runtime environment, specify the following certificate path in the serverless agent directory: /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ <KeyStore_filename>
Client Certificate Key Store Password	The password to access the keystore file.
JDBC Cipher Suites	Colon-separated cipher suite values in RFC format. For example: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

The following table describes the MySQL connection properties for the ODBC driver version 8.x when you enable **Use SSL**:

Connection property	Description
SSL Certificate Authority	The path and name of the CA certificate. For example, C:\SSL\mysql_new\ca.pem
SSL Certificate	The path and name of the client certificate. For example, C:\SSL\mysql_new\client-cert.pem
SSL Key	The path and the name of the private key of the client. For example, C:\SSL\mysql_new\client-key.pem
SSL Cipher	Colon-separated cipher-suite values in OpenSSL format. For example: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256:
Verify Server's Identity	Verifies the host name in the certificate while verifying the server CA certificate. This property is applicable only when you enable <b>Verify Server Certificate</b> in the SSL properties.

## CHAPTER 151

# Netezza connection properties

Create a Netezza connection to securely read data from or write data to Netezza.

## Prerequisites

Before you can use Netezza Connector, install the Netezza client on Windows or Linux.

Ensure that you have access to the Secure Agent directory that contains the success and error files. This directory path must be the same on each Secure Agent machine in the runtime environment selected for your connection.

Before you create a Netezza connection, be sure to configure the Netezza ODBC and JDBC drivers.

## Download the Netezza JDBC Driver

1. Download the Netezza JDBC driver version from the IBM website:  
To download the Netezza JDBC driver on Windows, follow the instructions from the following Knowledge Base article:  
<https://kb.informatica.com/howto/6/Pages/23/619186.aspx>  
If you want to use the Netezza JDBC driver on Linux, you can use the Netezza JDBC driver downloaded for Windows on the Linux machine.
2. After you download the Netezza JDBC driver, navigate to the following location:  
<Secure Agent installation directory>/apps/Data\_Integration\_Server/ext/
3. Manually create the following directory structure:  
deploy\_to\_main/bin/rdtm-extra/Netezza
4. Copy the Netezza JDBC driver jar file, `nzjdbc.jar`, to the following directory you created on the Secure Agent machine:  
<Secure Agent installation directory>/apps/Data\_Integration\_Server/ext/  
deploy\_to\_main/bin/rdtm-extra/Netezza
5. Restart the Secure Agent.

## Download the Netezza ODBC Driver

1. Download the Netezza ODBC driver version from the IBM website:  
To download the Netezza ODBC driver, follow the instructions from the following Knowledge Base article:  
[https://knowledge.informatica.com/s/article/HOW-TO-Download-the-Netezza-ODBC-driver?language=en\\_US](https://knowledge.informatica.com/s/article/HOW-TO-Download-the-Netezza-ODBC-driver?language=en_US)
2. Perform the following tasks to use the Netezza ODBC driver based on the operating system:
  - On Windows, verify if the NetezzaSQL driver appears in the ODBC Data Source Administrator driver list.
  - On Linux, add the driver entries in the `odbcinst.ini` file in the Secure Agent installation directory. The following code shows a sample entry:

```
[NetezzaSQL]
Driver          = /data/home/adputf_9/cloud_td/Netezza/installer/linux64/lib64/
libzodbc.so
Setup          = /data/home/adputf_9/cloud_td/Netezza/installer/linux64/lib64/
libzodbc.so
APILevel       = 1
ConnectFunctions = YYN
Description     = Netezza ODBC driver
DriverODBCVer  = 03.51
DebugLogging   = true
LogPath        = /tmp
UnicodeTranslationOption = utf8
CharacterTranslationOption = all
PreFetch       = 256
Socket         = 16384
```

## Connect to Netezza

Let's configure the Netezza connection properties to connect to Netezza.

### Before you begin

Before you get started, you need to get Netezza database and authentication details from your Netezza account. You also need to install Netezza client and drivers.

Check out ["Prerequisites" on page 455](#) to learn more about the tasks you must perform.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Netezza.
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment. Specify a Secure Agent.
Database	The name of the Netezza database.
Schemaname	The schema used for the Netezza source or target. Schema name is case sensitive.
Servername	The Netezza database host name.
Port	Network port number used to connect to the database server. Default is 1521.

Property	Description
Username	Database user name with the appropriate read and write database permissions to access the database.
Password	Password for the database user name.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Driver	The Netezza ODBC driver name that is used to connect to the Netezza database. The Netezza ODBC driver name is NetezzaSQL.
Runtime Additional Connection Configuration	Additional runtime attributes required to fetch data. For example, <code>securityLevel=preferredUnSecured;caCertFile =</code>
Metadata Additional Connection Configuration	The values to set the optional properties of the JDBC driver to fetch the metadata.

## Database privileges

Database privileges define the level of access for the operations that you can perform in the Netezza database.

Verify that you have the following privileges on the Netezza database:

- CREATE TABLE
- CREATE EXTERNAL TABLE
- DELETE
- DROP
- INSERT
- LIST
- SELECT
- TRUNCATE
- UPDATE

# CHAPTER 152

## NetSuite connection properties

Create a NetSuite connection to securely read data from or write data to NetSuite.

### Connect to NetSuite

Let's configure the NetSuite connection properties to connect to NetSuite.

#### Before you begin

Before you configure the connection properties, you'll need to get service URL, account, token ID, and token secret from your NetSuite account.

The following video shows you how to get the information you need:



#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	NetSuite

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Do not use a Hosted Agent if you use the connection in mappings in advanced mode.</p>
Service URL	<p>NetSuite Web Service Description Language (WSDL) URL to access NetSuite data.</p> <p>Consider the following rules for the authentication type that you can use for the WSDL versions:</p> <ul style="list-style-type: none"> <li>- <b>WSDL version 2016_1 to 2019_2.</b> You can use username and password or token-based authentication. If you use both, the agent considers the token-based authentication to access NetSuite.</li> </ul> <p><b>Note:</b> Informatica recommends you to use the token-based authentication for a more secure access to NetSuite.</p> <ul style="list-style-type: none"> <li>- <b>WSDL version 2020_1 and later</b> - You can use only token-based authentication.</li> </ul> <p>From version 2019_2 of the NetSuite WSDL URL, you can enter the WSDL URL used by your NetSuite account instead of the default service URL.</p> <p>The service URL used by the NetSuite account is in the following format:</p> <pre>&lt;NetSuite account URL&gt;/wsdl/v2019_2_0/netsuite.wsdl</pre> <p>Informatica recommends that you use the WSDL URL that is specific to your NetSuite account. For more information, see <i>Configuring NetSuite account-specific service URL</i>.</p> <p>By default, NetSuite connections use version 2021_2_0 of the NetSuite WSDL URL as shown in the following URL:</p> <pre>https://webservices.netsuite.com/wsdl/v2021_2_0/netsuite.wsdl</pre> <p>Informatica claims support for 2021_2, 2021_1, and 2020_2 WSDLs. You can continue to use WSDL versions older than 2019_2. However, these versions will not receive bug fixes or support.</p> <p>You can use NetSuite Connector with the NetSuite 2023_2 sandbox account or release preview account.</p>
Account	<p>NetSuite account ID.</p> <p>To get your account ID, log in to NetSuite, and then click <b>Setup &gt; Integration &gt; SOAP Web Services Preferences</b>.</p>
Token ID	<p>The token ID generated in NetSuite.</p> <p>Applies to token-based authentication.</p>
Token Secret	<p>The token secret generated in NetSuite.</p> <p>Applies to token-based authentication.</p>



## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Username	Applicable only when you use the username and password for authentication. User name for a NetSuite account. User name is an email address.
Password	Applicable only when you use the username and password for authentication. Password for the NetSuite account.
Application ID	Optional. NetSuite application ID. If the application ID property is blank, the agent uses the Informatika application ID. To find your application ID, log in to NetSuite and click <b>Setup &gt; Integration &gt; Manage Integrations</b> . If you do not have an application ID, you can create one. On the <b>Manage Integrations</b> page, click <b>New</b> . After you save the application ID, you can view the application ID number on the <b>Manage Integrations</b> page.
Record Custom Fields	Specify custom NetSuite fields. <ul style="list-style-type: none"> <li>- Add the custom fields using the following format, where the value of scriptId is the ID field in the NetSuite user interface for each custom field:  <pre>[&lt;Object Name&gt;] scriptIds = &lt;custom field name1&gt;, &lt;custom field name2&gt;,&lt;custom field name3&gt;</pre> <p>For example, [Sales] scriptIds = discountPrice, salesDescription,salesEvent3</p> </li> <li>- Add the custom fields for NetSuite advanced search using the following format, where the value of scriptId is the ID field in the NetSuite user interface for each custom field:  <pre>[&lt;Object Name&gt;] scriptIds = &lt;custom field name1&gt;, &lt;custom field name2&gt;,&lt;custom field name3&gt;</pre> <p>For example, [EmployeeSearchAdvanced]scriptId = custentity74,custentity66</p> </li> <li>- To read custom segment data, use the following format to add the custom segment fields:  <pre>[&lt;Object Name&gt;] custSegScriptIds=custseg1: select,custseg2:multiselect,custseg3:select...</pre> <p>Where the value of scriptId is the ID field in the NetSuite user interface for each custom segment field. For example, [Employee] custSegScriptIds=custentity_cseg1: select,custentity_csegcs_multsel:multiselect</p> </li> <li>- To read data from child record custom segments, use the following format to add the child custom segment fields:  <pre>[&lt;Object Name&gt;] custSegScriptIds =custseg1:select,custseg2: multiselect,custseg3:select...</pre> <p>For example, [JournalEntry] custSegScriptIds =custbody_cseg1:select,custbody_cseg2:select, custbody_cseg3:select [JournalEntryLineList] custSegScriptIds =custcol_cseg1:select,custcol_cseg2:select, custcol_cseg3:select</p> </li> </ul>

Property	Description
Record Filter Fields	<p>Map NetSuite record field names with related NetSuite search record field names so that you can use the fields in filters.</p> <p>List the record field names and related SearchBasic field names, as follows:</p> <pre>[&lt;record 1&gt;] &lt;record field name&gt; =&lt;SearchBasic field name&gt;&lt;record field name2&gt; =&lt;SearchBasic field name2&gt; [&lt;record 2&gt;] &lt;record field name&gt; =&lt;SearchBasic field name&gt;&lt;record field name2&gt; =&lt;SearchBasic field name2&gt;&lt;record field name3&gt; =&lt;SearchBasic field name3&gt;</pre> <p>For example, [Account] acctName=nameaddr1=address1</p> <p>To read transactional data from NetSuite when memorized transaction is enabled in the NetSuite account, add the record field names and related SearchBasic field name in the following format:</p> <pre>[&lt;record 1&gt;] &lt;record field name&gt; =&lt;SearchBasic field name&gt; For example: [JournalEntry] reversalEntry=memorized</pre>
Saved Search Record Fields	<p>Create a separate section for each NetSuite saved search record for which you want to add a saved search field, identified by a unique scriptId.</p> <ul style="list-style-type: none"> <li>- Add the search fields using the following format: <pre>&lt;savedSearchId1&gt;=&lt;savedSearchDeclaredField1Name&gt;, &lt;savedSearchDeclaredField2Name&gt;,&lt;savedSearchCustomFieldScriptId1&gt;, &lt;savedSearchCustomFieldScriptId2&gt;,&lt;StandardJoin&gt; &lt;FieldName1&gt;, customSearchJoin &lt;scriptID1&gt;</pre> <p>For example, 1000=phone,email,custentity78,custentity65, userJoin email,customSearchJoin custrecord1424</p> </li> <li>- To read custom segment data, use the following format to add the search custom segment fields: <pre>[savedSearchId1]=custseg1:select, custseg2:multiselect, custseg3:select...</pre> <p>For example, [741]=custseg1:select,custentity_cseg1:select,custentity_csegcs_multsel:multiselect</p> </li> <li>- To override the metadata of a task, which is created to read custom record standard fields with custom join, use the following format to add the search custom record standard fields: <pre>&lt;savedSearchId1&gt;=CustomSearchJoin  &lt;scriptId of custom record&gt;__&lt;standard field name&gt;</pre> <p>For example, 356=CustomSearchJoin uss_custom_code__internalId</p> </li> </ul>

## NetSuite account-specific service URL

Perform the following steps to use your NetSuite account-specific service URL:

1. Log in to NetSuite and click **Setup > Company > Company Information**.
2. On the **Company Information** page, click **Company URLs**.  
The **SUITETALK (SOAP AND REST WEB SERVICES)** field displays the account-specific URL in the following format:

```
https://<NetSuite_account_ID>.suitetalk.api.netsuite.com
```
3. Copy and paste the account-specific URL from step 2 in the following format in the service URL:

```
https://<Netsuite_account_ID>.suitetalk.api.netsuite.com/wsd1/v2019_2_0/netsuite.wsd1
```

# Token-based authentication

Token-based authentication is the preferred method to access NetSuite. When a connection uses token-based authentication, the agent uses a token ID and token secret to access NetSuite instead of a user name and password.

To use token-based authentication, install an Informatica token-based authentication bundle and generate the token ID and token secret in NetSuite. The token does not expire unless you revoke it from your NetSuite account. However, you might need to update the bundle and generate a new token if Informatica updates the bundle version in the future.

1. Log in to NetSuite using a Full Access or Administrator account.
2. Navigate to **Customization > SuiteBundler > Search and Install Bundles**.
3. Search for the keyword, "InformaticaTBABundle".  
A bundle with Bundle ID of 116143 appears in the search results.
4. Select InformaticaTBABundle and install it.
5. Navigate to **Setup > Users/Roles > Access Tokens > New**.
6. For **Application Name**, select InformaticaTBAIntegration.
7. Write down the access token and token secret displayed on the page.  
You enter the token ID and token secret in Data Integration when you configure the NetSuite connection.

**Note:** If you lose the token information, you need to generate another token in NetSuite. NetSuite does not provide token information for previously generated tokens.

## Rules and guidelines for a NetSuite connection

Consider the following rules and guidelines for NetSuite connections:

- When you select a connection in a mapping, synchronization task, or mapping task wizard, you can search for the object or objects that you want to use. You can search for objects using the name, label, description, or type parameter.
- Connections display business names for field names instead of technical names by default. You can configure tasks to display technical names instead of business names with the **Display technical names instead of labels** option.
- You need a separate license for each connection to the same NetSuite account that a task makes. For example, to use the same NetSuite account as source, target, and lookup in a task, you need three NetSuite licenses.
- You can use multiple concurrency threads to improve the performance of a task when you use NetSuite. Informatica recommends that you use token-based authentication when you have a basic NetSuite account to improve the performance.

**Note:** For web services that use request-level credentials for authentication, the governance limit for concurrent requests is set to 1 for a basic NetSuite account (without SuiteCloud Plus License). For web services that use token-based authentication, the limit for concurrent requests is set to 5 for a basic NetSuite account (without SuiteCloud Plus License).

# Troubleshoot a NetSuite connection

When you create a NetSuite connection, the following error might occur:

```
Test Connection Failed for <connection name>. ConnectionFailedException: [Connection].  
ExceededRequestLimitFault: Only one request may be made against a session at a time.
```

You might receive this message because you can use no more than one NetSuite connection at a time. To resolve the issue, you can request the Suite Cloud Plus account from NetSuite, which allows up to 10 mappings for each user.

## CHAPTER 153

# NetSuite Mass Ingestion connection properties

When you set up a NetSuite Mass Ingestion connection, you must configure the connection properties.

**Note:** Before you configure the connection properties, install the SuiteAnalytics Connect JDBC driver and copy the NQjc.jar file to the following directory: <Secure\_Agent>\ext\connectors\thirdparty\informatica.netsuiteami

For more information about installing the SuiteAnalytics Connect JDBC driver, see the [SuiteAnalytics Connect documentation](#).

The following table describes the connection properties for a NetSuite Mass Ingestion connection:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Netsuite Mass Ingestion</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the NetSuite account. The user name is an email address.
Password	Password for the NetSuite account.
Service Host	Name of the SuiteAnalytics Connect Service host. The value in this field must match the value specified in the <b>Service Host</b> field under the <b>Your Configuration</b> section of the <b>SuiteAnalytics Connect Driver Download</b> page in NetSuite. To access the <b>SuiteAnalytics Connect Driver Download</b> page, log in to NetSuite and click the Set Up SuiteAnalytics Connect link in the Settings portlet.
Service Port	TCP/IP port on which the SuiteAnalytics Connect server is listening. Default is 1708.

Connection property	Description
Service Datasource	<p>Data source that you want to use to access NetSuite data. You can select one of the following data sources:</p> <ul style="list-style-type: none"> <li>- NetSuite.com</li> <li>- NetSuite2.com</li> </ul> <p>Default is NetSuite2.com.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- In connections configured before the August 2022 release, the default value for this field is NetSuite.com.</li> <li>- To use a NetSuite2.com data source, the NetSuite user account must be configured with some specific roles and permissions. For more information about the roles and permissions required to access NetSuite2.com data sources, see the <a href="#">NetSuite documentation</a>.</li> </ul>
Account ID	<p>NetSuite account ID.</p> <p>To find your account ID, log in to NetSuite and click <b>Setup &gt; Integration &gt; Web Services Preferences</b>.</p> <p>If you cannot access the <b>Setup</b> menu, navigate to <b>Support &gt; Go to Suite Answers &gt; Contact support by phone</b>. The page displays your account ID.</p>
Role ID	<p>Role ID associated with the NetSuite account.</p>
Additional Connection Properties	<p>Additional properties for the SuiteAnalytics Connect Driver that is used to connect to the NetSuite service data source. Specify the properties in <code>&lt;property&gt;=&lt;value&gt;</code> format. If you want to specify multiple properties, separate each property-value pair with a semicolon (;).</p> <p>You can specify the following connection properties in this field:</p> <ul style="list-style-type: none"> <li>- <b>ValidateServerCertificate:</b> Determines whether the driver validates the certificate sent by the SuiteAnalytics Connect server. During SSL server authentication, the SuiteAnalytics Connect server sends a certificate issued by a trusted Certificate Authority (CA). The required CAs are usually included in the Java truststore but you can also specify them using the TrustStore property. Valid values for the ValidateServerCertificate property are <i>true</i> and <i>false</i>.</li> <li>- <b>TrustStore:</b> Contains the path to a valid truststore containing the security certificates to be used for server authentication. The TrustStore property is ignored if the ValidateServerCertificate property is set to <i>false</i>.</li> </ul> <p><b>Note:</b> For more information about the additional connection properties, see the <a href="#">NetSuite documentation</a>.</p>

## CHAPTER 154

# NetSuite RESTlet V2 connection properties

When you set up a NetSuite RESTlet V2 connection, you must configure the connection properties.

The following table describes the NetSuite RESTlet V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	NetSuite RESTlet V2.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	User name for a NetSuite account. User name is an email address. Optional if you use token-based authentication to access NetSuite.
Password	Password for the NetSuite account. Optional if you use token-based authentication to access NetSuite.
Rest Domain	Rest domain name: <code>https://rest.netsuite.com</code> For instance, you can enter the following values: - <code>rest.nal.beta.netsuite.com</code> for beta environment - <code>rest.sandbox.netsuite.com</code> for sandbox account - <code>rest.netsuite.com</code> or <code>rest.nal.netsuite.com</code> for production account You can also enter the domain name URL specific to your NetSuite account instead of the default domain name URL. The domain name URL used by the NetSuite account is in the following format: <code>https://&lt;NetSuite_account_ID&gt;.restlets.api.netsuite.com.</code> Informatica recommends that you use the domain name URL specific to the NetSuite account that you use. <b>Note:</b> You can use NetSuite Connector with the NetSuite 2023_1 sandbox account or release preview account.

Property	Description
Account ID	<p>NetSuite account ID. To find your account ID, log in to NetSuite and click <b>Setup &gt; Integration &gt; Web Services Preferences</b>.</p> <p>If you cannot access the <b>Setup</b> menu, navigate to <b>Support &gt; Go to Suite Answers &gt; Contact support by phone</b>. The page displays your account ID.</p>
Consumer Key	<p>The client key associated with the web service application.</p> <p>Required only for token-based authentication.</p>
Consumer Secret	<p>The client password to connect to the web service application.</p> <p>Required only for token-based authentication.</p>
Token ID	<p>The token ID generated in NetSuite.</p> <p>Required if you want to use token-based authentication to access NetSuite. Optional if you use a user name and password to access NetSuite.</p>
Token Secret	<p>The token secret generated in NetSuite.</p> <p>Required if you want to use token-based authentication to access NetSuite. Optional if you use a user name and password to access NetSuite.</p>



## CHAPTER 155

# NICE Satmetrix connection properties

When you set up a NICE Satmetrix connection, you must configure the connection properties.

The following table describes the NICE Satmetrix connection properties:

Connection property	Description
Connection Name	Name of the NICE Satmetrix connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the NICE Satmetrix connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Satmetrix URL	The URL with which the Secure Agent connects to the Satmetrix APIs. The URL has the following format: <i>http://&lt;company name&gt;.satmetrix.com</i>
Username	Username of the Satmetrix integration user account.
Password	Password of the Satmetrix integration user account.

# CHAPTER 156

## OData connections properties

Create an OData connection to read data from or write data to an OData service.

Use the connection to specify sources and targets in mappings and mapping tasks.

### Connect to OData

Let's configure the OData connection properties to connect to OData.

#### Before you begin

Before you configure the connection properties, keep the user name, password, and endpoint URI from the OData service handy.

#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	OData
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.

Property	Description
Runtime Environment	Name of the runtime environment where you want to run tasks. Select Secure Agent, Hosted Agent, or serverless runtime environment.
User Name	User name to connect to the OData service.
Password	Password associated with the user name.
Service Root URI	Root URI of the OData service. The service root URI must follow the <a href="#">OData URI conventions</a> .

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
OData Parameter File Path	Absolute path to a file that you append to the URL. The file contains key value pairs separated by a new line. You can use this file to check additional parameter values required in the URL. <b>Note:</b> Ensure that you use percent encoding to encode the key value pairs in the file.
Data Serialization Format	The format of data you want to transfer. Choose from ATOM/XML or JSON. Default is ATOM/XML.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 157

# OData consumer connection properties

Use OData Consumer connections to read data from and write data to an OData Consumer service.

Create a connection and associate it with a synchronization task, mapping, or mapping task. Define the source properties to read data from and write data to an OData Consumer object. You can also configure data filters based on your requirements.

Use the connection in the Mapping Designer when you create a mapping or in the synchronization Task wizard when you create a task.

## Connect to OData Consumer

Let's configure the OData Consumer connection properties to connect to OData Consumer.

### Before you begin

Before you configure the connection properties, keep the user name, password, and the URL for the OData Consumer service handy.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	OData Consumer

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>Name of the runtime environment where you want to run tasks.</p> <p>Select Secure Agent, Hosted Agent, or serverless runtime environment.</p>
User Name	User name to connect to the OData Consumer service.
Password	Password associated with the user name.
URL	<p>URL for the OData Consumer service data source offered through the OData V4 protocol. The URL must not contain \$metadata or the object name.</p> <p>For example, <a href="http://services.odata.org/V4/Northwind/Northwind.svc/">http://services.odata.org/V4/Northwind/Northwind.svc/</a></p> <p><b>Note:</b> For information about the URL conventions, see <a href="http://docs.oasis-open.org/odata/odata/v4.0/odata-v4.0-part2-url-conventions.html">http://docs.oasis-open.org/odata/odata/v4.0/odata-v4.0-part2-url-conventions.html</a></p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Data Serialization Format	<p>The format of data you want to transfer. Select <b>JSON</b>.</p> <p><b>ATOM/XML</b> is not applicable.</p>
Security Type	<p>Security protocol that you can use to establish a secure connection with the OData Consumer server.</p> <p>You can choose from the following options:</p> <ul style="list-style-type: none"> <li>- SSL. Two-way SSL is not applicable.</li> <li>- None</li> </ul> <p>Default is None.</p> <p>TLS is not applicable.</p> <p>For more information on how to use one-way SSL, see <a href="#">"Setting up one-way SSL" on page 474</a>.</p>
TrustStore File Name	<p>Required if you select the SSL security type.</p> <p>Name of the truststore file that contains the public certificate for the OData Consumer server.</p> <p>The truststore file must be in the JKS format.</p>
TrustStore Password	<p>Password for the truststore file that contains the public certificate for the OData Consumer server.</p>

Property	Description
KeyStore File Name	Required if you select a security type. Name of the keystore file that contains the private key for the OData Consumer server. The keystore file must be in the JKS format.
KeyStore Password	The password for the keystore file required for secure communication.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Setting up one-way SSL

You can use OData Consumer Connector to connect to an SSL-enabled OData Consumer service after you create a truststore certificate and keystore certificate. You can use one-way SSL to establish a secure connection with OData Consumer.

Perform the following steps to use one-way SSL:

- Import the server certificates to the `<Secure Agent installation directory>\jre\lib\security\cacerts` file.
- To set the `INFA_TRUSTSTORE` environmental variable to the directory path that contains the certificates:
  - Add the following environmental variable in system variables in the Secure Agent machine:  
`INFA_TRUSTSTORE`
  - Set the value of the `INFA_TRUSTSTORE` variable to the directory that contains the truststore and keystore certificates.

After you make these updates, restart the Secure Agent.

## CHAPTER 158

# OData V2 Protocol Reader connection properties

When you set up an OData V2 Protocol Reader connection, you must configure the connection properties.

The following table describes the OData V2 Protocol Reader connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The OData V2 Protocol Reader connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Service Type	The service type of the OData V2 application endpoint to which you want to connect. Choose one of the following service types: <ul style="list-style-type: none"><li>- SAP S/4HANA Catalog. Use the SAP S/4HANA Catalog service type for endpoints such as SAP S/4HANA that exposes specialized OData V2 service to list the services present in the endpoint.</li><li>- Default. Use the Default service type for all other endpoints.</li></ul>

Connection property	Description
Service URL	<p>The service URL for the selected OData V2 service type.</p> <p>For the Default service type, enter the root URL of the service.</p> <p>For example, enter the service URL in the following format:</p> <pre>https://sandbox.api.sap.com/s4hanacloud/sap/opu/odata/sap/API_CHARTOFACCOUNTS_SRV</pre> <p>You can verify if the URL is valid by appending <code>\$metadata</code> to the URL.</p> <p>For SAP S/4HANA catalog service type, enter the URL of the catalog service in SAP S/4HANA.</p> <p>For example, to access the data from the SAP S/4HANA catalog service, enter the service URL in the following format:</p> <pre>http://&lt;hostname of the OData server&gt;:&lt;port number&gt;/sap/opu/odata/iwfd/CATALOGSERVICE;v=2/</pre> <p>If the host name and port number is <code>inphal.informatica.com:8001</code> and the service endpoint is SAP S/4HANA Catalog, enter the following URL:</p> <pre>https://inphal.informatica.com:8001/sap/opu/odata/iwfd/CATALOGSERVICE;v=2/</pre>
Authentication Type	<p>The type of user authentication to connect to the OData service.</p> <p>Choose from the following authentication types:</p> <ul style="list-style-type: none"> <li>- Basic. Requires the user name and password to log in to the OData V2 application.</li> <li>- API Key. Requires a unique API key to connect to the OData V2 application.</li> <li>- OAuth 2.0 authorization code. Requires authorized access to connect to the OData V2 endpoint.</li> <li>- OAuth 2.0 client credentials. Requires client credentials to connect to the OData V2 endpoint.</li> </ul>
Username	<p>Applies to basic authentication.</p> <p>The user name to connect to the OData V2 application.</p>
Password	<p>Applies to basic authentication.</p> <p>The password associated with the OData V2 application user name.</p>
API Key	<p>Applies to API key authentication.</p> <p>Unique API key required to connect to the OData V2 application.</p>

## Authorization code authentication

To use authorization code authentication, you must first register the following Informatica redirect URL in your application:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires and the response returns 401 error code, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieve a new access token.



The following table describes the OData V2 Protocol Reader connection properties for an OAuth 2.0 authorization code authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the OData V2 endpoint. Select <b>OAuth 2.0 authorization code</b> . Default is Basic.
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the OData V2 endpoint has defined custom scopes. Enter space-separated scope attributes. For example: ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</pre>
Client Authentication	The client authentication details for authorization. Select an option to send client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send client credentials in body</b> .
Generate Access Token	Generates access token and refresh token based on the specified authentication details.
Access Token	The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.
Refresh Token	Allows the Secure Agent to fetch new access token if the access token is not valid or expires. Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the refresh token expires, you must either provide a valid refresh token or click <b>Generate Access Token</b> to regenerate a new refresh token.

# Client credential authentication

The following table describes the OData V2 Protocol Reader connection properties for OAuth 2.0 client credentials authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the OData V2 endpoint. Select <b>OAuth 2.0 client credentials</b> . Default is Basic.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the rest endpoint has defined custom scopes. Enter space-separated scope attributes. For example: ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>
Client Authentication	The client authentication details for authorization. Select an option to send client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send client credentials in body</b> .
Generate Access Token	Generates access token based on the specified authentication details.
Access Token	The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.

## OData V2 Protocol Writer connection properties

When you set up an OData V2 Protocol Writer connection, you must configure the connection properties.

The following table describes the OData V2 Protocol Writer connection properties:

Connection property	Description
Connection Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~`!\$%^&*()-+={[] \:;'"<, > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>OData V2 Protocol Writer</b> connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication Type	The type of user authentication to connect to the OData V2 service. You can select from the following authentication types: - <b>Basic Authentication.</b> Requires the user name and password to log in to the OData V2 application. - <b>API Key.</b> Requires a unique API key to connect to the OData V2 application.
Token Type	The token used by the OData V2 application endpoint to perform the required CRUD operations. Default is CSRF Token.
Service Type	The service type of the OData V2 application endpoint to which you want to connect. Default is Catalog Service.

Connection property	Description
Service URL	<p>The OData service URL of the catalog service that contains the APIs exposed by the OData V2 application.</p> <p>For example, enter the service URL to access the data from the SAP catalog service in the following format:</p> <pre>http://&lt;hostname of the SAP server&gt;:&lt;port number&gt;/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre> <p>If the host name and port number is <i>inpha1.informatica.com:8001</i> and the service endpoint is <i>CATALOGSERVICE</i>, enter the following URL:</p> <pre>https://inpha1.informatica.com:8001/sap/opu/odata/iwfnd/CATALOGSERVICE;v=2/</pre>
Data Serialization Format	<p>The data serialization format that the OData V2 catalog service supports.</p> <p>You can select from one of the following formats:</p> <ul style="list-style-type: none"> <li>- ATOM/XML</li> <li>- JSON</li> </ul> <p>Default is ATOM XML.</p>
Username	<p>Required for basic authentication.</p> <p>The user name to connect to the OData V2 application.</p>
Password	<p>Required for basic authentication.</p> <p>The password associated with the OData V2 application user name.</p>
API Key	<p>Required for API key authentication.</p> <p>The unique API key that the OData V2 application client provides for authorization when you make API calls to the OData V2 service.</p>

# CHAPTER 160

## ODBC connection properties

Create an ODBC connection to securely read data from and write data to any ODBC-compliant database.

### Prerequisites

To connect to a specific ODBC-compliant endpoint, you need to perform certain prerequisite tasks to install the database or data warehouse-specific ODBC driver and ODBC client on the Secure Agent machine to connect to your database or data warehouse.

Additionally, when you use Kerberos authentication to connect to DB2 or SAP Sybase ASE, you need to complete Kerberos authentication prerequisites.

### Configure the ODBC driver

To use an ODBC connection, you'll need to set up a system Data Source Name (DSN) for the database or data warehouse-specific ODBC driver, and then install the ODBC driver and ODBC client on the Secure Agent machine.

An ODBC client can access any database and data warehouse for which you install an ODBC driver. Ensure that the ODBC driver you install complies with the ODBC-compliant endpoint to which you want to connect.

An ODBC connection uses only the system DSN. You can't use the user DSN when you configure an ODBC driver. When you set up the system DSN, you need to specify the data source name and connection string.

This section provides instructions to configure the ODBC driver on Windows and Linux machines that host the Secure Agent. You can use these instructions to set up your endpoint-specific ODBC driver. In certain cases, you might need to set environment variables after the driver configuration. You can refer to the examples to help you set up your driver.

### Configure the ODBC driver on Linux

Before you establish an ODBC connection to connect to an ODBC-compliant database or data warehouse on Linux, configure the ODBC driver.

1. Download the ODBC drivers from the database or data warehouse-specific website.  
**Note:** To get the DB2 ODBC 64-bit driver and SAP IQ ODBC 64-bit driver, contact Informatica Global Customer Support.
2. Install the ODBC drivers on the Secure Agent machine.
3. Add entries for the data sources in the `odbc.ini` file.

Check out [“Sample odbc.ini files for ODBC connection types” on page 482](#) to know more about the odbc.ini file samples that you can use for different connection types.

- From the command line, run the following command to export the odbc.ini file:

```
Export ODBCINI=<odbc.ini file path>/odbc.ini
```

- Additionally, set environment variables for certain ODBC drivers on the Secure Agent machine. For example, set environment variables for the following ODBC drivers:

ODBC drivers	Environment variables
Microsoft Azure SQL Data Warehouse ODBC driver	<p>Set the following environment variables:</p> <ul style="list-style-type: none"> <li>- setenv ODBCINI "/data/home/adputf_9/cloud_td/ODBCINI/odbc.ini"</li> <li>- setenv LD_LIBRARY_PATH "/opt/microsoft/msodbcsql/lib64/libmsodbcsql-11.0.so.2270.0"</li> </ul>
Netezza ODBC driver	<p>Set the following environment variables:</p> <ul style="list-style-type: none"> <li>- setenv ODBCINI "/data/home/qamercury/cloud_td/ODBCINI/odbc.ini"</li> <li>- setenv ODBCINST /data/home/qamercury/cloud_td/ODBCINI/odbcinst.ini</li> <li>- setenv LD_LIBRARY_PATH ".:export/qa_adp/thirdparty/netezza/linux.64/lib64:\$LD_LIBRARY_PATH"</li> </ul>
Teradata ODBC driver	<p>Set the following environment variables:</p> <ul style="list-style-type: none"> <li>- setenv ODBCINI "/data/home/adputf_9/cloud_td/ODBCINI/odbc.ini"</li> <li>- setenv LD_LIBRARY_PATH "/opt/teradata/client/&lt;Version&gt;/lib64"</li> </ul>

- Restart the Secure Agent.

#### Sample odbc.ini files for ODBC connection types

You can use the odbc.ini file for configuring data sources when you create an ODBC connection.

This section provides sample entries for certain ODBC connection types in the odbc.ini file. You can refer to these samples to specify connection entries for your specific endpoint.

#### Microsoft Azure SQL Data Warehouse ODBC connection

Create this connection to connect to the Microsoft Azure SQL Data Warehouse endpoint.

The following sample shows a connection entry for the Microsoft Azure SQL Data Warehouse data sources in the odbc.ini file:

```
[Sample Azure DW ODBC DSN]
[SD_Azure_DW]
Driver=/opt/microsoft/msodbcsql/lib64/libmsodbcsql-11.0.so.2270.0
Description=Microsoft ODBC Driver 11 for SQL Server
Server=dghhgx2ad3.database.windows.net
Database=INFASQLDW_DEV
LogonID=infadwadmin
Password=
QuotedId=Yes
AnsiNPW=Yes
EncryptionMethod=1
SeedBeforeConnect=1
EnableQuotedIdentifiers=1
ValidateServerCertificate=0
DriverUnicodeType=1
```

#### Netezza ODBC connection

Create this connection to connect to the Netezza endpoint.

The following sample shows a connection entry for the Netezza data sources in the `odbc.ini` file:

```
[Sample Netezza ODBC DSN]
Driver=/export/qa_adp/thirdparty/netezza/linux.64/lib64/libnzodbc.so
Description=NetezzaSQL ODBC
Servername=adaptersnz2.informatica.com
Port=5480
Database=ADPQA_DB
Username=adpqa
Password=adpqa
StripCRLF=false
ReadOnly=false
ShowSystemTables=false
DateFormat=1
NumericAsChar=false
DebugLogging=true
```

### Teradata ODBC connection

Create this connection to connect to the Teradata endpoint.

The following sample shows a connection entry for the Teradata data sources in the `odbc.ini` file:

```
[Sample Teradata ODBC DSN]
[ODBC Data Sources]
<DSN_NAME>=tdata.so

[<DSN_NAME>]
Driver=<Teradata_ClientHome>/lib64/tdata.so
Description=DataDirect 7.1 Teradata
AccountString=
AuthenticationDomain=
AuthenticationPassword=
AuthenticationUserid=
CharacterSet=ASCII
DBCName=<Teradata_Server>
Database=
EnableDataEncryption=0
EnableExtendedStmtInfo=0
EnableLOBs=1
EnableReconnect=0
IntegratedSecurity=0
LoginTimeout=20
LogonID=
MapCallEscapeToExec=0
MaxRespSize=8192
Password=
PortNumber=1025
PrintOption=N
ProcedureWithSplSource=Y
ReportCodePageConversionErrors=0
SecurityMechanism=
SecurityParameter=
ShowSelectableTables=1
TDProfile=
TDRole=
TDUserName=
```

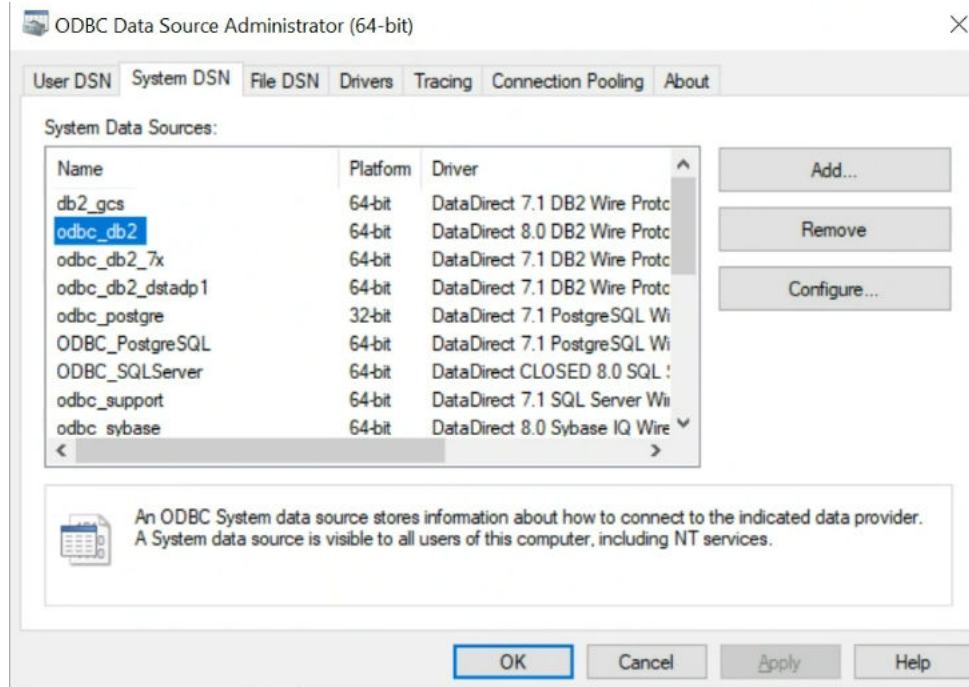
## Configure the ODBC driver on Windows

Before you establish an ODBC connection to connect to an ODBC-compliant database or data warehouse on Windows, configure the ODBC driver.

1. Download the ODBC drivers from the database or data warehouse-specific website.

**Note:** To get the DB2 ODBC 64-bit driver and SAP IQ ODBC 64-bit driver, contact Informatica Global Customer Support.

2. Install the ODBC drivers on the Secure Agent machine.
3. Open the folder in which ODBC data source file is installed.
4. Run the `odbcad32.exe` file.  
The **ODBC Data Source Administrator** dialog box appears.
5. Click **System DSN**.



**Note:** An ODBC connection uses only system DSNs. You can't use user DSNs when you configure an ODBC driver.

6. Select the system data source that you want to use, and click **Add**.  
The **Create New Data Source** dialog box appears.
7. Select an ODBC driver for which you want to set up a data source.
8. Click **Finish**.  
A dialog box appears for setting up the selected driver.
9. Specify the required connection properties for the driver.



- Click **OK** to save the changes for the configured ODBC driver.  
If you configure the DB2 ODBC driver, click **Test Connect** to test the connection that you configured, and then specify the credentials of the DB2 database in the **Logon to DB2 Wire Protocol** dialog box. Click **OK** to save the changes.

Logon to DB2 Wire Protocol

Ip Address: IRL65ADQ13.informa

Top Port: 50000

DB2 for z/OS and iSeries

Location:

Collection:

DB2 for Linux/UNIX/Windows

Database: DB11RND

User Name:

Password:

OK

Cancel

Help

## Prepare for Kerberos authentication

You can use Kerberos authentication to connect to DB2 or SAP Sybase ASE databases by placing the required configuration files on the Secure Agent machine. You can also use Kerberos authentication to connect to SSL-enabled DB2 or SAP Sybase ASE databases.

When you configure Kerberos authentication to connect to DB2 or SAP Sybase ASE, consider the following guidelines:

- You can't use the Hosted Agent or serverless runtime environment.
- Ensure that the Secure Agent and database server that you use are registered in the KDC server.
- You can't add more than one KDC to a `krb5.conf` file.
- You can't generate a credential cache file for more than one Kerberos principal user.

## Configure Kerberos authentication

Before you use Kerberos authentication to connect to DB2 or SAP Sybase ASE on Linux or Windows, the organization administrator needs to perform the prerequisite tasks.

- To configure the `krb5.conf` file, perform the following tasks:
  - Create a `krb5.conf` file on the Secure Agent machine.
  - Add the details of the Key Distribution Center (KDC) and admin server to the `krb5.conf` file in the following format:

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
```

```

<REALM NAME> = {
kdc = <Location where KDC is installed>
admin_server = <Location where KDC is installed>
}
[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>

```

2. Set the following environment variables on the Secure Agent machine.  
For more information about the required environment variables, see [“Set environment variables” on page 486](#).
3. Restart the Secure Agent.
4. To generate the credential cache file on the Secure Agent machine and use Kerberos authentication to connect to the selected ODBC subtype, perform the following tasks:
  - a. On the Secure Agent machine, run the following command and specify the user name and realm name of the selected ODBC subtype:

```
Kinit <user name>@<realm_name>
```
  - b. When prompted, enter the password for the Kerberos principal user.

## Set environment variables

To use Kerberos authentication to connect to DB2 or SAP Sybase ASE, you need to set the required environment variables on the Secure Agent machine.

- `setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>`
- `setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf`

After you set the environmental variables, you need to restart the Secure Agent.

Alternatively, you can add the environment variables when you create an ODBC connection with the subtype as **DB2** or **SAP Sybase ASE**.

Enter the `KRB5_CONFIG` and `KRB5CCNAME` details in the **Kerberos Connection Properties** field in the ODBC connection.

For example, add the properties in the following format:

```

KRB5_CONFIG=<Absolute path of the Kerberos configuration file>
\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File name>

```

**Note:** Ensure that you separate each key-value pair with a semicolon.

## Connect to ODBC

Let's configure the ODBC connection properties to connect to ODBC-compliant databases or data warehouses.

You can use the ODBC connection to connect to any ODBC-compliant endpoint. However, the connection also provides you with ODBC subtypes to connect to specific endpoints. The subtype defines the additional capabilities that you can configure in the connection or the mapping when you connect to the endpoint to read from or write data.

See the following table for the ODBC subtypes and the defined functionalities:

ODBC Subtype	Endpoint	Functionality
Azure DW	Microsoft Azure SQL Data Warehouse	Enable SQL ELT optimization in mappings for read and write operations.
DB2	DB2 databases	You can configure the following functionalities: <ul style="list-style-type: none"> <li>- Enable SQL ELT optimization in mappings for read and write operations.</li> <li>- Call a stored procedure using an SQL transformation.</li> <li>- Use Kerberos authentication to connect to DB2.</li> </ul>
Google BigQuery	Google BigQuery	Enable SQL ELT optimization in mappings for read and write operations.
PostgreSQL	PostgreSQL	Enable SQL ELT optimization in mappings for read and write operations.
Redshift	Amazon Redshift	Enable SQL ELT optimization in mappings for read and write operations.
SAP IQ	SAP IQ database	Read data from the SAP IQ database.
SAP Sybase ASE	Sybase ASE databases	You can configure the following functionalities: <ul style="list-style-type: none"> <li>- Read from or write to Sybase ASE databases.</li> <li>- Use Kerberos authentication to connect to SAP Sybase ASE.</li> </ul>
Snowflake	Snowflake	Enable SQL ELT optimization in mappings for read and write operations.
Teradata	Teradata	You can configure the following functionalities: <ul style="list-style-type: none"> <li>- Read from and write to a Teradata database.</li> <li>- Enable SQL ELT optimization in mappings for read and write operations.</li> <li>- Call a stored procedure using an SQL transformation.</li> <li>- Run SQL queries in Teradata using saved queries from an SQL transformation.</li> </ul> <p><b>Note:</b> If you want to use an SSL-enabled ODBC Teradata connection, ensure that the <b>SSL Mode</b> option under <b>WebSocket</b> is set to an appropriate value while configuring the Teradata ODBC driver.</p>
Other	Microsoft Access, Microsoft Excel, and Netezza	Enable SQL ELT optimization in mappings for read and write operations. You can also use the <b>Other</b> subtype to connect to any ODBC-compliant endpoint to read or write data.

## Before you begin

Before you get started, you'll need to install the ODBC driver and ODBC client on the Secure Agent machine to establish an ODBC connection.

Check out ["Prerequisites" on page 481](#) to learn more about the configuration prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - ; Maximum length is 255 characters.
Description	
Type	ODBC
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 491</a> .
ODBC Subtype	The ODBC connection subtype that you need to select to connect to a specific ODBC-compliant endpoint. For information on the ODBC subtypes and their capabilities, see <a href="#">"Connect to ODBC" on page 486</a> .
Authentication Mode	The authentication method to connect to DB2 or SAP Sybase ASE. This property appears only if you select the ODBC subtype as <b>DB2</b> or <b>SAP Sybase ASE</b> . Select one of the following authentication modes from the list: <ul style="list-style-type: none"><li>- Database. Uses the user name and password to connect to the selected ODBC subtype.</li><li>- Kerberos. Uses Kerberos authentication to connect to the selected ODBC subtype.</li></ul> When you choose this option on Windows, ensure that the user account that starts the Secure Agent service exists in the endpoint for the selected ODBC subtype and must have the required permissions to interact with it. <b>Note:</b> You can't configure Kerberos authentication when you use a Hosted Agent or serverless runtime environment. Default is Database.

Property	Description
Kerberos Connection Properties	<p>Additional connection properties to use Kerberos authentication to connect to DB2 or SAP Sybase ASE.</p> <p>This property appears only if you select the ODBC subtype as <b>DB2</b> or <b>SAP Sybase ASE</b> and authentication mode as <b>Kerberos</b>.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, if you don't set the required environment variables on the Secure Agent machine before you use Kerberos authentication, add the <i>KRB5_CONFIG</i> and <i>KRB5CCNAME</i> properties in the following format:</p> <pre>KRB5_CONFIG=&lt;Absolute path of the Kerberos configuration file&gt; \krb5.conf;KRB5CCNAME=&lt;Absolute path of the credential cache file&gt;/&lt;File name&gt;</pre>
User Name	The user name to connect to the ODBC-compliant endpoint.
Password	<p>The password to connect to the ODBC-compliant endpoint.</p> <p>The password cannot contain a semicolon.</p>
Data Source Name	The data source name of the ODBC object.

Property	Description
Schema	The schema name of the ODBC object.
Code Page	<p>The code page of the ODBC-compliant endpoint server or flat file defined in the connection.</p> <p>Select one of the following code pages:</p> <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data</li> <li>- UTF-8. Select for Unicode data</li> <li>- Shift-JIS. Select for double-byte character data</li> <li>- ISO 8859-15 Latin 9 (Western European)</li> <li>- ISO 8859-2 Eastern European</li> <li>- ISO 8859-3 Southeast European</li> <li>- ISO 8859-5 Cyrillic</li> <li>- ISO 8859-9 Latin 5 (Turkish)</li> <li>- IBM EBCDIC International Latin-1</li> <li>- Japanese Extended UNIX Code (incl. JIS X 0212)</li> <li>- Japanese EUC (with \&lt;-&gt; Yen mapping)</li> <li>- Japanese EUC (Packed Format)</li> <li>- IBM EBCDIC Japanese</li> <li>- IBM EBCDIC Japanese CP939</li> <li>- Japanese EBCDIC Fujitsu</li> <li>- HITACHI KEIS Japanese</li> <li>- NEC ACOS JIPSE Japanese</li> <li>- UNISYS Japanese</li> <li>- MITSUBISHI MELCOM Japanese</li> <li>- Japanese EBCDIC-Kana Fujitsu</li> <li>- HITACHI KEIS-Kana Japanese</li> <li>- NEC ACOS JIPSE-Kana Japanese</li> <li>- UNISYS-Kana Japanese</li> <li>- MITSUBISHI MELCOM-Kana Japanese</li> <li>- EBCDIC Japanese</li> <li>- EBCDIK Japanese</li> <li>- PC Japanese SJIS-78 syntax (IBM-942)</li> <li>- PC Japanese SJIS-90 (IBM-943)</li> <li>- EBCDIC Japanese Katakana SBCS</li> <li>- EBCDIC Japanese Katakana (w/ euro)</li> <li>- EBCDIC Japanese Latin-Kanji (w/ euro)</li> <li>- EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399)</li> <li>- EBCDIC Japanese Latin (w/ euro update)</li> <li>- EBCDIC Japanese Katakana SBCS (w/ euro update)</li> <li>- MS Taiwan Big-5 w/ HKSCS extensions</li> <li>- MS Windows Traditional Chinese, superset of Big 5</li> <li>- Taiwan Big-5 (w/ euro update)</li> <li>- Taiwan Big-5 (w/o euro update)</li> <li>- PC Chinese GBK (IBM-1386)</li> <li>- Chinese EUC</li> <li>- Simplified Chinese (GB2312-80)</li> <li>- Hong Kong Supplementary Character Set</li> <li>- ISO 8859-8 Hebrew</li> <li>- PC Hebrew (old)</li> <li>- PC Hebrew (w/o euro update)</li> <li>- PC Hebrew (w/ euro update)</li> <li>- MS Windows Hebrew (older version)</li> <li>- MS Windows Hebrew (w/o euro update)</li> <li>- Lotus MBCS encoding for Windows Hebrew</li> <li>- EBCDIC Hebrew (updated with sheqel, control characters)</li> <li>- EBCDIC Hebrew (w/ euro)</li> <li>- EBCDIC Hebrew (updated w/ euro and new sheqel, control characters)</li> <li>- Israeli Standard 960 (7-bit Hebrew encoding)</li> </ul>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Driver Manager for Linux	<p>The driver manager for the Secure Agent machine hosted on Linux.</p> <p>When you create a new ODBC connection on Linux, select one of the following driver managers from the list:</p> <ul style="list-style-type: none"><li>- Data Direct</li><li>- unixODBC2.3.0</li><li>- unixODBC2.3.4</li></ul> <p>Default is UnixODBC2.3.0.</p> <p>To connect to Teradata, you can use only Data Direct as the driver manager on Linux.</p>
Connection Environment SQL	<p>The SQL statement to set up the ODBC-compliant endpoint environment when you connect to a PostgreSQL or Teradata database. The database environment applies for the entire session that uses this connection.</p> <p>You can add single or multiple SQL statements. Separate each SQL statement with a semicolon.</p> <p>For example, you can enter this statement to set the time zone:</p> <pre>SET timezone to 'America/New_York';</pre> <p>You can set SQL statements in a Teradata connection used in mappings enabled with or without SQL ELT optimization. However, when you connect to a PostgreSQL database, this property applies only when you enable SQL ELT optimization in a mapping.</p>

## Rules and guidelines for an ODBC connection

Consider the following rules and guidelines when you create an ODBC connection:

- You can't use the Snowflake ODBC driver when the Secure Agent machine is hosted on SUSE Linux. For more information about the Snowflake ODBC driver that you can use to connect to Snowflake, and steps to configure a Snowflake ODBC connection, see [Configure SQL ELT optimization for Snowflake using ODBC Connector](#) Informatica How-To Library article.
- When you use Teradata as the ODBC subtype in the connection, you can provide only one SQL statement in the **Connection Environment SQL** property.

## Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS or Azure to connect to ODBC-compliant databases.

Before you configure an ODBC connection using the serverless runtime environment, perform the following tasks:

- Add the ODBC drivers in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the .yaml serverless configuration file.

## Add the ODBC drivers in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to use a serverless runtime environment in an ODBC connection:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the ODBC drivers in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/ODBC

## Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment:

1. Copy the following code snippet to a text editor and specify the driver file names and DSN entries:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      odbc:
        drivers:
          - fileCopy:
              sourcePath: ODBC/<Driver_file name>
          - fileCopy:
              sourcePath: ODBC/<Driver_file name>
        dsns:
          - name: "<Name of the ODBC database>"
            entries:
              - key: Driver
                value: <Driver_file name>
              - key: Description
                value: "<Description of the driver>"
```

where the source path is the directory path of the ODBC drivers in AWS or Azure.

**Note:** The DSN entries vary based on the driver you want to add to the serverless runtime location.

The following example shows the DNS entries for the Microsoft SQL Server driver:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      odbc:
        drivers:
          - fileCopy:
              sourcePath: ODBC/DWdb227.so
          - fileCopy:
              sourcePath: ODBC/DWdb227.so
        dsns:
          - name: "<SQL server>"
            entries:
              - key: Driver
                value: DWsqls227.so
              - key: Description
                value: "SQL Server 2014 Connection for ODL"
              - key: HostName
                value: INVW16SQL19
              - key: PortNumber
                value: 1433
              - key: Database
                value: adapter_semantic
              - key: QuotedId
                value: No
              - key: AnsiNPW
                value: Yes
```



2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`

When the `.yml` file runs, the ODBC drivers are copied from the AWS or Azure location to the serverless agent directory and the DNS entries are updated in the `odbc.ini` file.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 161

# OpenAir connection properties

When you create an OpenAir connection, you must configure the connection properties.

**Important:** OpenAir Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the OpenAir connection properties:

Property	Description
Secure Agent	The Secure Agent used to access OpenAir.
Username	User name of the OpenAir account.
Password	Password of the OpenAir account.
Company	Enter the company name.
API NameSpace	Enter the API NameSpace.
API Key	Enter the API Key.
Client Name	Enter the client name.
WSDL Url	Enter WSDL URL.
Endpoint Url	Enter end-point URL.
Batch Size	Enter the OpenAir write batch size. Default is 100.
Version	Enter the version number.
Enable Logging	Select to enable logging.

## CHAPTER 162

# Open Table connection properties

Create an Open Table connection to securely read from or write data to Open Table formats available in a catalog. For example, you can use Open Table connection to read from or write data to Apache Iceberg tables available in AWS Glue Catalog.

You can use an Open Table connection to specify sources, targets, and lookups in mappings and mapping tasks.

## Prerequisites

Before you create an Open Table connection, complete the prerequisites.

To interact with Apache Iceberg and Delta Lake tables, you need to have access to the following AWS services that manage the tables on AWS:

- **Amazon S3:** Amazon S3 stores the Apache Iceberg and Delta Lake tables containing actual records in columnar format, organized in partitioned directories.
- **AWS Glue Catalog:** AWS Glue Data Catalog manages the metadata associated with the Apache Iceberg and Delta Lake tables.
- **Amazon Athena:** Amazon Athena connects to the Glue catalog to access Apache Iceberg and Delta Lake tables metadata and perform SQL queries on data stored in S3.

You need to create separate policies to access these services.

## Adding the Amazon Athena JDBC driver

Before you use Open Table Connector, you must copy the Amazon Athena JDBC driver on the Windows or Linux machine where you installed the Secure Agent.

1. Download the latest Amazon Athena JDBC driver from the Amazon website.
2. Navigate to the following directory on the Secure Agent machine:  
`<Secure Agent installation directory>/ext/connectors/thirdparty/`
3. Create the following folders:  
`informatica.opentableformat/common`
4. Add the JDBC driver to the folder created in step 3.
5. Restart the Secure Agent.

## Create minimal IAM policies

You need to create IAM policies with the minimum required permissions to interact with Apache Iceberg and Delta Lake tables managed by AWS Glue Catalog. For more information on configuring these policies, refer to the AWS documentation.

### Minimum policy for Amazon Athena

The following sample policy shows the minimal Amazon IAM policy to access Amazon Athena:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:GetTableMetadata",
        "athena:StartQueryExecution",
        "athena:GetQueryResultsStream",
        "athena:ListDatabases",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetDatabase",
        "athena:ListTableMetadata",
        "athena:GetDataCatalog",
        "athena>DeletePreparedStatement"
      ],
      "Resource": [
        "arn:aws:athena:*:*:workgroup/*",
        "arn:aws:athena:*:*:datacatalog/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "athena:ListDataCatalogs",
        "athena:GetQueryExecution",
        "athena:ListWorkGroups",
        "athena:GetPreparedStatement"
      ],
      "Resource": "*"
    }
  ]
}
```

### Minimum policy for AWS Glue

The following sample policy shows the minimal Amazon IAM policy to access AWS Glue catalog:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

### Minimum policy for AWS S3

The following sample policy shows the minimal Amazon IAM policy to read from or write data to an Amazon S3 bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## Connect to Open Table

Let's configure the Open Table connection properties to connect to AWS Glue Catalog.

### Before you begin

Before you get started, you'll need to add the Athena JDBC driver and configure the authentication-specific prerequisites.

Permanent IAM Credentials authentication requires the access key and secret key values of the IAM user. Keep the access key and secret key handy before creating the connection. For more information about creating an access key and secret key, see the AWS documentation.

Check out ["Prerequisites" on page 495](#) to learn more about how to configure policies and role to access Apache Iceberg and Delta Lake tables.

## Connection details

The following table describes the Open Table connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Open Table
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or in a serverless runtime environment.
Open Table Format	The Open Table format that you want to use to read from or write data to a catalog.
Catalog Type	The catalog that you want to connect to manage the metadata of the Open Table format.
Storage Type	The storage type that you want to use to store the Open Table format tables.
Athena JDBC URL	Enter the JDBC URL in the following format: <code>jdbc:athena://Region=&lt;AWS_Region&gt;;OutputLocation=&lt;S3_Location&gt;</code> For example, <code>jdbc:athena://Region=us-west1;OutputLocation=s3://working/dir.</code>
Authentication Type	The authentication type to access Open Table formats.
Access Key	The key to access the AWS Glue Catalog.
Secret Key	The secret key to access the AWS Glue Catalog. The secret key is associated with the access key and uniquely identifies the account.

## CHAPTER 163

# Oracle connection properties

Create a Oracle connection to securely read data from and write data to Oracle databases.

## Prerequisites

You can use Oracle Connector to connect to an SSL-enabled Oracle database with Oracle database authentication or Kerberos authentication.

To connect to an SSL-enabled Oracle database, see [“SSL configuration” on page 499](#).

To connect to Oracle databases with Kerberos authentication, see [“Kerberos authentication” on page 501](#).

## SSL configuration

Before you use a secure Oracle connection with Oracle database authentication or Kerberos authentication to connect to an SSL-enabled Oracle database, the organization administrator needs to perform the prerequisite tasks.

1. Create a truststore certificate.
2. Create a keystore certificate. Applicable only when Client authentication is enabled in the Oracle database.

### Adding the server certificate to the truststore

Add the server certificate to the client's truststore to establish a secure Oracle connection.

Use the following keytool command to add the server certificate to the client's truststore:

```
keytool -import -trustcacerts -alias ca -file <server certificate with path> -keystore  
<name of truststore to be generated with extension> -storepass <password for truststore>  
-storetype <store type>
```

For example, consider you have a server certificate `oratls_server.cert` in the following location: `C:\SSL\oracle`

1. Run the following command to create the truststore `truststore.jks` with the truststore password “password”:

```
C:\SSL\oracle> keytool -import -trustcacerts -alias ca -file oratls_server.cert -keystore  
truststore.jks -storepass password -storetype JKS
```

2. Run the following command to create the PKCS12 truststore `truststore.p12` with truststore password "password":

```
C:\SSL\oracle> keytool -import -trustcacerts -alias ca -file oratls_server.cert -keystore truststore.p12 -storepass password -storetype PKCS12
```

## Creating a keystore certificate

Create a keystore certificate when client authentication is enabled in the Oracle server. You must create a keystore certificate that contains all the client certificates to establish an Oracle connection.

Perform the following steps to create a keystore certificate:

1. Download and install the Oracle client from the Oracle website.
2. Run the following command to create an Oracle wallet:

```
orapki wallet create -wallet <Path where wallet is to be created> -auto_login -pwd <wallet password>
```

3. Run the following command to create a self-signed client certificate to the Oracle wallet:

```
orapki wallet add -wallet <Path where wallet is to be created> -dn "CN=<common name>, OU=<organization unit>, O=<organization>, L=<locality>, ST=<state>, C=<country>" -keysize <key size in bits> -self_signed -validity <number of days> -pwd <wallet password>
```

The command runs and creates the pkcs12 certificate at the specified location.

You must specify the values of the `CN=<common name>`, `OU=<organization unit>`, `O=<organization>`, `L=<locality>`, `ST=<state>`, `C=<country>`, `keysize <key size in bits>`, `self_signed -validity <number of days>`, and `pwd <wallet password>` from the server certificate.

4. Run the following `orapki` command to export the self-signed client certificate:

```
orapki wallet export -wallet <wallet path> -dn "CN=<common name>, OU=<organization unit>, O=<organization>, L=<locality>, ST=<state>, C=<country>" -cert <Name of the exported certificate with path>
```

The `-dn` command identifies the client certificate uniquely as the server wallet contains multiple client certificates installed.

5. Install the self-signed client certificate in the server Oracle wallet.

**Note:** The client authentication fails if you do not add the self-signed client certificate to the server database Oracle wallet.

6. Add the server certificate as a trusted certificate to the Oracle wallet.

Run the following command to add the server certificate:

```
orapki wallet add -wallet <wallet path> -trusted_cert -cert <Name of the server certificate with path> -pwd <wallet password>
```

**Note:** You must use the same wallet password for all `orapki` commands.

### Example Tasks

Perform the following tasks to create a keystore certificate:

1. Run the following command to create an Oracle wallet:

```
C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet create -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -auto_login -pwd oracle4u
```

2. Run the following command to create a self-signed client certificate to the Oracle wallet:

```
C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet add -wallet C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -dn "CN=inw1pc07_kriti, OU=DEV, O=infa,L=blr, ST=ka, C=IN" -keysize 2048 -self_signed -validity 3650 -pwd oracle4u
```



The ewallet.p12 certificate is created in the following location: C:\app\client\ksuwalka\product\12.1.0\client\_1\owm\wallet

3. Run the following orapki command to export the self-signed client certificate:

```
C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet export -wallet
C:\app\client\ksuwalka\product\12.1.0\client_1\owm\wallet -dn "CN=inw1pc07_kriti,
OU=DEV, O=infa,L=blr, ST=ka, C=IN" -cert C:\Users\ksuwalka\Desktop
\client_inw1pc07.cert
```

4. Add the server certificate as a trusted certificate to the Oracle wallet. Run the following command to add the server certificate:

```
C:\app\client\ksuwalka\product\12.1.0\client_1\BIN>orapki wallet add -wallet C:\app
\client\ksuwalka\product\12.1.0\client_1\owm\wallet -trusted_cert -cert C:\SSL\oracle
\oratls_server.cert -pwd oracle4u
```

You can now use the keystore C:\app\client\ksuwalka\product\12.1.0\client\_1\owm\wallet\ewallet.p12 with keystore password oracle4u.

## Kerberos authentication

You can use Kerberos authentication to connect to Oracle databases by placing the required configuration files on the Secure Agent machine. You can also use Kerberos authentication to connect to SSL-enabled Oracle databases.

When you configure Kerberos authentication to connect to Oracle, consider the following guidelines:

- You can't use the Hosted Agent or serverless runtime environment.
- Ensure that the Secure Agent and database server that you use are registered in the KDC server.
- You can't add more than one KDC to a krb5.conf file.
- You can't generate a credential cache file for more than one Kerberos principal user.

## Configuring Kerberos authentication

Before you use Kerberos authentication to connect to Oracle on Linux or Windows, the organization administrator needs to perform the prerequisite tasks.

1. To configure the Java Authentication and Authorization Service configuration file (JAAS), perform the following tasks:

- a. Create a JAAS configuration file on the Secure Agent machine.
- b. Add the following entries to the JAAS configuration file:

```
JDBC_DRIVER_01 {
com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;
};
```

2. To configure the krb5.conf file, perform the following tasks:

- a. Create a krb5.conf file on the Secure Agent machine.
- b. Add the details of the Key Distribution Center (KDC) and admin server to the krb5.conf file in the following format:

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
```

```

<REALM NAME> = {
kdc = <Location where KDC is installed>
admin_server = <Location where KDC is installed>
}
[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>

```

3. Set the following environment variables on the Secure Agent machine.  
For more information about the required environment variables, see [“Setting environment variables” on page 502](#).
4. Restart the Secure Agent.
5. To generate the credential cache file on the Secure Agent machine and use Kerberos authentication to connect to Oracle, perform the following tasks:
  - a. On the Secure Agent machine, run the following command and specify the Oracle user name and realm name:

```
Kinit <user name>@<realm_name>
```
  - b. When prompted, enter the password for the Kerberos principal user.

## Setting environment variables

To use Kerberos authentication to connect to Oracle, you need to set the required environment variables on the Secure Agent machine.

Set the following environment variables:

- `setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>`
- `setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf`
- `setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf`

After you set the environmental variables, you need to restart the Secure Agent.

Alternatively, you can add the environment variables when you create an Oracle connection.

To add the environment variables when you configure a connection and use Kerberos authentication, you need to add the `KRB5_CONFIG`, `KRB5CCNAME`, and `JAASCONFIG` properties in the **Metadata Advanced Connection Properties** field in an Oracle connection.

For example, add the properties in the following format:

```

KRB5_CONFIG=<Absolute path of the Kerberos configuration file>
\krb5.conf;KRB5CCNAME=<Absolute path of the credential cache file>/<File
name>;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf

```

**Note:** Ensure that you separate each key-value pair with a semicolon.

# Connect to Oracle

Let's configure the Oracle connection properties to connect to Oracle databases.

## Before you begin

Check out the [“Prerequisites” on page 499](#) to learn about the authentication requirements before you configure a connection.

## Connection details

The following table describes the Oracle connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Type of connection. Select Oracle from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Oracle Subtype	The Oracle connection subtype that you can use to connect to Oracle on-premises or Oracle Autonomous Database. Select one of the following options: - Oracle ADB. Connects to Oracle Autonomous Database. - Oracle On-premise. Connects to Oracle on-premises.

## Authentication types

You can configure one of the following authentication modes to connect to Oracle databases:

- Oracle Database Authentication: Uses your Oracle user name and password to connect to Oracle.
- Kerberos: Uses Kerberos authentication to connect to Oracle.  
When you choose this option on Windows, ensure that the user account that starts the Secure Agent service is available in the Oracle database. You don't need to enter your credentials to access Oracle.  
**Note:** You can't configure Kerberos authentication when you use a Hosted Agent or serverless runtime environment.

Select the required authentication type and then configure the authentication-specific parameters.

Default is Oracle Database Authentication.

### Oracle Database authentication

The following table describes the basic connection properties for Oracle Database authentication:

Property	Description
User Name	User name for the database login. The user name can't contain a semicolon.
Password	Password for the database login. The password can't contain a semicolon.
Host	Name of the machine that hosts the database server.

Property	Description
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Schema	Schema used for the Oracle connection.
Code Page	The code page of the database server.

## Kerberos authentication

The following table describes the basic connection properties for Kerberos authentication:

Property	Description
Host	Name of the machine that hosts the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Schema	Schema used for the Oracle connection.
Code Page	The code page of the database server.

## Advanced settings

The following table describes the advanced connection property for Oracle Database authentication:

Property	Description
Encryption Method	The method that the Secure Agent uses to encrypt the data exchanged between the Secure Agent and the database server. Default is No Encryption. This property doesn't apply if you use the Hosted Agent.
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption. Not applicable when you use the Hosted Agent or the serverless runtime environment.
Validate Server Certificate	Validates the certificate that is sent by the database server. If you specify the <code>HostNameInCertificate</code> parameter, the Secure Agent also validates the host name in the certificate.

Property	Description
Trust Store	<p>The location and name of the truststore file.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Trust Store Password	The password to access the contents of the truststore file.
Host Name in Certificate	<p>Host name of the machine that hosts the secure database.</p> <p>If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
Key Store	<p>The location and the file name of the keystore.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</pre>
Key Store Password	The password for the keystore file required for secure communication.
Key Password	The password for the individual keys in the keystore file required for secure communication.
Connection Retry Period	<p>Number of seconds the Secure Agent attempts to reconnect to the Oracle database if the connection fails. If the Secure Agent can't connect to the database in the retry period, the operation fails.</p> <p>Used for all operations. Default is 0.</p>

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata. Enter properties in the following format:</p> <pre>&lt;parameter name&gt;=&lt;parameter value&gt;</pre> <p>If you enter more than one property, separate each key-value pair with a semicolon.</p> <p>For example, enter the following property to configure the connection timeout when you test a connection:</p> <pre>LoginTimeout=&lt;value_in_seconds&gt;</pre> <p><b>Note:</b> The default connection timeout is 270 seconds.</p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the JDBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;</code>  <code>EncryptionLevel=accepted;DataIntegrityLevel=accepted;</code>  <code>DataIntegrityTypes=SHA1</code></p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver to run mappings.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, <code>charset=sjis;</code>  <code>readtimeout=180</code></p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the ODBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;EncryptionLevel=1;</code>  <code>DataIntegrityLevel=1;DataIntegrityTypes=SHA1;</code>  <code>DataIntegrityTypes=SHA1</code></p>

## Configuring SSL with the serverless runtime environment

You can use the serverless runtime environment with Oracle Connector to connect to an SSL-enabled Oracle database.

Before you configure a secure Oracle connection using the serverless runtime environment, complete the following prerequisite tasks to add the SSL certificates to the serverless runtime location:

1. Create the following structure for the serverless agent configuration in AWS or Azure: `<Supplementary file location>/serverless_agent_config`
2. Add the truststore and keystore certificates in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: `<Supplementary file location>/serverless_agent_config/SSL`
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<TrustStore_filename>
```

```
- fileCopy:
  sourcePath: SSL/<KeyStore_filename>
```

where the source path is the directory path of the certificate files in AWS or Azure.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`  
When the `.yml` file runs, the SSL certificates are copied from the AWS or Azure location to the serverless agent directory.
5. In the Oracle connection properties, specify the following certificate path in the serverless agent directory in the **Trust Store** and **Key Store** fields: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>`

## Oracle Connection Rules and Guidelines

Consider the following rules and guidelines when you create an Oracle connection:

- An Oracle table name can have a maximum of 30 characters.
- When you run a task that contains an Oracle database in the Public schema, ensure that the schema does not contain too many objects. If the schema contains too many objects, the task times out. You can remove some objects from the Oracle database or move the objects into another database schema.
- When you run a task for an Oracle database target, ensure that the UTF-8 characters do not exceed the maximum length of the varchar or char fields. Data Integration might truncate UTF-8 characters if they exceed the maximum length of the varchar or char fields.
- If the data that you write from a flat file to Oracle contains Portuguese characters, ensure that the code page for the Oracle server is not set to MS Windows Latin 1. Select the code page as ISO 8859-15 Latin 1 when you create an Oracle connection.
- Schema name is case sensitive when the name of the schema contains hyphens.

## CHAPTER 164

# Oracle Autonomous Database connections

Create an Oracle Autonomous Database connection to read data from or write data to Oracle Autonomous Database. You can use Oracle Autonomous Database connections to specify sources and targets in mappings and mapping tasks.

## Prerequisites

Before you create an Oracle Autonomous Database connection to read from or write to Oracle Autonomous Database, be sure to complete the prerequisites.

### Prepare for object storage authentication

You can configure the following object storage authentication methods for Oracle Autonomous Database Connector:

#### **ConfigFile authentication**

The ConfigFile authentication uses identity credentials of Oracle Cloud Infrastructure (OCI) account provided through a configuration file for authentication. This authentication method is based on the profile selected in the configuration file.

You can create a configuration file in the following format:

```
[<profile name>]
user=<user ocid>
fingerprint=<fingerprint>
tenancy=<tenancy ocid>
region=<region>
key_file=<private key file location>
```

You require the user OCID, fingerprint, and tenancy OCID information from the OCI account for the configuration file.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the [Oracle Cloud Infrastructure documentation](#).

By default, the OCI configuration file is located at `~/.oci/config` on the Secure Agent machine. The `~/.oci/config` file can contain several profiles. The default profile name is `DEFAULT`. You can change the default profile name to any new profile names based on the profiles that you add to the `~/.oci/config` file. The `~/.oci/config` file cannot contain two profiles with the same name.



### Simple authentication

The simple authentication uses API keys for authentication. You can provide the authentication details in the Oracle Autonomous Database connection. You need to place the private key file in the Secure Agent machine.

You require the user OCID, fingerprint, and tenancy OCID information from the Oracle Cloud Infrastructure account to create an Oracle Autonomous Database connection.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the [Oracle Cloud Infrastructure documentation](#).

## Connect to Oracle Autonomous Database

Let's configure the Oracle Autonomous Database connection properties to connect to Oracle Autonomous Database.

### Before you begin

Before you get started, get the required information from your Oracle Cloud Infrastructure account based on the object storage authentication type that you want to configure.

Check out ["Prerequisites" on page 508](#) to learn more about this task.

### Connection details

When you create an Oracle Autonomous Database connection, configure the connection properties.

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Oracle Autonomous Database
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.

Property	Description
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
User Name	The user name to access the Oracle Autonomous Database. It is used to authenticate the connection.
Password	The password associated with the user name.

## Authentication types

You can configure TLS or mutual TLS authentication to connect to Oracle Autonomous Database. Select the required authentication type and then configure the authentication-specific parameters. Default is mutual TLS authentication.

### Mutual TLS authentication

The following table describes the basic connection properties for mutual TLS authentication:

Property	Description
Service Name	The specific database service accessed for the secured connection.
Wallet Path	The location of the wallet file for the secured connection.

### TLS authentication

The following table describes the basic connection properties for TLS authentication:

Property	Description
TNS Name	The TNS name defined in the <code>tnsnames.ora</code> file. For example, <code>String tnsEntry = "(description= ... (security=(ssl_server_dn_match=yes)))"</code>

## Object storage authentication types

You can configure ConfigFile or simple authentication for staging the connection when you connect to Oracle Autonomous Database. Select the required authentication type and then configure the authentication-specific parameters.

Default is ConfigFile authentication.

## ConfigFile authentication

The following table describes the basic connection property for ConfigFile authentication:

Property	Description
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.

## Advanced settings

The following table describes the advanced connection properties for ConfigFile authentication:

Property	Description
Configuration File Location	The absolute path of the configuration file on the Secure Agent machine. If you do not enter the value, the Secure Agent uses the following configuration file path: <code>~/.oci/config</code>
Profile Name	The name of the profile in the configuration file that you want to use. Default is <code>DEFAULT</code> .

## Simple authentication

The following table describes the basic connection properties for simple authentication:

Property	Description
User OCID	The unique identifier of the user in Oracle Cloud Infrastructure. For example, <code>ocid1.user.oc1..aaaaaaaaherdgpkngzrwbdc7n5ksokkot7c5jngtx3pgolr7oqbw7xzksza</code>
Fingerprint	The fingerprint of the public key.
Tenancy OCID	The unique identifier of the tenancy in Oracle Cloud Infrastructure. The tenancy is the globally unique name of the Oracle Cloud Infrastructure account. For example, <code>ocid1.tenancy.oc1..aaaaaaaaba3pv6wkc4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq</code>
Private Key File Location	The location of the private key file in .PEM format on the Secure Agent machine.
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.

## CHAPTER 165

# Oracle Business Intelligence Publisher connection properties

Create an Oracle Business Intelligence Publisher V1 connection to connect to Oracle Business Intelligence Publisher and read data from Oracle Business Intelligence Publisher. You can use an Oracle Business Intelligence Publisher V1 connection to specify sources in mappings.

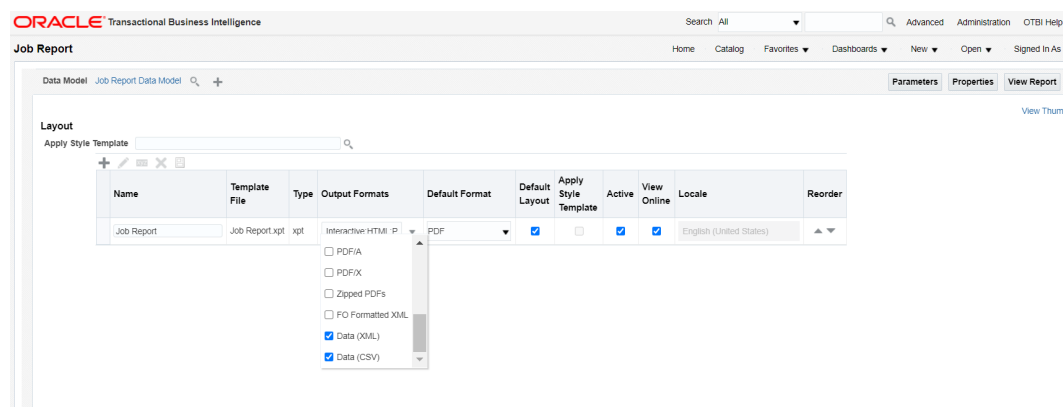
## Connect to Oracle Business Intelligence Publisher

Let's configure the Oracle Business Intelligence Publisher connection properties to connect to Oracle Business Intelligence Publisher.

### Before you begin

Before you use an Oracle Business Intelligence Publisher V1 connection to read data from Oracle Business Intelligence Publisher, configure the output format of the reports as **Data (XML)** and **Data (CSV)**. In the Oracle Business Intelligence Publisher application. Consider using Oracle Business Intelligence Publisher application for data extraction of smaller data volumes only.

The following image shows the page where you can set the value of the output format:



## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Oracle Business Intelligence Publisher
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	Name of the runtime environment where you want to run tasks. Select Secure Agent, Hosted Agent, or serverless runtime environment.
BI Publisher URL	URL of the Oracle Business Intelligence Publisher application that you want to access. <b>Note:</b> To validate the BI Publisher URL, type the following URL in the web browser: <BI Publisher URL>/xmlpserver/services/ExternalReportWSSService?wsdl If the URL opens a WSDL file, the Business Intelligence Publisher URL is valid.
Authentication Type	Type of user authentication to connect to the Oracle Business Intelligence Publisher application. You can select <b>Basic Authentication</b> type.
Username	User name of the Oracle Business Intelligence Publisher account.

Property	Description
Password	Password for the Oracle Business Intelligence Publisher account.
Report Directory	<p>The directory path where the reports are stored in the Oracle Business Intelligence Publisher application.</p> <p>You can read a report from the following folders:</p> <ul style="list-style-type: none"> <li>- Shared Folders</li> <li>- My Folders</li> </ul> <p>To read a report from Shared Folders, exclude <code>Shared Folders</code> from the directory path.</p> <p>For example, if the report is in <code>Shared Folders/Samples/Sales</code>, specify the report directory as follows:</p> <pre>/Samples/Sales</pre> <p>To read a report from My Folders, exclude <code>My Folders</code> from the directory path and include <code>~username</code> as the first node in the directory path.</p> <p>For example, if the report is in <code>My Folders/Samples/Sales</code>, and the username is <code>weblogic</code>, specify the report directory as follows:</p> <pre>/~weblogic/Samples/Sales</pre> <p>Default value of the report directory is <code>/Custom</code>.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Output Directory	<p>The directory path on the Secure Agent machine where you want to download the CSV files from Oracle Business Intelligence Publisher.</p> <p><b>Note:</b> This property applies only when you want to read data in the CSV data format.</p>

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 166

# Oracle CDC V2 connection properties

When you configure an Oracle CDC connection, you must set the connection properties.

The following table describes Oracle CDC connection properties:

Property	Description
Connection Name	A name for the Oracle CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the Oracle CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For Oracle CDC, the type must be <b>Oracle CDC V2</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for Oracle change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  ORACDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	Oracle instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains capture registrations for the Oracle source tables and in the ORACLEID statement in the PowerExchange dbmover configuration file. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Source Schema Override	If you created a single capture registration for a set of source tables that have the same table name but different schemas and defined an override schema name in a PowerExchange Logger group definition file, enter that override schema name. Otherwise, PowerExchange cannot extract the change data for the source table that has the override schema from the log files. For more information about PowerExchange Logger group definitions, see the <i>PowerExchange CDC Guide for Linux, UNIX, and Windows</i> .
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Enter the host name or IP address of the system that contains the extraction maps. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: ORACDC2B:25100 The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.



Property	Description
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be an Oracle table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="506 787 959 814">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="506 1102 1404 1207" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 167

# Oracle Cloud Object Storage connections

Create a Oracle Cloud Object Storage connection to read data from or write data to Oracle Cloud Object Storage files. You can use Oracle Cloud Object Storage connections to specify sources and targets in mappings and mapping tasks.

## Prerequisites

Before you create an Oracle Cloud Object Storage connection to read from or write to Oracle Cloud Object Storage, be sure to complete the prerequisites.

### Configure Oracle Cloud Infrastructure policies

As a user, you can use Oracle Cloud Object Storage Connector after the organization administrator creates a minimal Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) policy for Oracle Cloud Object Storage Connector.

The Oracle Cloud Infrastructure policy defines the resources that users and groups can access in an OCI account and how to access them. You can use policies to manage certain types of resources in a specific compartment in certain ways.

You need to perform the following tasks:

1. Define users, groups, and one or more compartments to hold the cloud resources for your organization.
2. Create the policies.
3. Place users into the appropriate groups depending on the compartments and resources they need to work with.
4. Provide the users with the one-time passwords that they need to access the console and work with the compartments.

For more information about adding users, groups, and policies, see [Oracle Cloud Infrastructure documentation](#).

You can create a policy in the following format:

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
```

For example,

```
Allow group ObjectReaders to read buckets in compartment ABC
```

Allow group ObjectWriters to manage objects in compartment ABC where any  
{request.permission='OBJECT\_CREATE', request.permission='OBJECT\_INSPECT'}

You need to add the following policies to configure the Oracle Cloud Object Storage connection, access objects, and run mappings:

- **Policies for Oracle Cloud Object Storage test connection**  
Allow group <group\_name> to inspect object-family in compartment <compartment\_name>  
Allow group <group\_name> to inspect buckets in compartment <compartment\_name>
- **Policies for Oracle Cloud Object Storage sources**  
Allow group <group\_name> to inspect buckets in compartment <compartment\_name>  
Allow group <group\_name> to read object-family in compartment <compartment\_name>
- **Policies for Oracle Cloud Object Storage targets**  
Allow group <group\_name> to manage inspect buckets in compartment <compartment\_name>  
Allow group <group\_name> to manage object-family in compartment <compartment\_name>

## Prepare for authentication

You can configure the following authentication methods for Oracle Cloud Object Storage Connector:

### ConfigFile authentication

The ConfigFile authentication uses identity credentials of Oracle Cloud Infrastructure (OCI) account provided through a configuration file for authentication. This authentication method is based on the profile selected in the configuration file.

You can create a configuration file in the following format:

```
[<profile name>]
user=<user ocid>
fingerprint=<fingerprint>
tenancy=<tenancy ocid>
region=<region>
key_file=<private key file location>
```

You require the user OCID, fingerprint, and tenancy OCID information from the OCI account for the configuration file.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the [Oracle Cloud Infrastructure documentation](#).

By default, the OCI configuration file is located at `~/.oci/config` on the Secure Agent machine. The `~/.oci/config` file can contain several profiles. The default profile name is `DEFAULT`. You can change the default profile name to any new profile names based on the profiles that you add to the `~/.oci/config` file. The `~/.oci/config` file cannot contain two profiles with the same name.

### Simple authentication

The simple authentication uses API keys for authentication. You can provide the authentication details in the Oracle Cloud Object Storage connection. You need to place the private key file in the Secure Agent machine.

You require the user OCID, fingerprint, and tenancy OCID information from the Oracle Cloud Infrastructure account to create an Oracle Cloud Object Storage connection.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the [Oracle Cloud Infrastructure documentation](#).

# Connect to Oracle Cloud Object Storage

Let's configure the Oracle Cloud Object Storage connection properties to connect to Oracle Cloud Object Storage.

## Before you begin

Before you get started, configure the Oracle Cloud Infrastructure policies and get the required information from your Oracle Cloud Infrastructure account based on the authentication type that you want to configure.

Check out [“Prerequisites” on page 518](#) to learn more about these tasks.

## Connection details

When you create an Oracle Cloud Object Storage connection, configure the connection properties.

The following table describes the basic connection properties:

Property	Description
Connection Name	The name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	The description of the connection. Maximum length is 4000 characters.
Type	Oracle Cloud Object Storage
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.

## Authentication types

You can configure ConfigFile or simple authentication to connect to Oracle Cloud Object Storage. Select the required authentication type and then configure the authentication-specific parameters.  
Default is ConfigFile Authentication.

### ConfigFile authentication

The following table describes the basic connection properties for ConfigFile authentication:

Property	Description
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.
Bucket Name	The Oracle Cloud Object Storage bucket name that contains the objects.

## Advanced settings

The following table describes the advanced connection properties for ConfigFile authentication:

Property	Description
Configuration File Location	The absolute path of the configuration file on the Secure Agent machine. If you do not enter the value, the Secure Agent uses the following configuration file path: <code>~/.oci/config</code>
Profile Name	The name of the profile in the configuration file that you want to use. Default is <code>DEFAULT</code> .
Folder Path	The folder under the specified Oracle Cloud Object Storage bucket. For example, <code>bucket/Dir_1/Dir_2/FileName.txt</code> . Here, <code>Dir_1/Dir_2</code> is the folder path.

## Simple authentication

The following table describes the basic connection properties for simple authentication:

Property	Description
User OCID	The unique identifier of the user in Oracle Cloud Infrastructure. For example, <code>ocid1.user.oc1..aaaaaaaaherdgpjknqzrwbdc7n5ksokkot7c5jngtx3pgolr7oqbw7xzksza</code>
Fingerprint	The fingerprint of the public key.
Tenancy OCID	The unique identifier of the tenancy in Oracle Cloud Infrastructure. The tenancy is the globally unique name of the Oracle Cloud Infrastructure account. For example, <code>ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq</code>
Private Key File Location	The location of the private key file in .PEM format on the Secure Agent machine.
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.
Bucket Name	The Oracle Cloud Object Storage bucket name that contains the objects.

## Advanced settings

The following table describes the advanced connection property for simple authentication:

Property	Description
Folder Path	The folder under the specified Oracle Cloud Object Storage bucket. For example, <code>bucket/Dir_1/Dir_2/FileName.txt</code> . Here, <code>Dir_1/Dir_2</code> is the folder path.

# Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server.

**Note:** You cannot use a proxy server with managed identity authentication.

You can use one of the following types of proxy servers:

- Unauthenticated proxy - Requires only the host and port address for configuration.
- Authenticated proxy - Requires the host address, port address, user name, and password for configuration.

To configure proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

## CHAPTER 168

# Oracle CRM Cloud V1 connections properties

The following table describes the Oracle CRM Cloud V1 connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Endpoint URL	The URL of CRM application server.
Authentication Type	The type of user authentication to connect to the Oracle CRM Cloud application. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Authentication</li><li>- JWT Authentication</li></ul>
Username	The user name of the Oracle CRM Cloud account.
Password	The password for the Oracle CRM Cloud account.
JWT ID	The ID of the JWT authentication type. Enter the JWT ID if you select the authentication type as <b>JWT Auth</b> .
REST API Version	The version number of the CRM REST API.

# Oracle CRM On Demand connection properties

When you create an Oracle CRM On Demand connection, you must configure the connection properties.

**Important:** Oracle CRM On Demand Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Oracle CRM On Demand connection properties:

Connection property	Description
User Name	Oracle CRM On Demand user name. Use the following format: <domain>/<user_name> For example: domain/jsmith@companyname.com
Password	Oracle CRM On Demand password.
Service URL	URL of the Oracle CRM On Demand service. For example: <a href="https://secure-company.crmondemand.com">https://secure-company.crmondemand.com</a>



## CHAPTER 170

# Oracle Database Ingestion connection properties

When you define an Oracle Database Ingestion connection for a database ingestion and replication task, you must configure connection properties.

The following table describes the connection properties:

Property	Description
Connection Name	<p>A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -</p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	<p>An optional description for the connection. Maximum length is 255 characters.</p>
Type	<p>The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Oracle Database Ingestion</b>.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.</p>
Authentication Mode	<p>The authentication mode that the connector must use to log in to Oracle. Options are:</p> <ul style="list-style-type: none"><li>- <b>Oracle Database Authentication</b>. Uses your Oracle user name and password to connect to Oracle.</li><li>- <b>Kerberos</b>. Uses Kerberos authentication to connect to Oracle.</li></ul> <p><b>Note:</b> If you select Kerberos, the <b>Schema</b> list that's displayed when you define an Oracle source or target in an application or database ingestion and replication task will include the schemas of other Kerberos users as well as your schemas.</p> <p>Default is Oracle Database Authentication.</p>

Property	Description
User Name	If you use Oracle Database Authentication, the user name for the Oracle database login. The user name cannot contain a semicolon. <b>Note:</b> This property is not displayed if you use Kerberos authentication.
Password	If you use Oracle Database Authentication, the password for the Oracle database login. The password cannot contain a semicolon. <b>Note:</b> This property is not displayed if you use Kerberos authentication.
Host	Host name of the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format, including the leading semicolon (;), to connect to Oracle databases: ;SID=<ORACLE_SID>
Schema	Schema used for the Oracle connection.
Code Page	The code page of the database server. Database ingestion and replication tasks use the UTF-8 code page. Default is UTF-8.
Encryption Method	For initial load jobs, determines whether the data exchanged between the Secure Agent and the Oracle database server is encrypted: Options are: - <b>SSL</b> . Establishes a secure connection using SSL for data encryption. If the Oracle database server cannot configure SSL, the connection fails. - <b>No Encryption</b> . Establishes a connection without using SSL. Data is not encrypted. Default is No Encryption.
Crypto Protocol Version	If you selected SSL as the encryption method, you must specify a cryptographic protocol or a list of cryptographic protocols supported by your server to use with an encrypted connection. Options are: - SSLv2 - SSLv3 - TLSv1.2 Default is TLSv1.2.

Property	Description
Validate Server Certificate	<p>If you selected SSL as the encryption method, controls whether the Secure Agent validates the server certificate that is sent by the Oracle database server.</p> <ul style="list-style-type: none"> <li>- <b>True</b>. Validate the server certificate.</li> <li>- <b>False</b>. Do not validate the server certificate.</li> </ul> <p>Default is False.</p> <p>If you also specify the <b>Host Name in Certificate</b> property, the Secure Agent also validates the host name in the certificate.</p>
Trust Store	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the client trusts for SSL authentication.</p>
Trust Store Password	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify a password for accessing the contents of the truststore file.</p>
Host Name in Certificate	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the host name of the machine that hosts the Oracle database to provide for additional security. The Secure Agent validates the host name included the connection with the host name in the SSL certificate.</p>
Key Store	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the path and name of the keystore file. The keystore file contains the certificates that the client sends to the Oracle server in response to the server's certificate request.</p>
Key Store Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keystore file.</p>
Key Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keys in the keystore file. Use this property when the keys have a different password than the keystore file.</p>
Database Connect String	<p>A TNS name, an Oracle Net keyword-value pair, or a SQL connect string URL that OCI uses to connect to Oracle.</p>

Property	Description
TDE Wallet Directory	<p>The path to the directory that contains the Oracle wallet file used for Oracle Transparent Data Encryption (TDE). Specify this property value only if you capture change data from TDE-encrypted tablespaces and one of the following conditions are true:</p> <ul style="list-style-type: none"> <li>- The Oracle wallet is not available to the database.</li> <li>- The Oracle database is running on a server that is remote from Oracle redo logs.</li> <li>- The wallet directory is not in the default location on the database host or the wallet name is not the default name of ewallet.p12.</li> <li>- The wallet directory is not available to the Secure Agent host.</li> </ul>
TDE Wallet Password	<p>A clear text password that is required to access the Oracle TDE wallet and get the master key. This property value is required if you need to read and decrypt data from TDE-encrypted tablespaces in the Oracle source database.</p>
Directory Substitution	<p>A local path prefix to substitute for the server path prefix of the redo logs on the Oracle server. This substitute local path is required when the log reader runs on a system other than the Oracle server and uses a different mapping to access the redo log files. Use this property in the following situations:</p> <ul style="list-style-type: none"> <li>- The redo logs reside on shared disk.</li> <li>- The redo logs have been copied to a system other than the Oracle system.</li> <li>- The archived redo logs are accessed by using a different NFS mount.</li> </ul> <p>Do <i>not</i> use this statement if you use Oracle Automatic Storage Management (ASM) to manage the redo logs. You can define one or more substitutions in the following format:</p> <pre>server_path_prefix,local_path_prefix;server_path_prefix,local_path_prefix;...</pre> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader Active Log Mask	<p>A mask that the log reader uses for selecting active redo logs when the Oracle database uses multiplexing of redo logs. The log reader compares the mask against the member names in an active redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>

Property	Description
Reader Archive Destination 1	<p>The primary log destination from which the log reader reads archived logs, when Oracle is configured to write more than one copy of each archived redo log. Enter a number that corresponds to a <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10.</p> <p>If you set only one of the Reader Archive Destination 1 and Destination 2 properties, the log reader uses that property setting. If you specify neither property, the archive log queries are not filtered by the log destination.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader Archive Destination 2	<p>The secondary log destination from which the log reader reads archived logs when the primary destination becomes unavailable or when the logs at the primary destination cannot be read. For example, logs might have been corrupted or deleted. Enter a number that corresponds to the <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10. Usually, this value is a number greater than 1.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader ASM Connect String	<p>In an Oracle ASM environment, the Oracle connection string, defined in TNS, that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader ASM User Name	<p>In an Oracle ASM environment, an Oracle user ID that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database. This user ID must have SYSDBA or SYSASM authority. To use SYSASM authority, set the <b>Reader ASM Connect As SYSASM</b> property to Y.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader ASM Password	<p>In an Oracle ASM environment, a clear text password for the user that is specified in the <b>Reader ASM User Name</b> property. The log reader uses this password and the ASM user name to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader ASM Connect As SYSASM	<p>If you use Oracle 11g ASM or later and want the log reader to use a user ID that has SYSASM authority to connect to the ASM instance, select this check box. Also specify a user ID that has SYSASM authority in the <b>Reader ASM User Name</b> property. To use a user ID that has SYSDBA authority, clear this check box. By default, this check box is cleared.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>

Property	Description
Reader Mode	<p>Indicates the source of and types of Oracle redo logs that the log reader reads. Valid options are:</p> <ul style="list-style-type: none"> <li>- <b>ACTIVE</b>. Read active and archived redo logs from the Oracle online system. Optionally, you can use the <b>Reader Active Log Mask</b> property to filter the active redo logs and use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVEONLY</b>. Read only archived redo logs. Optionally, you can use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVECOPY</b>. Read archived redo logs that have been copied to an alternate file system. For combined initial and incremental load jobs, you must also set the source custom property <code>pwx.cdcreader.oracle.reader.additional</code> with the dir and file parameters, at the direction of Informatica Global Customer Support.</li> </ul> <p>You can use this option in the following situations:</p> <ul style="list-style-type: none"> <li>- You do not have the authority to access the Oracle archived redo logs directly.</li> <li>- The archived redo logs are written to ASM, but you do not have access to ASM.</li> <li>- The archived log retention policy for the database server causes the archived logs to not be retained long enough.</li> </ul> <p>With this option, the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties are ignored.</p> <p>Default is <b>ACTIVE</b>.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Reader Standby Log Mask	<p>A mask that the log reader uses for selecting redo logs for an Oracle physical standby database when the database uses multiplexing of redo logs. The log reader compares the mask against the member names in an redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Standby Connect String	<p>An Oracle connection string, defined in TNS, that the log reader uses to connect to the Oracle physical standby database for change capture when the database is not open with read only access.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>
Standby User Name	<p>A user ID that the log reader uses to connect to the Oracle physical standby database for change capture. This user ID must have SYSDBA authority.</p> <p><b>Note:</b> This property does not apply to Oracle targets.</p>

Property	Description
Standby Password	A password that the log reader uses to connect to the Oracle physical standby database for change capture. <b>Note:</b> This property does not apply to Oracle targets.
RAC Members	The maximum number of active redo log threads, or <i>members</i> , in an Oracle Real Application Cluster (RAC) that can be tracked. For a Data Guard physical standby database that supports a primary database in a RAC environment, this value is the number of active threads for the primary database.  Valid values are 1 to 100. Default is 0, which causes an appropriate number of log threads to be determined automatically. If this value is not appropriate for your environment, set this property to a value greater than 0. <b>Note:</b> This property does not apply to Oracle targets.
BFILE Access	Select this check box in the following circumstances: <ul style="list-style-type: none"> <li>- You use BFILE access to redo logs in physical directories on the local Oracle server file system. BFILE access uses Oracle directory objects to remotely access the redo logs in the file system. This method is an alternative to other log access methods such as ASM or NFS mounts.</li> <li>- You have an Amazon Relational Database Service (RDS) for Oracle source. In this case, this option enables access to the redo logs of a cloud-based database instance deployed in RDS.</li> </ul> By default, this check box is cleared. <b>Note:</b> This property does not apply to Oracle targets.

## Prerequisites for Kerberos authentication

To use Kerberos authentication to connect to Oracle source or target databases, you must place some required configuration files on the Secure Agent machine and set some environment variables.

When you configure Kerberos authentication to connect to Oracle, consider the following guidelines:

- The Secure Agent and database server that you use must be registered in the KDC server.
- You can't add more than one KDC to a krb5.conf file. Multiple KDCs are not supported.
- You can't generate a credential cache file for more than one Kerberos principal user.
- Kerberos cross-realm authentication is not supported.
- The environment variables you define for Kerberos authentication must be consistent with the entries in the Oracle sqlnet.ora and tnsnames.ora files.

# Configuring Kerberos authentication

Before you use Kerberos authentication to connect to an Oracle database on Linux or Windows, your organization administrator needs to create a few configuration files and set some environment variables.

1. Configure the Java Authentication and Authorization Service configuration file (JAAS) that the JDBC driver will use for Java client authentication.
  - a. Create a JAAS configuration file on the Secure Agent machine.
  - b. Add an entry to the JAAS configuration file that specifies the authentication technology to use for a particular driver. For example:

```
JDBC_DRIVER_01 {
    com.sun.security.auth.module.Krb5LoginModule required
    useTicketCache=true
    principal="user@EXAMPLE.COM";
};
```

The Krb5LoginModule authenticates users by using Kerberos protocols. You can add LoginModule options such as useTicketCache and principal as needed. For more information, see the Oracle Java documentation at

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/jgss/tutorials/LoginConfigFile.html>.

2. Configure the Kerberos configuration file, krb5.conf, which defines Kerberos settings and realm details.
  - a. Create a krb5.conf file on the Secure Agent machine.
  - b. Add the details for the Key Distribution Center (KDC) and admin server to the krb5.conf file in the following format:

```
[libdefaults]
    default_realm = <realm_name>

[realms]
<realm_name> = {
    kdc = <location where KDC is installed>
    admin_server = <location where KDC is installed>
}
```

Where [libdefaults] sets the default realm, and [realms] specifies the KDC and admin server for the realm.

For example:

```
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
EXAMPLE.COM = {
    kdc = rnd.EXAMPLE.COM
    admin_server = rnd.EXAMPLE.COM
}
```

For more information, see the Oracle documentation at

[https://docs.oracle.com/cd/E86824\\_01/html/E54775/krb5.conf-4.html](https://docs.oracle.com/cd/E86824_01/html/E54775/krb5.conf-4.html).

3. Set the following environment variables on the machine where Data Ingestion and Replication and Secure Agent run:

```
setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf>
setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf>
setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>
```

These variables are required to test Oracle Database Ingestion connections, deploy tasks, and run jobs when Kerberos authentication is in use.



Alternatively, you can specify these environment variables in Administrator for the Secure Agent. If you set environment variables in Administrator and on the Secure Agent machine, the variables that you specify in Administrator take precedence.

To define environment variables for the Secure Agent in Administrator, go to **Runtime Environments**. Then open a Secure Agent and click **Edit**. Under **System Configuration Details > Custom Configuration Details**, enter the variables for the Database Ingestion service and DBMI\_AGEN\_ENV type. For example:

System Configuration Details Reset All

Service: Database Ingestion

Type: DBMI\_AGEN\_ENV

Type	Name	Value	Sensitive
DBMI_AGEN_ENV	testProperty	'testValue'	<input type="checkbox"/>

Custom Configuration Details

Service	Type	Sub-type	Name	Value	Sensitive
Database Ingestion	DBMI_AGEN_ENV		KRB5_CONFIG	C:\Users\arapura\Perforce\MyModule\untitled\	<input type="checkbox"/> <span>+</span> <span>✖</span>
Database Ingestion	DBMI_AGEN_ENV		JAASCONFIG	C:\Users\arapura\Perforce\MyModule\untitled\	<input type="checkbox"/> <span>+</span> <span>✖</span>
Database Ingestion	DBMI_AGEN_ENV		KRB5CCNAME	C:\DBML_WORKSPACE\krb5cc_5-1-5-21-38895	<input type="checkbox"/> <span>+</span> <span>✖</span>

4. Restart the Secure Agent.

5. Generate the credential cache file by using the kinit or okinit tool.

- To use the kinit tool on Windows, first install the MIT Kerberos Client and make sure that the KRB5CCNAME system environment variable or the default\_ccache\_name variable in the [libdefaults] section of krb5.conf is set. Then issue the following command to run the kinit tool. Enter the password when prompted.

```
kinit user@<realm_name>
```

- To use the kinit tool on Linux, first install the kinit tool and make sure that the KRB5CCNAME system environment variable is set. Then issue the following command to run the kinit tool. Enter the password when prompted.

```
kinit user@<realm_name>
```

- To use the okinit tool, first install the Oracle Instant Client. The credential cache file will be created based on the SQLNET.KERBEROS5\_CC\_NAME property in the sqlnet.ora file. Then issue the following command to run the okinit tool. Enter the password when prompted.

```
okinit user@<realm_name>
```

# CHAPTER 171

## Oracle Financials Cloud V1 connection properties

Create a Oracle Financials Cloud V1 connection to securely read data from or write data to Oracle Financials Cloud.

### Prerequisites

Before you create an Oracle Financials Cloud V1 connection to read from or write to Oracle Financials Cloud application, be sure to complete the prerequisites.

#### Access the XLSM template files

To write to the Oracle Financials Cloud application, access the XLSM template files and CTL files for objects that require control files.

1. Select the specific Oracle Financials Cloud instance version from the **File-Based Data Import for Financials** page in the Oracle documentation.

For example, to access the XLSM template in the Oracle Financials Cloud instance 20A, go to the following URL:

<https://docs.oracle.com/en/cloud/saas/financials/20a/oefbf/overview.html#overview>

2. Select the required operation that you want to use that are listed under the **File-Based Data Imports** section.

The selected operation page appears.

3. Click the XLSM template file link to download the XLSM template file of the operation from the **File Links** section.

The following image shows a sample XLSM template file link that you download from the **File Links** section:

#### File Links

File	Link
XLSM template	<a href="#">AutoInvoiceImportTemplate.xlsm</a>

4. Ensure that you have access to the Secure Agent machine or to the directory path that you have specified in the **IO Directory** connection property.

5. Place the XLSM template file in the following directory path that is specified in the **IO Directory** connection property: `IO Directory/Writer/Schema`

For the following write objects, place the XLSM template file and the CTL file in the directory:

- Billing Data Import
- Revenue Basis Data Import
- AutoInvoice Import

**Note:** To create a mapping using the operation that you selected, retain the name of the XLSM template file or the CTL file as provided by Oracle. Only when you retain the file names, the file names appear in the **Object Selection** window.

## Get the ERP endpoint URL

Get the ERP Integration Service end point URL to read from or write data to Oracle Financials Cloud application.

1. In the Oracle Financials Cloud application, click **Navigator**.
2. Click **Developer Connect** in the **Tool** section.
3. In the **WebServices** section, type **ERP Integration Service** in the **Find** field.  
The **Web Service: ERP Integration Service: Summary** page appears that displays the ERP Endpoint URL.  
The following example shows a sample ERP Integration Service end point URL:

```
https://adc-fap0011-fin.oracle-demos.com:443/publicFinancialCommonErpIntegration/  
ErpIntegrationService
```

4. Edit the URL by removing the following path: `443/publicFinancialCommonErpIntegration/ErpIntegrationService`  
The following URL is a sample of the ERP Endpoint URL:

```
https://adc-fap0011-fin.oracle-demos.com
```

# Connect to Oracle Financials Cloud

Let's configure the Oracle Financials Cloud V1 connection properties to connect to Oracle Financials Cloud.

## Before you begin

Before you configure a connection, access the XLSM template file and obtain the ERP Endpoint URL of the Oracle Financials Cloud application.

Check out [Prerequisites](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Oracle Financials Cloud V1
Use secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
ERP Endpoint URL	The endpoint URL of the Oracle Financials application server. <b>Note:</b> To validate the ERP Endpoint URL, type the following URL in the web browser: <ERP Endpoint URL>/publicFinancialCommonErpIntegration/ErpIntegrationService?WSDL The URL should open a WSDL file that indicates that the ERP Endpoint URL is valid.
Authentication Type	The type of user authentication to connect to the Oracle Financials Cloud application. Select <b>Basic Authentication</b> type.
Username	User name of the Oracle Financials Cloud account.
Password	Password for the Oracle Financials Cloud account.
IO Directory	The directory path where the schema files and data are stored. Store the schema files in the Secure Agent machine. Click the <b>Test</b> button after you create an Oracle Financials Cloud V1 connection. The Secure Agent creates following directories under the IO directory: - <b>Reader:</b> The reader directory contains an <b>Output</b> sub-directory. The .csv file that you download from the Oracle Financials Cloud application is downloaded as a ZIP file and stored in the following directory: IO Directory\Reader\Output <b>Note:</b> You can override the directory path where you download the .csv file in the <b>Outbound_Output_Directory</b> advanced property field. - <b>Writer:</b> The writer directory contains <b>Logs</b> and <b>Schema</b> sub-directories. Place all the XLSM and CTL files after you download them in the following directory: IO Directory\Writer\Schema - <b>Temp:</b> The temp directory contains a <b>WorkingDirectory</b> sub-directory that contains the staging files.

## Encryption mode

To access Oracle Financials Cloud, configure PGPUNSIGNED and PGPSIGNED encryption modes. Default is None.

Select the required encryption mode to encrypt or decrypt the data when you run a mapping to write data to a target.

### PGPSIGNED

Encrypts and signs the data using the PGP encryption method.

The following table describes the basic connection properties for PGP encryption method:

Property	Description
PassPhrase	The passphrase to encrypt the private key.
PrivateKey Path	The file path of the private key. Store the private key on the Secure Agent machine. Provide the private key corresponding to the public key that you uploaded in the Oracle Financials Cloud application.
ERP Public Key Path	The file path of the fusion public key. Store the fusion public key on the Secure Agent machine. You can use the file path of the fusion public key when you run a mapping to write data to a target. Raise a service request to Oracle Financials Cloud to get the fusion public key. For more information about the fusion public key, see the Oracle documentation.
ERP Private Key Alias Name	The fusion key alias name that you provided when you generated the private-public key pair in the Oracle Financials application. You can use the fusion key alias name when you run a mapping to write data to a target.
Customer Public Key Alias Name	The customer public key alias name that you provided when you uploaded the public key in the Oracle Financials application.

### PGPUNSIGNED

Encrypts data using the PGP encryption method. Use the same encryption key that you configured in the Oracle Financials Cloud application.

The following table describes the basic connection properties for PGP encryption method to read from Oracle Financials Cloud:

Property	Description
PassPhrase	The passphrase to encrypt the private key.
PrivateKey Path	The file path of the private key. Store the private key on the Secure Agent machine. Provide the private key corresponding to the public key that you uploaded in the Oracle Financials Cloud application.
Customer Public Key Alias Name	The customer public key alias name that you have provided when you uploaded the public key in the Oracle Financials application.

The following table describes the basic connection properties for PGP encryption method to write to Oracle Financials Cloud:

Property	Description
PassPhrase	The passphrase to encrypt the private key.
ERP Public Key Path	The file path of the fusion public key. Store the fusion public key on the Secure Agent machine. You can use the file path of the fusion public key when you run a mapping to write data to a target. Raise a service request with Oracle Financials Cloud to get the fusion public key. For more information about the fusion public key, see the Oracle documentation.
ERP Private Key Alias Name	The fusion key alias name that you provided when you generated the private-public key pair in the Oracle Financials application. You can use the fusion key alias name when you run a mapping to write data to a target.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 172

# Oracle Fusion Cloud Mass Ingestion connection properties

When you set up an Oracle Fusion Cloud Mass Ingestion connection, you must configure the connection properties.

**Note:** Oracle Fusion Cloud Mass Ingestion connections can access the data of only Enterprise Resource Planning (ERP), Human Capital Management (HCM), and Oracle Supply Chain and Manufacturing (SCM) modules of Oracle Fusion Cloud Applications Suite.

The following table describes the connection properties for an Oracle Fusion Cloud Mass Ingestion connection:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. Select the <b>Oracle Fusion Cloud Mass Ingestion</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Authentication	Authentication method of the connection. By default, the connection uses the Basic authentication method.
User Name	User name of the Oracle Cloud account.
Password	Password for the Oracle Cloud account.
Server URL	URL of the Oracle Cloud service that you want to access.
API Version	Version of the Oracle Cloud REST API that you want to use for the connection. Optional for the BICC replication approach.

## CHAPTER 173

# Oracle HCM Cloud V1 connection properties

Create a Oracle HCM Cloud V1 connection to securely read data from or write data to Oracle HCM Cloud.

## Prerequisites

Before you create an Oracle HCM Cloud V1 connection to read from or write to Oracle HCM Cloud V1, be sure to complete the prerequisites.

### Get the WebCenter Content URL

To read data from an Oracle HCM Cloud source, get the WebCenter content URL where Oracle HCM Cloud uploads the output XML data.

1. From the **Service Details** section in the cloud environments provisioning email from Oracle, get the URL for Oracle HCM Cloud Setup and Maintenance.  
The following example shows a sample URL: `https://fs-<domain_name>.oracleoutsourcing.com/setup/faces/TaskListManagerTop`
2. Edit the URL by removing the following path: `/setup/faces/TaskListManagerTop`  
The following URL is a sample of the WebCenter Content URL: `https://fs-<domain_name>.oracleoutsourcing.com`

### Verify roles

Verify that you are assigned the following roles:

Role	Role Code
Application Administrator	ORA_FND_APPLICATION_ADMINISTRATOR_JOB
Application Developer	ORA_FND_APPLICATION_DEVELOPER_JOB
Application Diagnostics Administrator	ORA_FND_DIAG_ADMINISTRATOR_JOB



Role	Role Code
Application Implementation Administrator	ORA_ASM_APPLICATION_IMPLEMENTATION_ADMIN_ABSTRACT
Application Implementation Consultant	ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB
Application Implementation Manager	ORA_ASM_APPLICATION_IMPLEMENTATION_MANAGER_JOB
Human Capital Management Application Administrator	ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_APPLICATION_ADMINISTRATOR_JOB
Human Capital Management Integration Specialist	ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_INTEGRATION_SPECIALIST_JOB
IT Security Manager	ORA_FND_IT_SECURITY_MANAGER_JOB
Integration Specialist	ORA_FND_INTEGRATION_SPECIALIST_JOB

## Connect to Oracle HCM

Let's configure the Oracle HCM Cloud V1 connection properties to connect to Oracle HCM Cloud.

### Before you begin

Before you configure a connection, get the WebCenter Content URL where Oracle HCM Cloud uploads the output XML data and ensure that the required roles are assigned to you.

Check out [Prerequisites](#) to learn more about these tasks.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Oracle HCM Cloud V1

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p>
WebCenter Content URL	<p>The URL of WebCenter Content Server where Oracle HCM Cloud uploads the output XML data.</p> <p><b>Note:</b> To validate the WebCenter Content URL, type the following URL in the web browser:  <code>&lt;Webcenter Content URL&gt;/idcws/GenericSoapPort?WSDL</code>  If the URL opens a WSDL file, then the WebCenter Content URL is valid.</p>
HCM URL	<p>The URL of the HCM Application Server that contains newly created data after the Secure Agent loads the XML data from the WebServer Content Server to the HCM Application Server.</p> <p>The following URL shows a sample HCM URL: <code>https://adc-xxx-hcm.oracledemo.com/</code></p> <p>To validate the HCM URL, type the following URL in the web browser:  <code>&lt;HCM URL&gt;/hcmProcFlowCoreController/FlowActionsService?WSDL</code></p> <p>If the URL opens a WSDL file, then the HCM URL is valid.</p> <p><b>Note:</b> This property applies when you create an Oracle HCM Cloud V1 connection to write data to the Oracle HCM Cloud application or when you select <b>Submit Extract</b> in the advanced connection properties.</p>
Authentication Type	<p>The type of user authentication to connect to the Oracle HCM Cloud application.</p> <p>Select <b>Basic Authentication</b> type.</p>
Username	User name of the Oracle HCM Cloud account.
Password	Password for the Oracle HCM Cloud account.
Schema Directory	<p>The directory path where HCM extract definitions XSD and XLSX are stored on the Secure Agent machine.</p> <p>Click the <b>Test</b> button after you create an Oracle HCM Cloud V1 connection.</p> <p>The Secure Agent creates following directories under the schema directory:</p> <p><b>Reader</b></p> <p>The reader directory contains the XSD files. Place all the XSD files after you generate them under the reader directory.</p> <p><b>Writer</b></p> <p>The writer directory contains the XLSX files. Place all the XLSX files after you download them under the writer directory.</p> <p><b>Temp</b></p> <p>The temp directory contains the staging files before loading.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Submit Extract	<p>Submits HCM extract definitions with the parameter values that you specify in the request message. Default is disabled.</p> <p>When you enable the <b>Submit Extract</b> option, the Secure Agent submits the instance of the HCM extract definition that you specify and downloads the latest output data file corresponding to the HCM extract definition from the WebCenter Content Server.</p> <p>You can also submit HCM extract definitions from the Oracle HCM Cloud application directly.</p> <p><b>Note:</b> This property applies when you read data from the Oracle HCM Cloud application.</p>

## Encryption mode

You can configure PGPUNSIGNED and PGPSIGNED encryption mode to access Oracle HCM Cloud. Default is None.

Select the required encryption mode to encrypt or decrypt the data when you run a mapping to write data to a target.

### PGPSIGNED

Encrypts and signs the data using the PGP encryption method.

The following table describes the basic connection properties for PGP encryption method:

Property	Description
Private Key Passphrase	<p>The passphrase to encrypt the private key.</p> <p>For more information about the private key passphrase, see the Oracle documentation.</p>
Private Key Path	<p>The file path of the private key.</p> <p>Store the private key on the Secure Agent machine.</p> <p><b>Note:</b> Specify the private key corresponding to the public key that you uploaded in the Oracle HCM Cloud application.</p>
Fusion Public Key Path	<p>The file path of the fusion public key.</p> <p>Store the fusion public key on the Secure Agent machine.</p> <p><b>Note:</b> Raise a service request with Oracle HCM Cloud to retrieve the fusion public key.</p> <p>For more information about the fusion public key, see the Oracle documentation.</p>

### PGPUNSIGNED

Encrypts data using the PGP encryption method. Use the same encryption key that you configured in the Oracle HCM Cloud application.

The following table describes the basic connection properties for PGP encryption method to read from Oracle HCM Cloud:

Property	Description
Private Key Passphrase	The passphrase to encrypt the private key. For more information about the private key passphrase, see Oracle documentation.
Fusion Public Key Path	The file path of the fusion public key. Store the fusion public key on the Secure Agent machine. <b>Note:</b> Raise a service request with Oracle HCM Cloud to retrieve the fusion public key. For more information about the fusion public key, see Oracle documentation.

The following table describes the basic connection properties for PGP encryption method to write to Oracle HCM Cloud:

Property	Description
Private Key Passphrase	The passphrase to encrypt the private key. For more information about the private key passphrase, see the Oracle documentation.
Private Key Path	The file path of the private key. Store the private key on the Secure Agent machine. <b>Note:</b> Specify the private key corresponding to the public key that you uploaded in the Oracle HCM Cloud application.

## Extract definition

To read data from an Oracle HCM Cloud source, create HCM extract definitions for the data that you want to extract from the Oracle HCM Cloud application.

1. When you create HCM extract definitions, configure the following properties on the Oracle HCM Cloud application:
  - a. In the **Extract Deliver Options** page under the **Manage Extract Definitions** tab, set the value of the **Output Type** field as **Data** and **Delivery Type** field as **WebCenter Content**.

- b. Specify the values of the **Integration Name** and **Encryption Mode** fields. The following image shows the **Extract Deliver Options** page where you can set the value of the **Output Type**, **Delivery Type**, **Integration Name**, and **Encryption Mode** fields.

Extract Delivery Options

View Format Add Delete Edit

Start Date	End Date	Delivery Option Name	Output Type	Report	Template Name	Output Name	Delivery Type
1/1/01	12/31/12		Data				WebCenter C

Columns Hidden 3

Additional Details:

View Format

Property	Value	Attribute
Compress		
Time Zone		
Locale		
Key		
Integration Name		
Run Time File Name		
Encryption Mode		

- Submit the HCM extract definitions to the Oracle WebCenter Content Server from the Oracle HCM Cloud application. You can also use the **Submit Extract** connection property to submit the HCM extract definitions to the Oracle WebCenter Content Server.
- Generate the XML schema in the XSD file format for all the HCM extract definitions and store the XSD files on the machine where the Secure Agent is installed. Store all the XSD files in the following directory that you specify in the **Schema Directory** connection property: `Schema Directory\Reader`

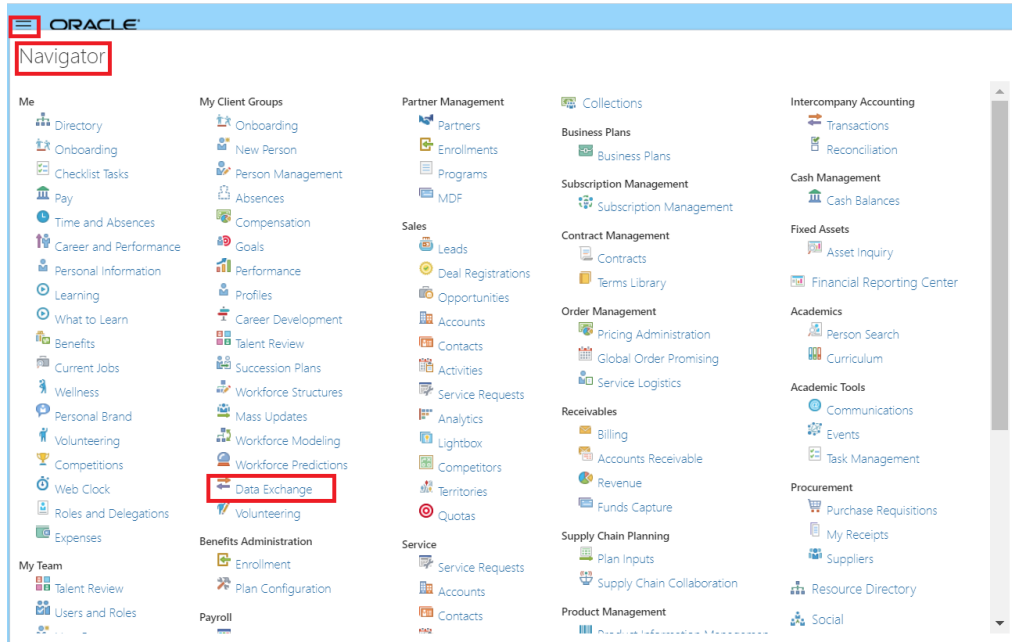
Oracle HCM Cloud V1 Connector supports the XSD files with a `DATA_DS` single root element.

**Note:** Use a third-party tool to generate the XML schema from the output XML data. Provide the XSD files that are compatible with the output XML data and name in the `<TemplateName>.xsd` format.

## Download the excel templates

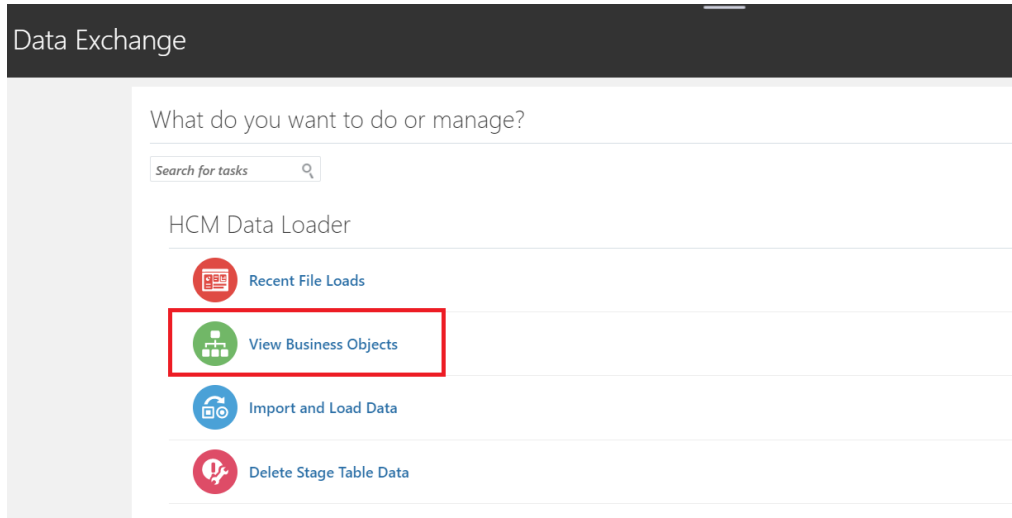
Download the excel templates that relates to the object that you want to write data to.

- Log in to the Oracle HCM Cloud Application.
- Click **Navigator > Data Exchange**.

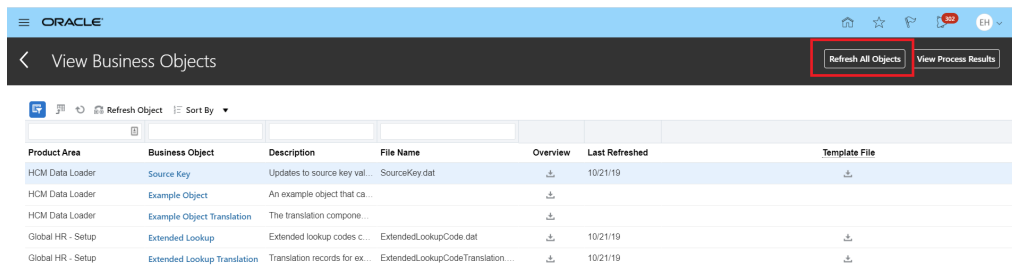


The Data Exchange page is displayed.

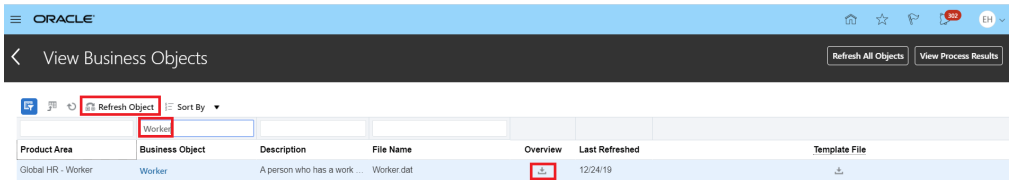
3. Click **View Business Objects** in the HCM Data Loader section.



4. Click **Refresh All Objects**.



5. You can filter a particular business object and refresh that specific object. Click the download icon on the **View Business Objects** page, under the **Overview** column.



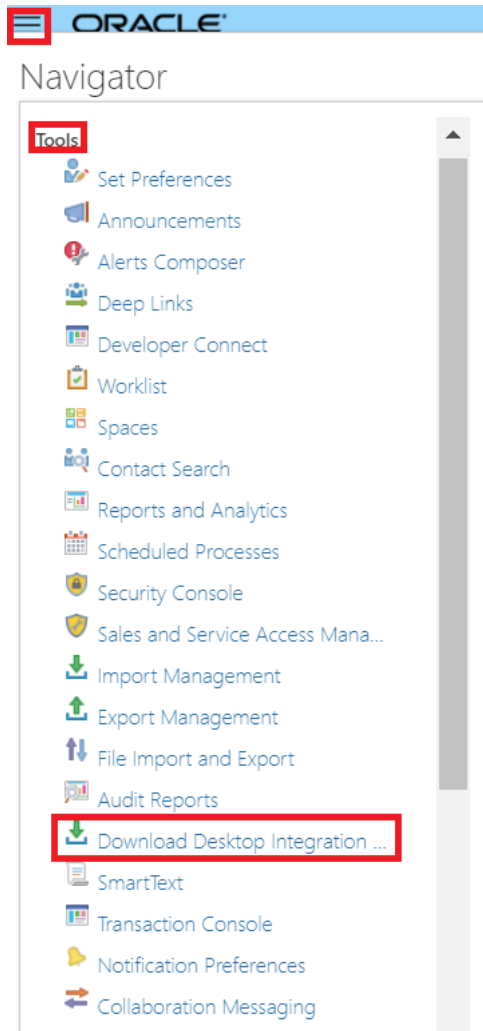
The **GenericBusObjDetails.xlsx** template is downloaded.

**Note:** All Excel templates are downloaded with the same name, **GenericBusObjDetails.xlsx**. Rename the Excel templates as required.

## Download and install ADF desktop integration tool

After you download the Excel templates, install the tool to connect to the endpoint through the Excel templates. The tool downloads data from the endpoint and autopopulates the excel templates.

1. Log in to the Oracle HCM Cloud Application.
2. Click **Navigator > Tools > Download Desktop Integration Installer**.



The application is downloaded to the desktop.

3. Run the installer, `adfdi-excel-addin-installer.exe`.

**Note:** For the Excel configuration to work with the ADF Desktop Integration, see the following Oracle documentation:

<https://docs.oracle.com/middleware/11119/adf/develop-desktop-integration/adf-desktop-config-env.htm>

## Set up the excel templates

To enable the write operation, set up the excel templates.

1. Open the downloaded excel templates.
2. To generate the metadata for a particular object, click **Yes** in the **Connect** dialog box. If you haven't already logged in to the Oracle HCM Cloud V1 application, you are prompted to log in.
3. To ensure that you populate the template with complete metadata, navigate to the Hierarchy Details, Attributes, and Flexfield Attribute sheets and save the excel template.



**Note:** If the data isn't populated in the excel template, verify that you have followed the steps accurately or contact **Oracle Support**.

4. Place all the excel templates in the **Writer** subdirectory under the **schema** directory.

**Note:** Consider using excel templates corresponding to the latest release version of Oracle Cloud.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

# CHAPTER 174

## Pinecone connection properties

Create a Pinecone connection to securely write data to Pinecone vector database.

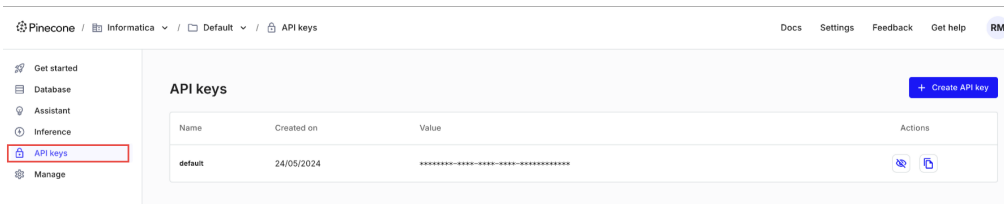
### Prepare for authentication

Before you configure the connection properties, you need to get the API key of your Pinecone account to authenticate access to the Pinecone APIs.

#### Get the Pinecone API key

You need an API key to make API calls to your Pinecone project. To get the Pinecone API key, perform the following steps:

1. Open the Pinecone console.
2. Select your project.
3. Go to **API Keys**.



4. Copy the API key.

### Connect to Pinecone

Let's configure the Pinecone connection properties to connect to Pinecone.

#### Before you begin

Before you get started, you'll need to get the API key from your Pinecone account.

Check out [“Prepare for authentication” on page 550](#) to learn about the authentication requirements before you configure a connection.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Pinecone
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure agent or serverless runtime environment. Hosted Agent is not applicable for mappings in advanced mode.
API Key	The API key of your Pinecone account to authenticate access to the Pinecone APIs.

## CHAPTER 175

# PostgreSQL CDC connection properties

When you configure a PostgreSQL CDC connection, you must set the connection properties.

The following table describes PostgreSQL CDC connection properties:

Property	Description
Connection Name	A name for the PostgreSQL CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the PostgreSQL CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For PostgreSQL CDC, the type must be <b>PostgreSQL CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for PostgreSQL change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <code>host_name:port_number</code>  For example:  <code>MYS CDC1A:1467</code>
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	PostgreSQL instance name that is specified in the <b>Instance</b> field of the registration group that contains capture registrations for the PostgreSQL source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.

Property	Description
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system that contains the extraction maps. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address: <i>host_name:port_number</i> For example: PSQCDC2B:25100 <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a PostgreSQL table on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator. Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab. In the parameter file, set the connection overrides for the parameter in the format of name value pairs, where multiple values are delimited with a semicolon.</p> <p>For example:</p> <pre data-bbox="516 806 1081 831">\$UserPass="User Name=jdoe;Password=mypassword"</pre> <p>The parameter name you specify in this field must match an entry defined in the parameter file. For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 176

# PostgreSQL connection properties

Create a PostgreSQL connection to securely read data from or write data to PostgreSQL.

## Prepare for authentication

You can configure database or Kerberos authentication method to connect to a PostgreSQL database. Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

To configure database authentication, you need the user name, password, host name, port, and database name from your PostgreSQL account. To configure Kerberos authentication, you need the service principal name, host name, port, and database name from your PostgreSQL account.

To configure Kerberos authentication, you need to perform certain prerequisite tasks.

## Prepare for Kerberos authentication

To connect to PostgreSQL databases with Kerberos authentication, place the required Kerberos configuration files on the Secure Agent machine.

When you configure Kerberos authentication to connect to PostgreSQL, consider the following guidelines:

- You can't use the Hosted Agent or serverless runtime environment.
- Ensure that the Secure Agent and database server that you use are registered in the KDC server.
- You can't add more than one KDC to a `krb5.conf` file.
- You can't generate a credential cache file for more than one Kerberos principal user.
- When you use Kerberos authentication on Windows, ensure that the user account that starts the Secure Agent service is available in the PostgreSQL database. You don't need to enter your credentials to access PostgreSQL.

## Configuring Kerberos authentication

Before you use Kerberos authentication to connect to PostgreSQL on Linux or Windows, the organization administrator needs to perform the prerequisite tasks.

1. To configure the Java Authentication and Authorization Service configuration file (JAAS), perform the following tasks:

- a. Create a JAAS configuration file on the Secure Agent machine.
- b. Add the following entries to the JAAS configuration file:

```
JDBC_DRIVER_01 {
    com.sun.security.auth.module.Krb5LoginModule required useTicketCache=true;
};
```

2. To configure the `krb5.conf` file, perform the following tasks:

- a. Create a `krb5.conf` file on the Secure Agent machine.
- b. Add the details of the Key Distribution Center (KDC) and admin server to the `krb5.conf` file in the following format:

```
[libdefaults]
default_realm = <Realm name>
forwardable = true
ticket_lifetime = 24h

[realms]
<REALM NAME> = {
    kdc = <Location where KDC is installed>
    admin_server = <Location where KDC is installed>
}

[domain_realm]
<domain name or host name> = <Domain name or host name of Kerberos>
<domain name or host name> = <Domain name or host name of Kerberos>
```

3. Set the following environment variables on the Secure Agent machine.  
For more information about the required environment variables, see [“Setting environment variables” on page 556](#).
4. Restart the Secure Agent.
5. To generate the credential cache file on the Secure Agent machine and use Kerberos authentication to connect to PostgreSQL, perform the following tasks:
  - a. From the command line on the Secure Agent machine, run the following command and specify the PostgreSQL user name and realm name:

```
Kinit <user name>@<realm_name>
```
  - b. When prompted, enter the password for the Kerberos principal user.

## Setting environment variables

To use Kerberos authentication to connect to PostgreSQL, you need to set the required environment variables on the Secure Agent machine.

Run the following commands to set the environment variables:

- `setenv KRB5CCNAME <Absolute path and file name of the credentials cache file>`
- `setenv KRB5_CONFIG <Absolute path of the Kerberos configuration file>\krb5.conf`
- `setenv JAASCONFIG <Absolute path of the JAAS config file>\<File name>.conf`

After you set the environmental variables, you need to restart the Secure Agent.

Alternatively, you can add the `KRB5_CONFIG` and `JAASCONFIG` environment variables when you create a PostgreSQL connection.



To add the environment variables when you configure a connection with Kerberos authentication, you need to add the `KRB5_CONFIG` and `JAASCONFIG` properties in the **Additional Kerberos Properties** field in a PostgreSQL connection.

For example, add the properties in the following format:

```
KRB5_CONFIG=<Absolute path of the Kerberos configuration file>
\krb5.conf;JAASCONFIG=<Absolute path of the JAAS config file>\<File name>.conf
```

**Note:** Ensure that you separate each key-value pair with a semicolon.

## Connect to PostgreSQL

Let's configure the PostgreSQL connection properties to connect to PostgreSQL.

### Before you begin

Before you get started, get the required information from your PostgreSQL account based on the authentication method that you want to use.

Check out ["Prepare for authentication" on page 555](#) to learn more about the authentication prerequisites.

### Connection details

The following table describes the PostgreSQL connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	PostgreSQL
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run a database ingestion task on a Hosted Agent or in a serverless runtime environment.

### Authentication types

You can configure database or Kerberos authentication methods to connect to PostgreSQL databases.

Select the required authentication type and then configure the authentication-specific parameters.

#### Database authentication

To configure database authentication, you need the user name, password, host name, port, and database name from your PostgreSQL account.

The following table describes the basic connection properties for database authentication:

Property	Description
User Name	User name to access the PostgreSQL database.
Password	Password for the PostgreSQL database user name.
Host Name	Host name of the PostgreSQL server to which you want to connect.
Port	Port number for the PostgreSQL server to which you want to connect. Default is 5432.
Database Name	The PostgreSQL database name.

## Kerberos authentication

To configure Kerberos authentication, you need the service principal name, host name, port, and database name from your PostgreSQL account.

The following table describes the basic connection properties for Kerberos authentication:

Property	Description
Service Principal Name	Service principal name that you want to use for Kerberos authentication. Specify the service principal name in the following format: <code>&lt;Service_Name&gt;/&lt;Fully_Qualified_Domain_Name&gt;@&lt;REALM.COM&gt;</code> <ul style="list-style-type: none"> <li>- Service_Name is the name of the service hosting the instance.</li> <li>- Fully_Qualified_Domain_Name is the fully qualified domain name of the host machine.</li> <li>- REALM.COM is the domain name of the host machine. This value is optional. If you do not specify the realm name, the default realm is used.</li> </ul>
Host Name	Host name of the PostgreSQL server to which you want to connect.
Port	Port number for the PostgreSQL server to which you want to connect. Default is 5432.
Database Name	The PostgreSQL database name.

The following table describes the advanced connection property for Kerberos authentication:

Property	Description
Additional Kerberos Properties	Additional connection properties to use Kerberos authentication to connect to PostgreSQL. Enter properties in the following format: <code>&lt;parameter name&gt;=&lt;parameter value&gt;</code> If you enter more than one property, separate each key-value pair with a semicolon.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Schema Name	The schema name. If you don't specify the schema name, all the schemas available in the database are listed when you import the source object in Data Integration.
Connection Environment SQL	The SQL statement to set up the database environment when you connect to the database. The database environment applies for the entire session that uses this connection. For example, you can enter this statement to set the time zone: <code>SET timezone to 'America/New_York';</code>
Additional Connection Properties	Additional connection parameters that you want to use. Provide the connection parameters as semicolon-separated key-value pairs.

## Encryption types

The encryption method determines if the Secure Agent and the PostgreSQL database server exchange encrypted data. If you do not want to establish a connection using SSL, select `noEncryption`. PostgreSQL establishes a connection without using SSL. Data is not encrypted. Default is `noEncryption`.

To use SSL, select the required encryption method and then configure the encryption-specific parameters.

**Note:** You can configure SSL when you use the Secure Agent or the serverless runtime environment. You can't configure SSL when you use the Hosted Agent.

### SSL

When you use the SSL encryption method, data is encrypted using SSL. If the PostgreSQL database server can't configure SSL, the connection fails.

The following table describes the advanced connection properties for SSL encryption:

**Note:** You need to select the **Validate Server Certificate** check box for some SSL properties, while others need client authentication enabled on the PostgreSQL server.

Property	Description
Validate Server Certificate	Determines if the Secure Agent validates the server certificate sent by the PostgreSQL database server. If you specify the Host Name In Certificate property, the Secure Agent also validates the host name in the certificate. Select this option to validate the server certificate.
Truststore	This property applies if you select the Validate Server Certificate option. The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;TrustStore_filename&gt;</code>
Truststore Password	This property applies if you select the Validate Server Certificate option. The password to access the truststore file that contains the SSL certificate.

Property	Description
Host Name In Certificate	Optional when you select the Validate Server Certificate option. A host name for providing additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.
Keystore	This property applies when client authentication is enabled on the PostgreSQL database server. The path and the file name of the key store. The keystore file contains the certificates that the PostgreSQL client sends to the PostgreSQL server in response to the server's certificate request. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</code>
Keystore Password	This property applies when client authentication is enabled on the PostgreSQL database server. The password for the keystore file required for secure communication.
Key Password	This property applies when client authentication is enabled on the PostgreSQL database server. Required when individual keys in the keystore file have a different password than the keystore file.
Use SSLv3	Uses SSLv3 as the cryptographic protocol for an encrypted connection.
Use TLSv1.2	Uses TLSv1.2 as the cryptographic protocol for an encrypted connection.

#### Request SSL

When you use the requestSSL encryption method, PostgreSQL attempts to establish a connection using SSL. If the PostgreSQL database server can't configure SSL, the Secure Agent establishes an unencrypted connection.

The following table describes the advanced connection properties for Request SSL encryption:

Property	Description
Validate Server Certificate	Determines if the Secure Agent validates the server certificate sent by the PostgreSQL database server. If you specify the Host Name In Certificate property, the Secure Agent also validates the host name in the certificate. Select this option to validate the server certificate.
Truststore	This property applies if you select the Validate Server Certificate option. The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</code>
Truststore Password	This property applies if you select the Validate Server Certificate option. The password to access the truststore file that contains the SSL certificate.
Host Name In Certificate	Optional when you select the Validate Server Certificate option. A host name for providing additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.

Property	Description
Use SSLv3	Uses SSLv3 as the cryptographic protocol for an encrypted connection.
Use TLSv1.2	Uses TLSv1.2 as the cryptographic protocol for an encrypted connection.

## Configure SSL with serverless runtime environment

You can use the serverless runtime environment with PostgreSQL Connector to connect to an SSL-enabled PostgreSQL database.

Before you configure a secure PostgreSQL connection using the serverless runtime environment, complete the following prerequisite tasks to add the SSL certificates to the serverless runtime location:

1. Create the following structure for the serverless agent configuration in AWS or Azure: <Supplementary file location>/serverless\_agent\_config
2. Add the truststore and keystore certificates in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/SSL

3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<TrustStore_filename>
        - fileCopy:
            sourcePath: SSL/<KeyStore_filename>
```

where the source path is the directory path of the certificate files in AWS or Azure.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the SSL certificates are copied from the AWS or Azure location to the serverless agent directory.
5. In the PostgreSQL connection properties, specify the following certificate path in the serverless agent directory in the **Trust Store** and **Key Store** fields: `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_filename>`

## CHAPTER 177

# Power BI connection properties

When you set up a Power BI connection, you must configure the connection properties.

The following table describes the Power BI connection properties:

Connection Property	Description
Storage Account Name	The name of the Microsoft Azure Blob Storage account where you want to store the <code>.csv</code> files in the container.
Storage Account Key	The key of the Microsoft Azure Blob Storage account to access the account.
Storage Container Name	The name of the Microsoft Azure Blob Storage container to store the <code>.csv</code> files. <b>Note:</b> To avoid errors, ensure that a container does not contain a subfolder.
Azure ResourceGroup Name	The name of the Microsoft Azure Blob Storage resource group that is associated with the Microsoft Azure Blob Storage account name.
Azure Subscription ID	The ID of the Microsoft Azure Blob Storage account to which you have subscribed.
Azure Tenant ID	The tenant ID of the Microsoft Azure Blob Storage account.
Power BI Access Token	The valid access token for Power BI to create an external data flow on the Power BI Online. You must use the Informatica Power BI OAuth tool to generate a valid Power BI access token. After you generate an access token, it is valid for 60 minutes. Power BI Connector refreshes the access token as long as the refresh token is not expired.
Power BI Refresh Token	The valid refresh token for Power BI to create an external data flow on the Power BI Online. You must use the Informatica Power BI OAuth tool to generate a valid Power BI refresh token. After you generate a refresh token, it is valid for 90 days.
Azure Key Vault Name	The key vault name of the Microsoft Azure Blob Storage account.
Azure Key Secret Name	The key secret name of the Microsoft Azure Blob Storage account.

## CHAPTER 178

# QuickBooks V2 Connection Properties

When you set up a QuickBooks V2 connection, you must configure the connection properties.

The following table describes the QuickBooks V2 connection properties:

Connection Property	Description
Username	Username of the QuickBooks account.
Password	Password of the QuickBooks account.
Connection URL	The Connection URL to connect to the QuickBooks application.
Schema	The value of Schema is set to default automatically.
QBXML version	QBXML version of the QuickBooks. The default QBXML version is 6.0.
Enable Logging	Enable logging to see the session logs of tasks.

## CHAPTER 179

# Redis connection properties

When you create a Redis connection, you must configure the connection properties.

The following table describes the Redis connection properties:

Property	Description
Connection Name	The name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	The Redis connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. You can specify a Secure Agent or serverless runtime environment.
Host	Host name or IP address of the Redis server.
Port	Redis server port number.
User	Username to access the Redis server.
Password	Password to access the Redis server.
Max Clients Per Worker	The maximum number of Redis client connections used by each worker node.
Flat Hierarchy	Enable this property to perform the following actions based on the data that you read: <ul style="list-style-type: none"><li>- Read top-level HASH keys as multiple rows with one row for each key-value pair in the hash.</li><li>- Read top-level LIST keys as multiple rows with one row for each string value in the list.</li></ul>
Use TLS	Uses TLS to secure the communication with Redis server.



<b>Property</b>	<b>Description</b>
KeyStore File Path	Absolute path of the KeyStore file in the Secure Agent machine that contains private keys and certificates for the Redis server.
KeyStore Passphrase	Passphrase for the KeyStore file.
TrustStore File Path	Absolute path of the TrustStore file that contains certificates for the Redis server.
TrustStore Passphrase	Passphrase for the TrustStore file.

## CHAPTER 180

# REST API connection properties

When you set up a REST API connection, you must configure the connection properties.

Consider the following categories for the REST API connection properties:

- General properties
- URL properties
- Form properties
- Header properties
- Authentication properties

# CHAPTER 181

## REST V2 connection properties

Create a REST V2 connection to interact with web service applications built on REST architecture.

### Prerequisites

Before you configure a REST V2 connection, be sure to complete the prerequisites.

- Install the Secure Agent on a 64-bit machine.
- Ensure that the machine hosting the Secure Agent has a minimum memory size of 2048 MB.

### Connect to REST V2

Let's configure the REST V2 connection properties to interact with web service applications built on REST architecture.

#### Before you begin

Before you get started, be sure to complete the prerequisites.

#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ - + -, Maximum length is 255 characters.
Description	
Type	REST V2

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>Name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>You cannot run a streaming ingestion task on a Hosted Agent or serverless runtime environment.</p>

## Authentication types

You can configure standard, OAuth 2.0 client credentials, OAuth 2.0 authorization code, JWT bearer token, and API key authentication types to connect to a REST endpoint.

Select the required authentication method and then configure the authentication-specific parameters.

### Standard authentication

Standard authentication requires an authentication user ID and password to connect to a REST endpoint. When you configure a standard authentication type, you can further configure basic and OAuth authentication types.

**Note:** Digest authentication is not applicable.

The following table describes the basic connection properties for standard authentication:

Property	Description
Authentication Type	<p>The authentication type that you can use when you select the Standard authentication.</p> <p>You can select one of the following authentication types:</p> <ul style="list-style-type: none"> <li>- BASIC</li> <li>- OAUTH</li> <li>- NONE</li> </ul> <p>Default is NONE.</p>
Auth User ID	<p>The user name to log in to the web service application when you select the standard authentication.</p> <p>Required for Basic authentication type.</p>
Auth Password	<p>The password associated with the user name when you select the standard authentication.</p> <p>Required for Basic authentication type.</p>

Property	Description
OAuth Consumer Key	The client key associated with the web service application. Required only for OAuth authentication type.
OAuth Consumer Secret	The client password to connect to the web service application. Required only for OAuth authentication type.
OAuth Token	The access token to connect to the web service application. Required only for OAuth authentication type.
OAuth Token Secret	The password associated with the OAuth token. Required only for OAuth authentication type.
Swagger File Path	<p>The path of the Swagger file or OpenAPI file.</p> <p>You can specify one of the following file paths:</p> <ul style="list-style-type: none"> <li>- Path and file name of the Swagger or OpenAPI file on the Secure Agent machine.</li> <li>- The URL on which the Swagger or OpenAPI file is hosted. The hosted URL must return the content of the file without prompting for further authentication and redirection.</li> </ul> <p>For example, the path of the Swagger file can be:</p> <pre>C:\Swagger\sampleSwagger.json</pre> <p>The user must have the read permission for the folder and the file.</p>

## OAuth 2.0 Client Credentials authentication

OAuth 2.0 client credentials authentication requires at a minimum the client ID, access token URL, client secret, scope, and the access token.

The following table describes the basic connection properties for OAuth 2.0 client credentials authentication:

Property	Description
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.
Client Secret	Client secret of your application.
Scope	<p>Specifies access control if the API endpoint has defined custom scopes. Enter scope attributes, each separated by a space. For example:</p> <pre>root_readonly root_readwrite manage_app_users</pre>
Access Token Parameters	<p>Additional parameters to use with the access token URL. Define the parameters in the JSON format.</p> <p>For example,</p> <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>

Property	Description
Client Authentication	Select an option to send the client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .
Generate Access Token	Generates an access token based on the information provided in the above fields.
Access Token	The access token value. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server in the Secure Agent properties. The proxy configured in the connection configuration does not apply to the generate access token call.
Swagger File Path	The path of the Swagger file or OpenAPI file. You can specify one of the following file paths: <ul style="list-style-type: none"> <li>- Path and file name of the Swagger or OpenAPI file on the Secure Agent machine.</li> <li>- The URL on which the Swagger or OpenAPI file is hosted. The hosted URL must return the content of the file without prompting for further authentication and redirection.</li> </ul> For example, the path of the swagger file can be: C:\swagger\sampleSwagger.json The user must have the read permission for the folder and the file. <b>Note:</b> In a streaming ingestion and replication task, use only a hosted URL of the swagger specification file as the swagger file path.

## OAuth 2.0 Authorization Code authentication

To use authorization code authentication, register the following Informatica redirect URL in your application:

`https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback`

If the access token expires and the error codes 400, 401, and 403 are returned in the response, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieves a new access token.

The following table describes the basic connection properties for OAuth 2.0 authorization code authentication:

Property	Description
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	Client ID of your application.

Property	Description
Client Secret	Client secret of your application.
Scope	Specifies access control if the API endpoint has defined custom scopes. Enter scope attributes, each separated by a space. For example, root_readonly root_readwrite manage_app_users
Access Token Parameters	Additional parameters to use with the access token URL. Define the parameters in the JSON format. For example, <pre>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</pre>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define the parameters in the JSON format. For example, <pre>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</pre>
Client Authentication	Select an option to send the client ID and client secret for authorization either in the request body or in the request header. Default is <b>Send Client Credentials in Body</b> .
Generate Access Token	Generates an access token and refreshes the token based on the information provided in the above fields.
Access Token	The access token value. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server in the Secure Agent properties. The proxy configured in the connection configuration does not apply to the generate access token call.

Property	Description
Refresh Token	<p>The refresh token value.</p> <p>Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent fetches a new access token with the help of refresh token.</p> <p>If the refresh token expires, you must either provide a valid refresh token or regenerate a new refresh token by clicking <b>Generate Access Token</b>.</p>
Swagger File Path	<p>The path of the Swagger file or OpenAPI file.</p> <p>You can specify one of the following file paths:</p> <ul style="list-style-type: none"> <li>- Path and file name of the Swagger or OpenAPI file on the Secure Agent machine.</li> <li>- The URL on which the Swagger or OpenAPI file is hosted. The hosted URL must return the content of the file without prompting for further authentication and redirection.</li> </ul> <p>For example, the path of the swagger file can be:</p> <pre>C:\swagger\sampleSwagger.json</pre> <p>The user must have the read permission for the folder and the file.</p> <p><b>Note:</b> In a streaming ingestion and replication task, use only a hosted URL of the swagger specification file as the swagger file path.</p>

## JWT bearer token authentication

JWT bearer token authentication requires at a minimum the JWT header, JWT payload, and authorization server URL.



The following table describes the basic connection properties for JWT bearer token authentication:

Property	Description
JWT Header	<p>JWT header in JSON format.</p> <p>Sample:</p> <pre>{   "alg": "RS256",   "kid": "xxyyzz" }</pre> <p>You can configure <code>HS256</code> and <code>RS256</code> algorithms.</p>
JWT Payload	<p>JWT payload in JSON format.</p> <p>Sample:</p> <pre>{   "iss": "abc",   "sub": "678",   "aud": "https://api.box.com/oauth2/token",   "box_sub_type": "enterprise",   "exp": "120",   "jti": "3ee9364e" }</pre> <p>The expiry time represented as <b>exp</b> is the relative time in seconds. The expiry time is calculated in the UTC format from the token issuer time (<i>iat</i>).</p> <p>When <i>iat</i> is defined in the payload and the expiry time is reached, mappings and Generate Access Token fails. To generate a new access token, you must provide a valid <i>iat</i> in the payload.</p> <p>If <i>iat</i> is not defined in the payload, the expiry time is calculated from the current timestamp.</p> <p>To pass the expiry time as a string value, enclose the value with double quotes. For example:</p> <pre>"exp": "120"</pre> <p>To pass the expiry time as an integer value, do not enclose the value with double quotes.</p> <p>For example,</p> <pre>"exp": 120"</pre>
Authorization Server	Access token URL configured in your application.
KeyStore File Path	<p>The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the keystore file name and path as a JVM option or import the certificate to any directory.</p> <p>For the serverless runtime environment, specify the keystore file path in the serverless agent directory.</p> <p>For example, <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</code></p>

Property	Description
KeyStore Password	The password for the keystore file required for a secure communication. You can also configure the keystore password as a JVM option.
Private Key Alias	Alias name of the private key used to sign the JWT payload.
Private Key Password	The password for the keystore file required for a secure communication. The private key password must be same as the keystore password.
Access Token	The access token value. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value. To pass the generate access token call through a proxy server, you must configure an unauthenticated proxy server in the Secure Agent properties. The proxy configured in the connection configuration does not apply to the generate access token call.
Swagger File Path	The path of the Swagger file or OpenAPI file. You can specify one of the following file paths: <ul style="list-style-type: none"> <li>- Path and file name of the Swagger or OpenAPI file on the Secure Agent machine.</li> <li>- The URL on which the Swagger or OpenAPI file is hosted. The hosted URL must return the content of the file without prompting for further authentication and redirection.</li> </ul> For example, the path of the swagger file can be: <code>C:\swagger\sampleSwagger.json</code> The user must have the read permission for the folder and the file. <b>Note:</b> In a streaming ingestion and replication task, use only a hosted URL of the swagger specification file as the swagger file path.

## Advanced settings

The following table describes the advanced connection properties for JWT bearer token authentication:

Property	Description
Authorization Advanced Properties	<p>Additional parameters to use with the access token URL. Parameters must be defined in the JSON format.</p> <p>For example,</p> <pre>[{"Name": "client_id", "Value": "abc"}, {"Name": "client_secret", "Value": "abc"}]</pre>
TrustStore File Path	<p>The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;\jre\lib\security\cacerts.</pre> <p>For the serverless runtime environment, specify the truststore file path in the serverless agent directory.</p> <p>For example, <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</code></p>
TrustStore Password	<p>The password for the truststore file that contains the SSL certificate.</p> <p>You can also configure the truststore password as a JVM option.</p>
Proxy Type	<p>Type of proxy.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"><li>- No Proxy. Bypasses the proxy server configured in the agent or the connection properties.</li><li>- Platform Proxy. Considers the proxy configured in the agent.</li><li>- Custom Proxy. Considers the proxy configured in the connection properties.</li></ul>

Property	Description
Proxy Configuration	<p>The format required to configure proxy. You can configure proxy using the following format: &lt;host&gt;:&lt;port&gt; You cannot configure an authenticated proxy server.</p>
Advanced Fields	<p>Enter the arguments that the agent uses when connecting to a REST endpoint. When you specify multiple arguments, separate each argument by a semicolon. For example, <code>connectiondelaytime:10000;retryattempts:5</code> You can specify the following arguments:</p> <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout.</b> The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API. <b>Note:</b> If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime.</b> The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts.</b> Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema.</b> Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <p><b>Note:</b> In a streaming ingestion and replication task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.</p>

## API key authentication

API key authentication allows you to provide a unique key and a corresponding value to authenticate API calls made to the REST endpoint.

The following table describes the basic connection properties for API key authentication:

Property	Description
Key	The unique API key that REST V2 Connector uses to authenticate the API calls made to the REST endpoint.
Value	The value corresponding to the API key that is required to make the API calls.

Property	Description
Add API Key to	<p>Determines if the API key and its corresponding value must be sent as a request header or a query parameter to make API calls to the REST endpoint.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- Request Header</li> <li>- Query Parameter</li> </ul>
Swagger File Path	<p>The path of the Swagger file or OpenAPI file.</p> <p>You can specify one of the following file paths:</p> <ul style="list-style-type: none"> <li>- Path and file name of the Swagger or OpenAPI file on the Secure Agent machine.</li> <li>- The URL on which the Swagger or OpenAPI file is hosted. The hosted URL must return the content of the file without prompting for further authentication and redirection.</li> </ul> <p>For example, the path of the swagger file can be:</p> <pre>C:\swagger\sampleSwagger.json</pre> <p>The user must have the read permission for the folder and the file.</p> <p><b>Note:</b> In a streaming ingestion and replication task, use only a hosted URL of the swagger specification file as the swagger file path.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
TrustStore File Path	<p>The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the truststore file name and password as a JVM option or import the certificate to the following directory:</p> <pre>&lt;Secure Agent installation directory&gt;\jre\lib\security\cacerts.</pre> <p>For the serverless runtime environment, specify the truststore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>
TrustStore Password	<p>The password for the truststore file that contains the SSL certificate.</p> <p>You can also configure the truststore password as a JVM option.</p>
KeyStore File Path	<p>The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Specify a directory path that is available on each Secure Agent machine.</p> <p>You can also configure the keystore file name and path as a JVM option or import the certificate to any directory.</p> <p>For the serverless runtime environment, specify the keystore file path in the serverless agent directory.</p> <p>For example, /home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;cert_name&gt;.jks</p>

Property	Description
KeyStore Password	The password for the keystore file required for secure communication. You can also configure the keystore password as a JVM option.
Proxy Type	Type of proxy. Select one of the following options: <ul style="list-style-type: none"> <li>- No Proxy: Bypasses the proxy server configured in the agent or the connection properties.</li> <li>- Platform Proxy: Considers the proxy configured in the agent.</li> <li>- Custom Proxy: Considers the proxy configured in the connection properties.</li> </ul>
Proxy Configuration	The format required to configure proxy. Configure proxy using the following format: <host>:<port> You cannot configure an authenticated proxy server.
Advanced Fields	Enter the arguments that the agent uses when connecting to a REST endpoint. When you specify multiple arguments, separate each argument by a semicolon. For example, <code>connectiondelaytime:10000;retryattempts:5</code> You can specify the following arguments: <ul style="list-style-type: none"> <li>- <b>ConnectionTimeout.</b> The wait time in milliseconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is the timeout defined in the endpoint API. <b>Note:</b> If you define both the REST V2 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</li> <li>- <b>connectiondelaytime.</b> The delay time in milliseconds to send a request to a REST endpoint. Default is 10000.</li> <li>- <b>retryattempts.</b> Number of times the connection is attempted when 400 and 500 series error codes are returned in the response. Default is 3. Specify 0 to disable the retry attempts.</li> <li>- <b>qualifiedSchema.</b> Determines if the schema selected is qualified or unqualified. Default is false.</li> </ul> <b>Note:</b> In a streaming ingestion and replication task, only <code>ConnectionTimeout</code> and <code>retryattempts</code> are applicable.

## Secure communication with TLS authentication

Configure TLS authentication to establish one-way or two-way secure communication between the Secure Agent and the REST API over TLS.

To establish one-way secure communication, perform the following steps:

1. Generate the truststore. For more information on the steps, see *Generate a Truststore*.
2. Configure the REST V2 connection for one-way SSL. You can specify the truststore file and truststore password in the connection, or set them in the JVM options of the Secure Agent.

To establish two-way secure communication, you must first configure one-way secure communication, and then perform the following steps:

1. Generate the keystore. For more information on the steps, see *Generate a Keystore*.
2. Configure the REST V2 connection for two-way SSL. You can specify the keystore file and keystore password in the connection, or set them in the JVM options of the Secure Agent.

If you specify keystore and truststore properties in the connection and in the JVM options, the Secure Agent processes the certificates based on the properties configured in the connection.

## Generate a truststore

To generate a truststore, you need a server certificate. Get the server certificate and perform the following steps to generate the truststore:

1. Import the server certificate to the following file path:  
`<Secure Agent installation directory>\jre\lib\security\cacerts`
2. To generate the truststore, run the following command from the command line:  
`keytool -importcert -alias <Specify alias name here> -file <Specify server certificate here> -keystore <Specify the name of custom truststore to be generated> -storepass <Specify password for the custom truststore>`

For example, `keytool -importcert -alias RESTV2CACert -file ca.pem -keystore sampletruststore -storepass JKSTrustStorePassword`

In the example, a truststore file is generated by the name *sampletruststore* and password *JKSTrustStorePassword*.

## Generate a keystore

To generate a keystore, you need a client certificate and a client private key. Get the client certificate and client private key, and then perform the following steps to generate the keystore:

1. Import the certificate to the following file path:  
`<Secure Agent installation directory>\jre\lib\security\cacerts`

2. To generate the keystore, run the following command from the command line:

```
openssl pkcs12 -export -in <Specify client certificate here> -inkey <Specify client private key here> -name "<Specify any name here>" -passout pass:<Specify password for the keystore to be generated> -out <Specify name for the keystore with p12 extension>
```

For example, `openssl pkcs12 -export -in /home/samplefolder/certs/client-cert.pem -inkey /home/samplefolder/certs/client-key.pem -name "restclient" -passout pass:PKCSKeyStorePassword -out samplekeystore.p12`

In the example, a keystore file by the name `samplekeystore.p12` is generated in the PKCS12 format.

To convert the keystore file from .p12 format to .jks format, run the following command from the command line:

```
keytool -importkeystore -srckeystore <Specify name of the p12 keystore file> -srcstoretype pkcs12 -srcstorepass <Specify password for generated p12 keystore file> -destkeystore <Specify name for the JKS keystore file> -deststoretype JKS -deststorepass <Specify password for the JKS keystore file>
```

**Note:** Ensure that the password specified in `-srcstorepass` must be the same as the `-deststorepass`.

For example, `keytool -importkeystore -srckeystore samplekeystore.p12 -srcstoretype pkcs12 -srcstorepass PKCSKeyStorePassword -destkeystore keystore -deststoretype JKS -deststorepass PKCSKeyStorePassword`

In the example, a keystore file is generated by the name `samplekeystore` and password `PKCSKeyStorePassword`.

## Configuring one-way or two-way secure communication

You can configure a connection for one-way or two-way SSL.

### Configuring the connection for one-way SSL

You can either specify the name of the truststore file and truststore password in the TrustStore File Name and TrustStore Password fields in the connection properties. Alternatively, you can set the truststore file name and truststore password in the JVM options in the Secure Agent properties.

1. Click **Administrator > Runtime Environments**, and select an agent.
2. Select **Type** as DTM under **System Configuration Details**.
3. Add the following JVM options:
  - `JVMOption1=-Djavax.net.ssl.trustStore=<absolute path of the .jks truststore file>`
  - `JVMOption2=-Djavax.net.ssl.trustStorePassword=<truststore password>`

### Configuring the connection for two-way SSL

You can either specify the name of the keystore file and keystore password in the KeyStore File Name and KeyStore Password connection properties. Alternatively, you can set the keystore file and keystore password in the JVM options in the Secure Agent properties.

To use two-way SSL, you must first configure one-way SSL, and then perform the following steps to configure two-way SSL:

1. Click **Administrator > Runtime Environments**, and select an agent.
2. Select **Type** as DTM under **System Configuration Details**.
3. Add the following JVM options:
  - `JVMOption3=-Djavax.net.ssl.keyStore=<absolute path of the .jks keystore file>`



- `JVMOption4=-Djavax.net.ssl.keyStorePassword=<keystore password>`

## Secure communication in a serverless runtime environment

When you use the serverless runtime environment, you can configure TLS authentication and establish one-way or two-way secure communication with the REST API.

Ensure that the certificates are in the `.jks` format.

To configure a secure REST V2 connection using the serverless runtime environment, complete the following prerequisite tasks to add the TLS certificates to the serverless runtime location:

1. Create the following structure for the serverless agent configuration in AWS:  
`<Supplementary file location>/serverless_agent_config`
2. For one-way secure communication, add the truststore certificates and for the two-way secure communication, add the truststore and keystore certificates in the Amazon S3 bucket in the following location in your AWS account:  
`<Supplementary file location>/serverless_agent_config/SSL`
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<RESTV2_trustStore_cert_name>.jks
        - fileCopy:
            sourcePath: SSL/<RESTV2_keyStore_cert_name>.jks
```

where the source path is the directory of the certificate files in AWS.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS location:  
`<Supplementary file location>/serverless_agent_config`  
 When the `.yml` file runs, the SSL certificates are copied from the AWS location to the serverless agent directory.
5. In the REST V2 connection properties, specify the following certificate path in the serverless agent directory in the **TrustStore File Path** and **KeyStore File Path** fields:  
`/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<cert_name>.jks`

## Swagger specification file in a serverless runtime environment

To configure a swagger file in a serverless runtime environment, be sure to complete the prerequisites.

In the serverless runtime environment, you can configure a swagger file in one of the following ways:

- Provide the swagger file public hosted URL in the **Swagger File Path** connection property. Ensure that the URL must return the content of the file without prompting for further authentication and redirection.
- Place the swagger file in the serverless agent directory.

To configure a swagger file in a serverless runtime environment, complete the following prerequisite tasks to add the swagger file to the serverless runtime location:

1. Create the following structure for the serverless agent configuration in AWS or Azure:

```
<Supplementary file location>/serverless_agent_config
```

2. Add the swagger specification file in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account:

```
<Supplementary file location>/serverless_agent_config/restv2
```

- a. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoApply:
      restv2:
        swaggers:
          - fileCopy:
              sourcePath: restv2/<swagger_file_name1>.json
          - fileCopy:
              sourcePath: restv2/<swagger_file_name2>.json
```

where the source path is the directory path of the swagger files in AWS or Azure.

3. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location:

```
<Supplementary file location>/serverless_agent_config
```

When the .yml file runs, the SSL certificates are copied from the AWS or Azure location to the serverless agent directory.

4. In the REST V2 connection properties, specify the following swagger path in the serverless agent directory in the **Swagger File Path** field:

```
/home/cldagnt/SystemAgent/serverless/configurations/restv2/<swagger_file_name>.json
```

## Rules and guidelines for runtime environment

Consider the following guidelines when you run tasks in different runtime environments:

- You cannot use a proxy server to connect to Informatica Intelligent Cloud Services when you use the Hosted Agent or the serverless runtime environment.
- You cannot connect to the REST API endpoints that require custom server certificate signed by CA and are not a part of Informatica cacerts truststore, when you use the Hosted Agent.
- You cannot configure JWT bearer token authentication when you use the Hosted Agent.
- Ensure that the swagger specification file URL is a public URL and returns the content of the file without prompting for further authentication and redirection when you use the Hosted Agent.

# Rules and guidelines for a REST V2 connection

Consider the following rules and guidelines for a Rest V2 connection:

- When you test the connection, the Secure Agent validates the following parameters:
  - Path of the local Swagger file or the URL of the hosted Swagger file.
  - JSON format of the Swagger file.

However, the Secure Agent does not validate endpoint credentials when you test the connection.

- You can configure proxy at the agent level or connection level. See the following table to understand the proxy settings that take precedence when you define the System proxy and proxy at the connection level:

System proxy	REST V2 connection attribute			Result
	No proxy	Platform proxy	Custom proxy	
No	Yes	No	No	Does not consider proxy.
No	No	Yes	No	Does not consider proxy.
No	No	No	Yes	Considers custom proxy.
Yes	Yes	No	No	Does not consider proxy.
Yes	No	Yes	No	Considers platform proxy.
Yes	No	No	Yes	Considers custom proxy.

## REST V3 Connection Properties

When you set up a REST V3 connection, you must configure the connection properties.

When you create a connection, you can specify the following authentication methods:

- **None.** Does not require an authentication method to connect to the REST endpoint.
- **Basic.** Requires user ID and password to connect to the REST endpoint.
- **OAuth 2.0 authorization code.** Requires an authorization server to connect to the REST endpoint. Authorization Code allows authorized access to the endpoint without sharing or storing your credentials.
- **OAuth 2.0 client credentials.** Requires client ID and client secret to connect to the REST endpoint.

The following table describes the REST V3 connection properties for a basic authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select <b>Basic</b> . Default is None.
Auth User ID	The user name to log in to the web service application when you select the Basic authentication type.
Auth Password	The password associated with the user name when you select the Basic authentication type.
TrustStore File Path	The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.

Connection property	Description
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: <ul style="list-style-type: none"> <li>- None. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Custom. Considers proxy configured at the connection level.</li> <li>- Platform. Considers proxy configured at the agent level.</li> </ul> Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	The IP address or host name of the proxy server. Required only for the Custom proxy type.
Proxy Port	The port number of the proxy server. Required only for the Custom proxy type.
Proxy User	The user name for the proxy server. Required only for the Custom proxy type.
Proxy Password	The password for the proxy server. Required only for the Custom proxy type.
Connection Timeout	The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is 60 seconds. <b>Note:</b> If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the REST endpoint. You can select one of the following options: <ul style="list-style-type: none"> <li>- HTTP 2</li> <li>- HTTP 1.1</li> </ul> Default is HTTP 2.

## Authorization Code Authentication

To use authorization code authentication, you must first register the following Informatica redirect URL in your application:

`https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback`

If the access token expires and the error codes 400, 401, and 403 are returned in the response, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieve a new access token.

The following table describes the REST V3 connection properties for an OAuth 2.0 authorization code authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select <b>OAuth 2.0 authorization code</b> . Default is None.
Authorization Token URL	Authorization server URL configured in your application.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the REST endpoint has defined custom scopes. Enter space-separated scope attributes. For example: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
Authorization Code Parameters	Additional parameters to use with the authorization token URL. Define parameters in the JSON format. For example: <code>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</code>
Client Authentication	The client authentication details for authorization. Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is <b>Send client credentials in body</b> .
Generate Access Token	Generates access token and refresh token based on the authentication details provided.
Access Token	The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.  To pass the generate access token call through a proxy server, you must configure a proxy server at the Secure Agent level. The REST V3 connection-level proxy configuration does not apply to the generate access token call.

Connection property	Description
Refresh Token	Allows the Secure Agent to fetch new access token if the access token is not valid or expires. Enter the refresh token value or click <b>Generate Access Token</b> to populate the refresh token value. If the refresh token expires, you must either provide a valid refresh token or click <b>Generate Access Token</b> to regenerate a new refresh token.
TrustStore File Path	The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API. Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API. Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	Type of proxy. You can select one of the following options: <ul style="list-style-type: none"> <li>- None. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Custom. Proxy configured at the connection level is considered.</li> <li>- Platform. Proxy configured at the agent level is considered.</li> </ul> Proxy is not applicable when you use the serverless runtime environment.
Proxy Host	The IP address or hostname of the proxy server. Required only for the Custom proxy type.
Proxy Port	The port number of the proxy server. Required only for the Custom proxy type.
Proxy User	The user name for the proxy server. Required only for the Custom proxy type.
Proxy Password	The password for the proxy server. Required only for the Custom proxy type.
Connection Timeout	The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over. Default is 60 seconds. <b>Note:</b> If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.

Connection property	Description
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the REST endpoint. You can select one of the following options: - HTTP 2 - HTTP 1.1 Default is HTTP 2.

## Client Credential Authentication

The following table describes the REST V3 connection properties for OAuth 2.0 client credentials authentication type connection:

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent or serverless runtime environment.
Auth Type	The authentication method that the connector must use to connect to the REST endpoint. Select <b>OAuth 2.0 client credentials</b> . Default is None.
Access Token URL	Access token URL configured in your application.
Client ID	The client identifier issued during the application registration process.
Client Secret	The client secret issued during the application registration process.
Scope	The scope of the access request when the rest endpoint has defined custom scopes. Enter space-separated scope attributes. For example: <code>root_readonly root_readwrite manage_app_users</code>
Access Token Parameters	Additional parameters to use with the access token URL. Define parameters in the JSON format. For example: <code>[{"Name": "resource", "Value": "https://&lt;serverName&gt;"}]</code>
Client Authentication	The client authentication details for authorization. Select an option to send Client ID and Client Secret for authorization either in the request body or in the request header. Default is <b>Send client credentials in body</b> .
Generate Access Token	Generates access token based on the authentication details provided.



Connection property	Description
Access Token	<p>The access token granted by the authorization server to access the data using a specific role. Enter the access token value or click <b>Generate Access Token</b> to populate the access token value.</p> <p>To pass the generate access token call through a proxy server, you must configure a proxy server at the Secure Agent level. The REST V3 connection-level proxy configuration does not apply to the generate access token call.</p>
TrustStore File Path	<p>The absolute path of the truststore file that contains the TLS certificate to establish a one-way or two-way secure connection with the REST API.</p> <p>Ensure that the truststore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.</p>
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Path	<p>The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure communication with the REST API.</p> <p>Ensure that the keystore file is in .jks format. Specify a directory path that is available on each Secure Agent machine in the runtime environment.</p>
KeyStore Password	The password for the keystore file required for secure communication.
Proxy Type	<p>Type of proxy.</p> <p>You can select one of the following options:</p> <ul style="list-style-type: none"> <li>- None. Bypasses the proxy server configured at the agent or the connection level.</li> <li>- Custom. Considers proxy configured at the connection level.</li> <li>- Platform. Considers proxy configured at the agent level.</li> </ul> <p>Proxy is not applicable when you use the serverless runtime environment.</p>
Proxy Host	<p>The IP address or host name of the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy Port	<p>The port number of the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy User	<p>The user name for the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Proxy Password	<p>The password for the proxy server.</p> <p>Required only for the Custom proxy type.</p>
Connection Timeout	<p>The wait time in seconds to get a response from a REST endpoint. The connection ends after the connection timeout is over.</p> <p>Default is 60 seconds.</p> <p><b>Note:</b> If you define both the REST V3 connection timeout and the endpoint API timeout, the connection ends at the shortest defined timeout.</p>

Connection property	Description
Retry Attempts	Number of times to retry the connection when 100, 300, 400, and 500 series error codes are returned in the response. Default is 0. Specify 0 to disable the retry attempts. In case of 408 error code, silent retries are attempted. Therefore, the number of retry attempts can be more than the value you specify.
Retry Delay	The wait time in seconds before a retry is attempted. Default is 0.
HTTP version	The HTTP version to connect to the rest endpoint. You can select one of the following options: - HTTP 2 - HTTP 1.1 Default is HTTP 2.

## Rules and guidelines for REST V3 connections

Consider the following rules and guidelines for Rest V3 connections:

- Test the connection to verify if the mandatory parameters are valid.
- You can configure proxy at the agent level or connection level. See the following table to understand the proxy settings that take precedence when you define the System proxy and proxy at the connection level:

System Proxy	REST V3 Connection Attribute			Result
	No Proxy	Platform Proxy	Custom Proxy	
No	Yes	No	No	Does not consider proxy.
No	No	Yes	No	Does not consider proxy.
No	No	No	Yes	Considers Custom proxy.
Yes	Yes	No	No	Does not consider proxy.
Yes	No	Yes	No	Considers Platform proxy.
Yes	No	No	Yes	Considers Custom proxy.

## CHAPTER 183

# Salesforce Analytics connection properties

When you set up a Salesforce Analytics connection, you must configure the connection properties.

The following table describes the Salesforce Analytics connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	User name of the Salesforce Analytics account.
Password	Password for the Salesforce Analytics account.
Security Token	The token used to login to Salesforce Analytics from an untrusted network.
Service URL	URL of the Salesforce Analytics service that you want to access. For example: <code>https://login.salesforce.com/services/Soap/u/48.0</code> In a test or development environment, you might want to access the Salesforce Analytics Sandbox testing environment.
Temp Folder Name	The directory where the Secure Agent stores the JSON files and data archive files. After the successful execution of a task, the temporary .gz files are deleted.
Default Date Format	The date format to read date columns in the JSON file.

## CHAPTER 184

# Salesforce Commerce Cloud connection properties

When you create a Salesforce Commerce Cloud connection, you must configure the connection properties.

**Important:** Salesforce Commerce Cloud Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table lists the Salesforce Commerce Cloud connection properties:

Connection property	Description
Connection Name	The name of the connection.
Description	Optional. The description of the connection.
Type	Type of connection. Select <b>Salesforce Commerce Cloud</b> .
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Base URL	The base URL to connect to Salesforce Commerce Cloud. For example, <code>https://demo-ocapi.demandware.net</code>
Client ID	The client ID for OAuth 2.0 authentication to connect to Salesforce Commerce Cloud.
Client Secret	The client secret key for OAuth 2.0 authentication to connect to Salesforce Commerce Cloud.
API Type	The type of Salesforce Commerce Cloud API that you want to use. Select one of the following APIs: <ul style="list-style-type: none"><li>- <b>data</b>. Accesses backend system resources such as your product inventory and customer lists.</li><li>- <b>meta</b>. Gets the metadata of OCAPI resources from Salesforce Commerce Cloud.</li><li>- <b>shop</b>. Gets details related to the shopper persona such as cart activities, product information, product pricing.</li></ul>
API Version	The version of the data API, meta API, or shop API that you want to connect to.
Site ID	Required for shop API. The ID of the site you want to connect to.

## CHAPTER 185

# Salesforce connection properties

Create a Salesforce connection to securely read data from or write data to Salesforce. Use a Salesforce connection to access objects in a Salesforce application.

## Prepare for authentication

You can configure standard and OAuth authentication types to access Salesforce. Consider using OAuth authentication to connect more securely to Salesforce.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

### Standard

To use a standard connection, you need the Salesforce account user name, password, and service URL. You also need your Salesforce security token to connect to Salesforce. If you do not want to use the security token, you need to add the Data Integration IP addresses to the trusted IP ranges in your Salesforce account. For more information about the list of IP address ranges used by the Secure Agent and your service, see [POD Availability and Networking](#). For information about setting the IP address in your Salesforce account, see the Salesforce documentation.

### OAuth

Create an OAuth connection that uses the OAuth 2.0 protocol to access Salesforce through the Salesforce API. OAuth is a standard protocol that allows for secure API authorization.

To create an OAuth connection, you need an OAuth refresh token. Informatica provides the SFDC OAuth 2.0 tool to generate the OAuth refresh token.

You also need the consumer key and consumer secret from your Snowflake account to generate the OAuth refresh token.

1. Download the SFDC OAuth tool from [Informatica Marketplace](#).
2. Extract the `OAuth.zip` file.
3. Go to the `oauth\conf` folder, open the `server.xml` file, and update the `mystore.jks` file path to the one on your system. Save and close the file.
4. Go to `\oauth\bin` and run the command `catalina.bat start`.
5. Open `http://localhost:8090/salesforce` from the browser.
6. Enter your Salesforce user name and password to log in.

7. Enter the client ID and client secret, and click **Submit**.  
The client ID is the consumer key in Salesforce and the client secret is the consumer secret in Salesforce.  
The OAuth refresh token is generated.

## Connect to Salesforce

Let's configure the Salesforce connection properties to connect to Salesforce.

By default, Salesforce connections for new organizations use the Salesforce API version 60.0. You can edit existing Salesforce connections or create new connections to use any Salesforce API version up to 60.0, except the version 58.0.

### Before you begin

Before you get started, you'll need to get information from your Salesforce account based on the connection type that you want to configure.

To configure a standard connection, get the Salesforce user name, password, service URL, and security token from your Salesforce account.

To configure an OAuth connection, get the consumer key, consumer secret, and service URL from your Salesforce account. You also need to get the OAuth refresh token that is generated from the SFDC OAuth tool provided by Informatica.

Check out [“Prepare for authentication” on page 593](#) to learn more about the authentication prerequisites.

The following video shows you how to get the information that you need from your Salesforce account and how to generate an OAuth refresh token using the SFDC OAuth tool:



### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Salesforce

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Hosted Agent doesn't apply to mappings in advanced mode.</p> <p>You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.</p>

## Salesforce connection types

You can configure standard and OAuth connection types to access Salesforce. Select the required connection type and then configure the connection-specific parameters.

### Standard connection

A Salesforce standard connection requires at a minimum your Salesforce account user name, password, and service URL.

The following table describes the basic connection properties for standard connection:

Property	Description
User Name	The user name to connect to the Salesforce account.
Password	The password to connect to the Salesforce account.
Service URL	<p>URL of the Salesforce service.</p> <p>For example: <code>https://login.salesforce.com/services/Soap/u/60.0</code></p> <p>By default, Salesforce connections for new organizations use version 60.0 of the Salesforce API. You can use any Salesforce API version up to 60.0, except the version 58.0.</p> <p>Maximum length is 100 characters.</p> <p>If you edit the service URL for an existing standard connection, you need to re-enter the password and security token.</p>

## Advanced settings

The following table describes the advanced connection properties for standard connection:

Property	Description
Security Token	Security token generated from the Salesforce application. <b>Note:</b> If you don't enter the Salesforce security token in this field, you need to add the Data Integration IP addresses to the trusted IP ranges in your Salesforce account. Otherwise, the connection might fail. For more information about the list of IP address ranges, see <a href="#">"Standard" on page 593</a> .
Bypass proxy server settings defined for the Secure Agent	Bypasses the proxy server settings defined for the Secure Agent in the Secure Agent Manager and directly connects to Salesforce. If you do not select this option, the Salesforce connection uses the proxy server setting defined for the Secure Agent to connect to Salesforce.

## OAuth connection

OAuth connection requires your Salesforce consumer key, secret, and refresh token. When you use OAuth connection, you need to use the OAuth 2.0 protocol.

The following table describes the basic connection properties for OAuth connection:

Property	Description
OAuth Consumer Key	The consumer key to generate a refresh token.
OAuth Consumer Secret	The consumer secret to generate a refresh token.
OAuth Refresh Token	The refresh token that you generated using the SFDC OAuth 2.0 tool. For more information about how to generate the OAuth refresh token, see the <i>Before you begin</i> section.
Service URL	URL of the Salesforce service endpoint. For example: <code>https://login.salesforce.com/services/Soap/u/60.0</code> You can use any Salesforce API version up to 60.0, except the version 58.0. Maximum length is 100 characters. When you edit the service URL for an existing OAuth connection, you need to re-enter the consumer key, consumer secret, and refresh token.

## Advanced settings

The **Service End Point** and **OAuth Access Token** fields do not apply to OAuth authentication.

# Firewall configuration

If your organization passes data through a firewall, you need to configure the firewall to allow access to Salesforce.



If you cannot connect to Salesforce servers and receive a connection error, contact your network administrator to allow access to Salesforce servers.

For more information, see the following Knowledge Base article: [Firewall rules](#)

**Note:** IP addresses for Salesforce servers might change. For the latest information about the server IP addresses of Salesforce, see the Salesforce documentation.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent and the serverless runtime environment to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Connection timeout

You can set the `SalesForceConnectionTimeout` property for the DTM in the Secure Agent configuration properties to the duration, in seconds, that the connection waits for a response to its requests from the Salesforce web service. If the web service doesn't respond within the specified timeout period, the request times out.

The following image shows the configured `SalesForceConnectionTimeout` property for the Secure Agent:

The screenshot shows a window titled "System Configuration Details" with a "Reset All" button. Below the title bar, there are two dropdown menus: "Service" set to "Data Integration Server" and "Type" set to "DTM". Below these is a table with three columns: "Type", "Name", and "Value". The table contains one row with "DTM" in the Type column, "SalesForceConnectionTimeout" in the Name column, and "300" in the Value column.

Type	Name	Value
DTM	SalesForceConnectionTimeout	300

## Troubleshooting a Salesforce connection

If you encounter errors when you configure a Salesforce connection, you might have to enter the Salesforce security token in the Salesforce connection properties.

If the security token is required and the **Security Token** field in the Salesforce connection is empty or not valid, the following error message appears when you test or create a connection:

```
The login to Salesforce.com failed with the following message -  
LOGIN_MUST_USE_SECURITY_TOKEN:
```

Go to the Salesforce web site to get the security token. To avoid adding the security token to the connection details, you can also add Data Integration IP addresses to the trusted IP ranges in your Salesforce account.

## CHAPTER 186

# Salesforce Data Cloud connection properties

Create a Salesforce Data Cloud connection to securely write data to Salesforce. You can use a Salesforce Data Cloud connection to specify targets in mappings and mapping tasks.

## Connect to Salesforce Data Cloud

Let's configure the Salesforce Data Cloud connection properties to connect to Salesforce Data Cloud.

### Before you begin

Before you get started, create a connected app for the Data Cloud Ingestion API in Salesforce Data Cloud, with the required scopes.

You need at a minimum the *Manage user data via APIs (api)* and *Manage Data Cloud Ingestion API data (cdp\_ingest\_api)* scopes for Salesforce Data Cloud.

To load data, you also need to create an ingestion API data stream.

Configure your connected app and get the consumer key and consumer secret to generate the access token.

For more information about these steps, see the Salesforce Data Cloud documentation.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Salesforce Data Cloud

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent or Hosted Agent.</p>
Authentication Type	<p>The authentication method to connect to Salesforce Data Cloud.</p> <p>Default is OAuth 2.0 client credentials.</p>
Access Token URL	<p>The endpoint where OAuth 2.0 requests are sent to obtain an access token to connect to the Salesforce Data Cloud instance.</p> <p>The format of the URL is: <code>https://&lt;Salesforce Data Cloud organization ID&gt;my.salesforce.com/services/oauth2/token</code></p>
Client ID	<p>Client ID of your application to connect to Salesforce Data Cloud.</p>
Client Secret	<p>The client secret associated with the client ID.</p>
Access Token	<p>The access token value.</p> <p>Click <b>Generate Access Token</b> to populate the access token value.</p>

## CHAPTER 187

# Salesforce Marketing Cloud connection properties

When you set up a Salesforce Marketing Cloud connection, configure the connection properties.

The following table describes the Salesforce Marketing Cloud connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - , Maximum length is 255 characters.
Description	
Type	The Salesforce Marketing Cloud connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. You cannot run an application ingestion and replication task on a Hosted Agent or serverless runtime environment.
Salesforce Marketing Cloud Url	The URL that the agent uses to connect to the Salesforce Marketing Cloud WSDL. The following URL is an example for OAuth 1.0 URL: <code>https://webservice.s7.exacttarget.com/etframework.wsdl</code> The following URL is an example for OAuth 2.0 URL: <code>https://&lt;SUBDOMAIN&gt;.soap.marketingcloudapis.com/etframework.wsdl</code> <b>Important:</b> Salesforce is going to deprecate the OAuth 1.0 APIs by September 30 <sup>th</sup> , 2022. Informatica recommends that you upgrade to OAuth 2.0 for new and existing packages.
Username	Applies to basic authentication. The user name of the Salesforce Marketing Cloud account. <b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.
Password	Applies to basic authentication. The password for the Salesforce Marketing Cloud account. <b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.
Client ID	The client ID of Salesforce Marketing Cloud required to generate a valid access token.
Client Secret	The client secret of Salesforce Marketing Cloud required to generate a valid access token.

Property	Description
Use Proxy Server	<p>Connects to Salesforce Marketing Cloud through proxy.</p> <p><b>Note:</b> When you use a serverless runtime environment, you cannot use a proxy server to connect to Informatica Intelligent Cloud Services.</p> <p><b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.</p>
Enable Logging	<p>Enables logging for the task.</p> <p>When you enable logging, you can view the session log for the log details.</p> <p><b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.</p>
UTC offset	<p>Uses the UTC offset connection property to read data from and write data to Salesforce Marketing Cloud in the UTC offset time zone.</p> <p><b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.</p>
Batch Size	<p>Number of rows that the agent writes in a batch to the target.</p> <p>When you insert or update data and specify the contact key, the data associated with the specified contact ID is inserted or updated in a batch to Salesforce Marketing Cloud. When you upsert data to Salesforce Marketing Cloud, do not specify the contact key.</p> <p><b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.</p>
Enable Multiple BU	<p>Uses the Salesforce Marketing Cloud connection to access data across all business units.</p> <p>Select this option if there are multiple business units in your Salesforce Marketing Cloud account.</p> <p><b>Note:</b> This property is not applicable to connections configured for application ingestion and replication tasks.</p>

## CHAPTER 188

# Salesforce Mass Ingestion connection properties

When you set up a Salesforce Mass Ingestion connection, you must configure the connection properties.

The Salesforce Mass Ingestion connection uses a connected app to access the Salesforce data. Before you configure the connection, you must configure a connected app in Salesforce to allow the connection to access the Salesforce data.

**Note:** For more information about configuring a connected app, see the Knowledge Base article [000172095](https://help.salesforce.com/s/articleView?id=000172095).

The properties of a Salesforce Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0 Username-Password Flow:** Authenticates the connection by using the Salesforce account login credentials and the consumer key and consumer secret that Salesforce generates for the connected app.
- **OAuth 2.0 JWT Bearer Flow:** Authenticates the connection by using the Salesforce account user name, private key alias, private key password, and the consumer key that Salesforce generates for the connected app. Informatica recommends that you use this authentication method because this method provides secured access to Salesforce without sharing sensitive information, such as consumer secret and Salesforce account password.

### Connection properties for OAuth 2.0 Username-Password Flow authentication

The following table describes the connection properties for a Salesforce Mass Ingestion connection configured with OAuth 2.0 Username-Password Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Salesforce Mass Ingestion</b> .

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Salesforce account.
Password	Password for the Salesforce account.
Security Token	Security token associated with the Salesforce account. You can configure the connection without specifying the security token if there are no IP restrictions specified for the connected app. However, you must specify the security token if IP restrictions are enforced for the connected app and if the Secure Agent is not running on the trusted IP range specified for your Salesforce organization. <b>Note:</b> If you do not have the security token, reset the security token in Salesforce. For more information about resetting the security token, see the <a href="#">Salesforce documentation</a> .
Consumer Key	Consumer key that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
Consumer Secret	Consumer secret that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
API Version	Version of the Salesforce API that you want to use to access the source data. Default is 51.0. <b>Note:</b> You cannot use a version older than 51.0.
OAuth token URL	OAuth 2.0 token endpoint of the Salesforce organization. The connected app sends access token requests to this endpoint. Default value is: <code>https://login.salesforce.com/services/oauth2/token</code> This default URL is used for all Salesforce instances. Alternatively, you can enter an instance-specific URL: <code>https://&lt;instance domain URL&gt;/services/oauth2/token</code> An instance-specific URL can establish a more direct and faster connection to the Salesforce host server. If the load on the common default endpoint is heavy and ingestion jobs fail with an authentication error when using it, use this alternative URL instead.

**Note:** For more information about the OAuth 2.0 Username-Password Flow authentication method, see the Salesforce documentation.



## Connection properties for OAuth 2.0 JWT Bearer Flow authentication

The following table describes the connection properties for a Salesforce Mass Ingestion connection configured with OAuth 2.0 JWT Bearer Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Salesforce Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the Salesforce account.
Consumer Key	Consumer key that Salesforce generates when you enable OAuth 2.0 authentication for the connected app.
Keystore Path	Absolute path to the keystore file that contains the X509 certificate required to validate a JSON Web Token (JWT) and establish a secure connection with Salesforce. The keystore file must be in the Java KeyStore (JKS) format.
Keystore Password	Password for the keystore file.
Private Key Alias	Alias name of the private key used to sign the JWT.
Private Key Password	Password for the private key.
API Version	Version of the Salesforce API that you want to use to access the source data. Default is 51.0. <b>Note:</b> You cannot use a version older than 51.0.
OAuth token URL	OAuth 2.0 token endpoint of the Salesforce organization. The connected app sends access token requests to this endpoint. Default value is: <code>https://login.salesforce.com/services/oauth2/token</code> This default URL is used for all Salesforce instances. Alternatively, you can enter an instance-specific URL: <code>https://&lt;instance domain URL&gt;/services/oauth2/token</code> An instance-specific URL can establish a more direct and faster connection to the Salesforce host server. If the load on the common default endpoint is heavy and ingestion jobs fail with an authentication error when using it, use this alternative URL instead.

**Note:** For more information about the OAuth 2.0 JWT Bearer Flow authentication method, see the Salesforce documentation.

## CHAPTER 189

# Salesforce Pardot connection properties

When you set up a Salesforce Pardot connection, configure the connection properties.

The following table describes the Salesforce Pardot connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - , Maximum length is 255 characters.
Description	
Type	Salesforce Pardot
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent or a Hosted Agent.
Authentication	The authentication method to access the Salesforce Pardot objects.
Authorization URL	The Salesforce Pardot server endpoint that is used to authorize the user request and get the authorization code. The authorization URL is <code>https://login.salesforce.com/services/oauth2/authorize</code> .
Access Token URL	The Salesforce Pardot access token endpoint that is used to exchange the authorization code for an access token. The access token URL is <code>https://login.salesforce.com/services/oauth2/token</code> .
Client ID	The client ID of the Salesforce Pardot application created during the registration process.
Client Secret	The client secret of the Salesforce Pardot application created during the registration process.

<b>Property</b>	<b>Description</b>
Scope	The scope of access that is granted to an access token.
Access Token	The access token generated by Salesforce Pardot to access data.
Refresh Token	The refresh token to get a new access token.
Pardot Business Unit ID	The ID of the Salesforce Pardot business unit from which you want to read the data.
Access Token Parameters	Additional parameters to use with the access token URL.
Authorization Code Parameters	Additional parameters to use with the authorization URL.

# CHAPTER 190

## SAP connection properties

Create an SAP connection to access data from SAP through the Intermediate Documents (IDocs) or BAPI/RFC interface.

When you select **SAP** as the type, you can configure the following connections from the **SAP Connection Type** list:

- IDoc Reader
- IDoc Writer
- SAP RFC/BAPI Interface

### Prerequisites

Before you use an SAP connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process IDocs and SAP BAPI/RFC functions, you also need to verify if the required licenses are enabled for the SAP system.

### Download and configure the SAP libraries

To access SAP data through the Intermediate Documents (IDocs) or BAPI/RFC interface, you need to download and configure the SAP NetWeaver RFC SDK libraries and SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.

**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).

2. Download the latest version of the SAP NetWeaver RFC SDK 7.50 libraries that are specific to the operating system that hosts the Secure Agent.

The following table lists the libraries corresponding to the different operating systems:

Operating System	SAP NetWeaver RFC SDK Libraries
Linux 64	<ul style="list-style-type: none"> <li>- libicudata.so.50</li> <li>- libicui18n.so.50</li> <li>- libicuuc.so.50</li> <li>- libsapnwrfc.so</li> <li>- libsapucum.so</li> </ul>
Windows 64	<ul style="list-style-type: none"> <li>- icudt50.dll</li> <li>- icuin50.dll</li> <li>- icuuc50.dll</li> <li>- libsapucum.dll</li> <li>- sapnwrfc.dll</li> </ul>

3. Copy the SAP NetWeaver RFC SDK 7.50 libraries to the following directory:  
 <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext  
 \deploy\_to\_main\bin\rdtm  
 Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.
4. Set the following permissions for each SAP NetWeaver RFC SDK library:
  - Read, write, and execute permissions for the current user.
  - Read and execute permissions for all other users.
5. From the [SAP Support Portal](#), download the latest version of the 64-bit SAP JCo libraries based on the operating system of the machine on which the Secure Agent runs:

Secure Agent System	SAP JCo Libraries
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

6. Copy the JCo libraries to the following directory:  
 <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext  
 \deploy\_to\_main\bin\rdtm-extra\tpl\sap  
 Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.
7. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.
  - b. Click **Runtime Environments** to access the **Runtime Environments** page.
  - c. To the left of the agent name, click **Edit Secure Agent**.
  - d. From the **Service** list, select **Data Integration Server**.
  - e. From the **Type** list, select **Tomcat JRE**.

- f. Enter the JAVA\_LIBS value based on the operating system of the machine on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

System Configuration Details Reset All

Service: Data Integration Server

Type: Tomcat JRE

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adc

- g. Click **Save**.
  - h. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
8. Restart the Secure Agent.

## Configure SAP user authorization

Configure the SAP user account in the SAP system to enable data exchange through Intermediate Documents (IDocs) and BAPI/RFC interfaces.

You need to add the authorization object in SAP to process IDocs and SAP BAPI/RFC functions that helps you interact with SAP at run time. You also need access to specific IDoc and SAP BAPI/RFC functions for the transactions that you want to process.

The following table describes the required authorization to process IDocs and SAP BAPI/RFC functions:

Function	Object Name	Authorization
SAP BAPI/RFC	S_RFC	SYST, SDTX, SDIFRUNTIME, RFC_METADATA, RFC1, RFC2, ABAP4_COMMIT_WORK, BAPI_TRANSACTION_COMMIT
IDocs	S_RFC	SYST, SDTX, SDIFRUNTIME, RFC1, RFC2, EDIMEXT

For more information about how to configure SAP user authorization in the SAP system, see [SAP user authorizations](#).

## Configure the sapnwrfc.ini file

SAP uses the communications protocol, Remote Function Call (RFC), to interact with external systems.

You need the `sapnwrfc.ini` file to process SAP IDocs or SAP BAPI/RFC functions that facilitate transfer of data when you read from or write to SAP through the SAP IDoc or SAP BAPI/RFC interface.

Create the `sapnwrfc.ini` file and include the necessary connection information and RFC-specific parameters required by the SAP connection type. You can use a DOS editor or WordPad to create the `sapnwrfc.ini` file, so that you can avoid errors commonly introduced by Notepad. Check out [“Sample sapnwrfc.ini files for connection types” on page 612](#) to know more about the `sapnwrfc.ini` file samples that you can use for different connection types.

After you create the `sapnwrfc.ini` file, you need to place the `sapnwrfc.ini` file in the agent directory. The agent verifies the `sapnwrfc.ini` file, and then use it for the configured connection.

### Placing the `sapnwrfc.ini` file in the agent directory

You can use the Secure Agent or serverless runtime environment to connect to the SAP system as an RFC client, as follows:

- To use a Secure Agent, place the `sapnwrfc.ini` file in the following location:  
`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\`
- To use a serverless runtime environment, place the `sapnwrfc.ini` file in the following location:  
`\data2\home\cldagnt\SystemAgent\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\`

**Note:** Ensure the `deploy_to_main\bin\rdtm` directory exists. If it does not, create it and then place the files.

Restart the agent after placing the file in the required directory.

### Upgrading from an earlier version

If you are upgrading from an earlier version, you do not need to create an `sapnwrfc.ini` file. The Secure Agent copies the `sapnwrfc.ini` file to the `deploy_to_main\bin\rdtm` directory.

### Verifying the `sapnwrfc.ini` file

When you create a connection, the Secure Agent first verifies if an `sapnwrfc.ini` file exists in the directory. If the `sapnwrfc.ini` file exists, the Secure Agent uses the `sapnwrfc.ini` file. Else, an exception occurs.

## Sample `sapnwrfc.ini` files for connection types

You can use the `sapnwrfc.ini` file to configure the following types of connections:

### Connection to an SAP application server

Create this connection to enable communication between an RFC client and an SAP system. Each connection entry specifies one application server and one SAP system.

The following sample shows a connection entry for a specific SAP application server in the `sapnwrfc.ini` file:

```
DEST=sapr3
ASHOST=sapr3
SYSNR=00
```

### Connection for SAP load balancing

Create this connection to enable SAP to create an RFC connection to the application server with the least load at run time. Use this connection when you want to use SAP load balancing.

The following sample shows a connection entry for SAP load balancing in the `sapnwrfc.ini` file:

```
DEST=sapr3
R3NAME=ABV
```



```

MSHOST=infamessageserver.informatica.com
GROUP=INFADEV

```

### Connection to an RFC server program registered at an SAP gateway

Create this connection to connect to an SAP system from which you want to receive outbound IDocs.

The following sample shows a connection entry for an RFC server program registered at an SAP gateway in the `sapnwrfc.ini` file:

```

DEST=sapr346CLSQA
PROGRAM_ID=PID_LSRECEIVE
GWHOST=sapr346c
GWSERV=sapgw00

```

You can configure the following parameters in the `sapnwrfc.ini` file for various connection types:

sapnwrfc.ini Parameter	Description	Applicable Connection Types
DEST	Logical name of the SAP system for the connection. All DEST entries must be unique. You need to have only one DEST entry for each SAP system. For SAP versions 4.6C and later, use up to 32 characters. For earlier versions, use up to eight characters.	Use this parameter for the following types of connections: <ul style="list-style-type: none"> <li>- Connection to a specific SAP application server</li> <li>- Connection to use load balancing</li> <li>- Connection to an RFC server program registered at an SAP gateway</li> </ul>
ASHOST	Host name or IP address of the SAP application. The Secure Agent uses this entry to attach to the application server.	Use this parameter to create a connection to a specific SAP application server.
SYSNR	SAP system number.	Use this parameter to create a connection to a specific SAP application server.
R3NAME	Name of the SAP system.	Use this parameter to create a connection to use SAP load balancing.
MSHOST	Host name of the SAP message server.	Use this parameter to create a connection to use SAP load balancing.
GROUP	Group name of the SAP application server.	Use this parameter to create a connection to use SAP load balancing.
PROGRAM_ID	Program ID. The Program ID must be the same as the Program ID for the logical system that you define in the SAP system to send or receive IDocs.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWHOST	Host name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.

sapnwrfc.ini Parameter	Description	Applicable Connection Types
GWSERV	Server name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
TRACE	Debugs RFC connection-related problems. Set one of the following values based on the level of detail that you want in the trace: <ul style="list-style-type: none"> <li>- 0. Off</li> <li>- 1. Brief</li> <li>- 2. Verbose</li> <li>- 3. Full</li> </ul>	Use this parameter for the following types of connections: <ul style="list-style-type: none"> <li>- Connection to a specific SAP application server</li> <li>- Connection to use load balancing</li> <li>- Connection to an RFC server program registered at an SAP gateway</li> </ul>

The following snippet shows a sample `sapnwrfc.ini` file:

```

/*=====*/
/* Connection to an RFC server program registered at an SAP gateway */
/*=====*/
DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSERV=<service name of the SAP gateway>
*=====*/
/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
/*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

## Define SAP Connector as a logical system in SAP

To receive IDocs from and send IDocs to SAP, you need to define SAP Connector as an external logical system in SAP.

To define SAP Connector as an external logical system, create a single logical system in SAP for IDoc ALE integration with SAP Connector, and then create an RFC destination configured with a tRFC port in the SAP system to communicate with SAP Connector.

To identify the external logical system, you also need to create a partner profile for the logical system that you created.

When you define SAP Connector as a logical system, SAP acknowledges SAP Connector as an external system that can receive outbound IDocs from SAP and send inbound IDocs to SAP.

**Note:** These instructions apply on the SAP version 4.6C. If you use a different version, the instructions may differ. For more information about how to create a logical system in SAP, see the SAP documentation.

## Create a logical system for SAP Connector

You need to define SAP Connector as an external logical system in SAP to uniquely identify SAP Connector as a client within a network.

1. Log in to SAP and go to the SALE transaction.
2. On the **Display IMG** window, expand the tree to navigate to the **Application Link Enabling > Sending and Receiving Systems > Logical Systems > Define Logical System** operation.
3. Click the **IMG - Activity** icon to run the **Define Logical System** operation.  
An informational dialog box appears.
4. Click **Enter**.  
The **Change View Logical Systems** window appears.
5. Click **New Entries**.
6. On the **New Entries** window, enter a name and description for the logical system entry for SAP Connector.

## Create an RFC destination

After you create a logical system, you need to create an RFC destination and program ID for SAP Connector in the SAP system.

1. Go to the SM59 transaction.
2. On the **Display and Maintain RFC Destinations** window, click **Create**.  
The **RFC Destination** window appears.
3. Enter the name of the logical system you created as the RFC destination.
4. To create a TCP/IP connection, enter T as the connection type.
5. Enter a description for the RFC destination.
6. Click **Save**.
7. For Activation Type, click **Registration**.
8. For Program ID, enter the same name as the RFC destination name.  
Use the Program ID as the value for the PROGRAM\_ID parameter in the `sapnwrfc.ini` file.

## Create a tRFC port for the RFC destination

After you create an RFC destination and program ID for SAP Connector, you need to create a tRFC port for the RFC destination you defined in SAP. SAP uses the tRFC port to communicate with SAP Connector.

1. Go to the WE21 transaction.
2. Click **Ports > Transactional RFC**.
3. Click **Create**.  
The **Ports in IDoc Processing** dialog box appears.
4. Click **Generate Port Name** or **Own Port Name** and enter a name.
5. Click **Enter**.
6. Enter a description for the port.
7. Select the IDoc record version type.
8. Enter the name of the RFC destination you created.

## Create a partner profile for SAP Connector

Create a partner profile for the logical system you defined for SAP Connector. When SAP communicates with an external system, it uses the partner profile to identify the external system.

1. Go to the WE20 transaction.
2. Click **Create**.
3. Enter the following properties:

Partner Profile Property	Description
Partner number	Name of the logical system you created for SAP Connector.
Partner type	Partner profile type. Enter LS for logical system for ALE distribution systems.

4. In the **Post-processing** tab, enter the following properties:

Partner Profile Property	Description
Type	User type. Enter US for user.
Agent	The SAP user login name.
Lang	Language code that corresponds to the SAP language. Enter EN for English.

5. In the **Classification** tab, enter the following properties:

Partner Profile Property	Description
Partner class	Enter ALE.
Partner status	Indicates the status of communication with the partner. To communicate with the partner, enter A for active.

## Create outbound and inbound parameters for the partner profile

After you define a partner profile for SAP Connector, you need to create outbound and inbound parameters for the partner profile.

Outbound parameters define the IDoc message type, IDoc basic type, and port number for outbound IDocs. Inbound parameters define the IDoc message type for inbound IDocs.

SAP uses outbound parameters when it sends IDocs to SAP Connector. Create an outbound parameter for each IDoc message type that SAP sends to SAP Connector. SAP uses inbound parameters when it receives IDocs from SAP Connector. Create an inbound parameter for each IDoc message type that SAP receives from SAP Connector.

1. From the **Partner Profiles** window in SAP, click **Create Outbound Parameter**.

2. On the **Partner Profiles: Outbound Parameters** window, enter the following properties:

Outbound Parameter Property	Description
Message Type	The IDoc message type the SAP system sends to SAP Connector.
Receiver Port	The tRFC port number you defined.
IDoc Type	The IDoc basic type of the IDocs the SAP system sends to SAP Connector.

3. Click **Save**.  
The **Packet Size** property appears.
4. Enter a value between 10 and 200 IDocs as the packet size.  
The packet size determines the number of IDocs that SAP sends in one packet to SAP Connector.
5. Click **Enter**.
6. Repeat steps from 1 to 5 to create an outbound parameter for each IDoc message type that SAP sends to SAP Connector.
7. Click **Create Inbound Parameter**.
8. On the **Partner Profiles: Inbound Parameters** window, enter the following properties:

Inbound Parameter Property	Description
Message Type	The IDoc message type the SAP system receives from SAP Connector.
Process Code	The process code. The SAP system uses the process code to call the appropriate function module to process the IDocs it receives.

9. Click **Enter**.
10. Repeat steps 7 through 9 to create an inbound parameter for each IDoc message type that SAP receives from SAP Connector.

## Connect to SAP

Let's configure the SAP connection properties to connect to SAP through the Intermediate Documents (IDocs) or BAPI/RFC interface.

### Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP connection.

Check out ["Prerequisites" on page 609](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 620</a> .

## SAP connection types

You can configure IDoc Reader, IDoc Writer, and SAP RFC/BAPI Interface connection types to access data in SAP through Intermediate Documents (IDocs) and BAPI/RFC interfaces.

Select the required SAP connection type and then configure the connection-specific parameters.

### SAP IDoc Reader connection

To read SAP data through the IDoc interface, select the **IDoc Reader** connection type and configure the connection properties.

The following table describes the basic connection properties for IDoc Reader connection:

Connection property	Description
Destination Entry	The DEST entry of the SAP application server specified in the <code>sapnwrfc.ini</code> file. Verify that the Program ID for this destination entry and the Program ID for the logical system you defined in the SAP system to receive IDocs are the same. For more information about the <code>sapnwrfc.ini</code> file, see <a href="#">"Configure the sapnwrfc.ini file" on page 611</a> .
Code Page	The code page of the SAP application server defined in the connection when you read SAP data through the IDoc interface. Select one of the following code pages from the list: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>

## SAP IDoc Writer connection

To write SAP data through the IDoc interface, select the **IDoc Writer** connection type and configure the connection properties.

The following table describes the basic connection properties for IDoc Writer connection:

Property	Description
User Name	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Connection String	The DEST entry of the SAP application server specified in the <code>sapnwrfc.ini</code> file. For more information about the <code>sapnwrfc.ini</code> file, see <a href="#">"Configure the sapnwrfc.ini file" on page 611</a> .
Code Page	The code page of the SAP application server defined in the connection when you write SAP data through the IDoc interface. Select one of the following code pages from the list: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>

Property	Description
Language Code	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
Client Code	The client number of the SAP application server. Get the required client number from the SAP system to which you want to connect.

## SAP RFC/BAPI Interface connection

To read or write SAP data through the SAP RFC/BAPI interface, select the **SAP RFC/BAPI Interface** connection type and configure the connection properties.

The following table describes the basic connection properties for SAP RFC/BAPI Interface connection:

Property	Description
User Name	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Connection String	The DEST entry of the SAP application server specified in the <code>sapnwrfc.ini</code> file. For more information about the <code>sapnwrfc.ini</code> file, see <a href="#">"Configure the sapnwrfc.ini file" on page 611</a> .
Code Page	The code page of the SAP application server defined in the connection when you read or write SAP data through the SAP RFC/BAPI interface. Select one of the following code pages from the list: <ul style="list-style-type: none"> <li>- MS Windows Latin 1. Select for ISO 8859-1 Western European data.</li> <li>- UTF-8. Select for Unicode data.</li> <li>- Shift-JIS. Select for double-byte character data.</li> <li>- ISO 8859-15 Latin 9 (Western European).</li> <li>- ISO 8859-2 Eastern European.</li> <li>- ISO 8859-3 Southeast European.</li> <li>- ISO 8859-5 Cyrillic.</li> <li>- ISO 8859-9 Latin 5 (Turkish).</li> <li>- IBM EBCDIC International Latin-1.</li> </ul>
Language Code	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
Client Code	The client number of the SAP server. Get the required client number from the SAP system to which you want to connect.

## Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS or Azure to connect to the SAP system when you configure an SAP connection on Linux.

You can't use the serverless runtime environment if you want to use SAP Secure Network Communication (SNC) Protocol.



Before you configure an SAP connection using the serverless runtime environment, perform the following tasks:

- Add the SAP libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the .yml serverless configuration file.
- Configure the JAVA\_LIBS property for the serverless runtime environment on Linux.

#### Add the SAP libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to configure an SAP connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the SAP libraries in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/sap

#### Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment, and to copy the SAP libraries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        nwrfdc:
          - fileCopy:
              sourcePath: sap/nwrfdc/<rfc_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfdc/<sapnwrfdc_filename>
```

where the source path is the directory path of the library files in AWS or Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as serverlessUserAgentConfig.yml in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the libraries are copied from the AWS or Azure location to the serverless agent directory.

#### Configure the JAVA\_LIBS property for the serverless runtime environment

Perform the following steps in Administrator to configure the JAVA\_LIBS property for the serverless runtime environment on Linux:

1. Log in to Informatica Intelligent Cloud Services.
2. Select **Administrator > Serverless Environments**.
3. On the **Serverless Environments** tab, expand the Actions menu for the required serverless runtime environment, and then select **Edit**.
4. On the **Runtime Configuration Properties** tab, select **Data Integration Server** as the service and **Tomcat\_JRE** as the type.
5. Click **Add Property**.
6. Enter JAVA\_LIBS in the **Name** field and set the following value:  
../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javaliib/sap/sap-adapter-common.jar
7. Click **Save**.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 191

# SAP ADSO Writer connection properties

When you set up an **SAP ADSO Writer** connection, configure the connection properties.

The following table describes the SAP ADSO Writer connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP ADSO Writer
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment.
SAP Server Connection Type	The SAP server connection type to use. Select from the following options: <ul style="list-style-type: none"><li>- <b>Application Server Connection.</b> Connect to an SAP Application Server using the SAP user name and password.</li><li>- <b>Application Server SNC Connection.</b> Connect to an SAP Application Server using the secured network connection:<ul style="list-style-type: none"><li>- With X.509 Certificate. You do not need to specify the SAP user name and password explicitly. You must provide the path of the x.509 certificate file.</li><li>- Without X.509 Certificate. You must provide the SAP user name.</li></ul></li><li>- <b>Load Balancing Server Connection.</b> Connect to an SAP Application Server with the least load at run time.</li><li>- <b>Load Balancing Server SNC Connection.</b> Connect to an SAP Application Server using SNC with the least load at run time.</li></ul> <b>Note:</b> Before you use an SNC connection, you must verify that SNC is configured both on the SAP Server and the machine where the Secure Agent runs.

The following table describes the properties that must configure when you select **Application Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SAP Username	The SAP user name with the appropriate user authorization.
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SAP Username	The SAP user name with the appropriate user authorization.

Connection property	Description
SAP Password	The SAP password.
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:            &lt;Informatica Secure Agent installation directory&gt;\apps            \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</p> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:            &lt;Informatica Secure Agent installation directory&gt;\apps            \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</p>

The following table describes the properties that must configure when you select **Application Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Application Server	The host name of the SAP Application Server.
SAP System Number	The system number of the SAP Server to connect.
SNC My Name	Optional. The Informatica client Personal Security Environment (PSE) or certificate name. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name. Default length is 256.
SNC Quality of Protection (QoP)	<p>Specifies the SAP PSE or certificate name.</p> <p>You can select from the following options:</p> <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> <p>Default is 3 - <i>Apply privacy protection (integrity and authentication)</i>.</p>
SAP Cryptographic Library Path	The path to the cryptographic library. Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.

Connection property	Description
X509 Certificate Path or SAP Username	<p>The path to the X509 certificate file.</p> <p>If you select to use the X509 certificate, specify the path to the X509 certificate file with .crt extension. You do not need to specify the SAP user name and password.</p> <p>If you do not want to use the X509 certificate, specify the SAP username for which SNC is configured in SAP Server.</p>
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system.</p> <p>For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

The following table describes the properties that must configure when you select **Load Balancing Server SNC Connection** as the connection type:

Connection property	Description
SAP Client Number	The client number of the SAP Server.
SAP Language	Language code that corresponds to the SAP language.
SAP Message Server	The IP address or the host name of the SAP Message Server.
SAP System ID	The system ID of the SAP Message Server.
SAP Group	The login group name, for example, PUBLIC.
SNC My Name	Optional. The Informatica client PSE or certificate name generated on the Secure Agent machine. Default length is 256.
SNC Partner Name	The Informatica client PSE or certificate name generated on the SAP Server. Default length is 256.
SNC Quality of Protection (QoP)	<p>Specifies the SAP PSE or certificate name.</p> <p>You can select from the following options:</p> <ul style="list-style-type: none"> <li>- 1 - Apply authentication only.</li> <li>- 2 - Apply integrity protection (authentication).</li> <li>- 3 - Apply privacy protection (integrity and authentication).</li> <li>- 8 - Apply the default protection.</li> <li>- 9 - Apply the maximum protection.</li> </ul> <p>Default is 3 - <i>Apply privacy protection (integrity and authentication)</i>.</p>
SAP Cryptographic Library Path	<p>The path to the cryptographic library.</p> <p>Specify <code>sapcrypto.dll</code> for Windows or <code>libsapcrypto.so</code> for Linux.</p>

Connection property	Description
Use X509 Certificate	Specifies the quality of protection. Select to use X509 Certificate based SNC connection.
X509 Certificate Path or SAP Username	<p>The path to the X509 certificate file.</p> <p>If you select to use the X509 certificate, specify the path to the X509 certificate file with .crt extension. You do not need to specify the SAP user name and password.</p> <p>If you do not want to use the X509 certificate, specify the SAP user name for which SNC is configured in the SAP Server.</p>
Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system. For example, to generate SAP JCo and SAP CPIC trace, specify the following properties:</p> <pre>jco.client.trace="1"; jco.client.cpic_trace="3";</pre> <p>During the runtime, the JCo and CPIC traces file are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the CPIC traces are generated in the tomcat.out files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>

# CHAPTER 192

## SAP BAPI connection properties

Create an SAP BAPI connection to connect to the SAP system and access a specific BAPI function.

### Prerequisites

Before you use an SAP BAPI connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process SAP BAPI functions, you also need to verify if the required licenses are enabled for the SAP system.

### Download and configure the SAP libraries

To use an SAP BAPI connection when you connect to the SAP system and access a specific BAPI function, you need to download and configure the SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.  
**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).
2. Download the latest version of the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs.

Operating System	SAP JCo Libraries
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. Copy the JCo libraries to the following directory:  
<Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext\deploy\_to\_main\bin\rdtm-extra\tpl\sap  
Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.
4. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.

- b. Click **Runtime Environments** to access the **Runtime Environments** page.
- c. To the left of the agent name, click **Edit Secure Agent**.
- d. From the **Service** list, select **Data Integration Server**.
- e. From the **Type** list, select **Tomcat JRE**.
- f. Enter the JAVA\_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

**System Configuration Details**

Service:

Type:

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar../bin/rdtm/javalib/sap/sap-adc

- g. Click **Save**.
  - h. Repeat steps 2 through 4 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

## Configure SAP user authorization

Configure the SAP user account in the SAP system to process SAP BAPI functions.

For more information about how to configure SAP user authorization in the SAP system, see [SAP user authorizations](#).

The following table describes the required authorization to process SAP BAPI functions:

Read Object Name	Authorization
S_RFC	SYST, SDTX, SDIFRUNTIME, RFC1, RFC2

## Connect to SAP BAPI

Let's configure the SAP BAPI connection properties to connect to SAP and process SAP BAPI functions.



## Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP BAPI connection.

Check out ["Prerequisites" on page 627](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP Bapi
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 631</a> .
Authentication	The authentication type to access the SAP system and process SAP BAPI functions. Select the <b>BAPI Connection</b> authentication type and then configure the authentication-specific parameters.
Username	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Host Name	The host name or IP address of the SAP server to which you want to connect.
Client	The client number of the SAP server in the SAP system to which you want to connect. Get the required client number from the SAP system to which you want to connect.

Property	Description
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
System Number	The system number of the SAP server. Get the required system number from the SAP system to which you want to connect.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. See the following examples where you can use this field to configure additional parameters for the connection:</p> <ul style="list-style-type: none"> <li>- To create a load balancing connection, define the additional arguments listed in the following sample:  <code>GROUP=interfaces MSHOST=&lt;Message server hostname&gt; R3NAME=&lt;System ID or name of SAP system&gt;</code>  SAP infers the connection type based on the parameters that you specify. For example, if you define the GROUP, MSHOST, and R3NAME parameters, SAP infers the connection type as a load balancing connection. The GROUP parameter defines the group name of the SAP application server. The MSHOST parameter defines the host name of the SAP message server. The R3NAME parameter defines the system ID or name of the SAP system.</li> <li>- To commit data to the SAP system with each BAPI/RFC call, define the <code>DOCOMMIT=true</code> parameter.</li> <li>- To create a connection with the Secure Network Communication (SNC) protocol, define the required additional parameters.  For more information, see <a href="#">How to configure the SAP Secure Network Communication protocol</a> Informatica How-To Library article.</li> </ul> <p>If you specify a property both in the dedicated connection field and in the <b>SAP Additional Parameters</b> field, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.  For more information about SAP parameters, see the SAP documentation.</p>
Jco Trace	<p>Determines whether to track the JCo calls that the SAP system makes.  Default is disable. By default, SAP doesn't store information about the JCo calls in a trace file.  If you enable JCo trace, you can access the JCo trace file from the following directory:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;latest_version&gt;\ICS\main\bin\rdtm</pre>

## Configure SAP BAPI Connector as a business service

Use an SAP BAPI connection in the Web Services transformation in a mapping or mapping task, and then use SAP BAPI Connector as a business service.

For more information, see [How to configure SAP BAPI Connector as a business service](#) Informatica How-To Library article.

# Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS or Azure to connect to the SAP system when you configure an SAP BAPI connection on Linux.

You can't create an SNC connection when you use the serverless runtime environment.

Before you configure an SAP BAPI connection using the serverless runtime environment, perform the following tasks:

- Add the libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the .yml serverless configuration file.
- Configure the JAVA\_LIBS property for the serverless runtime environment on Linux.

## Add the libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to configure an SAP BAPI connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the libraries in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/sap

## Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment, and to copy the libraries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jcos:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
```

where the source path is the directory path of the library files in AWS or Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the libraries are copied from the AWS or Azure location to the serverless agent directory.

## Configure the JAVA\_LIBS property for the serverless runtime environment

Perform the following steps in Administrator to configure the JAVA\_LIBS and JVMClassPath properties for the serverless runtime environment on Linux:

1. Log in to Informatica Intelligent Cloud Services.
2. Select **Administrator > Serverless Environments**.
3. On the **Serverless Environments** tab, expand the Actions menu for the required serverless runtime environment, and then select **Edit**.
4. On the **Runtime Configuration Properties** tab, select **Data Integration Server** as the service and **Tomcat\_JRE** as the type.

5. Click **Add Property**.
6. Enter JAVA\_LIBS in the **Name** field and set the following value:  
`../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar`
7. Click **Save**.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 193

# SAP BW Connector connection properties

Create an SAP BW Connector connection to securely read data from SAP BW objects.

You can use an SAP BW connection to read data from the following objects:

- InfoCubes
- InfoSets
- MultiProviders
- DataStore

## Prerequisites

Before you use an SAP BW connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process SAP BW data, you also need to verify if the required licenses are enabled for the SAP system.

## Download and configure the SAP libraries

To read data from SAP BW objects, you need to download and configure the SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.

**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).

2. Download the latest version of the 64-bit SAP JCo libraries based on the operating system of the machine on which the Secure Agent runs.

Operating System	SAP JCo Libraries
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. Copy the JCo libraries to the following directory:  
 <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext\deploy\_to\_main\bin\rdtm-extra\tpl\sap  
 Create the deploy\_to\_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.
4. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.
  - b. Click **Runtime Environments** to access the **Runtime Environments** page.
  - c. To the left of the agent name, click **Edit Secure Agent**.
  - d. From the **Service** list, select **Data Integration Server**.
  - e. From the **Type** list, select **Tomcat JRE**.
  - f. Enter the JAVA\_LIBS value based on the operating system of the machine on which the Secure Agent runs.

Operating System	Value
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

System Configuration Details Reset All

Service:

Type:

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

- g. Click **Save**.
5. After you save the JAVA\_LIBS value, configure the JVMClassPath property for the Secure Agent.
  - a. From the **Service** list, select **Data Integration Server**.
  - b. From the **Type** list, select **DTM**.
  - c. Enter the JVMClassPath value based on the operating system of the machine on which the Secure Agent runs.

Operating System	Value
Windows	pmserversdk.jar;..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	pmserversdk.jar;../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

System Configuration Details Reset All

Service:

Type:

Type	Name	Value
DTM	JVMClassPath	pmserversdk.jar:../bin/rdm-extra/tp/sap/sapjco3.jar:../bin/rdm/

- d. Click **Save**.
  - e. Repeat steps 2 through 5 on every machine where you installed the Secure Agent.
6. Restart the Secure Agent.

## Configure SAP user authorization

Configure SAP user authorization in the SAP system to access and read from SAP BW objects such as InfoCubes, InfoSets, MultiProviders, and DataStore objects.

The following table lists the authorization objects, fields, and values required to configure user permissions to access and read data from SAP BW:

Authorization Object	Field	Value
S_RFC	RFC_TYPE	FUNC, FUGR
	RFC_NAME	/INFADI/BWRDR, /INFADI/ZTEST_COMMUNICATION, BAPI_CUBE_GETLIST, DDIF_FIELDINFO_GET, BAPI_IOBJ_GETDETAIL, RFCPING, RFC_GET_FUNCTION_INTERFACE, RSAB, SYST
	ACTVT	16
S_BTCH_JOB	JOBACTION	RELE
	JOBGROUP	*
S_RS_ADMWB	RSADMWBOBJ	Provide the Administrator Workbench Object name from which you want to read data. For more information about Administrator Workbench Objects, see the SAP documentation.
	ACTVT	3
S_RS_ICUBE	RSINFOAREA	Provide the InfoArea names that you want to access. For more information about InfoAreas, see the SAP documentation.
	RSINFOCUBE	Provide the InfoCube object names that you want to access. For more information about InfoCubes, see the SAP documentation.
	RSIRSICUBE OBJ	DEFINITION, DATA, UPDATERULE
	ACTVT	3

You can also add the following authorization objects to configure user permissions to access and read data from SAP BW:

- The S\_RFC authorization object with the BAPI\_ODSO\_GETLIST and BAPI\_ISET\_GETLIST optional RFC objects.
- The S\_RS\_ISET and S\_RS\_ODSO authorization objects with the activity value ACTVT=3.

For more information about these objects and how to use them, see [SAP user authorizations](#).

## Install transport files for SAP BW

To read data from SAP BW objects from a Unicode SAP system, install the SAP BW transport files from the Secure Agent directory to the SAP system. The transport files are applicable for SAP NetWeaver BW version 7.x.

### Prerequisites to install the transport files

Before you install the SAP BW transports, make sure to perform the following prerequisite tasks:

- Ensure that the transport files you install on the SAP machines are the latest. Get the latest transport files from the following directory:  
`<Informatica Secure Agent installation directory>\downloads\package-bwreader.<Latest version>\package\rdtm\sap-transport\SAPBWReader`
- Before you install the transports on your production system, install and test the transports in a development system.

### Installing transport files

To install the SAP BW transport files, perform the following tasks:

1. Locate the transport files in the following directory on the Secure Agent machine:  
`<Informatica Secure Agent installation directory>\downloads\package-bwreader.<Latest version>\package\rdtm\sap-transport\SAPBWReader`
2. Copy the cofile transport file to the `Cofile` directory in the SAP transport management directory on each SAP machine that you want to access.  
The cofile transport file uses the following naming convention: `RUN_BWRDR_K<number>.g00`
3. Remove "RUN\_BWRDR\_" from the file name to rename the cofile. For example, for a cofile transport file named `RUN_BWRDR_K900723.g00`, rename the file to `K900723.g00`.
4. Copy the data transport file to the `Data` directory in the SAP transport management directory on each SAP machine that you want to access.  
The data transport file uses the following naming convention: `RUN_BWRDR_R<number>.g00`
5. Remove "RUN\_BWRDR\_" from the file name to rename the file.  
For example, for a data transport file named `RUN_BWRDR_R900723.g00`, rename the file to `R900723.g00`.
6. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.
7. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.  
The request number inverts the order of the renamed cofile as follows: `g00K<number>`  
For example, for a cofile transport file renamed as `K900723.g00`, enter the request number as `g00K900723`.
8. In the Request area of the import queue, select the transport request number that you added, and click **Import**.



# Connect to SAP BW

Let's configure the SAP BW connection properties to connect to SAP BW.

## Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP BW connection.

Check out ["Prerequisites" on page 633](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP BW Connector
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
Username	The user name with the appropriate user authorization to connect to the SAP BW account.
Password	The password to connect to the SAP BW account.

## Connection types

You can configure application and load balancing connection types to connect to SAP BW. Select the required connection type and then configure the connection-specific parameters.

### Application connection

Application connection is the default type which requires your SAP account name, password, client number, host name, system number, and language code.

The following table describes the basic connection properties for an application connection:

Connection property	Description
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect.
Client	The client number of the SAP BW server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

### Advanced settings

The following table describes the advanced connection properties for an application connection:

Property	Description
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8. By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0.</p> <p>For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- <b>Design time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- <b>Run-time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW data. You can enter multiple JCo connection parameters, separated by a semicolon, in the following format: &lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;...</p> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters:</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
Port Range	<p>HTTP port range. The SAP BW connection uses the specified port numbers to connect to SAP BW using the HTTP protocol. Default range is 10000-65535. Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>
Use HTTPS	<p>Connects to SAP through HTTPS protocol. To connect to SAP through HTTPS, verify that your administrator has configured HTTPS for the Secure Agent machine and the SAP system. For more information about how to connect to SAP through HTTPS, see <a href="#">"Configure HTTPS to connect to SAP" on page 641</a>.</p>

Property	Description
Keystore location	The path and file name of the keystore file to connect to SAP. Enter both the path and file name in the following format: <Directory>/<Keystore file name>.jks
Keystore password	The password to access the keystore file.
Private Key password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>MSHOST= &lt;Message server hostname&gt; GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about SNC parameters, see <a href="#">How to configure the SAP Secure Network Communication protocol</a> Informatica How-To Library article.</p> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

## Load balancing connection

Create a load balancing connection when you want to connect to the SAP BW server with the least load at run time.

When you create a load balancing connection, in addition to all the properties listed in the **Connection Details** section, you also need to enter the message host name, R3 name/SysID, and group values in the **Advanced Settings** section.

The following table describes the basic connection properties for a load balancing connection:

Connection property	Description
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect.

Connection property	Description
Client	The client number of the SAP BW server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

## Advanced settings

The following table describes the advanced connection properties for a load balancing connection:

Property	Description
Message host name	Required. The host name of the SAP message server to which you want to connect when you use a load balancing connection.
R3 name/ SysID	Required. The system ID of the SAP message server to which you want to connect when you use a load balancing connection.
Group	Required. The name of the SAP logon group through which you want to connect when you use a load balancing connection.
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8. By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0.</p> <p>For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- Design time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- Run-time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW data. You can enter multiple JCo connection parameters, separated by a semicolon, in the following format:</p> <pre>&lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;...</pre> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters:</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
Port Range	<p>HTTP port range. The SAP BW connection uses the specified port numbers to connect to SAP BW using the HTTP protocol. Default range is 10000-65535. Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>

Property	Description
Use HTTPS	<p>Connects to SAP through HTTPS protocol.</p> <p>To connect to SAP through HTTPS, verify that your administrator has configured HTTPS for the Secure Agent machine and the SAP system.</p> <p>For more information about how to connect to SAP through HTTPS, see <a href="#">“Configure HTTPS to connect to SAP” on page 641</a>.</p>
Keystore location	<p>The path and file name of the keystore file to connect to SAP.</p> <p>Enter both the path and file name in the following format:</p> <pre>&lt;Directory&gt;/&lt;Keystore file name&gt;.jks</pre>
Keystore password	The password to access the keystore file.
Private Key password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>MSHOST= &lt;Message server hostname&gt; GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/ Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/ sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about SNC parameters, see <a href="#">How to configure the SAP Secure Network Communication protocol</a> Informatica How-To Library article.</p> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

## Configure HTTPS to connect to SAP

To connect to SAP through HTTPS and read from SAP BW sources, ensure that an OpenSSL certificate is available on both the Secure Agent machine and the SAP system.

Create an OpenSSL certificate in the Secure Agent machine. Then, import the created certificate in the PSE format to the SAP system truststore.

Additionally, to enable HTTPS in an SAP BW connection, you need to specify the generated keystore password and private key password of the keystore file both in the SAP BW connection properties and in the SAP system.

## Create an OpenSSL certificate

Before you create an OpenSSL certificate, you need to perform the prerequisite tasks.

- Download and install OpenSSL on the Secure Agent machine.
- Based on the operating system of the machine that hosts the Secure Agent and the SAP system, download the latest available patch of the SAPGENPSE Cryptography tool from the SAP Service Marketplace.  
By default, the SAPGENPSE files are extracted to the `nt-x86_64` directory.
- Configure the following SAP parameters: `icm/server_port`, `ssl/ssl_lib`, `sec/libsapsecu`, `ssf/ssfapi_lib`, `ssf/name`, `icm/HTTPS/verify_client`, `ssl/client_pse`, and `wdisp/ssl_encrypt`.  
For more information, see the SAP documentation.

To create a self-signed certificate using OpenSSL, perform the following tasks:

1. From the command line, set the `OPENSSL_CONF` variable to the absolute path to the `openssl.cfg` file.  
For example, run the following command: `set OPENSSL_CONF= C:\OpenSSL-Win64\bin\openssl.cfg`
2. Navigate to the `<openssl installation directory>\bin` directory.
3. To generate a 2048-bit RSA private key, run the following command:  
`openssl.exe req -new -newkey rsa:2048 -sha1 -keyout <RSAkey File_Name>.key -out <RSAkey File_Name>.csr`
4. When prompted, enter the following values:
  - Private key password (PEM pass phrase). Enter a phrase that you want to use to encrypt the secret key. Re-enter the password for verification.  
**Important:** Make a note of this PEM password. You need to keep this password handy while creating a self-signed key and PKCS#12 certificate.
  - Two-letter code for country name.
  - State or province name.
  - Locality name.
  - Organization name
  - Organization unit name.
  - Common name (CN). Mandatory.  
**Important:** Enter the fully qualified host name of the machine that hosts the Secure Agent.
  - Email address.
5. Optionally, enter the following attributes that you want to pass along with the certificate request:
  - Challenge password.
  - Optional company name.

A RSA private key of 2048-bit size is created. The `<RSAkey File_Name>.key` and `<RSAkey File_Name>.csr` files are generated in the specified directory.
6. To generate a self-signed key using the RSA private key, run the following command:  
`openssl x509 -req -days 11499 -in <RSAkey File_Name>.csr -signkey <RSAkey File_Name>.key -out <Certificate File_Name>.crt`
7. When prompted, enter the PEM pass phrase for the RSA private key.  
The `<Certificate File_Name>.crt` file is generated in the specified directory.

8. To concatenate the contents of the `<Certificate File_Name>.cert` file and the `<RSAkey File_Name>.key` file to a `.pem` file, perform the following tasks:
  - a. Open the `<Certificate File_Name>.cert` file and the `<RSAkey File_Name>.key` files in a Text editor.
  - b. Create a file and save it as `<PEM File_Name>.pem`.
  - c. Copy the contents of the `<Certificate File_Name>.cert` file and paste it in the `.pem` file.
  - d. Copy the contents of the `<RSAKey_Name>.key` file and append it to the existing contents of the `.pem` file.
  - e. Save the `<PEM file name>.pem` file.
9. To create a PKCS#12 certificate, run the following command from the command line:
 

```
openssl pkcs12 -export -in <PEM File_Name>.pem -out <P12 File_Name>.p12 -name "domain name"
```
10. When prompted, enter the following details:
  - The PEM pass phrase for the `.pem` file.
  - An export password for the P12 file. Re-enter the password for verification.
 

**Important:** Make a note of this export password for the P12 file. You need to keep this password handy while creating a Java keystore file to connect to SAP through HTTPS.

The `<P12 File_Name>.p12` file is generated in the specified directory.
11. To create a Java keystore file, enter the following command:
 

```
keytool -v -importkeystore -srckeystore <P12 File_Name>.p12 -srcstoretype PKCS12 -destkeystore <JKS File_Name>.jks -deststoretype JKS -srcalias "source alias" -destalias "destination alias"
```
12. When prompted, enter the following details:
  - Password for the destination keystore, the JKS file.
 

**Important:** Make a note of this password. You need to keep this password handy while creating an SAP BW connection.
  - Password for the source keystore, the P12 file. Enter the Export password for the P12 file.
 

The `<JKS File_Name>.jks` file is generated in the specified directory.

While enabling HTTPS in an SAP BW connection, specify the name and location of this keystore file. You also need to specify the destination keystore password as the Keystore Password and the source keystore password as the Private Key Password both in the SAP BW connection properties and in the SAP system.

## Convert an OpenSSL certificate to PSE format

After you create an OpenSSL certificate, you need to convert the OpenSSL certificate to PSE format using the SAPGENPSE tool.

1. From the command line, navigate to the `<SAPGENPSE Extraction Directory>` directory.
2. To generate a PSE file, run the following command:
 

```
sapgenpse import_p12 -p <PSE_Directory>\<PSE File_Name>.pse <P12 Certificate_Directory>\<P12 File_Name>.p12
```
3. When prompted, enter the following details:
  - Password for the P12 file. Enter the Export password for the P12 file.

- Personal identification number (PIN) to protect the PSE file. Re-enter the PIN for verification.

The <PSE File\_Name>.pse file is generated in the specified directory.

4. To generate the certificate based on the PSE format, run the following command:

```
sapgenpse export_own_cert -p <PSE File_Directory>\<PSE File_Name>.pse -o  
<Certificate_Name>.crt
```

5. When prompted, enter the PSE PIN number.

The <Certificate\_Name>.crt file is generated in the specified directory. Import this certificate file to the SAP system trust store.

## Enable the HTTPS service on the SAP system

To configure HTTPS to connect to an SAP system, you need to enable the HTTPS service from the transaction code SAP ICM Monitor (SMICM) in the SAP system.

For more information about how to enable the HTTPS service on the SAP system, see the SAP documentation.

## Import the certificate to the SAP system truststore

You need to import the certificate in PSE format to the SAP system trust store to connect to SAP through HTTPS.

1. Log in to SAP and go to the STRUST transaction.
2. Select SSL Client (Standard) and specify the password.
3. In the **Import Certificate** dialog, select Base64 format as the certificate file format.
4. Click the **Import** icon, and select the <Certificate\_Name>.crt file in PSE format.

**Note:** If a user is on a different SAP network, you might need to add a DNS entry of the agent host on the SAP application server.

5. Click **Add to Certificate List**.
6. Restart the Internet Communication Manager.



# CHAPTER 194

## SAP BW BEx Query connection properties

Create an SAP BW BEx Query connection to securely read SAP BW BEx queries from SAP BW.

### Prerequisites

Before you use an SAP BW BEx Query connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process SAP BW BEx Query data, you also need to verify if the required licenses are enabled for the SAP system.

### Download and configure the SAP libraries

To read data from SAP BW BEx Query, you need to download and configure the SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.

**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).

2. Download the latest version of the 64-bit SAP JCo libraries based on the operating system of the machine on which the Secure Agent runs.

Operating System	SAP JCo Libraries
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. Copy the JCo libraries to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.

4. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.
  - b. Click **Runtime Environments** to access the **Runtime Environments** page.
  - c. To the left of the agent name, click **Edit Secure Agent**.
  - d. From the **Service** list, select **Data Integration Server**.
  - e. From the **Type** list, select **Tomcat JRE**.
  - f. Enter the JAVA\_LIBS value based on the operating system of the machine on which the Secure Agent runs.

Operating System	Value
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

**System Configuration Details**

Service:  ▼

Type:  ▼

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-ada

- g. Click **Save**.
  - h. Repeat steps 2 through 4 on every machine where you installed the Secure Agent.
5. Restart the Secure Agent.

## Configure SAP user authorization

Configure the SAP user account in the SAP system to process SAP BW BEx Query data.

The following table lists the objects and authorization required to configure user permissions to access and read data from SAP BW BEx Query:

Read Object Name	Authorization
S_RFC	RFC1, RFC_METADATA, RFC_METADATA_GET, RSAB, RSOB, RS_UNIFICATION, SDTX, SUGU, SU_USER, SYST
S_RS_COMP	ACTVT=3 (DISPLAY)
S_RS_COMP1	ACTVT=3 (DISPLAY)
S_RS_ICUBE	ACTVT=3 (DISPLAY)

For more information about these objects and how to use them, see [SAP user authorizations](#).

# Connect to SAP BW BEx Query

Let's configure the SAP BW BEx Query connection properties to connect to SAP BW and read data from SAP BW BEx Query.

## Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP BW BEx Query connection.

Check out ["Prerequisites" on page 645](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP BW BEx Query
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 651</a> .
Authentication	The authentication type to access SAP BW and read SAP BW BEx queries. Select the <b>SAP</b> authentication type and then configure the authentication-specific parameters.
Username	The user name with the appropriate user authorization to connect to the SAP BW account.
Password	The password to connect to the SAP BW account.

## Connection types

You can configure application and load balancing connection types to connect to SAP BW and read data from SAP BW BEx Query.

Select the required connection type and then configure the connection-specific parameters.

### Application connection

Application connection is the default type which requires your SAP account name, password, client number, host name, system number, and language code.

The following table describes the basic connection properties for an application connection:

Connection property	Description
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect.
Client	The client number of the SAP BW server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

## Advanced settings

The following table describes the advanced connection properties for an application connection:

Property	Description
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8.</p> <p>By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0.</p> <p>For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- <b>Design time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- <b>Run-time information:</b> &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW BEx queries from SAP BW.</p> <p>You can enter multiple JCo connection parameters, separated by a semicolon, in the following format: &lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;....</p> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters: SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</p>
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>GROUP=interfaces ASHOST=&lt;Application server hostname&gt; SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt; SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt; SNC_LIB=&lt;Secure Agent installation directory&gt;/apps/server/bin/ &lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt; TRACE=2</pre> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

## Load balancing connection

Create a load balancing connection when you want to connect to the SAP BW server with the least load at run time.

When you create a load balancing connection, in addition to all the properties listed in the **Connection Details** section, you also need to enter the message host name, R3 name/SysID, and group values in the **Advanced Settings** section.

The following table describes the basic connection properties for a load balancing connection:

Connection property	Description
Username	The user name with the appropriate user authorization to connect to the SAP BW account.
Password	The password to connect to the SAP BW account.
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect.
Client	The client number of the SAP BW server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

### Advanced settings

The following table describes the advanced connection properties for a load balancing connection:

Property	Description
Message host name	Required. The host name of the SAP message server to which you want to connect when you use a load balancing connection.
R3 name/ SysID	Required. The system ID of the SAP message server to which you want to connect when you use a load balancing connection.
Group	Required. The name of the SAP logon group through which you want to connect when you use a load balancing connection.
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8. By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0.</p> <p>For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- Design time information: &lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- Run-time information: &lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>

Property	Description
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW BEx queries from SAP BW.</p> <p>You can enter multiple JCo connection parameters, separated by a semicolon, in the following format:            &lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;....</p> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters:</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>GROUP=interfaces ASHOST=&lt;Application server hostname&gt; SYSNR=20 SNC_MODE=1 SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt; SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt; SNC_LIB=&lt;Secure Agent installation directory&gt;/apps/server/bin/ &lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt; TRACE=2</pre> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

## Use the serverless runtime environment

You can use a serverless runtime environment hosted on Azure to connect to the SAP system when you configure an SAP BW BEx Query connection on Linux.

You can't use the serverless runtime environment if you want to use SAP Secure Network Communication (SNC) Protocol.

Before you configure an SAP BW BEx Query connection using the serverless runtime environment, perform the following tasks:

- Add the SAP libraries in the Azure container in your Azure account.
- Configure the .yaml serverless configuration file.
- Configure the JAVA\_LIBS property for the serverless runtime environment on Linux.

### Add the SAP libraries in the Azure container in your Azure account

Perform the following steps to configure an SAP BW BEx Query connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in Azure: <Supplementary file location>/serverless\_agent\_config
2. Add the SAP libraries in the Azure container in the following location in your Azure account: <Supplementary file location>/serverless\_agent\_config/sap

### Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment, and to copy the SAP libraries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        nwrfdc:
          - fileCopy:
              sourcePath: sap/nwrfdc/<rfc_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfdc/<sapnwrfdc_filename>
```

where the source path is the directory path of the SAP library files in Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as serverlessUserAgentConfig.yml in the following Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the SAP libraries are copied from the Azure location to the serverless agent directory.

### Configure the JAVA\_LIBS property for the serverless runtime environment

Perform the following steps in Administrator to configure the JAVA\_LIBS property for the serverless runtime environment on Linux:

1. Log in to Informatica Intelligent Cloud Services.
2. Select **Administrator > Serverless Environments**.
3. On the **Serverless Environments** tab, expand the Actions menu for the required serverless runtime environment, and then select **Edit**.
4. On the **Runtime Configuration Properties** tab, select **Data Integration Server** as the service and **Tomcat\_JRE** as the type.
5. Click **Add Property**.
6. Enter JAVA\_LIBS in the **Name** field and set the following value:  
../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar
7. Click **Save**.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.



## CHAPTER 195

# SAP HANA CDC Connection Properties

When you configure a SAP HANA CDC connection, you must set the connection properties.

The following table describes SAP HANA CDC connection properties:

Property	Description
Connection Name	<p>A name for the SAP HANA CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code></p> <p>Spaces at the beginning or end of the name are trimmed and are not saved as part of the name.</p> <p>Maximum length is 100 characters. Connection names are not case sensitive.</p>
Description	<p>Description of the SAP HANA CDC connection. Maximum length is 4000 characters.</p>
Type	<p>Type of connection. For SAP HANA CDC, the type must be <b>SAP HANA CDC</b>.</p>
Runtime Environment	<p>Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.</p>
Listener Location	<p>Host name or IP address of the system where the PowerExchange Listener that processes PWX CDC Reader requests for SAP HANA change data and the PowerExchange Logger for LUW run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:</p> <pre>host_name:port_number</pre> <p>For example:</p> <pre>HANADB1:1467</pre>
User Name	<p>A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. If you enabled PowerExchange LDAP user authentication, the user name is an enterprise user name. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i>.</p>
Password	<p>Password that is associated with the user name that is specified in the <b>User Name</b> property.</p>

Property	Description
Collection Name	SAP HANA instance name that is specified in the <b>Database</b> field of the registration group that contains capture registrations for the SAP HANA source tables. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None.</b> Do not use encryption.</li> <li>- <b>AES 128-bit.</b> Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit.</b> Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit.</b> Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Enter the host name or IP address of the system that contains the extraction maps. Also include the port number. This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  SAPHANA2B:25100  The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.

Property	Description
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The event table must be a SAP HANA table on the CDC source system.
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="662 871 1117 898">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="662 1241 1419 1346" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 196

# SAP HANA connection properties

Create an SAP HANA connection to connect to and read data from SAP HANA. You can use an SAP HANA connection in mappings and mapping tasks.

## Prerequisites

Before you create an SAP HANA connection to read from or write to SAP HANA databases, ensure to complete certain prerequisites.

An SAP HANA administrator must perform the following tasks on a Windows or Linux machine where the Secure Agent is installed:

1. Install the 64-bit HANA ODBC driver.
2. Append an entry to the `odbcinst.ini` file on Linux.
3. Download and configure the `ngdbc.jar` file.

After the administrator completes the configurations, you can set up and use an SAP HANA connection in mappings and mapping tasks.

## Adding entries in Linux operating system

To use SAP HANA Connector on a Secure Agent machine on Linux, install the 64-bit HANA ODBC on this machine. Additionally, you need to add the HANA driver details to the `odbcinst.ini` file.

The `odbcinst.ini` file is available in Secure Agent installation directory.

Append the following HANA driver details to the `odbcinst.ini` file in Linux to connect to the HANA database as shown in the following example:

```
[HDBODBC]
Driver=/usr/sap/hdbclient/libodbcHDB.so
Description=HANA Driver
Setup=/usr/sap/hdbclient/libodbcHDB.so
CPOutput=0
```

**Note:** In the example, the following path is the location for the driver installation: `/usr/sap/hdbclient/`

The `odbc.ini` and `odbcinst.ini` files must be in the same location.

## Downloading and configuring libraries

SAP HANA Connector uses JDBC to import the metadata. Hence, to read data from the SAP HANA database, download the `ngdbc.jar` file and configure it on the Secure Agent machine. Contact SAP Customer Support if you encounter any issues with downloading the file.

1. Go to the SAP Service Marketplace: <http://service.sap.com/connectors>

**Note:** You need SAP credentials to access the Service Marketplace.

2. Download the `ngdbc.jar` file on the Linux or Windows machine where the Secure Agent runs. Verify that you download the most recent version of the file.

3. Copy the `ngdbc.jar` file to the following directory:

```
C:\Program Files\Informatica Cloud Secure Agent\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm-extra\HANA
```

Create the `deploy_to_main\bin\rdtm-extra\HANA` directory if it does not already exist.

4. Restart the Secure Agent.

## Connect to SAP HANA

Let's configure the SAP HANA connection properties to connect to SAP HANA.

### Before you begin

Before you configure a connection, append an entry to the `odbcinst.ini` file on Linux and download and configure the `ngdbc.jar` file from the 64-bit HANA ODBC driver.

Check out "[Prerequisites](#)" on page 656 to learn more about these tasks.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Maximum length is 255 characters.
Description	
Type	SAP HANA.

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent or serverless runtime environment.</p> <p>For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 659</a>.</p>
Host	SAP HANA server host name.
Port	SAP HANA server port number.
Database Name	Name of the SAP HANA database.
Current Schema	<p>SAP HANA database schema name.</p> <p>Specify <b>_SYS_BIC</b> when you use SAP HANA database modelling views.</p>
Code Page	<p>The code page of the database server defined in the connection.</p> <p>Select the UTF-8 code page.</p>
Username	User name of the SAP HANA account.
Password	<p>Password of the SAP HANA account.</p> <p>The password can contain alphanumeric characters and the following special characters: ~ ` ! @ # \$ % ^ &amp; * ( ) _ - + = { [ ]   : ; ' &lt; , &gt; . ? /</p> <p><b>Note:</b> You can't use a semicolon character in combination with a left brace or right brace character.</p>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Metadata Advanced Connection Properties	<p>The optional properties for the JDBC driver to fetch the metadata.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example,</p> <pre>connectTimeout=180000</pre> <p>For more information, see <a href="#">"Downloading and configuring libraries" on page 657</a>.</p>
Run-time Advanced Connection Properties	<p>The optional properties for the ODBC driver to run the mappings.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example,</p> <pre>charset=sjis;readtimeout=180</pre> <p>For more information, see <a href="#">"Adding entries in Linux operating system" on page 656</a>.</p>

## Use the serverless runtime environment

You can use the serverless runtime environment to connect to the SAP system when you configure an SAP HANA connection in Data Integration.

Before you configure a SAP HANA connection using the serverless runtime environment, you need to perform certain prerequisites.

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the libraries in the Amazon S3 bucket or Azure container in the following directory in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/hana
3. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        hanas:
          - fileCopy:
              sourcePath: sap/jco/ngdbc.jar
    odbcInst:
      drivers:
        - fileCopy:
            sourcePath: ODBC/libodbcHDB.so
      dsns:
        - name: "HDBODBC"
          entries:
            - key: Driver
              value: libodbcHDB.so
            - key: Description
              value: "HANA Driver"
            - key: CPTimeout
```

value: 0

where the source path is the directory path of the library files in AWS or Azure.

4. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure directory:  
`<Supplementary file location>/serverless_agent_config`

When the .yml file runs, the libraries are copied from the AWS or Azure directory to the serverless agent directory.

For more information about serverless runtime environment properties, see the *Administrator* help.



## CHAPTER 197

# SAP HANA Database Ingestion connection properties

When you set up an SAP HANA connection for a database ingestion and replication task, you must configure connection properties.

The following table describes the SAP HANA connection properties:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	Select <b>SAP HANA Database Ingestion</b> as the connection type.
Runtime Environment	The name of the runtime environment where you want to run database ingestion and replication tasks. You define runtime environments in Administrator.
User Name	The user name for connecting to the SAP HANA instance. Enter the user name in the same case as in the database user name specified in SAP HANA.
Password	The password for connecting to the SAP HANA instance.
Host	The name of the machine that hosts the SAP HANA database server.
Port	The port number for the SAP HANA server to which you want to connect. Default is 30015.
Database Name	The SAP HANA source database name.
Advanced Connection Properties	Optional advanced properties for the SAP HANA JDBC driver, which is used to connect to the SAP HANA source. If you specify more than one <i>property=value</i> entry, separate them with an ampersand (&). The JDBC connection properties that you can enter in this field are described in the <a href="#">SAP JDBC Connection Properties</a> documentation. For example: <code>encrypt=true</code> .

Connection property	Description
Capture Type	<p>Select one of the following options to indicate the capture method that database ingestion incremental load jobs use to capture change data from SAP HANA databases:</p> <ul style="list-style-type: none"> <li>- <b>Trigger Based.</b> Capture change data from SAP HANA source tables in the schema by using AFTER DELETE, AFTER INSERT, and AFTER UPDATE triggers. The triggers get before images and after images of DML changes for each source table and write entries for the changes to the PKLOG and shadow _CDC tables. This method is the original capture method.</li> <li>- <b>Log Based (Preview).</b> Capture change data from the SAP HANA database logs. This method is available only in Preview mode. Preview functionality is supported for evaluation purposes but is unwarranted and is not supported in production environments or any environment that you plan to push to production. For more information, contact Informatica Global Customer Support.</li> </ul>
Log Clear	<p>Required for incremental loads. Enter the time interval, in days, after which the PKLOG table entries and shadow _CDC table entries are purged. The purging occurs only while an incremental load job is running.</p> <p>Valid values for a database ingestion job are 0 to 366. Any positive value in this range cause automatic housekeeping to run while the incremental job is running. Default is 14.</p> <p>A value of 0 means that the table entries are not purged. For manual housekeeping, enter 0 and use your in-house process.</p> <p>Any value outside the range of 0 to 366, including a negative number or non-numeric value, causes database ingestion jobs that use the connection to fail with the following error:</p> <pre>LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.</pre>
Trigger Prefix	<p>If you use the Trigger Based capture type, you can add a prefix to the names of the AFTER DELETE, AFTER INSERT, and AFTER UPDATE triggers that the CDC script generates for each source table to get before images and after images of the DML changes. Enter any prefix value up to 16 characters in length. An underscore (_) follows the prefix in the trigger name, for example, <b>TX_SAP_DEMO_TABLE_DBMI_USER_t_d</b>. You can use the prefix to comply with your site's trigger naming conventions.</p>
Cache Type	<p>If you selected the Log Based (Preview) capture type, select <b>Hana</b> or <b>Oracle</b> as the cache type.</p>
Cache Host	<p>If you selected the Log Based (Preview) capture type, enter the host name of the machine that hosts the cache database.</p>
Cache Port	<p>If you selected the Log Based (Preview) capture type, enter the port number for the cache database server.</p>
Cache User Name	<p>If you selected the Log Based (Preview) capture type, enter the user name to use for connecting to the cache database.</p>
Cache Password	<p>If you selected the Log Based (Preview) capture type, enter the password to use for connecting to the cache database.</p>
Cache Database/ Service Name	<p>If you selected the Log Based (Preview) capture type, enter either the Hana cache database name or the Oracle cache service name, depending on the cache type you selected.</p>

Connection property	Description
Cache Additional Connection Properties	<p>If you selected the Log Based (Preview) capture type, you can enter a list of optional cache connection properties. If you use Hana cache, use the ampersand (&amp;) separator. If you use Oracle cache, use the semicolon (;) separator.</p> <p>Examples:</p> <p>Hana: <code>latency=0&amp;communicationtimeout=0</code></p> <p>Oracle: <code>EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.1</code></p>
Cache Security Connection Properties	<p>If you selected the Log Based (Preview) capture type, you can enter a list of optional security properties for the cache connection. If you use Hana cache, use the ampersand (&amp;) separator. If you use Oracle cache, use the semicolon (;) separator.</p> <p>Examples:</p> <p>Hana: <code>encrypt=true&amp;validateCertificate=false</code></p> <p>Oracle: <code>KeyStorePassword=xyz;TrustStorePassword=xy</code></p>
Server Log Path	<p>If you selected the Log Based (Preview) capture type, enter the log path for the SAP HANA DB server.</p>
Client Log Path	<p>If you selected the Log Based (Preview) capture type, enter the mapping of the Secure Agent machine mount path to the source database log location.</p>
Client Archive Log Path	<p>If you selected the Log Based (Preview) capture type, enter the mapping of the Secure Agent machine mount path to the source database archive log location.</p>

**Note:** If you test the connection and the test fails, check that the SAP HANA JDBC driver file, `ngdbc.jar`, has been installed at `Secure Agent installation directory>/ext/connectors/thirdparty/informatica.hanami`.

# CHAPTER 198

## SAP IQ connection properties

Create an SAP IQ connection to securely write data to SAP IQ.

### Prerequisites

Before you create an SAP IQ connection to write to SAP IQ, be sure to complete the prerequisites.

#### Install the SAP IQ JDBC driver and Sybase client

To write data to SAP IQ databases, you need to install the SAP IQ JDBC driver and Sybase client on the Secure Agent machine.

- Install the SAP IQ JDBC driver on the Secure Agent machine.  
To install the driver, perform the following steps:
  1. From the [SAP Support Portal](#), download the jconn4.jar SAP IQ JDBC driver.
  2. Create the `informatica.sapiq` folder manually in the following directory based on whether the Secure Agent machine is a Windows or a Linux machine:

Secure Agent machine	Directory
Linux	<Secure Agent installation directory>/ext/connectors/thirdparty
Windows	<Secure Agent installation directory>\ext\connectors\thirdparty

3. Copy the SAP IQ JDBC driver to the `informatica.sapiq` folder.
- Install the Sybase client on the Secure Agent machine.  
To install the Sybase client, perform the following steps:
    1. Download the Sybase client from the SAP website and install it on the Secure Agent machine.
    2. On Linux, additionally set the following environmental variables:
      - `setenv SYBASE <Sybase client directory>/sybase`
      - `setenv SYBROOT <Sybase client directory>/sybase`
      - `setenv IQDIR16 <Sybase client directory>/sybase/IQ-16_1`

- setenv LD\_LIBRARY\_PATH <Sybase client directory>/sybase/IQ-16\_1/lib64
- setenv PATH <Sybase client directory>/sybase/IQ-16\_1/bin64

After you install the SAP IQ JDBC driver and set the environmental variables, you need to restart the Secure Agent.

## Connect to SAP IQ

Let's configure the SAP IQ connection properties to connect to SAP IQ.

### Before you begin

Before you get started, you'll need to install the SAP IQ JDBC driver and Sybase client on the Secure Agent machine to establish an SAP IQ connection.

Check out ["Prerequisites" on page 664](#) to learn more about the configuration prerequisites.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP IQ
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
Host Name	The name of the machine that hosts the SAP IQ database server.

Property	Description
Port	The port number that connects to the SAP IQ database server. Default is 2638.
Database	The SAP IQ database that you want to connect to.
Schema	The schema name in the SAP IQ server to fetch the metadata.
User Name	The user name to connect to the SAP IQ account.
Password	The password to connect to the SAP IQ account.
Datafile Directory	The SAP IQ directory that stores data files at run time. The directory needs to be accessible from the Secure Agent machine. If the directory is on a Windows system, use a backslash (\) in the path. For example, \root\mydirectory\inputfile.out If the directory is on a UNIX system, use a slash (/) in the path. For example, /root/mydirectory/inputfile.out

### Advanced settings

The following table describes the advanced connection properties:

Property	Description
Checkpoint	Enable the SAP IQ database to issue a checkpoint after successfully loading data into tables. If disabled, the database does not issue a checkpoint. Default is enabled.
Notify Interval	Number of rows that the SAP IQ external loader loads before it writes a status message to the external loader log. Default is 1000.
External Loader Executable	The file name and path of the external loader executable. The name of the external loader executable file is set to <b>dbisql</b> by default. If you configure the connection on Windows, you must enter <b>dbisql -nogui</b> . If the external loader executable file name is abc.exe and the path is /root/<folder name>, enter both the path and file name in the following format: <code>/root/&lt;folder name&gt;/abc.exe</code>
Is Staged	Method of loading data Enable to write data to a staging location before loading data into an SAP IQ database. Default is enabled.

## CHAPTER 199

# SAP Mass Ingestion connection properties

When you set up a SAP Mass Ingestion connection, you must configure the connection properties.

The following table describes the connection properties for a SAP Mass Ingestion connection:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>SAP Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the SAP instance.
Password	Password for the SAP instance.
Language Code	Language code that corresponds to the SAP language.
System Number	System number of the SAP server.
Client Number	Client number of the SAP server.
Port Range	HTTP port range to run the Netty server.
Connection Type	Type of connection to access the ABAP application server. Options are: <ul style="list-style-type: none"><li>- <b>Direct Connection:</b> Accesses a single ABAP application server using the server host.</li><li>- <b>Load Balancing Connection:</b> Accesses a group of ABAP application servers through the message server.</li></ul>

Connection property	Description
Application Server	Name of the SAP application server host. <b>Note:</b> This field appears only for the <b>Direct Connection</b> type.
Message Server	IP address or name of the SAP message server. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
SAP Logon Group	Name of the group of servers that belong to the SAP system you want to access. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
SAP System ID	ID of the SAP system that you want to access. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
Message Server Port	Port number on which the SAP message server is listening. <b>Note:</b> This field appears only for the <b>Load Balancing Connection</b> type.
Database	The name of the underlying database. Select one of the following options: - Oracle - SAP HANA (S/4 trigger based)
For Oracle database	
Database user name	User name of the database instance.
Database password	Password for the database instance.
Host	Host name of the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Code Page	The code page of the database server. Application ingestion and replication tasks use the UTF-8 code page. Default is UTF-8.
Encryption Method	For initial load jobs, determines whether the data exchanged between the Secure Agent and the Oracle database server is encrypted: Select one of the following options: - <b>SSL</b> . Establishes a secure connection using SSL for data encryption. If the Oracle database server cannot configure SSL, the connection fails. - <b>No Encryption</b> . Establishes a connection without using SSL. Data is not encrypted. Default is <b>No Encryption</b> .
Crypto Protocol Version	If you selected SSL as the encryption method, you must specify a cryptographic protocol or a list of cryptographic protocols supported by your server to use with an encrypted connection. Select one of the following options: - <b>SSLv2</b> - <b>SSLv3</b> - <b>TLSv1.2</b> Default is <b>TLSv1.2</b> .



Connection property	Description
Validate Server Certificate	<p>If you selected SSL as the encryption method, this option controls whether the Secure Agent validates the server certificate that is sent by the Oracle database server.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>True</b>. Validate the server certificate.</li> <li>- <b>False</b>. Do not validate the server certificate.</li> </ul> <p>Default is <b>False</b>.</p> <p>If you also specify the <b>Host Name in Certificate</b> property, the Secure Agent also validates the host name in the certificate.</p>
Trust Store	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the client trusts for SSL authentication.</p>
Trust Store Password	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify a password for accessing the contents of the truststore file.</p>
Host Name in Certificate	<p>If you selected SSL as the encryption method and enabled validation of the server certificate, specify the host name of the machine that hosts the Oracle database to provide for additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
Key Store	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the path and name of the keystore file. The keystore file contains the certificates that the client sends to the Oracle server in response to the server's certificate request.</p>
Key Store Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keystore file.</p>
Key Password	<p>If you selected SSL as the encryption method and client authentication is enabled on the Oracle database server, specify the password for the keys in the keystore file. Use this property when the keys have a different password than the keystore file.</p>
Database Connect String	<p>An Oracle connection string, defined in TNS, that application ingestion and replication tasks use to connect to the Oracle database.</p>
TDE Wallet Directory	<p>The path to the directory that contains the Oracle wallet file used for Oracle Transparent Data Encryption (TDE). Specify this property value only if you capture change data from TDE-encrypted table spaces and one of the following conditions are true:</p> <ul style="list-style-type: none"> <li>- The Oracle wallet is not available to the database.</li> <li>- The Oracle database is running on a server that is remote from Oracle redo logs.</li> <li>- The wallet directory is not in the default location on the database host or the wallet name is not the default name of ewallet.p12.</li> <li>- The wallet directory is not available to the Secure Agent host.</li> </ul>
TDE Wallet Password	<p>A clear text password that is required to access the Oracle TDE wallet and get the master key. This property value is required if you need to read and decrypt data from TDE-encrypted tablespaces in the Oracle source database.</p>

Connection property	Description
Directory Substitution	<p>A local path prefix to substitute for the server path prefix of the redo logs on the Oracle server. This substitute local path is required when the log reader runs on a system other than the Oracle server and uses a different mapping to access the redo log files.</p> <p>Use this property in the following situations:</p> <ul style="list-style-type: none"> <li>- The redo logs reside on shared disk.</li> <li>- The redo logs have been copied to a system other than the Oracle system.</li> <li>- The archived redo logs are accessed by using a different NFS mount.</li> </ul> <p><b>Note:</b> Do not use this property if you use Oracle Automatic Storage Management (ASM) to manage the redo logs.</p> <p>You can define one or more substitutions. Use the following format:</p> <pre>server_path_prefix,local_path_prefix;server_path_prefix,local_path_prefix;...</pre>
Reader Active Log Mask	<p>A mask that the log reader uses for selecting active redo logs when the Oracle database uses multiplexing of redo logs. The log reader compares the mask against the member names in an active redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Reader Archive Destination 1	<p>The primary log destination from which the log reader reads archived logs, when Oracle is configured to write more than one copy of each archived redo log. Enter a number that corresponds to an <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10.</p> <p>If you set only one of the Reader Archive Destination 1 and Destination 2 properties, the log reader uses that property setting. If you specify neither property, the archive log queries are not filtered by the log destination.</p>
Reader Archive Destination 2	<p>The secondary log destination from which the log reader reads archived logs when the primary destination becomes unavailable or when the logs at the primary destination cannot be read. For example, logs might have been corrupted or deleted. Enter a number that corresponds to the <i>n</i> value in an Oracle LOG_ARCHIVE_DEST_<i>n</i> initialization parameter, where <i>n</i> is a value from 1 to 10. Usually, this value is a number greater than 1.</p>
Reader ASM Connect String	<p>In an Oracle ASM environment, the Oracle connection string, defined in TNS, that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p>
Reader ASM User Name	<p>In an Oracle ASM environment, an Oracle user ID that the log reader uses to connect to the ASM instance that manages storage of active and archived redo logs for the source database. This user ID must have SYSDBA or SYSASM authority. To use SYSASM authority, set the <b>Reader ASM Connect As SYSASM</b> property to Y.</p>
Reader ASM Password	<p>In an Oracle ASM environment, a clear text password for the user that is specified in the <b>Reader ASM User Name</b> property. The log reader uses this password and the ASM user name to connect to the ASM instance that manages storage of active and archived redo logs for the source database.</p>

Connection property	Description
Reader ASM Connect As SYSASM	<p>If you use Oracle 11g ASM or later and want the log reader to use a user ID that has SYSASM authority to connect to the ASM instance, select this check box. Also specify a user ID that has SYSASM authority in the <b>Reader ASM User Name</b> property. To use a user ID that has SYSDBA authority, clear this check box. By default, this check box is cleared.</p>
Reader Mode	<p>Indicates the source of and types of Oracle redo logs that the log reader reads. Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>ACTIVE</b>. Read active and archived redo logs from the Oracle online system. Optionally, you can use the <b>Reader Active Log Mask</b> property to filter the active redo logs and use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVEONLY</b>. Read only archived redo logs. Optionally, you can use the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties to limit the archived log destinations from which to read archived logs.</li> <li>- <b>ARCHIVECOPY</b>. Read archived redo logs that have been copied to an alternate file system. Use this option in the following situations: <ul style="list-style-type: none"> <li>- You do not have the authority to access the Oracle archived redo logs directly.</li> <li>- The archived redo logs are written to ASM, but you do not have access to ASM.</li> <li>- The archived log retention policy for the database server causes the archived logs to not be retained long enough.</li> </ul> <p>With this option, the <b>Reader Archive Destination 1</b> and <b>Reader Archive Destination 2</b> properties are ignored.</p> <p>Default is <b>ACTIVE</b>.</p> </li> </ul>
Reader Standby Log Mask	<p>A mask that the log reader uses for selecting redo logs for an Oracle physical standby database when the database uses multiplexing of redo logs. The log reader compares the mask against the member names in an redo log group to determine which log to read. In the mask, you can use the asterisk (*) wildcard to represent zero or more characters.</p> <p>The mask can be up to 128 characters in length. It is case-sensitive on Linux or UNIX systems but not on Windows systems.</p>
Standby Connect String	<p>An Oracle connection string, defined in TNS, that the log reader uses to connect to the Oracle physical standby database for change capture when the database is not open with read only access.</p>
Standby User Name	<p>A user ID that the log reader uses to connect to the Oracle physical standby database for change capture. This user ID must have SYSDBA authority.</p>
Standby Password	<p>A password that the log reader uses to connect to the Oracle physical standby database for change capture.</p>
RAC Members	<p>The maximum number of active redo log threads, or <i>members</i>, in an Oracle Real Application Cluster (RAC) that can be tracked. For a Data Guard physical standby database that supports a primary database in a RAC environment, this value is the number of active threads for the primary database.</p> <p>Valid values are 1 to 100. Default is 0, which causes an appropriate number of log threads to be determined automatically. If this value is not appropriate for your environment, set this property to a value greater than 0.</p>

Connection property	Description
BFILE Access	<p>Select this check box in the following circumstances:</p> <ul style="list-style-type: none"> <li>- You use BFILE access to redo logs in physical directories on the local Oracle server file system. BFILE access uses Oracle directory objects to remotely access the redo logs in the file system. This method is an alternative to other log access methods such as ASM or NFS mounts.</li> <li>- You have an Amazon Relational Database Service (RDS) for Oracle source. In this case, this option enables access to the redo logs of a cloud-based database instance deployed in RDS.</li> </ul> <p>By default, this check box is cleared.</p>
For SAP HANA (S/4 trigger based) database	
User Name	The user name to connect to the SAP HANA instance.
Password	The password to connect to the SAP HANA instance.
Host	The name of the machine that hosts the SAP HANA database server.
Port	The port number of the SAP HANA server that you want to connect to. Default is 30015.
Database Name	The SAP HANA source database name.
Advanced Connection Properties	Advanced properties for the SAP HANA JDBC driver, which is used to connect to the SAP HANA source. If you specify more than one <i>property=value</i> entry, separate them with an ampersand (&). The JDBC connection properties that you can enter in this field are described in the SAP <a href="#">JDBC Connection Properties</a> documentation. For example: <code>encrypt=true</code> .
Log Clear	<p>Required for incremental loads. The time interval, in days, after which the PKLOG table entries and shadow _CDC table entries are purged. The purging occurs only while an incremental load job is running.</p> <p>Valid values for a database ingestion job are 0 to 366. Any positive value in this range causes automatic housekeeping to run while the incremental job is running. Default is 14.</p> <p>A value of 0 means that the table entries are not purged. For manual housekeeping, enter 0 and use your in-house process.</p> <p>Any value outside the range of 0 to 366, including a negative number or non-numeric value, causes database ingestion jobs that use the connection to fail with the following error:</p> <pre>LogClear contains a non numeric number. Caused by: LogClear contains a non numeric number.</pre>
Trigger Prefix	<p>If you use the trigger-based capture type, you can add a prefix to the names of the AFTER DELETE, AFTER INSERT, and AFTER UPDATE triggers that the CDC script generates for each source table to get before images and after images of the DML changes. Enter any prefix value up to 16 characters in length. An underscore (_) follows the prefix in the trigger name, for example, <code>TX_SAP_DEMO_TABLE_DBML_USER_t.d</code>. You can use the prefix to comply with your site's trigger naming conventions.</p>

## CHAPTER 200

# SAP OData V2 connection properties

Create an SAP OData V2 connection to securely read from or write to OData V2-compliant applications in SAP deployed in the cloud or on-premises.

## Prepare for authentication

You can configure basic, API key, authorization code, and client credentials authentication types to access OData V2-compliant applications in SAP.

Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

### Basic

To connect to SAP OData V2 services using basic authentication, you need the SAP account user name and password.

Get the required details from the SAP application to which you want to connect.

For more information about basic authentication in SAP, see [Basic authentication](#) in the SAP documentation.

### API key

To connect to SAP OData V2 services using API key authentication, you need a unique API key that SAP OData V2 Connector uses to authenticate the API calls made to the SAP OData endpoint.

Get the API key from the SAP application to which you want to connect.

For more information about how to generate and use an API key, see [Add API keys to an environment](#) in the SAP documentation.

### Authorization code

To connect to SAP OData V2 services using the OAuth 2.0 authorization code, you need the SAP client ID, client secret, authorization token URL, access token URL, and access token.

To get the authorization details, you need to create an authorization integration in SAP, and register the Informatica redirect URL in SAP Integration Suite. SAP Integration Suite is an integration platform-as-a-

service that enables clients that support OAuth to redirect users to an authorization page and generate access tokens, and optionally, refresh tokens to access SAP.

Register the following Informatica redirect URL in SAP Integration Suite:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires and the response returns 401 error code, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieves a new access token.

For more information about how to create an authorization integration and get the authorization details, see [OAuth 2.0 authorization code](#) in the SAP documentation.

## Client credentials

To connect to SAP OData V2 services using OAuth 2.0 client credentials, you need the SAP client ID, client secret, access token URL, and access token.

Configure the OAuth endpoint with the client credentials grant type and then create an authorization integration to get the authorization details.

For more information about how to create an authorization integration and get the authorization details, see [OAuth 2.0 client credentials](#) in the SAP documentation.

# Connect to SAP OData V2

Let's configure the SAP OData V2 connection properties to connect to SAP OData V2 services, and read from or write to OData V2-compliant applications in SAP.

## Before you begin

Before you get started, you'll need to get information from your SAP account based on the authentication type that you want to configure.

Check out ["Prepare for authentication" on page 673](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP OData V2

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent.</p>
Service Type	<p>The service type of the OData V2 application endpoint to which you want to connect.</p> <p>Select one of the following service types from the list:</p> <ul style="list-style-type: none"> <li>- Default. Connects to a specific SAP service.</li> <li>- SAP Gateway Catalog. Connects to the SAP catalog service that provides a list of all available services on SAP Gateway.</li> </ul> <p>Default is Default.</p>
Service URL	<p>The service URL for the selected service type.</p> <p>If you select the <b>Default</b> service type, enter the root URL of the service in the following format:</p> <pre>http://&lt;Host name of the SAP server&gt;:&lt;Port number&gt;/sap/opu/odata/sap/&lt;Service name&gt;/</pre> <p>For example, if you want to connect to the ZALL_DATATYPE_SRV service in SAP when the host name is http://invs15con01.informatica.com and port number is 8081, enter the following service URL:</p> <pre>http://&lt;Host name of the SAP server&gt;:&lt;Port number&gt;/sap/opu/odata/sap/ZALL_DATATYPE_SRV/</pre> <p>If you select the <b>SAP Gateway Catalog</b> service type, enter the service URL in the following format:</p> <pre>http://&lt;Host name of the SAP server&gt;:&lt;Port number&gt;/sap/opu/odata/IWFND/&lt;Catalog service name&gt;</pre> <p>For example, if you want to connect to the CATALOGSERVICE;v=2 catalog service in SAP when the host name is abcd01con02.example.com and port number is 8081, enter the following service URL:</p> <pre>http://abcd01con02.example.com:8081/sap/opu/odata/IWFND/CATALOGSERVICE;v=2</pre>

## Authentication types

You can configure basic, API key, authorization code, and client credentials authentication types to access OData V2-compliant applications in SAP.

Select the required authentication method and then configure the authentication-specific parameters.

### Basic authentication

Basic authentication is the default type which requires at a minimum your SAP account name and password.

The following table describes the basic connection properties for basic authentication:

Property	Description
Username	The user name to connect to the SAP OData V2 service.
Password	The password to connect to the SAP OData V2 service.

### Advanced settings

The following table describes the advanced connection properties for basic authentication:

Property	Description
SAP Custom Query Options	<p>Additional custom queries that you can use when you connect to the SAP OData V2 service.</p> <p>You can enter multiple SAP custom queries, separated by an ampersand (&amp;), in the following format:</p> <pre>&lt;Custom query1&gt;=&lt;value&gt;&amp;&lt;Custom query2&gt;=&lt;value&gt;&amp;&lt;Custom query3&gt;=&lt;value&gt;...</pre> <p>For example, if you want to pass the SAP client number and language code when you connect to the SAP OData V2 service, enter the following custom queries:</p> <pre>sap-client=400&amp;sap-language=DE</pre> <p>When you add queries, ensure that there is no space before and after the equal sign (=).</p> <p>For more information about the list of SAP custom queries that you can configure, see <a href="#">SAP URL parameters</a> in the SAP documentation.</p>

### API key authentication

API key authentication requires at a minimum a unique API key from the SAP application.

The following table describes the basic connection properties for API key authentication:

Property	Description
API Key	The unique API key that SAP OData V2 Connector uses to authenticate the API calls made to the SAP OData endpoint.



## Advanced settings

The following table describes the advanced connection properties for API key authentication:

Property	Description
SAP Custom Query Options	<p>Additional custom queries that you can use when you connect to the SAP OData V2 service.</p> <p>You can enter multiple SAP custom queries, separated by an ampersand (&amp;), in the following format:</p> <pre data-bbox="841 548 1365 596">&lt;Custom query1&gt;=&lt;value&gt;&amp;&lt;Custom query2&gt;=&lt;value&gt;&amp;&lt;Custom query3&gt;=&lt;value&gt;....</pre> <p>For example, if you want to pass the SAP client number and language code when you connect to the SAP OData V2 service, enter the following custom queries:</p> <pre data-bbox="841 709 1208 732">sap-client=400&amp;sap-language=DE</pre> <p>When you add queries, ensure that there is no space before and after the equal sign (=).</p> <p>For more information about the list of SAP custom queries that you can configure, see <a href="#">SAP URL parameters</a> in the SAP documentation.</p>

## Authorization code authentication

OAuth 2.0 authorization code authentication requires at a minimum the SAP client ID, client secret, authorization token URL, access token URL, and access token.

The following table describes the basic connection properties for OAuth 2.0 authorization code authentication:

Property	Description
Authorization Token URL	<p>The SAP authorization token endpoint of the OAuth 2.0 authorization server that is used to authorize the user request.</p> <p>Enter the authorization token URL in the following format:</p> <pre>https://&lt;Host name of the server&gt;:&lt;Port number&gt;/sap/bc/sec/oauth2/authorize?sap-client=&lt;SAP client number&gt;</pre> <p>For example, If the host name is <code>abcd01con02.example.com</code> and port number is <code>44301</code>, enter the following authorization token URL when the SAP client number is <code>800</code>:</p> <pre>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/authorize?sap-client=800</pre>
Access Token URL	<p>The SAP access token endpoint of the OAuth 2.0 authorization server that is used to exchange the authorization code to get an access token.</p> <p>Enter the access token URL in the following format:</p> <pre>https://&lt;Host name of the server&gt;:&lt;Port number&gt;/sap/bc/sec/oauth2/token?sap-client=&lt;SAP client number&gt;</pre> <p>For example, If the host name is <code>abcd01con02.example.com</code> and port number is <code>44301</code>, enter the following access token URL when the SAP client number is <code>800</code>:</p> <pre>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/token?sap-client=800</pre>
Client ID	The client identifier of your application generated when you configure the application for OAuth.
Client Secret	The client secret generated for the client ID.
Access Token	<p>The access token granted by the authorization server to access the SAP data.</p> <p>Enter the populated access token value that you get from the OAuth endpoint, or click <b>Generate Access Token</b> to populate the access token value.</p>

## Advanced settings

The following table describes the advanced connection properties for OAuth 2.0 authorization code authentication:

Property	Description
Scope	<p>The scope of the access request when the SAP OData V2 endpoint has defined custom scopes.</p> <p>You can enter multiple scope attributes, each separated by a space, in the following format:</p> <pre>&lt;Scope attribute1&gt; &lt;Scope attribute2&gt; &lt;Scope attribute3&gt;....</pre> <p>For example, enter the following scope attributes:</p> <pre>ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001</pre>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the access token parameters in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For more information about the access token parameters that you can define, see the SAP documentation.</p>
Authorization Code Parameters	<p>Additional parameters to use with the authorization token URL.</p> <p>Define multiple parameters, separated by a comma, in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}, {"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For example, you can use the following maximum age and state parameters when you connect to the SAP OData V2 service:</p> <pre>[{"Name": "max_age", "Value": 60}, {"Name": "state", "Value": "test"}]</pre> <p>For more information about the authorization code parameters that you can define, see the SAP documentation.</p>
Client Authentication	<p>The method of sending client authentication details for authorization to connect to the SAP OData V2 service.</p> <p>Select one of the following client authentications from the list:</p> <ul style="list-style-type: none"> <li>- Send client credentials in body. Sends the client ID and client secret for authorization in the body of the request.</li> <li>- Basic auth header. Sends the client ID and client secret for authorization in the header of the request.</li> </ul> <p>Default is <b>Send client credentials in body</b>.</p>

Property	Description
Refresh Token	<p>The refresh token value.</p> <p>Enter the populated refresh token value that you get from the OAuth endpoint, or click <b>Generate AccessToken</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent fetches a new access token with the help of the refresh token.</p> <p><b>Note:</b> If the refresh token expires, provide a valid refresh token or regenerate a new refresh token by clicking <b>Generate Access Token</b>.</p>
SAP Custom Query Options	<p>Additional custom queries that you can use when you connect to the SAP OData V2 service.</p> <p>You can enter multiple SAP custom queries, separated by an ampersand (&amp;), in the following format:</p> <pre>&lt;Custom query1&gt;=&lt;value&gt;&amp;&lt;Custom query2&gt;=&lt;value&gt;&amp;&lt;Custom query3&gt;=&lt;value&gt;...</pre> <p>For example, if you want to pass the SAP client number and language code when you connect to the SAP OData V2 service, enter the following custom queries:</p> <pre>sap-client=400&amp;sap-language=DE</pre> <p>When you add queries, ensure that there is no space before and after the equal sign (=).</p> <p>For more information about the list of SAP custom queries that you can configure, see <a href="#">SAP URL parameters</a> in the SAP documentation.</p>

## Client credential authentication

OAuth 2.0 client credential authentication requires at a minimum the SAP client ID, client secret, access token URL, and access token.

The following table describes the basic connection properties for OAuth 2.0 client credential authentication:

Property	Description
Access Token URL	<p>The SAP access token endpoint of the OAuth 2.0 authorization server that is used to exchange the authorization code to get an access token.</p> <p>Enter the access token URL in the following format:</p> <pre>https://&lt;Host name of the server&gt;:&lt;Port number&gt;/sap/bc/sec/oauth2/token?sap-client=&lt;SAP client number&gt;</pre> <p>For example, If the host name is abcd01con02.example.com and port number is 44301, enter the following access token URL when the SAP client number is 800:</p> <pre>https://abcd01con02.example.com:44301/sap/bc/sec/oauth2/token?sap-client=800</pre>
Client ID	<p>The client identifier of your application generated when you configure the application for OAuth.</p>

Property	Description
Client Secret	The client secret generated for the client ID.
Access Token	<p>The access token granted by the authorization server to access the SAP data.</p> <p>Enter the populated access token value that you get from the OAuth endpoint, or click <b>Generate Access Token</b> to populate the access token value.</p>

### Advanced settings

The following table describes the advanced connection properties for OAuth 2.0 client credential authentication:

Property	Description
Scope	<p>The scope of the access request when the SAP OData V2 endpoint has defined custom scopes.</p> <p>You can enter multiple scope attributes, each separated by a space, in the following format:</p> <pre>&lt;Scope attribute1&gt; &lt;Scope attribute2&gt; &lt;Scope attribute3&gt;...</pre> <p>For example, enter the following scope attributes:</p> <pre>ZGWSAMPLE_BASIC_0001 /IWFND/SG_MED_CATALOG_0002 ZAPI_CHARTOFACCOUNTS_SRV_0001</pre>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the access token parameters in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For more information about the access token parameters that you can define, see the SAP documentation.</p>

Property	Description
Client Authentication	<p>The method of sending client authentication details for authorization to connect to the SAP OData V2 service.</p> <p>Select one of the following client authentications from the list:</p> <ul style="list-style-type: none"> <li>- Send client credentials in body. Sends the client ID and client secret for authorization in the body of the request.</li> <li>- Basic auth header. Sends the client ID and client secret for authorization in the header of the request.</li> </ul> <p>Default is <b>Send client credentials in body</b>.</p>
SAP Custom Query Options	<p>Additional custom queries that you can use when you connect to the SAP OData V2 service.</p> <p>You can enter multiple SAP custom queries, separated by an ampersand (&amp;), in the following format:</p> <pre data-bbox="841 716 1370 762">&lt;Custom query1&gt;=&lt;value&gt;&amp;&lt;Custom query2&gt;=&lt;value&gt;&amp;&lt;Custom query3&gt;=&lt;value&gt;...</pre> <p>For example, if you want to pass the SAP client number and language code when you connect to the SAP OData V2 service, enter the following custom queries:</p> <pre data-bbox="841 873 1211 898">sap-client=400&amp;sap-language=DE</pre> <p>When you add queries, ensure that there is no space before and after the equal sign (=).</p> <p>For more information about the list of SAP custom queries that you can configure, see <a href="#">SAP URL parameters</a> in the SAP documentation.</p>

## CHAPTER 201

# SAP OData V4 connection properties

Create an SAP OData V4 connection to securely read from OData V4-compliant applications in SAP.

## Prepare for authentication

You can configure authorization code authentication type to read from OData V4-compliant applications in SAP.

Before you configure the connection properties, you need to keep the authentication details handy.

### Authorization code

To connect to SAP OData V4 services using the OAuth 2.0 authorization code, you need the SAP client ID, client secret, authorization token URL, access token URL, and access token.

To get the authorization details, you need to create an authorization integration in SAP, and register the Informatica redirect URL in SAP Integration Suite. SAP Integration Suite is an integration platform-as-a-service that enables clients that support OAuth to redirect users to an authorization page and generate access tokens.

Register the following Informatica redirect URL in SAP Integration Suite:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires and the response returns 401 error code, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieves a new access token.

For more information about how to create an authorization integration and get the authorization details, see [OAuth 2.0 authorization code](#) in the SAP documentation.

## Connect to SAP OData V4

Let's configure the SAP OData V4 connection properties to connect to SAP OData V4 services and read from OData V4-compliant applications in SAP.

## Before you begin

Before you get started, you'll need to get information from your SAP account to configure the authorization code authentication type.

Check out ["Prepare for authentication" on page 683](#) to learn more about the authentication prerequisites.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP OData V4
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
Service Type	The service type of the OData V4 application endpoint to which you want to connect. When you create a connection, the agent connects to the SAP Datasphere service type of the OData V4 application endpoint. Default is SAP Datasphere.
Service URL	The service URL for the SAP Datasphere service type. Enter the service URL in the following format: <code>https://&lt;Host name of the SAP server&gt;/api/v1/dwc/consumption/relational/&lt;Space name of SAP Datasphere&gt;/&lt;Asset name of SAP Datasphere&gt;/</code> For example, if you want to connect to the ZALLDATATYPES asset in the INFA_DEV space of SAP Datasphere, enter the following service URL: <code>https://example.us01.hcs.cloud.sap/api/v1/dwc/consumption/relational/INFA_DEV/ZALLDATATYPES/</code>

## Authentication types

Configure the authorization code authentication type to access OData V4-compliant applications in SAP.



Select the authorization code authentication method and then configure the authentication-specific parameters.

## Authorization code authentication

Authorization code authentication is the default type which requires at a minimum the SAP client ID, client secret, authorization token URL, access token URL, and access token.

The following table describes the basic connection properties for authorization code authentication:

Property	Description
Authorization Token URL	<p>The SAP authorization token endpoint of the OAuth 2.0 authorization server that is used to authorize the user request.</p> <p>Enter the authorization token URL in the following format:</p> <pre>https://&lt;Host name of the server&gt;/oauth/authorize</pre> <p>For example, If the host name is <code>example.authentication.us01.hana.ondemand.com</code>, enter the following authorization token URL:</p> <pre>https://example.authentication.us01.hana.ondemand.com/oauth/authorize</pre>
Access Token URL	<p>The SAP access token endpoint of the OAuth 2.0 authorization server that is used to exchange the authorization code to get an access token.</p> <p>Enter the access token URL in the following format:</p> <pre>https://&lt;Host name of the server&gt;/oauth/token</pre> <p>For example, If the host name is <code>example.authentication.us01.hana.ondemand.com</code>, enter the following access token URL:</p> <pre>https://example.authentication.us01.hana.ondemand.com/oauth/token</pre>
Client ID	The client identifier of your application generated when you configure the application for OAuth.
Client Secret	The client secret generated for the client ID.
Access Token	<p>The access token granted by the authorization server to access the SAP data.</p> <p>Enter the populated access token value that you get from the OAuth endpoint, or click <b>Generate Access Token</b> to populate the access token value.</p>

## CHAPTER 202

# SAP ODP Extractor connection properties

Create an SAP ODP Extractor connection to securely read data from SAP ODP objects.

You can use an SAP ODP Extractor connection to read data from the following applications:

- SAP S/4HANA
- ECC
- Applications enabled with Operational Data Provisioning (ODP)
- Applications enabled with Operational Delta Queue (ODQ)

## Prerequisites

Before you use an SAP ODP Extractor connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process SAP ODP data, you also need to verify if the required licenses are enabled for the SAP system.

## Verify the required SAP Notes in the SAP server

To read data from the SAP ODP objects, you need to verify that the required SAP Notes are available in the SAP server.

- 1931427 - ODP Data Replication API 2.0
- 2232584 - Release of SAP extractors for ODP replication (ODP SAPI)

SAP ODP Extractor Connector uses the ODP Replication APIs version 2.0 when you read data from SAP ODP objects.

## Download and configure the SAP libraries

To read data from SAP ODP objects, you need to download and configure the SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.

**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).

2. Download the latest version of the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs.

Operating System	SAP JCo Libraries
Windows	- sapjco3.jar - sapjco3.dll
Linux	- sapjco3.jar - libsapjco3.so

3. Copy the JCo libraries to the following directory:  
<Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext\deploy\_to\_main\bin\rdtm-extra\tpl\sap  
Create the deploy\_to\_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.
4. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.
  - b. Click **Runtime Environments** to access the **Runtime Environments** page.
  - c. To the left of the agent name, click **Edit Secure Agent**.
  - d. From the **Service** list, select **Data Integration Server**.
  - e. From the **Type** list, select **Tomcat JRE**.
  - f. Enter the JAVA\_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

**System Configuration Details** Reset All

Service:

Type:

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javalib/sap/sap-adc

- g. Click **Save**.
5. After you save the JAVA\_LIBS value, configure the JVMClassPath property for the Secure Agent.
  - a. From the **Service** list, select **Data Integration Server**.
  - b. From the **Type** list, select **DTM**.

- c. Enter the JVMClassPath value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	pmserverjdk.jar;..\bin\rdtm-extra\tpl\sap\sapjco3.jar;..\bin\rdtm\javalib\sap\sap-adapter-common.jar
Linux	pmserverjdk.jar:../../bin/rdtm-extra/tpl/sap/sapjco3.jar:../../bin/rdtm/javalib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

System Configuration Details

Service:

Type:

Type	Name	Value
DTM	JVMClassPath	pmserverjdk.jar;../../bin/rdtm-extra/tpl/sap/sapjco3.jar;../../bin/rdtm/

- d. Click **Save**.
- e. Repeat steps 2 through 5 on every machine where you installed the Secure Agent.
6. Restart the Secure Agent.

## Configure SAP user authorization

Configure the SAP user account in the SAP system to process SAP ODP data.

For more information about how to configure SAP user authorization in the SAP system, see [SAP user authorizations](#).

The following table describes the required authorization to read from SAP ODP objects:

Read Object Name	Authorization Values	Value	Activity	Design Time/Run Time
S_RFC	RFC_TYPE - Function Group(FUGR)	SYST	16	Both
	RFC_TYPE - Function Module(FUGR)	RFC1	16	Both
	RFC_TYPE - Function Module(FUNC)	RFCPING	16	Both
	RFC_TYPE - Function Group(FUGR)	RFC_METADATA	16	Both
	RFC_TYPE - Function Module(FUNC)	RFC_METADATA_GET	16	Both
	RFC_TYPE - Function Module(FUNC)	RFC_GET_FUNCTION_INTERFACE	16	Both

Read Object Name	Authorization Values	Value	Activity	Design Time/Run Time
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_CONTEXT_GET_LIST	16	Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_GET_DETAIL	16	Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_GET_LIST	16	Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_OPEN	16	Both
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_CLOSE	16	Both
	RFC_TYPE - Function Module(FUNC)	/INFADI/ODP_FETCH_XML	16	Run Time
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_FETCH	16	Run Time
	RFC_TYPE - Function Module(FUNC)	RODPS_REPL_ODP_FETCH_XML	16	Run Time
	RFC_TYPE - Function Module(FUNC)	DDIF_FIELDINFO_GET	16	Both
S_BTCH_ADM	FIELD NAME - BTCADMIN	Y	N/A	Both
S_BTCH_JOB	FIELD NAME - JOBACTION	RELE	RELE(Release Jobs)	Both
	FIELD NAME - JOBGROUP	' '	N/A	Both
S_RS_ODP_H	FIELD NAME - RSODPHNAME	*	3	Both
	FIELD NAME - RSODPHPKG	*	3	Both
S_RO_OSOA	FIELD NAME - OLTPSOURCE	*	3	Both
	FIELD NAME - OSOAPCO	*	3	Both
	FIELD NAME - OSOAPART	Data, Definition	3	Both
S_RS_HYBR	FIELD NAME - RSHYBRPROV	'*'	3	Both
	FIELD NAME - RSHYBRPROJ	Definition	3	Both

Read Object Name	Authorization Values	Value	Activity	Design Time/Run Time
S_RS_ICUBE	FIELD NAME - OLTPSOURCE	*	3	Both
	FIELD NAME - OSOAPCO	*	3	Both
	FIELD NAME - OSOAPART	Data, Definition	3	Both
S_RS_IOMAD	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSAPPLNM	*	3	Both
	FIELD NAME - RSIOBJNM	*	3	Both
S_RS_MPRO	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSMPRO	*	3	Both
	FIELD NAME - RSMPROOBJ	Data	3	Both
S_RS_ODSO	FIELD NAME - RSINFOAREA	*	3	Both
	FIELD NAME - RSODSOBJ	*	3	Both
	FIELD NAME - RSODSPART	Data	3	Both
S_ADMI_FCD	FIELDNAME - S_ADMI_FCD	PADM	N/A	Both

## Configure the Secure Network Communication protocol

To use the SAP ODP Extractor connection with the Secure Network Communication (SNC) protocol, you need to configure the SNC protocol on both the SAP server and Secure Agent machine.

To create a connection with the SNC protocol, use the application server SNC connection and load balancing server SNC connection.

For more information about the prerequisites and steps to configure an SAP SNC connection, see [Configure the SAP Secure Network Communication protocol](#) Informatica How-To Library article.

## Connect to SAP ODP

Let's configure the SAP ODP Extractor connection properties to connect to SAP ODP objects.

## Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP ODP Extractor connection.

Check out ["Prerequisites" on page 686](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP ODP Extractor
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks to access SAP S/4HANA or SAP ECC. Select a Secure Agent or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 697</a> .

## SAP server connection types

You can configure application server, application server SNC, load balancing server, and load balancing server SNC connection types to access SAP ODP.

Select the required connection type and then configure the connection-specific parameters.

### Application server connection

Application server connection is the default type which requires your SAP client details.

The following table describes the basic connection properties for an application server connection:

Connection property	Description
SAP Client Number	The client number of the SAP application server. Get the required client number from the SAP system to which you want to connect.
SAP Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
SAP Application Server	The host name of the SAP application Server.
SAP System Number	The system number of the SAP application server to connect. Get the required system number from the SAP system to which you want to connect.
SAP Username	The user name with the appropriate user authorization to connect to the SAP account.
SAP Password	The password to connect to the SAP account.
Subscriber Name	A name that defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) in case of delta read from ODP.

## Application server SNC connection

Application server SNC connection requires the Secure Agent PSE certificate name, SAP server PSE certificate name, and path to the X509 certificate file along with your SAP client details.

The following table describes the basic connection properties for an application server SNC connection:

Connection property	Description
SAP Client Number	The client number of the SAP application server. Get the required client number from the SAP system to which you want to connect.
SAP Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
SAP Application Server	The host name of the SAP application Server.
SAP System Number	The system number of the SAP application server to connect. Get the required system number from the SAP system to which you want to connect.
SNC My Name	The agent Personal Security Environment (PSE) or certificate name generated for the Secure Agent. Default length is 256.
SNC Partner Name	The server PSE or certificate name generated on the SAP server. Default length is 256.



Connection property	Description
SNC Quality of Protection (QoP)	<p>The level of protection applied to a communication path when you create an SAP SNC connection.</p> <p>Select one of the following options from the list:</p> <ul style="list-style-type: none"> <li>- 1 - Apply authentication only</li> <li>- 2 - Apply authentication and integrity protection</li> <li>- 3 - Apply authentication, integrity, and privacy protection (encryption)</li> <li>- 8 - Apply global default protection (usually 3)</li> <li>- 9 - Apply the maximum protection</li> </ul> <p>Default is 3 - Apply authentication, integrity, and privacy protection (encryption).</p>
Use X509 Certificate	<p>Method of logging in.</p> <p>Select <b>Use X509 Certificate</b> to log in with SNC encryption that uses the X.509 certificate.</p> <p>If you don't select this option, you need to enter your SAP user name in the <b>X509 Certificate Path or SAP Username</b> property.</p> <p>Default is disabled.</p>
X509 Certificate Path or SAP Username	<p>The path and file name of the X509 certificate file.</p> <p>If the X509 certificate file name is abc.crt and the path is \root\<folder and="" both="" enter="" file="" following="" format:<="" in="" name="" name&gt;,="" p="" path="" the=""> <pre>\root\<folder name="">\abc.crt</folder></pre> <p>If you select to use the X509 certificate, you don't need to enter the SAP user name.</p> <p>If you don't want to use the X509 certificate, enter the SAP user name for which SNC is configured in the SAP server.</p> </folder></p>
Subscriber Name	<p>A name that defines the Secure Agent as a unique subscriber in the SAP system.</p> <p>SAP uses this name to define unique operational delta queue (ODQ) when the Secure Agent reads delta data from ODP.</p>

The following table describes the advanced connection properties for application server SNC connection:

Property	Description
SAP Cryptographic Library Path	<p>The path and file name of the SAP cryptographic library.</p> <p>Enter both the path and file name in the following format based on the operating system on which the Secure Agent runs:</p> <ul style="list-style-type: none"> <li>- On Windows: \root\<folder name="">\sapcrypto.dll</folder></li> <li>- On Linux: /root/&lt;folder name&gt;/libsapcrypto.so</li> </ul>

## Load balancing server connection

Create a load balancing server connection when you want to connect to the SAP system with the least load at run time.

Load balancing server connection requires your SAP client details and message server group name.

The following table describes the basic connection properties for a load balancing server connection:

Connection property	Description
SAP Client Number	The client number of the SAP message server. Get the required client number from the SAP system to which you want to connect.
SAP Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
SAP Message Server	The host name of the SAP message server.
SAP System ID	The system ID of the SAP message server. Get the required system ID from the SAP system to which you want to connect.
SAP Group	The name of the SAP logon group through which you want to connect. For example, PUBLIC.
SAP Username	The user name with the appropriate user authorization to connect to the SAP account.
SAP Password	The password to connect to the SAP account.
Subscriber Name	A name that defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) when you read delta data from ODP.

## Load balancing server SNC connection

Create a load balancing server SNC connection when you want to connect to the SAP system using the (SNC) protocol with the least load at run time.

Load balancing server SNC connection requires the Secure Agent PSE certificate name, SAP server PSE certificate name, and path to the X509 certificate file along with your SAP client details and message server group name.

The following table describes the basic connection properties for a load balancing server SNC connection:

Connection property	Description
SAP Client Number	The client number of the SAP message server. Get the required client number from the SAP system to which you want to connect.
SAP Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
SAP Message Server	The host name of the SAP message server.
SAP System ID	The system ID of the SAP message server. Get the required system ID from the SAP system to which you want to connect.
SAP Group	The name of the SAP logon group through which you want to connect. For example, PUBLIC.

Connection property	Description
SNC My Name	The agent PSE or certificate name generated for the Secure Agent. Default length is 256.
SNC Partner Name	The server PSE or certificate name generated on the SAP server. Default length is 256.
SNC Quality of Protection (QoP)	The level of protection applied to a communication path when you create an SAP SNC connection. Select one of the following options from the list: <ul style="list-style-type: none"> <li>- 1 - Apply authentication only</li> <li>- 2 - Apply authentication and integrity protection</li> <li>- 3 - Apply authentication, integrity, and privacy protection (encryption)</li> <li>- 8 - Apply global default protection (usually 3)</li> <li>- 9 - Apply the maximum protection</li> </ul> Default is 3 - Apply authentication, integrity, and privacy protection (encryption).
Use X509 Certificate	Method of logging in. Select <b>Use X509 Certificate</b> to log in with SNC encryption that uses the X.509 certificate. If you don't select this option, you need to enter your SAP user name in the <b>X509 Certificate Path or SAP Username</b> property. Default is disabled.
X509 Certificate Path or SAP Username	The path and file name of the X509 certificate file. If the X509 certificate file name is abc.crt and the path is \root\ <folder and="" both="" enter="" file="" following="" format:<br="" in="" name="" name&gt;,="" path="" the=""></folder> <code>\root\<folder name="">\abc.crt</folder></code> If you select to use the X509 certificate, you don't need to enter the SAP user name. If you don't want to use the X509 certificate, enter the SAP user name for which SNC is configured in the SAP server.
Subscriber Name	A name that defines the Secure Agent as a unique subscriber in the SAP system. SAP uses this name to define unique operational delta queue (ODQ) when you read delta data from ODP.

The following table describes the advanced connection properties for load balancing server SNC connection:

Property	Description
SAP Cryptographic Library Path	The path and file name of the SAP cryptographic library. Enter both the path and file name in the following format based on the operating system on which the Secure Agent runs: <ul style="list-style-type: none"> <li>- On Windows: \root\<folder name="">\sapcrypto.dll</folder></li> <li>- On Linux: /root/&lt;folder name&gt;/libsapcrypto.so</li> </ul>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Additional Parameters	<p>Additional SAP parameters that you can use when you connect to the SAP system.</p> <p>You can enter multiple additional parameters, separated by semicolon, in the following format:</p> <pre>&lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;....</pre> <p>For example, to generate SAP JCo and SAP CPIC trace files, enter the following additional parameters:</p> <pre>jco.client.trace="1";jco.client.cpic_trace="3";</pre> <p>During the run time, the SAP JCo and SAP CPIC trace files are generated in the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;\ICS\main\bin\rdtm</pre> <p>During the design time, the SAP CPIC traces are generated in the <code>tomcat.out</code> files at the following location:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;\apps \Data_Integration_Server\&lt;DIS version&gt;tomcat.out</pre>
Display Delta Fields	<p>Specifies whether the mapping displays the operation modes that caused the changed data on ODP sources.</p> <p>When enabled, the mapping generates the <code>ODQ_CHANGEMODE</code> and <code>ODQ_ENTITYCNTR</code> fields on the <b>Fields</b> tab for ODP sources that are enabled with Operational Delta Queue (ODQ).</p> <p>Default is disabled.</p>

## Hierarchical data extraction from SAP ODP objects

Before you use an SAP ODP Extractor connection to extract hierarchical data from SAP ODP objects in a Unicode SAP system, you need to install the SAP ODP Extractor transport files that you get from the Secure Agent directory to the SAP system.

### Prerequisites to install the transport files

Before you install the SAP ODP Extractor transports, make sure to perform the following prerequisite tasks:

- Ensure that the transport files you install on the SAP machines are the latest. Get the latest transport files from the following directory:  

```
<Informatica Secure Agent installation directory>\downloads\package-SAPODP.<Latest version>\package\sapodp\sap-transport
```
- Verify that the transport files are applicable for SAP version ERP 6.0 EHP7 system or later.
- Before you install the transports on your production system, install and test the transports in a development system.

The following table lists the transports that you need to install to read data from the SAP ODP objects:

Data and Cofile Names	Transport Request	Functionality
<ul style="list-style-type: none"><li>- K900426.IN7</li><li>- R900426.IN7</li></ul>	IN7K900426	<p>Install the transports only when you want to read from an SAP ODP that supports hierarchy.</p> <p>If the SAP ODP objects that do not contain hierarchical data, you can use SAP ODP Extractor Connector without installing the SAP ODP Extractor transport files.</p>

## Installing transport files

To install the SAP ODP Extractor transport files, perform the following steps:

1. Find the transport files in the following directory on the Secure Agent machine:  
`<Informatica Secure Agent installation directory>\downloads\package-SAPODP.<Latest version>\package\sapodp\sap-transport`
2. Copy the cofile transport file to the `Cofile` directory in the SAP transport management directory on each SAP machine that you want to access.  
The cofile transport file uses the following naming convention: `<number>.<sap system>`.
3. Copy the data transport file to the `Data` directory in the SAP transport management directory on each SAP machine that you want to access.  
The data transport file uses the following naming convention: `<number>.<sap-system>`.
4. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.
5. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.  
The request number inverts the order of the renamed cofile as follows: `<sap-system><number>`.
6. In the Request area of the import queue, select the transport request number that you added, and click **Import**.
7. If you want to upgrade from a previous version of the Informatica Transports, select the **Overwrite Originals** option.

# Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS or Azure to connect to the SAP system when you configure an SAP ODP Extractor connection on Linux.

You can't use the serverless runtime environment if you want to use SAP Secure Network Communication (SNC) Protocol.

Before you configure an SAP ODP Extractor connection using the serverless runtime environment, perform the following tasks:

- Add the SAP libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the `.yaml` serverless configuration file.
- Configure the `JAVA_LIBS` and `JVMClassPath` properties for the serverless runtime environment on Linux.

### Add the SAP libraries in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to configure an SAP ODP Extractor connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
<Supplementary file location>/serverless\_agent\_config
2. Add the libraries in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: <Supplementary file location>/serverless\_agent\_config/sap

### Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment, and to copy the SAP libraries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jcos:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
```

where the source path is the directory path of the SAP library files in AWS or Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as serverlessUserAgentConfig.yml in the following AWS or Azure location: <Supplementary file location>/serverless\_agent\_config  
When the .yml file runs, the SAP libraries are copied from the AWS or Azure location to the serverless agent directory.

### Configure the JAVA\_LIBS and JVMClassPath properties for the serverless runtime environment

Perform the following steps in Administrator to configure the JAVA\_LIBS and JVMClassPath properties for the serverless runtime environment on Linux:

1. Log in to Informatica Intelligent Cloud Services.
2. Select **Administrator > Serverless Environments**.
3. On the **Serverless Environments** tab, expand the Actions menu for the required serverless runtime environment, and then select **Edit**.
4. On the **Runtime Configuration Properties** tab, select **Data Integration Server** as the service.
5. Select the following **Type** and **Name**, and then enter the JAVA\_LIBS and JVMClassPath values:

Type	Name	Value
Tomcat_JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar
PMRDTM_CFG	JVMClassPath	pmserversdk.jar:../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javalib/sap/sap-adapter-common.jar

6. Click **Save**.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 203

# SAP Table Connector connection properties

Create an SAP Table Connector connection to access data directly from SAP tables and SAP ADSO objects.

You can use the SAP Table connection to read data from the following objects:

- Transparent tables
- Cluster tables
- Pool tables
- Views
- SAP ADSO

You can also use the SAP Table connection to write data to custom transparent tables.

## Prerequisites

Before you use an SAP Table connection, the SAP administrator needs to perform certain prerequisite tasks to configure the Secure Agent machine and SAP system.

To process SAP table data and read data from SAP BW/4HANA ADSO objects, you also need to verify if the required licenses are enabled for the SAP system.

## Download and configure the SAP libraries

To read data from or write data to SAP tables, you need to download and configure the SAP NetWeaver RFC SDK libraries and SAP JCo libraries on the Secure Agent machine. If you encounter any issues while you download libraries, contact SAP Customer Support.

1. Go to the [SAP Support Portal](#), and then click **Software Downloads**.

**Note:** You need to have SAP credentials to access **Software Downloads** from the [SAP Support Portal](#).

2. Download the latest version of the SAP NetWeaver RFC SDK 7.50 libraries that are specific to the operating system that hosts the Secure Agent.

The following table lists the libraries corresponding to the different operating systems:

Operating System	SAP NetWeaver RFC SDK Libraries
Linux 64	<ul style="list-style-type: none"> <li>- libicudata.so.50</li> <li>- libicui18n.so.50</li> <li>- libicuuc.so.50</li> <li>- libsapnwrfc.so</li> <li>- libsapucum.so</li> </ul>
Windows 64	<ul style="list-style-type: none"> <li>- icudt50.dll</li> <li>- icuin50.dll</li> <li>- icuuc50.dll</li> <li>- libsapucum.dll</li> <li>- sapnwrfc.dll</li> </ul>

3. Copy the SAP NetWeaver RFC SDK 7.50 libraries to the following directory:  
 <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext  
 \deploy\_to\_main\bin\rdtm  
 Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.
4. Set the following permissions for each NetWeaver RFC SDK library:
  - Read, write, and execute permissions for the current user.
  - Read and execute permissions for all other users.
5. From the [SAP Support Portal](#), download the latest version of the 64-bit SAP JCo libraries based on the operating system on which the Secure Agent runs:

Secure Agent System	SAP JCo Libraries
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

6. Copy the JCo libraries to the following directory:  
 <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext  
 \deploy\_to\_main\bin\rdtm-extra\tpl\sap  
 Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.
7. Log in to Informatica Intelligent Cloud Services and configure the JAVA\_LIBS property for the Secure Agent.
  - a. Select **Administrator > Runtime Environments**.
  - b. Click **Runtime Environments** to access the **Runtime Environments** page.
  - c. To the left of the agent name, click **Edit Secure Agent**.
  - d. From the **Service** list, select **Data Integration Server**.
  - e. From the **Type** list, select **Tomcat JRE**.



- f. Enter the JAVA\_LIBS value based on the operating system on which the Secure Agent runs.

Operating System	Value
Windows	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar
Linux	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar

**Warning:** If you copy the value directly from the table, the hyphens (-) in the value might be incorrectly copied. Copy the value to a text editor and make sure that the value you copied is not corrupted.

System Configuration Details

Service: Data Integration Server

Type: Tomcat JRE

Type	Name	Value
Tomcat JRE	JAVA_LIBS	../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adc

- g. Click **Save**.
- h. Repeat steps 2 through 7 on every machine where you installed the Secure Agent.
8. Restart the Secure Agent.

## Configure SAP user authorization

Configure the SAP user account in the SAP system to process SAP table data.

For more information about how to configure SAP user authorization in the SAP system, see [SAP user authorizations](#).

The following table describes the required authorization to read from SAP tables:

Read Object Name	Authorization
S_BTCH_JOB	DELE, LIST, PLAN, SHOW. Set Job Operation to RELE.
S_PROGRAM	BTCSUBMIT, SUBMIT
S_RFC	SYST, SDTX, SDIFRUNTIME, /INFADI/TBLRDR, RFC1
S_TABU_DIS / S_TABU_NUM	Provide SAP table name from which you want to read data.

The following table describes the required authorization to write to SAP tables:

Write Object Name	Authorization
S_RFC	/INFADI/GET_TRANSPORT_VERSION, /INFADI/ZPMW, DDIF_FIELDINFO_GET, RFC1, RFCPING, RFC_READ_TABLE
S_TABU_DIS / S_TABU_NUM	Provide SAP table name where you want to write data.

**Note:** You need to add S\_TABU\_DIS or S\_TABU\_NUM based on the version of the SAP system. For more information about S\_TABU\_DIS or S\_TABU\_NUM, see the SAP documentation.

## Install transport files to read from an SAP table

To read data from SAP tables from a Unicode SAP system, install the SAP Table Reader transport files that you get from the Secure Agent directory to the SAP system.

### Prerequisites to install the transport files

Before you install the SAP Table Reader transports, make sure to perform the following prerequisite tasks

- Ensure that the transport files you install on the SAP machines are the latest. Get the latest transport files from the following directory:  
`<Informatica Secure Agent installation directory>\downloads\package-SAPConnector.<Latest version>\package\rdtm\sap-transport\SAPTableReader`
- Verify that the transport files are applicable for SAP version ECC 5.0 or later.
- Verify that the RSODPABAPCDSVIEW table is available in SAP before you install the TABLE\_READER\_Addon transport files. If the RSODPABAPCDSVIEW table is not available, the TABLE\_READER\_Addon transport installation fails.
- Before you install the transports on your production system, install and test the transports in a development system.

The following table lists the transports that you need to install based on the SAP source type that you want to access:

Data and Cofile Names	Transport Request	Functionality
TABLE_READER_R900059.ER6 TABLE_READER_K900059.ER6	ER6K900059	To read data from SAP transparent tables, cluster tables, and pool tables, install only the TABLE_READER transport.
TABLE_READER_Addon_R900085.S4N TABLE_READER_Addon_K900085.S4N	S4NK900085	To read data from ABAP CDS views, install both the TABLE_READER and TABLE_READER_Addon transports. Use the TABLE_READER_Addon transports for SAP NetWeaver 7.50 SP4 version and later.  Whenever you install the TABLE_READER transport, you need to reinstall the TABLE_READER_Addon transport even though there is no change in the TABLE_READER_Addon transport version. <b>Note:</b> Ensure that you first install the TABLE_READER transport and only then install the TABLE_READER_Addon transport.

### Installing transport files

To install the SAP Table Reader transport files, perform the following steps:

1. Find the transport files in the following directory on the Secure Agent machine:  
`<Informatica Secure Agent installation directory>\downloads\package-SAPConnector.<Latest version>\package\rdtm\sap-transport\SAPTableReader`
2. Copy the cofile transport file to the Cofile directory in the SAP transport management directory on each SAP machine that you want to access.  
 The cofile transport file uses the following naming convention: TABLE\_READER\_K<number>.ER6.

3. Remove "TABLE\_READER\_" from the file name to rename the cofile.  
For example, for a cofile transport file named `TABLE_READER_K900059.ER6`, rename the file to `K900059.ER6`.
4. Copy the data transport file to the `Data` directory in the SAP transport management directory on each SAP machine that you want to access.  
The data transport file uses the following naming convention: `TABLE_READER_R<number>.ER6`.
5. Remove "TABLE\_READER\_" from the file name to rename the file.
6. To import the transports to SAP, in the STMS, click **Extras > Other Requests > Add** and add the transport request to the system queue.
7. In the **Add Transport Request to Import Queue** dialog box, enter the request number for the cofile transport.  
The request number inverts the order of the renamed cofile as follows: `ER6K<number>`.  
For example, for a cofile transport file renamed as `K900059.ER6`, enter the request number as `ER6K900059`.
8. In the Request area of the import queue, select the transport request number that you added, and click **Import**.
9. If you want to upgrade from a previous version of the Informatica Transports, select the **Overwrite Originals** option.

## Install transport files to write to an SAP table

To write data to SAP custom tables that have been created under the customer namespace, install the SAP Table Writer transport files.

To get and install the latest SAP Table Writer transport files, contact Informatica Global Customer Support.

## Connect to SAP table

Let's configure the SAP Table Connector connection properties to connect to SAP tables and SAP BW/4HANA ADSO objects.

### Before you begin

Before you get started, you'll need to configure the Secure Agent machine and SAP system to establish an SAP Table connection.

Check out ["Prerequisites" on page 699](#) to learn more about these tasks.

## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SAP Table Connector
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment. For more information about how to configure a serverless environment, see <a href="#">"Use the serverless runtime environment" on page 713</a> .
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Username	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Client	The client number of the SAP application server. Get the required client number from the SAP system to which you want to connect.
Application Server	The host name or IP address of the SAP application server when you read from SAP tables. If you enter the host name or IP address of the SAP application server in this field to read from SAP tables, do not enter the directory of the sapnwrfc.ini file in the <b>Saprfc.ini Path</b> field and the DEST entry in <b>Destination</b> field. <b>Note:</b> This property doesn't apply if you create the connection to write to SAP tables.
System Number	The system number of the SAP application server when you read from SAP tables. If you enter the system number of the SAP application server in this field to read from SAP tables, do not enter the directory of the sapnwrfc.ini file in the <b>Saprfc.ini Path</b> field and the DEST entry in <b>Destination</b> field. <b>Note:</b> This property doesn't apply if you create the connection to write to SAP tables.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Saprfc.ini Path	<p>The path and file name or the path to the <code>sapnwrfc.ini</code> file.</p> <p>This property is required if you want to use the connection to write to SAP tables.</p> <p>Enter the following directory where the <code>sapnwrfc.ini</code> file is available:</p> <pre>&lt;Informatica Secure Agent installation directory&gt;/apps/ Data_Integration_Server/ext/deploy_to_main/bin/rdtm</pre> <p>For the serverless runtime environment, the <code>sapnwrfc.ini</code> file is copied from the AWS location to the following serverless agent directory:</p> <pre>/data2/home/cldagnt/SystemAgent/apps/Data_Integration_Server/ext/ deploy_to_main/bin/rdtm</pre> <p>For more information about how to create the <code>sapnwrfc.ini</code> file, see <a href="#">"Configure the sapnwrfc.ini file" on page 706</a>.</p> <p>If you enter the directory of the <code>sapnwrfc.ini</code> file in this field, do not enter the host name or IP address, and system number of the SAP application server in the <b>Application Server</b> and <b>System Number</b> fields.</p>
Destination	<p>DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server.</p> <p>Use all uppercase letters for the destination.</p> <p>This property is required if you create the connection to write to SAP tables.</p> <p>If you enter the DEST entry in this field, do not enter the host name or IP address, and system number of the SAP application server in the <b>Application Server</b> and <b>System Number</b> fields.</p>
Port Range	<p>HTTP port range. The SAP Table connection uses the specified port numbers to connect to SAP tables using the HTTP protocol. Default range is 10000-65535.</p> <p>Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>
Test Streaming	<p>Tests the connection. When selected, tests the connection using both RFC and HTTP protocol. When not selected, tests connection using RFC protocol.</p>
Https Connection	<p>Connects to SAP through HTTPS protocol.</p> <p>To successfully connect to SAP through HTTPS, verify that your administrator has configured the Secure Agent machine and the SAP system.</p> <p>For more information about how to connect to SAP through HTTPS, see <a href="#">"Configure HTTPS to connect to SAP" on page 708</a>.</p>
Keystore Location	<p>Absolute path and file name of the keystore file to connect to SAP.</p> <p>Specify both the path and file name in the following format:</p> <pre>&lt;Directory&gt;/&lt;Keystore file name&gt;.jks</pre>
Keystore Password	<p>The destination password to access the keystore file.</p>

Property	Description
Private Key Password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client.</p> <p>Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the load balancing parameters listed in the following sample:</p> <pre>MSHOST=&lt;Host name of the message server&gt; R3NAME=&lt;Name of the SAP system&gt; group=&lt;Group name of the application server&gt;</pre> <p>If you configure a parameter in other connection property fields, do not enter the same parameter value in the <b>SAP Additional Properties</b> field.</p> <p>For more information about RFC-specific parameters, see the SAP documentation.</p>

## Configure the sapnwrfc.ini file

To enable the Secure Agent to connect to the SAP system as an RFC client, create and configure the `sapnwrfc.ini` file on the Secure Agent machine.

If you want to write data to SAP tables, you need to use the `sapnwrfc.ini` file.

SAP uses the communications protocol, Remote Function Call (RFC), to communicate with other systems. SAP stores RFC-specific parameters and connection information in the `sapnwrfc.ini` file.

If you are upgrading from an earlier version, you do not need to create an `sapnwrfc.ini` file. The Secure Agent copies the `sapnwrfc.ini` file to the `deploy_to_main\bin\rdtm` directory.

When you read data from or write data to SAP tables, if you define the path and file name of the `sapnwrfc.ini` file in the SAP connection, the Secure Agent uses the `sapnwrfc.ini` file. However, if you define only the path of the `sapnwrfc.ini` file in the connection, the Secure Agent first verifies if an `sapnwrfc.ini` file exists in the specified path. If the `sapnwrfc.ini` file exists, the Secure Agent uses the `sapnwrfc.ini` file. Else, an exception occurs.

To create the `sapnwrfc.ini` file, use a DOS editor or WordPad to configure the `sapnwrfc.ini` file. Notepad can introduce errors to the `sapnwrfc.ini` file.

After you create the `sapnwrfc.ini` file, copy the file to the following directory and restart the Secure Agent:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm\
```

Create the `deploy_to_main\bin\rdtm` directory if it does not already exist.

### Using the configured sapnwrfc.ini file in connections

You can use the `sapnwrfc.ini` file to configure the following types of connections:

#### Connection to an SAP application server

Create this connection to enable communication between an RFC client and an SAP system. Each connection entry specifies one application server and one SAP system.

The following sample shows a connection entry for a specific SAP application server in the `sapnwrfc.ini` file:

```
DEST=sapr3
ASHOST=sapr3
SYSNR=00
```

### Connection for SAP load balancing

Create this connection to enable SAP to create an RFC connection to the application server with the least load at run time. Use this connection when you want to use SAP load balancing.

The following sample shows a connection entry for SAP load balancing in the `sapnwrfc.ini` file:

```
DEST=sapr3
R3NAME=ABV
MSHOST=infamessageserver.informatica.com
GROUP=INFADEV
```

### Connection to an RFC server program registered at an SAP gateway

Create this connection to connect to an SAP system from which you want to receive outbound IDocs.

The following sample shows a connection entry for an RFC server program registered at an SAP gateway in the `sapnwrfc.ini` file:

```
DEST=sapr346CLSQA
PROGRAM_ID=PID_LSRECEIVE
GWHOST=sapr346c
GWSERV=sapgw00
```

You can configure the following parameters in the `sapnwrfc.ini` file for various connection types:

<b>sapnwrfc.ini Parameter</b>	<b>Description</b>	<b>Applicable Connection Types</b>
DEST	Logical name of the SAP system for the connection. All DEST entries must be unique. You need to have only one DEST entry for each SAP system. For SAP versions 4.6C and later, use up to 32 characters. For earlier versions, use up to eight characters.	Use this parameter for the following types of connections: - Connection to a specific SAP application server - Connection to use load balancing - Connection to an RFC server program registered at an SAP gateway
ASHOST	Host name or IP address of the SAP application. The Secure Agent uses this entry to attach to the application server.	Use this parameter to create a connection to a specific SAP application server.
SYSNR	SAP system number.	Use this parameter to create a connection to a specific SAP application server.
R3NAME	Name of the SAP system.	Use this parameter to create a connection to use SAP load balancing.
MSHOST	Host name of the SAP message server.	Use this parameter to create a connection to use SAP load balancing.
GROUP	Group name of the SAP application server.	Use this parameter to create a connection to use SAP load balancing.

sapnwrfc.ini Parameter	Description	Applicable Connection Types
PROGRAM_ID	Program ID. The Program ID must be the same as the Program ID for the logical system that you define in the SAP system to send or receive IDocs.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWHOST	Host name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
GWSERV	Server name of the SAP gateway.	Use this parameter to create a connection to an RFC server program registered at an SAP gateway.
TRACE	Debugs RFC connection-related problems. Set one of the following values based on the level of detail that you want in the trace: <ul style="list-style-type: none"> <li>- 0. Off</li> <li>- 1. Brief</li> <li>- 2. Verbose</li> <li>- 3. Full</li> </ul>	Use this parameter for the following types of connections: <ul style="list-style-type: none"> <li>- Connection to a specific SAP application server</li> <li>- Connection to use load balancing</li> <li>- Connection to an RFC server program registered at an SAP gateway</li> </ul>

The following snippet shows a sample `sapnwrfc.ini` file:

```

/*=====*/
/* Connection to an RFC server program registered at an SAP gateway */
/*=====*/
DEST=<destination in RfcRegisterServer>
PROGRAM_ID=<program-ID, optional; default: destination>
GWHOST=<host name of the SAP gateway>
GWSERV=<service name of the SAP gateway>
*=====*/
/* Connection to a specific SAP application server */
/*=====*/
DEST=<destination in RfcOpenConnection>
ASHOST=<Host name of the application server.>
SYSNR=<The back-end system number.>
/*=====*/
/* Connection to use SAP load balancing */
/* The application server will be determined at run time. */
/*=====*/
DEST=<destination in RfcOpenConnection>
R3NAME=<name of SAP system, optional; default: destination>
MSHOST=<host name of the message server>
GROUP=<group name of the application servers, optional; default: PUBLIC>

```

## Configure HTTPS to connect to SAP

To connect to SAP through HTTPS and read SAP table sources, you need the OpenSSL certificate in the Secure Agent machine and the SAP system.

Create an OpenSSL certificate in the Secure Agent machine. Then, import the created certificate in the PSE format to the SAP system truststore.

To enable HTTPS in an SAP Table connection, you also need to specify the generated keystore password and private key password of the keystore file in the SAP system from transaction code SAP ICM Monitor (SMICM).



## Create an OpenSSL certificate

Before you create an OpenSSL certificate, you need to perform the prerequisite tasks.

- Download and install OpenSSL on the Secure Agent machine.
- Based on the operating system of the machine that hosts the Secure Agent and the SAP system, download the latest available patch of the SAPGENPSE Cryptography tool from the SAP Service Marketplace.  
By default, the SAPGENPSE files are extracted to the `nt-x86_64` directory.
- Configure the following SAP parameters: `icm/server_port`, `ssl/ssl_lib`, `sec/libsapsecu`, `ssf/ssfapi_lib`, `ssf/name`, `icm/HTTPS/verify_client`, `ssl/client_pse`, and `wdisp/ssl_encrypt`.  
For more information, see the SAP documentation.

To create a self-signed certificate using OpenSSL, perform the following tasks:

1. From the command line, set the `OPENSSL_CONF` variable to the absolute path to the `openssl.cfg` file.  
For example, run the following command: `set OPENSSL_CONF= C:\OpenSSL-Win64\bin\openssl.cfg`
2. Navigate to the `<openssl installation directory>\bin` directory.
3. To generate a 2048-bit RSA private key, run the following command:  
`openssl.exe req -new -newkey rsa:2048 -sha1 -keyout <RSAkey File_Name>.key -out <RSAkey File_Name>.csr`
4. When prompted, enter the following values:
  - Private key password (PEM pass phrase). Enter a phrase that you want to use to encrypt the secret key. Re-enter the password for verification.  
**Important:** Make a note of this PEM password. You need to keep this password handy while creating a self-signed key and PKCS#12 certificate.
  - Two-letter code for country name.
  - State or province name.
  - Locality name.
  - Organization name
  - Organization unit name.
  - Common name (CN). Mandatory.  
**Important:** Enter the fully qualified host name of the machine that hosts the Secure Agent.
  - Email address.
5. Optionally, enter the following attributes that you want to pass along with the certificate request:
  - Challenge password.
  - Optional company name.

A RSA private key of 2048-bit size is created. The `<RSAkey File_Name>.key` and `<RSAkey File_Name>.csr` files are generated in the specified directory.
6. To generate a self-signed key using the RSA private key, run the following command:  
`openssl x509 -req -days 11499 -in <RSAkey File_Name>.csr -signkey <RSAkey File_Name>.key -out <Certificate File_Name>.crt`
7. When prompted, enter the PEM pass phrase for the RSA private key.  
The `<Certificate File_Name>.crt` file is generated in the specified directory.

8. To concatenate the contents of the `<Certificate File_Name>.cert` file and the `<RSAkey File_Name>.key` file to a `.pem` file, perform the following tasks:
  - a. Open the `<Certificate File_Name>.cert` file and the `<RSAkey File_Name>.key` files in a Text editor.
  - b. Create a file and save it as `<PEM File_Name>.pem`.
  - c. Copy the contents of the `<Certificate File_Name>.cert` file and paste it in the `.pem` file.
  - d. Copy the contents of the `<RSAKey_Name>.key` file and append it to the existing contents of the `.pem` file.
  - e. Save the `<PEM file name>.pem` file.
9. To create a PKCS#12 certificate, run the following command from the command line:
 

```
openssl pkcs12 -export -in <PEM File_Name>.pem -out <P12 File_Name>.p12 -name "domain name"
```
10. When prompted, enter the following details:
  - The PEM pass phrase for the `.pem` file.
  - An export password for the P12 file. Re-enter the password for verification.
 

**Important:** Make a note of this export password for the P12 file. You need to keep this password handy while creating a Java keystore file to connect to SAP through HTTPS.

The `<P12 File_Name>.p12` file is generated in the specified directory.
11. To create a Java keystore file, enter the following command:
 

```
keytool -v -importkeystore -srckeystore <P12 File_Name>.p12 -srcstoretype PKCS12 -destkeystore <JKS File_Name>.jks -deststoretype JKS -srcalias "source alias" -destalias "destination alias"
```
12. When prompted, enter the following details:
  - Password for the destination keystore, the JKS file.
 

**Important:** Make a note of this password. You need to keep this password handy while creating an SAP Table connection.
  - Password for the source keystore, the P12 file. Enter the Export password for the P12 file.

The `<JKS File_Name>.jks` file is generated in the specified directory.

While enabling HTTPS in an SAP Table connection, specify the name and location of this keystore file. You also need to specify the destination keystore password as the Keystore Password and the source keystore password as the Private Key Password.

## Convert an OpenSSL certificate to PSE format

After you create an OpenSSL certificate, you need to convert the OpenSSL certificate to PSE format using the SAPGENPSE tool.

1. From the command line, navigate to the `<SAPGENPSE Extraction Directory>` directory.
2. To generate a PSE file, run the following command:
 

```
sapgenpse import_p12 -p <PSE_Directory>\<PSE File_Name>.pse <P12 Certificate_Directory>\<P12 File_Name>.p12
```
3. When prompted, enter the following details:
  - Password for the P12 file. Enter the Export password for the P12 file.
  - Personal identification number (PIN) to protect the PSE file. Re-enter the PIN for verification.

The `<PSE File_Name>.pse` file is generated in the specified directory.

4. To generate the certificate based on the PSE format, run the following command:  

```
sapgenpse export_own_cert -p <PSE File Directory>\<PSE File Name>.pse -o  
<Certificate_Name>.cert
```
5. When prompted, enter the PSE PIN number.  
The <Certificate\_Name>.cert file is generated in the specified directory. Import this certificate file to the SAP system trust store.

## Enable the HTTPS service on the SAP system

To configure HTTPS to connect to an SAP system, you need to enable the HTTPS service from the transaction code SAP ICM Monitor (SMICM) in the SAP system

For more information about how to enable the HTTPS service on the SAP system, see the SAP documentation.

## Import the certificate to the SAP system trust store

You need to import the certificate in PSE format to the SAP system trust store to connect to SAP through HTTPS.

1. Log in to SAP and go to the STRUST transaction.
2. Select SSL Client (Standard) and specify the password.  
In the **Import Certificate** dialog, you need to select Base64 format as the certificate file format.
3. Click the **Import** icon, and select the <Certificate\_Name>.cert file in PSE format.  
**Note:** If a user is on a different SAP network, you might need to add a DNS entry of the agent host on the SAP app server.
4. Click **Add to Certificate List**.
5. Restart the Internet Communication Manager (ICM).

# Configure the Secure Network Communication protocol

You can use the SAP Table Connector connection with the Secure Network Communication Protocol to securely read from or write to SAP.

For more information about the steps to configure an SAP SNC connection, see [Configure the SAP Secure Network Communication protocol](#) Informatica How-To Library article.

# Enable the Secure Agent to operate as a whitelisted host in SAP (Optional)

You can enable the Secure Agent to operate as a whitelisted host when you read SAP table data. Before you enable the Secure Agent as a whitelisted host, verify that the latest transport files are installed.

1. To configure the **JVMOption** property in Administrator to define the Secure Agent as a host that you can add in the HTTP\_Whitelist table of the SAP system, perform the following steps:
  - a. Select **Administrator > Runtime Environments**.
  - b. On the **Runtime Environments** page, select the Secure Agent machine that runs the mapping.
  - c. Click **Edit**.
  - d. In the **System Configuration Details** section, from the **Service** list, select **Data Integration Server**.
  - e. Edit any **JVMOption** field to add the following value:  
`-Dsap_whitelist_check=1`
  - f. Click **Save**.
  - g. Repeat steps b through f for every Secure Agent that you want to define as a host in SAP.
2. Create an entry for the Secure Agent in the SAP HTTP\_Whitelist table using the transaction SE16. To create an entry for the Secure Agent, perform the following steps in the SAP system:
  - a. Go to transaction SE16.
  - b. Configure properties to define the Secure Agent as a host in SAP.  
The following table describes the properties that you need to configure:

Property	Description
MANDT	Required. SAP client number.
ENTRY TYPE	Required. URL type to be compared with this entry. Enter <b>01</b> to indicate that the URL is a CSS theme URL.
SORT KEY	Required. Unique value to be used as the primary key. You can enter numbers and alphabets.
PROTOCOL	Protocol that SAP must validate. Enter <b>HTTP</b> or <b>HTTPS</b> . If you do not enter a value, SAP does not validate the protocol.
HOST	Host machine that SAP must validate. Enter the IP address of the machine that hosts the Secure Agent.
PORT	Port number that SAP must validate. Leave the <b>Port</b> field blank to indicate that SAP does not need to validate the port.
URL	URL that SAP must validate. Enter <b>*</b> to indicate that SAP does not need to validate the URL.

**Note:** If you do not perform step 2, mappings and tasks that run on SAP fail.

3. Repeat steps 1 and 2 for every Secure Agent that you want to configure as a whitelisted host in SAP.

# Use the serverless runtime environment

You can use a serverless runtime environment hosted on AWS to connect to the SAP system when you configure an SAP Table Connector connection on Linux.

You can't use the serverless runtime environment if you want to use SAP Secure Network Communication (SNC) Protocol.

Before you configure an SAP Table Connector connection using the serverless runtime environment, perform the following tasks:

- Add the SAP libraries in the Amazon S3 bucket in your AWS account.
- Configure the .yaml serverless configuration file.
- Configure the JAVA\_LIBS property for the serverless runtime environment on Linux.

## Add the SAP libraries in the Amazon S3 bucket in your AWS account

Perform the following steps to configure an SAP Table Connector connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS: <Supplementary file location>/serverless\_agent\_config
2. Add the SAP libraries in the Amazon S3 bucket in the following location in your AWS account: <Supplementary file location>/serverless\_agent\_config/sap

## Configure the .yaml serverless configuration file

Perform the following steps to configure the .yaml serverless configuration file in the serverless runtime environment, and to copy the SAP libraries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  dataIntegrationServer:
    autoDeploy:
      sap:
        jcos:
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
          - fileCopy:
              sourcePath: sap/jco/<sapjco_library_filename>
        nwrfs:
          - fileCopy:
              sourcePath: sap/nwrfs/<rfs_library_filename>
          - fileCopy:
              sourcePath: sap/nwrfs/<sapnwrfs_filename>
```

where the source path is the directory path of the SAP library files in AWS.

2. Ensure that the syntax and indentations are valid, and then save the file as serverlessUserAgentConfig.yaml in the following AWS location: <Supplementary file location>/serverless\_agent\_config  
When the .yaml file runs, the SAP libraries are copied from the AWS location to the serverless agent directory.

## Configure the JAVA\_LIBS property for the serverless runtime environment

Perform the following steps in Administrator to configure the JAVA\_LIBS property for the serverless runtime environment on Linux:

1. Log in to Informatica Intelligent Cloud Services.

2. Select **Administrator > Serverless Environments**.
3. On the **Serverless Environments** tab, expand the Actions menu for the required serverless runtime environment, and then select **Edit**.
4. On the **Runtime Configuration Properties** tab, select **Data Integration Server** as the service and **Tomcat\_JRE** as the type.
5. Click **Add Property**.
6. Enter JAVA\_LIBS in the **Name** field and set the following value:  
`../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javajlib/sap/sap-adapter-common.jar`
7. Click **Save**.

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## Troubleshooting an SAP Table connection

The following error displays when I test an SAP Table connection:

```
Test Connection Failed for <connection name>/sap/conn/jco/JCoException
```

Verify that the sapjco3.jar is saved to the following directory:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Restart the Secure Agent after you copy the sapjco3.jar.

The following error displays when I test an SAP Table connection or use the connection in a task:

```
Test Connection Failed for <connection name>. Error getting the version of the native
layer: java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.
```

Verify that the location of the sapjco3.dll file is in the to PATH variable for the Secure Agent machine.

The following error displays when I test an SAP Table connection or use the connection in a task:

```
Test Connection Failed for <connection name>. Error getting the version of the native
layer: java.lang.UnsatisfiedLinkError: no sapjco3 in java.library.path.
```

Add the location of sapjco3.dll to PATH variable and restart the Secure Agent.

A task that reads from SAP tables fails with the following error:

```
Error occurred processing data from SAP : Unable to establish Http Communication between
SAP server and agent! Shutting down reader.
```

The HTTP port is not open or the incoming request is blocked by Windows Firewall. To resolve the issue, in Windows Firewall, use the advanced settings to create a new incoming rule. Apply the rule to TCP and all ports, and choose the HTTP-In protocol.

## CHAPTER 204

# SAS connection properties

When you create a SAS connection, you must configure the connection properties.

The following table describes the SAS connection properties:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * ( ) - + = { }   \ ; " ' < , > . ? /
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Type	The <b>SAS</b> connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent runtime environment.
Host	Host name of the machine that runs the SPI Server.
Port	Port number of the machine that runs the SPI Server.
User Name	User name specified in the SPI Server configuration.
Password	Password for the user.

## CHAPTER 205

# Satmetrix connection properties

When you set up a Satmetrix connection, you must configure the connection properties.

The following table describes the Satmetrix connection properties:

Connection property	Description
Connection Name	Name of the Satmetrix connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select the Satmetrix connection.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Satmetrix URL	The URL with which the Secure Agent connects to the Satmetrix APIs. The URL has the following format: <i>http://&lt;company name&gt;.satmetrix.com</i>
Username	Username of the Satmetrix integration user account.
Password	Password of the Satmetrix integration user account.



## CHAPTER 206

# Sequential File connection properties

When you configure a Sequential File connection, you must set the connection properties.

The following table describes the Sequential File connection properties:

Property	Description
Connection Name	A name for the sequential file connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the sequential file connection. Maximum length is 4000 characters.
Type	Type of connection. For sequential files, the type must be <b>Sequential File</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for sequential file runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.

Property	Description
Offload Processing	<p>Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are:</p> <ul style="list-style-type: none"> <li>- <b>Auto.</b> Cloud Data Integration determines whether to use offload processing.</li> <li>- <b>Filter After.</b> Offloads the bulk data processing to the target, including the filtering of data.</li> <li>- <b>Filter Before.</b> Offloads processing to the target but continues to filter data on the source system.</li> <li>- <b>No.</b> Disables offload processing.</li> </ul> <p>Default is No.</p>
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data. For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs. Valid values are 1 through 64. Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For VSAM data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions. For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size. Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>

Property	Description
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre data-bbox="500 453 954 478">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of \$&lt;ParameterName&gt;, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="500 768 1398 873" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the “Connection overrides reference” chapter.</p>
Write Properties	<p>Write Mode. Options are:</p> <ul data-bbox="500 968 1406 1094" style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

# CHAPTER 207

## ServiceNow connection properties

Create a ServiceNow connection to securely read data from or write data to ServiceNow.

### Connect to ServiceNow

Let's configure the ServiceNow connection properties to connect to ServiceNow.

#### Before you begin

Before you configure the connection properties, you'll need to get the user name, password, and service URL from your ServiceNow account.

The following video shows you how to get the information you need:



#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	ServiceNow

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Do not use a Hosted Agent if you use the connection in mappings in advanced mode.</p>
Username	User name of the ServiceNow instance.
Password	Password for the ServiceNow instance.
EndPoint URL	The ServiceNow endpoint URL.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Instance Type	Type of ServiceNow instance. Select JSONv2.

## Firewall Configuration

If your organization uses a protective firewall, include the Secure Agent IP address ranges on the list of approved IP addresses to ensure that the Secure Agent can perform all the necessary tasks through the firewall.

The Secure Agent uses the following IP address ranges:

- 209.34.91.0-255
- 206.80.52.0-255
- 206.80.61.0-255
- 209.34.80.0-255

# Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use only the unauthenticated proxy server. You can configure proxy both in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the proxy server properties in the proxy.ini file.

When you use a serverless runtime environment, you cannot use a proxy server to connect to Informatica Intelligent Cloud Services.

Contact your network administrator for the correct proxy settings.

## Configure proxy server through proxy.ini file

To enable the proxy server, configure the Secure Agent through the proxy.ini file.

1. Navigate to the following directory on the Secure Agent machine: <Secure Agent installation directory>\Informatica Cloud Secure Agent\apps\agentcore\conf\proxy.ini
2. Add the host and port number of the proxy server in the proxy.ini file:

```
InfAgent.ProxyHost=<Proxy server hostname>
InfAgent.ProxyPort=<Proxy server port number>
```
3. Restart the Secure Agent.

# Test a ServiceNow connection

To verify if you can connect to ServiceNow, open any REST or SOAP client and test the connection. It is recommended that you use the following [SOAP URL](#) and test the REST, JSON, JSONv2, or SOAP endpoints.

You need to use the user credentials that has the SynQ\_User\_Role or the name that you specify for the role.

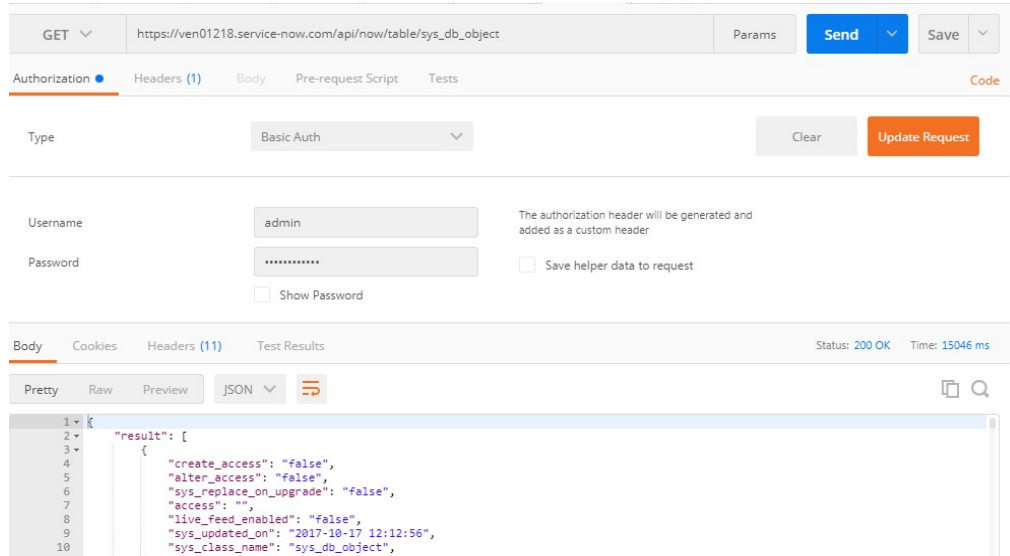
### Verify the connection status

To verify the connection status, call the REST API from any REST client.

Before you make a call to the API, ensure that you have set up the user, group, and role:

```
Purpose : Testing Connection with ServiceNow
URL :https://<instance>.service-now.com/api/now/table/sys_user
Authentication: Basic
```

If you set the appropriate roles, you will get a response similar to the following image:

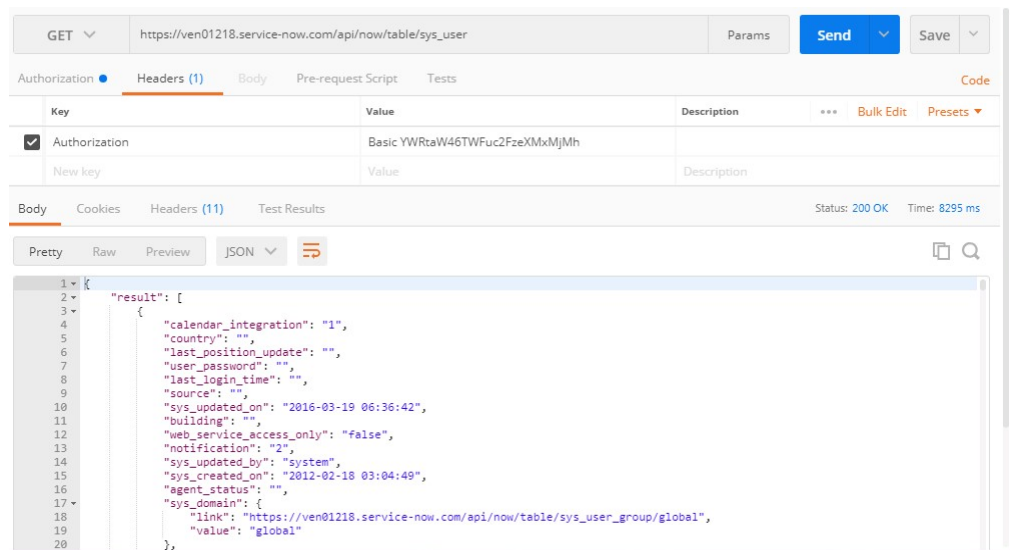


If you do not get the expected results, verify the user credentials and ServiceNow ACLs.

### Verify the credentials

To verify if the ACL and user settings are correct, call the REST API from a REST client.

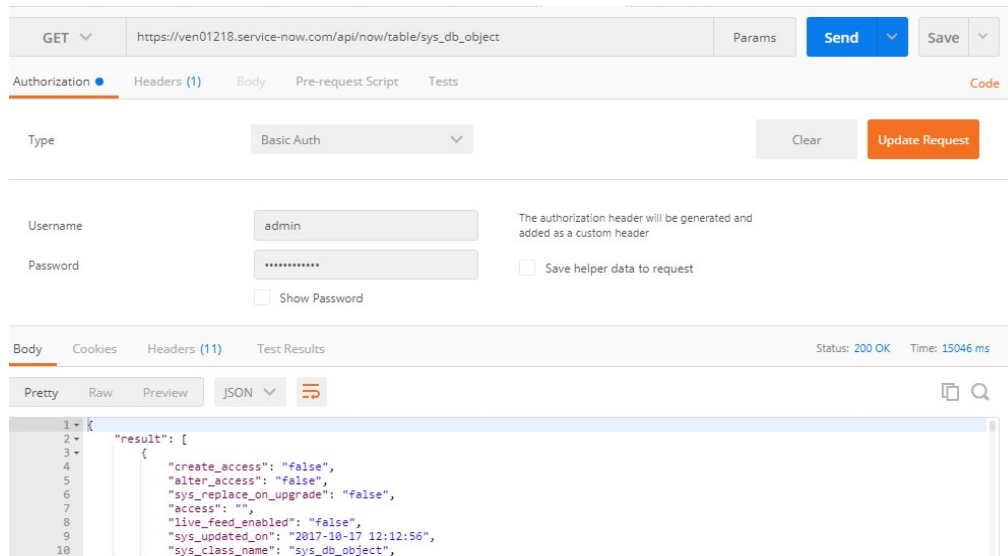
The following image shows an example of a GET request validation from a REST Client:



To create a successful connection with Data Integration, verify the credentials and ACLs with the following API:

API URL :https://<instance>.service-now.com/api/now/table/sys\_db\_object  
 Authentication:Basic

The following image shows an example of a GET request validation from a REST Client:



### Test the APIs

If you have access to read data from or write data to ServiceNow, test the APIs for metadata information.

- Test the following APIs if you can access the metadata:
  - `https://<instance>.service-now.com/api/now/table/sys_db_view.do`
  - `https://<instance>.service-now.com/api/now/table/sys_db_object.do`
  - `https://<instance>.service-now.com/api/now/table/<table_name>.do?SCHEMA`
- Test the SOAP and REST APIs to read from the ServiceNow tables or views.
- You can test the ACL and user-role setup using the REST clients. To test using a REST client, you require a valid REST API URL, the suitable methods, valid parameters, and authentication. For example, call a REST API to get data from a ServiceNow table. Use the following details to make a REST call:

```
Authentication : Basic (Requires username /password of user who is having
SynQ_User_Role)
Method : Get
URL : valid api url
```

For more information about the REST API URLs and parameters, see [Getting Started](#) in the ServiceNow documentation.



## CHAPTER 208

# ServiceNow Mass Ingestion connection properties

When you set up a ServiceNow Mass Ingestion connection, you must configure the connection properties.

The properties of a ServiceNow Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **OAuth 2.0:** Authenticates the connection by using the details of the OAuth API endpoint that is created for the connection in ServiceNow. To use this method, you must create OAuth API endpoint in ServiceNow and then specify the client ID and client secret of the API endpoint in the connection properties. For more information about creating an OAuth API endpoint in ServiceNow, see the [ServiceNow documentation](#).
- **Basic:** Authenticates the connection by validating the login credentials of the ServiceNow account.

### Connection properties for OAuth 2.0 authentication

The following table describes the connection properties for a ServiceNow Mass Ingestion connection configured with OAuth 2.0 authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>ServiceNow Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the ServiceNow account.
Password	Password for the ServiceNow account.
Client Secret	Client secret of the API endpoint created for the connection in ServiceNow.

Connection property	Description
Client ID	Client ID of the API endpoint created for the connection in ServiceNow.
Base URI	URL of the ServiceNow instance. You must enter the base URI in the following format: <code>https://{your_servicenow_instance}.service-now.com/</code>
OAuth Token URL	OAuth token endpoint of the ServiceNow instance. The API client associated with the connection sends the access token requests to this endpoint.

### Connection properties for Basic authentication

The following table describes the connection properties for a ServiceNow Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>ServiceNow Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
User Name	User name of the ServiceNow account.
Password	Password for the ServiceNow account.
Base URI	URL of the ServiceNow instance. You must enter the base URI in the following format: <code>https://{your_servicenow_instance}.service-now.com/</code>

# CHAPTER 209

## Shopify connection properties

Create a Shopify connection to read data from Shopify.

### Connect to Shopify

Let's configure a Shopify connection to read data from Shopify.

#### Before you begin

Before you configure the connection properties, you'll need to get the shop name and Shopify access token from your Shopify account.

The following video shows you how to get the information you need:



#### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Shopify

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Specify a Secure Agent or a Hosted Agent.</p>
Shop Name	<p>The store name that you specify when you create a Shopify account.</p> <p>For example, if the Shopify URL is <code>https://Example.myshopify.com</code>, your shop name is Example.</p>
Shopify Access Token	<p>The access token to authenticate access and make requests to the Shopify API.</p>

## CHAPTER 210

# Snowflake connection properties

When you set up a Snowflake connection, you must configure the connection properties.

The following table describes the Snowflake connection properties:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Username	The user name to connect to Snowflake account.
Password	The password to connect to Snowflake account.
Account	The name of the Snowflake account. In the Snowflake URL, your account name is the first segment in the domain. For example, <code>123abc</code> is your account name in <code>https://123abc.snowflakecomputing.com</code> .
Warehouse	The Snowflake warehouse name. You must specify the warehouse name.
Role	The Snowflake role assigned to user.

Connection property	Description
Additional JDBC URL Parameters	<p>The additional connection parameters. You can specify one or more parameters in the following format:</p> <pre data-bbox="495 422 1154 443">&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</pre> <p>For example:</p> <pre data-bbox="495 501 1045 522">user=jon&amp;warehouse=mywh&amp;db=mydb&amp;schema=public</pre> <p>To override the database and schema name used to create temporary tables in Snowflake, enter the database and schema name in the following format:</p> <pre data-bbox="495 613 1170 634">ProcessConnDB=&lt;DB name&gt;&amp;ProcessConnSchema=&lt;schema_name&gt;</pre> <p>To access Snowflake through Okta SSO authentication, enter the web-based IdP implementing SAML 2.0 protocol in the following format:</p> <pre data-bbox="495 724 1170 745">authenticator=https://&lt;Your_Okta_Account_Name&gt;.okta.com</pre> <p><b>Note:</b> Microsoft ADFS is not supported.</p> <p>For more information about configuring Okta authentication, see the following website:  <a href="https://docs.snowflake.net/manuals/user-guide/admin-security-fed-auth-configure-snowflake.html#configuring-snowflake-to-use-federated-authentication">https://docs.snowflake.net/manuals/user-guide/admin-security-fed-auth-configure-snowflake.html#configuring-snowflake-to-use-federated-authentication</a></p>
Database/Schema	<p>The Snowflake database and schema name. Specify the parameters in the following format:</p> <pre data-bbox="495 949 850 970">&lt;database name&gt;/&lt;schema name&gt;</pre> <p><b>Note:</b> You must specify both the database and schema name. If you specify only the database name, source objects do not appear in the Select Source Object window. If you specify only the schema name, an <code>Invalid Schema</code> exception occurs while reading data.</p>

## CHAPTER 211

# Snowflake Data Cloud connection properties

Create a Snowflake Data Cloud connection to securely read data from or write data to Snowflake.

## Prepare for authentication

You can configure standard, authorization code, key pair, and client credentials authentication types to access Snowflake.

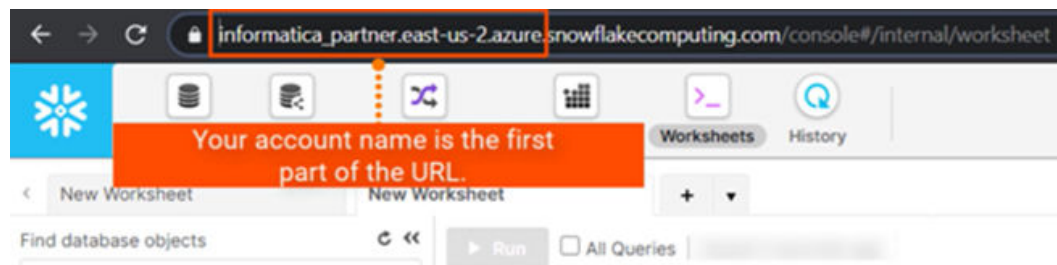
Before you configure the connection properties, you need to keep the authentication details handy based on the authentication type that you want to use.

### Standard

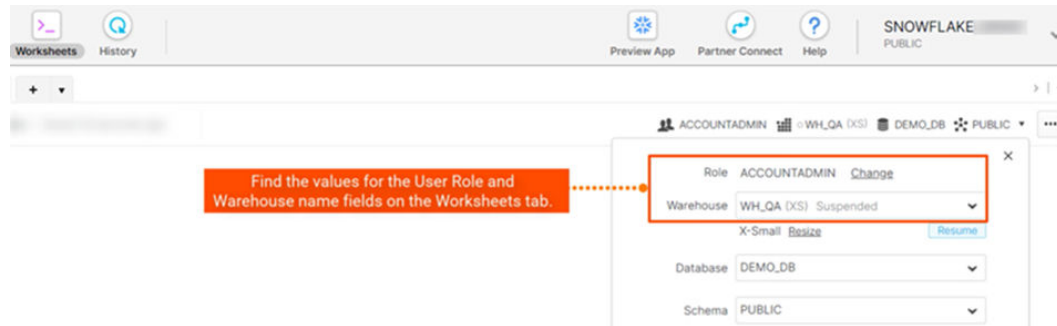
To connect to Snowflake using standard authentication, you need the Snowflake account user name and password.

Let's get the required details such as the Snowflake account name, warehouse, and role details from the Snowflake account.

The following image shows you where you can find the name of your Snowflake account:



The following image shows you where you can find the name of the warehouse and role details of your Snowflake account:



## Authorization code

To connect to Snowflake using the OAuth 2.0 authorization code, you need the Snowflake client ID, authorization URL, access token URL, and access token.

To get the authorization details, you need to create an authorization integration in Snowflake, and register the Informatica redirect URL in Security Integration. Security Integration is a type of integration that enables clients that support OAuth to redirect users to an authorization page and generate access tokens, and optionally, refresh tokens to access Snowflake.

Register the following Informatica redirect URL in Security Integration:

```
https://<Informatica cloud hosting facility for your organization>/ma/proxy/oauthcallback
```

If the access token expires, Informatica redirect URL, which is outside the customer firewall, tries to connect to the endpoint and retrieves a new access token.

For more information about how to create a security integration and get the authorization details, see [Create security integration](#) in the Snowflake documentation.

**Note:** You can't use connections configured with the authorization code authentication in mappings configured in advanced mode.

## Key pair

To connect to Snowflake using key pair authentication, you need the private key file and private key file password, along with your Snowflake account user name.

Generate the public and private key pair using OpenSSL. The key pair authentication method requires a 2048-bit RSA key pair. Specify the path to the private key file and password in the connection properties to access Snowflake.

### Generate the public and private key

Before you generate the public and private key for key pair authentication, you need to have the security admin role or higher in Snowflake.

1. From the OpenSSL command line, generate a private key:

- To generate a decrypted private key, run the following command, and provide a passphrase when prompted:

```
$ openssl genrsa 2048 | openssl pkcs8 -topk8 -inform PEM -out rsa_key.p8 -nocrypt
```



- To generate an encrypted private key, run the following command, and provide a passphrase when prompted:

```
$ openssl genrsa 2048 | openssl pkcs8 -topk8 -inform PEM -out rsa_key.p8
```

The passphrase is used to encrypt the private key file while connecting to Snowflake.

2. Generate the public key. Run the following command and specify the encrypted private key located in the file, for example, `rsa_key.p8`:

```
openssl rsa -in rsa_key.p8 -pubout -out rsa_key.pub
```

3. Copy the public and private key files in a directory that the Secure Agent can access.

For example, `C:\Program Files\Informatica Cloud Secure Agent\apps\Data_Integration_Server\data\snowflake\rsa_key.p8`

You require the path details when you configure the Snowflake connection.

4. In Snowflake, assign the public key to the Snowflake user using the ALTER USER command:

```
alter user <user> set rsa_public_key='<content of the public key
after removing the header and footer lines>';
```

For example, `alter user jsmith set rsa_public_key='MIIXBIjABCdef...';`

For more information about configuring a key pair authentication for Snowflake, see the Snowflake documentation.

## Configure the private key on an advanced cluster

After you generate the public and private key pair using OpenSSL, you need to additionally perform certain tasks for the connection to work in a mapping in advanced mode.

Before you run mappings with the configured connection on an advanced cluster, set the properties for the cluster application in the mapping task.

The following list describes the properties that you need to set in the advanced session properties in a mapping task:

### **Spark.NeedUserCredentialFileForAdapter=true**

Copies the contents of the private key from the location you specify in `Spark.UserCredentialDirOnDIS` from the Secure Agent machine to the Spark driver and executors. The folder that contains the credential file does not have the 1 MB limit. You need to ensure that the credential file of the secret key content that you copy to the cluster application does not exceed 1 MB. You need to set the value to true. Default is false.

If you do not set this flag or you set this flag to false, the private key file is not copied to the cluster application and the mapping fails.

### **Spark.UserCredentialDirOnDIS=<private key file directory>**

Overrides the default Secure Agent directory that contains the private key with the directory that you specify for copying the private key contents to the cluster application. The default directory is `/infa/user/credentials`. Ensure that the directory does not include the private key file name.

If you do not set this flag, the default location is used. To use the default location, create the `/infa/user/credentials` directory on the Secure Agent machine and copy the private key file here.

If you set the flag to override the location specified in the advanced session properties of the mapping task, make sure that the override location that you specify in `Spark.UserCredentialDirOnDIS` contains the private key file. Ensure that the override location and the private key file have the write permissions.

The following image shows the configured advanced custom property in the mapping task:

Session Property Name	Session Property Value
advanced.custom.property	Spark.NeedUserCredentialFileForAdapter=true&Spark.UserCredentialDirOnDIS=/cldagnt/pvtKey

## Client credentials

To connect to Snowflake using OAuth 2.0 client credentials, you need your Snowflake client ID, access token URL, client secret, scope, and the access token.

Configure the OAuth endpoint with the client credentials grant type and then create a security integration to get the authorization details.

Before you use the client credentials authentication to connect Snowflake, the organization administrator needs to perform the prerequisite tasks.

1. Create a client application that is compatible with OAuth to use with Snowflake.
2. Configure the authorization server with the client credentials Grant type.
3. Create a security integration of type OAuth in Snowflake.

For more information about how to create a security integration and get the authorization details, see [Create security integration for external OAuth](#) in the Snowflake documentation.

**Note:** You can't use connections configured with the client credentials authentication in mappings configured in advanced mode.

## Connect to Snowflake

Let's configure the Snowflake Data Cloud connection properties to connect to Snowflake.

### Before you begin

Before you get started, you'll need to get information from your Snowflake account based on the authentication type that you want to configure.

Check out [“Prepare for authentication” on page 731](#) to learn more about the authentication prerequisites.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Snowflake Data Cloud

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in <i>Runtime Environments</i> in the Administrator help.</p> <p>For more information about how to configure a serverless environment with key pair authentication, see <a href="#">"Use the serverless runtime environment with key pair authentication" on page 745</a>.</p> <p>Do not use a Hosted Agent if you use the connection in mappings in advanced mode.</p> <p>You cannot run application ingestion tasks and database ingestion tasks on a Hosted Agent or serverless runtime environment.</p>

## Authentication types

You can configure standard, authorization code, key pair, and client credentials authentication types to access Snowflake.

Select the required authentication method and then configure the authentication-specific parameters.

### Standard authentication

Standard authentication is the default type which requires at a minimum your Snowflake account name and password.

The following table describes the basic connection properties for standard authentication:

Property	Description
Username	The user name to connect to the Snowflake account.
Password	The password to connect to the Snowflake account.

Property	Description
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code>.</p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.

## Advanced settings

The following table describes the advanced connection properties for standard authentication:

Property	Description
Role	The Snowflake role assigned to the user.
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&amp;), in the following format:</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;...</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&amp;schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p> <p>For the list of additional JDBC parameters that you can configure, see <a href="#">"JDBC URL parameters" on page 742</a>.</p>

## Authorization code authentication

OAuth 2.0 authentication requires the OAuth 2.0 protocol with Authorization Code grant type to connect to Snowflake. Authorization Code allows authorized access to Snowflake without the need to share or store your login credentials.

The following table describes the basic connection properties for OAuth 2.0 authorization code authentication:

Property	Description
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#</code>, your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard</code>, your account name is <code>123abc.us-east-2.aws</code>.</p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.
Authorization URL	<p>The Snowflake server endpoint that is used to authorize the user request.</p> <p>The authorization URL is <code>https://&lt;account name&gt;.snowflakecomputing.com/oauth/authorize</code>, where <code>&lt;account name&gt;</code> specifies the full name of your account provided by Snowflake.</p> <p>For example, <code>https://&lt;abc&gt;.snowflakecomputing.com/oauth/authorize</code></p> <p><b>Note:</b> If the account name contains underscores, use the alias name.</p> <p>You can also use the Authorization Code grant type that supports the authorization server in a Virtual Private Cloud network.</p>
Access Token URL	<p>The Snowflake access token endpoint that is used to exchange the authorization code to get an access token.</p> <p>The access token URL is <code>https://&lt;account name&gt;.snowflakecomputing.com/oauth/token-request</code>, where <code>&lt;account name&gt;</code> specifies the full name of your account provided by Snowflake.</p> <p>For example, <code>https://&lt;abc&gt;.snowflakecomputing.com/oauth/token-request</code></p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Client ID	Client ID of your application generated when you create a security integration of type OAuth in Snowflake.

Property	Description
Client Secret	Client secret generated for the client ID.
Access Token	The access token value. Enter the populated access token value that you get from the OAuth endpoint, or click <b>Generate Access Token</b> to populate the access token value.

## Advanced settings

The following table describes the advanced connection properties for OAuth 2.0 authorization code authentication:

Property	Description
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&amp;), in the following format:</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;....</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&amp;schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p> <p>For the list of additional JDBC parameters that you can configure, see <a href="#">"JDBC URL parameters" on page 742</a>.</p>
Scope	<p>Determines the access control when the API endpoint has defined custom scopes.</p> <p>For example, specify <code>session:role:CQA_GCP</code> as the scope to override the value of the default user role. The value needs to be one of the roles assigned in Security Integration.</p> <p>To enter multiple scope attributes, separate each scope attribute with a space.</p>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the access token parameters in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For example, you can use the following <code>code_verifier</code> parameter when you connect to Snowflake:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre> <p>For more information about access token parameters that you can define, see <a href="#">Introduction to OAuth</a> in the Snowflake documentation.</p>

Property	Description
Authorization Code Parameters	<p>Additional parameters to use with the authorization token URL. Define multiple parameters, separated by comma, in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}, {"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For example, you can use the following <code>code_challenge</code> and <code>code_challenge_method</code> parameters when you connect to Snowflake:</p> <pre>[{"Name": "code_challenge", "Value": "Ikr-vv52th0UeVRi4"}, {"Name": "code_challenge_method", "Value": "S256"}]</pre>
Refresh Token	<p>The refresh token value.</p> <p>Enter the populated refresh token value that you get from the OAuth endpoint, or click <b>Generate AccessToken</b> to populate the refresh token value. If the access token is not valid or expires, the Secure Agent fetches a new access token with the help of the refresh token.</p> <p><b>Note:</b> If the refresh token expires, provide a valid refresh token or regenerate a new refresh token by clicking <b>Generate AccessToken</b>.</p>

## Key pair authentication

Key pair authentication requires the private key file and private key file password, along with your Snowflake account user name to connect to Snowflake.

The following table describes the basic connection properties for key pair authentication:

Property	Description
Username	The user name to connect to the Snowflake account.
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#</code>, your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard</code>, your account name is <code>123abc.us-east-2.aws</code>.</p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>

Property	Description
Warehouse	The Snowflake warehouse name.
Private Key File	<p>Path to the private key file, including the private key file name, that the Secure Agent uses to access Snowflake.</p> <p>For example, specify the following path and key file name in the Secure Agent machine:</p> <ul style="list-style-type: none"> <li>- On Windows: C:\Users\path_to_key_file\rsa_key.p8</li> <li>- On Linux: /export/home/user/path_to_key_file/rsa_key.p8</li> </ul> <p>To use the serverless runtime environment, specify the following path and key file name in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/&lt;Private key file name&gt;</pre> <p>For more information about how to use the serverless environment, see <a href="#">"Use the serverless runtime environment with key pair authentication" on page 745</a>.</p> <p><b>Note:</b> Verify that the keystore is FIPS-certified.</p>

## Advanced settings

The following table describes the advanced connection properties for key pair authentication:

Property	Description
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&amp;), in the following format:</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;....</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&amp;schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p> <p>For the list of additional JDBC parameters that you can configure, see <a href="#">"JDBC URL parameters" on page 742</a>.</p>
Private Key File Password	Password for the private key file.

## Client credentials authentication

OAuth 2.0 client credentials authentication requires at a minimum the client ID, access token URL, client secret, scope, and the access token.



The following table describes the basic connection properties for OAuth 2.0 client credentials authentication:

Property	Description
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://&lt;123abc&gt;.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/&lt;123abc&gt;/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code>.</p> <p><b>Note:</b> Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.
Access Token URL	<p>The Snowflake access token endpoint that is used to exchange the authorization code for an access token.</p> <p>Specify the access token URL that you get from the OAuth endpoint.</p>
Client ID	Client ID of your application generated when you configure the application for OAuth.
Client Secret	Client secret generated for the client ID.
Scope	<p>Determines the access control when the API endpoint has defined custom scopes.</p> <p>For example, specify <code>session:role:CQA_GCP</code> as the scope to override the value of the default user role. The value needs to be one of the roles assigned in Security Integration.</p> <p>To enter multiple scope attributes, separate each scope attribute with a space.</p>
Access Token	<p>The access token value.</p> <p>Enter the populated access token value that you get from the OAuth endpoint, or click <b>Generate Access Token</b> to populate the access token value.</p>

## Advanced settings

The following table describes the advanced connection properties for OAuth 2.0 client credentials authentication:

Property	Description
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&amp;), in the following format::</p> <pre>&lt;param1&gt;=&lt;value&gt;&amp;&lt;param2&gt;=&lt;value&gt;&amp;&lt;param3&gt;=&lt;value&gt;....</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&amp;schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p> <p>For the list of additional JDBC parameters that you can configure, see <a href="#">"JDBC URL parameters" on page 742</a>.</p>
Access Token Parameters	<p>Additional parameters to use with the access token URL.</p> <p>Define the access token parameters in the following JSON format:</p> <pre>[{"Name": "&lt;Parameter name&gt;", "Value": "&lt;Parameter value&gt;"}]</pre> <p>For example, you can use the following code_verifier parameter when you connect to Snowflake:</p> <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre> <p>For more information about access token parameters that you can define, see <a href="#">Introduction to OAuth</a> in the Snowflake documentation.</p>

## JDBC URL parameters

You can use the additional JDBC URL parameters field in the Snowflake Data Cloud connection to customize and set any additional parameters when you connect to Snowflake.

You can configure the following properties as additional JDBC URL parameters in the Snowflake Data Cloud connection:

- To override the database and schema name used to create temporary tables in Snowflake, enter the database and schema name in the following format:

```
ProcessConnDB=<DB name>&ProcessConnSchema=<schema_name>
```

- To view only the specified database and schema while importing a Snowflake table, enter the database and schema name in the following format:

```
db=<database_name>&schema=<schema_name>
```

- To read UDF string and numeric data from Snowflake, enter the database and schema where the UDF is created in Snowflake in the following format:

```
db=<database_name>&schema=<schema_name>
```

- To access Snowflake through Okta SSO authentication, enter the web-based IdP implementing SAML 2.0 protocol in the following format:

```
authenticator=https://<Your_Okta_Account_Name>.okta.com
```

**Note:** Microsoft ADFS is not applicable.

For more information about configuring Okta authentication, see

[Configuring Snowflake to use federated authentication.](#)

- To load data from Amazon S3, Google Cloud Storage, or Microsoft Azure Data Lake Storage Gen2 to Snowflake for SQL ELT optimization, enter the Cloud Storage Integration name created for the Amazon S3, Google Cloud Storage, or Microsoft Azure Data Lake Storage Gen2 account in Snowflake in the following format:

```
storage_integration=<Storage Integration name>
```

The storage integration name is case-sensitive. For example, if the storage integration name you created for Amazon S3, Google Cloud Storage, or Microsoft Azure Data Lake Storage Gen2 in Snowflake is *STORAGE\_INT*, you need to specify the same integration name:

```
storage_integration=STORAGE_INT
```

- To connect to Snowflake using the proxy server, enter the following parameters:

```
useProxy=true&
proxyHost=<Proxy host IP address>&
proxyPort=<Proxy server port number>&
proxyUser=<Proxy server user name>&
proxyPassword=<Proxy server password>
```

- To ignore double quotes in the table and treat all tables as case-insensitive, enter the following parameter:

```
QUOTED_IDENTIFIERS_IGNORE_CASE=true
```

When you set this property in the connection to true, Snowflake ignores the double quotes in the table and treats all tables as case-insensitive.

If you have set this property to true, you cannot access case-sensitive tables with the same connection. You need to create a new connection to fetch any existing case-sensitive tables.

- To filter queries that are executed in a Snowflake job on the Snowflake web interface, enter the tag name in the following format:

```
query_tag=<Tag name>
```

You have an option to override the query\_tag parameter that is defined in the Snowflake connection when you run a mapping task.

To override the query\_tag parameter, click the **Runtime Options** tab of the mapping task. In the **Advanced Session Properties** section, select **Custom Properties** from the **Session Property Name** list, and then enter the following value:

```
snowflake_query_tag=<Tag name>
```

**Note:** In advanced mode, you can't override the query\_tag parameter.

In addition to the parameters listed, this field provides you the flexibility to configure other Snowflake parameters based on your requirements.

## Microsoft Azure Active Directory for external OAuth authorization

You can use Microsoft Azure Active Directory as an external OAuth authorization server to authenticate Snowflake.

To use Microsoft Azure Active Directory as an external OAuth authorization server, select **Authorization Code** as the authentication type in the connection properties. Provide the account name, warehouse, authorization URL, access token URL, client ID, client secret, access token, and scope details from the Microsoft Azure Active Directory OAuth authorization server.

To configure the Microsoft Azure Active Directory OAuth authorization server, see [Configure Microsoft Entra ID for external OAuth](#) in the Snowflake documentation.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server. You can configure proxy for connections used both in mappings and in mappings in advanced mode.

To configure proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux. For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.
- Configure the proxy server properties in the additional JDBC URL parameters in the Snowflake connection. For more information, see [Set JDBC URL Parameters](#).

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## Private links to access Snowflake

You can access Snowflake using AWS or Azure Private Link endpoints.

When you create a Snowflake Data Cloud connection, specify the Snowflake private link account name in the **Account** field in the connection properties.

The AWS or Azure Private Link setup ensures that the connection to Snowflake uses the AWS or Azure internal network and does not take place over the public Internet.

To connect to the Snowflake account over the private AWS network, see [AWS Private Link and Snowflake](#).

To connect to the Snowflake account over the private Azure network, see [Azure Private Link and Snowflake](#).

# Use the serverless runtime environment with key pair authentication

You can use a serverless runtime environment hosted on AWS or Azure to connect to Snowflake with key pair authentication.

Before you configure a Snowflake connection using the serverless runtime environment, perform the following tasks:

- Add the private key file path and file name in the Amazon S3 bucket or Azure container in your AWS or Azure account.
- Configure the .yml serverless configuration file.
- Configure the connection properties to connect to Snowflake.

## Add the private key file path and file name in the Amazon S3 bucket or Azure container in your AWS or Azure account

Perform the following steps to configure a Snowflake connection in a serverless runtime environment:

1. Create the following structure for the serverless agent configuration in AWS or Azure:  
`<Supplementary file location>/serverless_agent_config`
2. Add the path to the private key file, including the private key file name, in the Amazon S3 bucket or Azure container in the following location in your AWS or Azure account: `<Supplementary file location>/serverless_agent_config/SSL`

## Configure the .yml serverless configuration file

Perform the following steps to configure the .yml serverless configuration file in the serverless runtime environment, and to copy the private key file path and file name entries to the serverless agent directory:

1. Copy the following code snippet to a text editor:

```
version: 1
agent:
  agentAutoApply:
    general:
      sslStore:
        - fileCopy:
            sourcePath: SSL/<Private key file name>
```

where the source path is the directory path of the private key file in AWS or Azure.

2. Ensure that the syntax and indentations are valid, and then save the file as `serverlessUserAgentConfig.yml` in the following AWS or Azure location: `<Supplementary file location>/serverless_agent_config`  
When the .yml file runs, the private key file is copied from the AWS or Azure location to the serverless agent directory.

## Configure the connection properties to connect to Snowflake

Specify the path to the private key file, including the private key file name in the **Private Key File** field in the Snowflake Data Cloud connection.

For example, `/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<Private key file name>`

For more information about how to configure and use the serverless environment, see "Serverless runtime environment setup" in *Runtime Environments* in the Administrator help.

## CHAPTER 212

# Stripe connection properties

Create a Stripe connection to read data from Stripe.

## Connect to Stripe

Let's configure a Stripe connection to read data from Stripe.

### Before you begin

Before you configure the connection properties, you'll need to get the account ID and secret key from your Stripe account.

The following video shows you how to get the information you need:



### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Stripe

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Specify a Secure Agent or a Hosted Agent.</p>
Account ID	<p>The ID of your Stripe account.</p>
Secret Key	<p>The secret key to authenticate access and make requests to the APIs on the Stripe server.</p>

## CHAPTER 213

# SuccessFactors LMS connection properties

When you set up a SuccessFactors LMS connection, configure the connection properties.

The following table describes the SuccessFactors LMS connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The SuccessFactors LMS connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Service URL	OData service root URL that exposes the data that you want to read. Enter the URL in the following format: <code>https://&lt;rooturl&gt;/learning/odatav4/&lt;webserviceName&gt;/v1/</code> For example, if the root URL is <code>partner0370.scdemo.successfactors.com:443</code> and the Web Service name is <code>curriculum</code> , enter the URL as follows: <code>https://partner0370.scdemo.successfactors.com:443/learning/odatav4/curriculum/v1/</code> For information about the Web Service names, see the <i>SuccessFactors Learning Web Services OData API Reference Guide</i> .
Client ID	The unique ID of the Web Service client that authenticates against the SAP SuccessFactors Learning server.
Client Secret	The secret code that an administrator generates to get OAuth tokens from the SAP SuccessFactors Learning server. The Web Service client then uses the client secret to request for OAuth tokens.
User ID	The unique ID of the user that authenticates against the SAP SuccessFactors Learning server.



Property	Description
Company ID	The tenant ID of the company that authenticates against the SAP SuccessFactors Learning server. The tenant ID is available in the page from where you generate the client ID and client secret.
User Type	The type of user account that runs the Web Service. Select one of the following values: <ul style="list-style-type: none"><li>- admin. Select <b>admin</b> if you run the Web Service with an administrator user account.</li><li>- user. Select <b>user</b> if you run the Web Service with an end-user account.</li></ul>

## CHAPTER 214

# Successfactor ODATA connection properties

Create a SuccessFactors ODATA connection to connect to SuccessFactors so that the Secure Agent can read data from and write data to SuccessFactors. You can use SuccessFactors ODATA connections to specify sources and targets in mappings, synchronization tasks, or mapping tasks.

## Connect to SuccessFactors

Let's configure the SuccessFactors ODATA connection properties to connect to SuccessFactors.

### Before you begin

Before you configure the connection properties, you'll need your company ID, user name, and service URL of your SAP SuccessFactors account.

To use HTTP basic authentication, you need your SuccessFactors user name and password.

To use OAuth 2. authentication, you need to register a OAuth 2.0 client application that is authorized to access the OData API and get the API associated with the client application and the private key.

The following video shows you how to get company ID, user name, and service URL from your SAP SuccessFactors account:



## Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - ; Maximum length is 255 characters.
Description	
Type	SuccessFactors ODATA
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment.
User name	The user name to access the SuccessFactors ODATA account. The user name uses a combination of company ID and user name of your SuccessFactors OData account in the following format: User name@Company ID
Password	The password to access the SuccessFactors ODATA account. <b>Important:</b> Even if you use OAuth 2.0 authentication, you must still enter the user name and password of the SuccessFactors ODATA account.
URL	SuccessFactors service root URL. For example, enter <a href="https://apisalesdemo8.successfactors.com/odata/v2">https://apisalesdemo8.successfactors.com/odata/v2</a> .

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Security Type	Security protocol that you can use to establish a secure connection with the SuccessFactors server. Select SSL or TLS.
TrustStore File Name	Applies to security type. Name of the truststore file that contains the public certificate for the SuccessFactors server.

Property	Description
TrustStore Password	Applies to security type. Password for the truststore file that contains the public certificate for the SuccessFactors server.
KeyStore File Name	Applies to security type. Name of the keystore file that contains the private key for the SuccessFactors server.
KeyStore Password	Applies to security type. Password for the keystore file that contains the private key for the SuccessFactors server.
Authentication Type	Method to authenticate access to the SuccessFactors ODATA account Select one of the following authentication types: - HTTP Basic Authentication. Requires administrator access to the OData API and credentials for a valid account. - OAuth 2.0. Requires you to register a OAuth 2.0 client application that is authorized to access the OData API and valid OAuth token associated with the client application.
API KEY	Enter the API key that the OAuth Utility returns when you register your OAuth 2.0 client application. For more information about how to get the API key,, see the SuccessFactors documentation.
PRIVATE KEY	Enter the private key that the OAuth Utility returns when you generate the X.509 certificate. For more information about how to get the private key, see the SuccessFactors documentation.
COMPANY ID	If you select OAuth 2.0 authentication, enter the company ID that SuccessFactors returns when you create an account in SuccessFactors.

## Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use only an unauthenticated proxy server. The proxy settings applies to connections used in mappings and in mappings in advanced mode.

To configure the proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.  
For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the [Proxy server settings](#) Knowledge Base article.

To configure proxy settings for the serverless runtime environment, see "Using a proxy server" in *Runtime Environments* in the Administrator help.

## CHAPTER 215

# SuccessFactors SOAP connection properties

When you set up a SuccessFactors SOAP connection, you must configure the connection properties.

**Important:** SuccessFactors SOAP Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use SuccessFactors ODATA Connector to access SuccessFactors.

The following table describes the SuccessFactors SOAP connection properties:

Connection property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select SuccessFactors SOAP from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
URL	SuccessFactors service root URL. For example, enter <a href="https://apisalesdemo8.successfactors.com/sfapi/v1/soap?wsdl">https://apisalesdemo8.successfactors.com/sfapi/v1/soap?wsdl</a> .
Company ID	Enter your company ID.
User name	Enter the username.
Password	Enter the password.

## CHAPTER 216

# SurveyMonkey connection properties

When you create a SurveyMonkey connection, configure the connection properties.

The following table describes the SurveyMonkey connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	SurveyMonkey
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent or a Hosted Agent.
Authentication	The authentication method that SurveyMonkey Connector must use to log in to SurveyMonkey. Default is <b>AuthorizationCode</b> .
Authorization URL	The authorization server endpoint from where you retrieve the authorization code. The authorization URL is <a href="https://api.surveymonkey.com/oauth/authorize">https://api.surveymonkey.com/oauth/authorize</a> .
Access Token URL	The SurveyMonkey access token URL that is used to exchange the authorization code for an access token. The access token URL is <a href="https://api.surveymonkey.com/oauth/token">https://api.surveymonkey.com/oauth/token</a> .
Client ID	The client identifier issued to the client during the application registration process.
Client Secret	The client secret key issued to the client during the application registration process.
Scope	The scope of the access request.
Access Token Parameters	Additional parameters to use with the access token URL.
Authorization Code Parameters	Additional parameters to use with the authorization URL.

Connection property	Description
Access Token	The access token granted by SurveyMonkey to access data. Enter the populated access token, or click <b>Generate Access Token</b> to populate the access token. <b>Note:</b> The access token granted by SurveyMonkey does not expire. For more information about the access token, see the SurveyMonkey documentation.
Refresh Token	Not applicable.

## CHAPTER 217

# Tableau V2 connection properties

When you set up a Tableau V2 connection, you must configure the connection properties.

The following table describes the Tableau V2 connection properties:

Connection property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the TDE file: <ul style="list-style-type: none"><li>- Tableau Desktop. Creates a TDE file in the Secure Agent machine. You can then manually import the TDE file to Tableau Desktop.</li><li>- Tableau Server. Publishes the generated TDE file to Tableau Server.</li><li>- Tableau Online. Publishes the generated TDE file to Tableau Online.</li></ul>
Connection URL	URL of Tableau Server or Tableau Online to which you want to publish the TDE file. The URL has the following format: <code>http://&lt;Host name of Tableau Server or Tableau Online&gt;:&lt;port&gt;</code>
User Name	User name of the Tableau Server or Tableau Online account.
Password	Password for the Tableau Server or Tableau Online account.
Content URL	The name of the site on Tableau Server or Tableau Online where you want to publish the TDE file. Contact the Tableau administrator to provide the site name.
Template File Path	The path to a sample TDE file from where the Secure Agent imports the Tableau metadata. Enter one of the following options for the template file path: <ul style="list-style-type: none"><li>- Absolute path to the TDE file.</li><li>- Directory path for the TDE files.</li><li>- Empty directory path.</li></ul> The path you specify for the template file becomes the default path for the target TDE file. <b>Note:</b> Ensure that there is at least one <code>.tde</code> file in the template file path when you select the value of the <b>Tableau Product</b> connection property as <b>Tableau Desktop</b> . If you do not specify a file path, the Secure Agent uses the following default file path for the target TDE file: <code>&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/&lt;latest version&gt;/bin/rtdm</code>



## CHAPTER 218

# Tableau V3 connection properties

When you set up a Tableau V3 connection, you must configure the connection properties.

The following table describes the Tableau V3 connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: <code>_ . + -</code> . Maximum length is 255 characters.
Description	
Type	Tableau V3
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the <code>.hyper</code> file: <b>Tableau Desktop</b> Creates a <code>.hyper</code> or TWBX files in the Secure Agent machine. You can then manually import the <code>.hyper</code> or TWBX files to Tableau Desktop and use the files to perform append or overwrite operation. <b>Tableau Server</b> Publishes the generated <code>.hyper</code> file to Tableau Server. <b>Tableau Online</b> Publishes the generated <code>.hyper</code> file to Tableau Online.
Authentication Method	The authentication method to connect to Tableau Server or Tableau Online. Select one of the following methods: - <b>Username &amp; Password.</b> Uses your Tableau account user name and password to connect to Tableau Server or Tableau Online. - <b>Personal Access Token.</b> Uses the personal access token and token secret from your Tableau account to connect to Tableau Server or Tableau Online.

Connection property	Description
Connection URL	<p>The URL of the Tableau Server or Tableau Online where you want to publish the data extract file.</p> <p>The URL has the following format:</p> <p>http://&lt;Host name of Tableau Server or Tableau Online&gt;:&lt;port&gt;</p>
User Name	The user name for the Tableau Server or Tableau Online account.
Password	The password for the Tableau Server or Tableau Online account.
Personal Access Token Name	The personal access token to connect to the Tableau Server or Tableau Online account.
Token Secret	The token secret associated with the personal access token to connect to the Tableau Server or Tableau Online account.
Site ID	<p>The site name that points to a specific site on Tableau Server or Tableau Online where you want to publish the data extract file.</p> <p>Contact the Tableau administrator to provide the site ID.</p>
Schema File Path	<p>The path of the data extract file required to import the Tableau metadata.</p> <p>Enter one of the following options for the schema file path:</p> <ul style="list-style-type: none"> <li>- Directory path for the <code>.hyper</code> files.</li> <li>- Empty directory path.</li> </ul> <p>When you provide the Tableau schema file path, the Secure Agent generates the <code>.hyper</code> file from the source object based on the data representation in the specified target directory. You can only specify an empty directory if you want to publish the <code>.hyper</code> file to Tableau Server or Tableau Online.</p> <p>When you do not specify a schema file path, the Secure Agent displays the projects and data sources that are present on Tableau Server or Tableau Online when you select the target object in the <b>Object</b> target properties.</p> <p>The Secure Agent uses the following default file path for the target <code>.hyper</code> file:</p> <pre>&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ &lt;latest version&gt;/main/bin/rdtm</pre>

## CHAPTER 219

# Teradata connection properties

Create a Teradata connection to securely read data from or write data to Teradata.

## Prerequisites

Before you can use Teradata Connector, ensure that you meet the prerequisite tasks.

Perform the following prerequisite tasks:

1. Install the Teradata Parallel Transporter utilities and set the environment variables.
2. Ensure that you have access to the Secure Agent directory that contains the success and error files. This directory path must be the same on each Secure Agent machine in the runtime environment. The Teradata JDBC driver is packaged with the Secure Agent. When you install the Secure Agent, the JDBC driver is installed and the JDBC jars are copied to the Secure Agent machine.
3. Configure the authentication prerequisites to connect to a Teradata database. You can configure Native, LDAP, or KRB5 authentication. Keep the authentication details handy based on the authentication type that you want to use.

## Teradata Parallel Transporter Utilities

Before you use Teradata Connector, install the Teradata Parallel Transporter utilities on the Secure Agent machine.

You must install the following Teradata Parallel Transporter utilities:

- Teradata Parallel Transporter Base
- Teradata Parallel Transporter Stream Operator
- Teradata CLlv2
- Teradata Generic Security Services
- Shared ICU Libraries for Teradata

## Configuring the Kerberos authentication

You can configure Kerberos for a Secure Agent only on a Linux machine. Configure the Secure Agent to use Kerberos to authenticate when you connect to a Teradata database.

Before you configure Kerberos authentication, ensure that you have the required Kerberos configuration files, such as `krb5.conf` and `IICSTPT.keytab`. The Secure Agent uses the `IICSTPT.keytab` file to generate Kerberos TGT cache entries at runtime.

## Create the Kerberos configuration files

The Secure Agent requires the keytab files to authenticate users to connect to Teradata.

To generate the keytab file, perform the following steps:

1. Edit the `krb5.conf` and set `default_tgs_etypes = arcfour-hmac-md5`.
2. Add the encryption configuration property in the `krb5.conf` file in the `[libdefaults]` section.  
For example, set the following entries for the `klist` output in the keytab file:

```
[devbld@invlrxrhdpdev05
jdbcConnectionSample]$ klist -ekt IICSTPT.keytab
Keytab name: FILE:IICSTPT.keytab
KVNO Timestamp Principal
1 12/11/2018 15:02:06 teradbqa_mit@INFAQAKERB
(arcfour-hmac)
```

The Secure Agent uses the keytab file information that you specify and creates the Kerberos TGT cache in the `$PMTempDir` directory at runtime. The Kerberos TGT cache is active during the length of the session and ends when the session completes.

## Add the Kerberos configuration files to the Kerberos artifacts directory

Add the `krb5.conf` and `IICSTPT.keytab` files to a directory on the Secure Agent machine.

When you select KRB5 as the authentication type in the Teradata connection, specify the directory that contains these files in the **Kerberos Artifacts Directory** field.

## Setting Environment Variables

You must configure Java and Teradata environment variables before you can use Teradata Connector.

The following table describes the environment variables you must set on UNIX:

Environment Variable	Value
THREADONOFF	On UNIX and Linux, set the <code>THREADONOFF</code> environment variable to 1 to enable multithreading support for Teradata processes.
NLSPATH	Set the <code>NLSPATH</code> variable to the location of the <code>opermsgs.cat</code> file. For example, <code>/opt/teradata/client/15.10/msg/%N</code>

Also, set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

Operating System	Value
Windows	<code>PATH</code>
Linux	<code>LD_LIBRARY_PATH</code>

For example, use the following syntax for Linux:

- Using a Bourne shell:

```
export LD_LIBRARY_PATH="/opt/teradata/client/15.10/lib64:${LD_LIBRARY_PATH}"
```
- Using a C shell:

```
LD_LIBRARY_PATH="/opt/teradata/client/15.10/lib64:${LD_LIBRARY_PATH}"
```

After you set the environment variables, restart the Secure Agent.

## Connect to Teradata

Let's configure the Teradata connection properties to connect to Teradata.

### Before you begin

Before you get started, be sure to complete the prerequisites.

Check out ["Prerequisites" on page 759](#) to learn more about the authentication prerequisites and tasks that you must perform.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Teradata
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent.
TDPID	The name or IP address of the Teradata database machine.

Property	Description
Database Name	The Teradata database name. If you do not enter a database name, Teradata PT API uses the default login database name.
Code Page	Code page associated with the Teradata database. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode and non-Unicode data.  When you run a task that extracts data from a Teradata source, the code page of the Teradata PT API connection must be the same as the code page of the Teradata source.

## Authentication types

You can configure the Native, LDAP, or KRB5 authentication type to connect to the Teradata database.

Select the required authentication type and then configure the authentication-specific parameters.

**Note:** Data Ingestion and Replication does not support the KRB5 and LDAP authentication types.

### Native authentication

To configure native authentication, you need the user name and password from your Teradata account.

The following table describes the basic connection properties for Native authentication:

Property	Description
Username	User name with the appropriate read and write database permissions to access the Teradata database.
Password	Password for the database user name.

### LDAP authentication

To configure LDAP authentication, you need to authenticate user credentials against the external LDAP directory service.

**Note:** Data Ingestion and Replication does not support the LDAP authentication type.

The following table describes the basic connection properties for LDAP authentication:

Property	Description
Username	User name with the appropriate read and write database permissions to access the LDAP database.
Password	Password for the LDAP database user name.

### KRB5 authentication

To configure KRB5 authentication, you must configure the Secure Agent hosted on the Linux machine and ensure that the Kerberos artifacts directory contains the Kerberos configuration files.

**Note:** Data Ingestion and Replication does not support the KRB5 authentication type.

The following table describes the basic connection properties for KRB5 authentication:

Property	Description
Username	The Kerberos user name that authenticates to the Teradata database.

The following table describes the advanced connection properties for KRB5 authentication:

Property	Description
Kerberos Artifacts Directory	Directory that contains the Kerberos configuration files. This directory contains the following configuration files: - krb5.conf - IICSTPT.keytab

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Tenacity	Amount of time, in hours, that the Teradata PT API continues attempting to log in again when the maximum number of operations runs on the Teradata database. Specify a positive integer. Default is 4.
Max Sessions	Maximum number of sessions allowed for the Teradata PT API to establish connection with the Teradata database. Specify a positive, non-zero integer. Default is 4.
Min Sessions	Minimum number of Teradata PT API sessions required for the Teradata PT API job to continue. Specify a positive integer between 1 and the value specified in the <b>Max Sessions</b> field. Default is 1.
Sleep	Amount of time, in minutes, that the Teradata PT API waits before it attempts to log in again when the maximum number of operations run on the Teradata database. Specify a positive, non-zero integer. Default is 6.
Data Encryption	Enables full security encryption of SQL requests, responses, and data. Default is disabled.
Block Size	Maximum block size, in bytes. Teradata PT API uses this property to read the data block size from source through the Export operator. Maximum is 16775168 bytes for Teradata database version 16.20 and later. If the Teradata database version is earlier than 16.20, Teradata scales down the block size from 16775168 bytes to the maximum allowed value. The block size 16775168 is not allowed in the Spool mode. For more information, see the Teradata logs and verify the Teradata documentation of the same version.

Property	Description
Metadata Advanced Connection Properties	The optional properties for the JDBC driver to fetch the metadata from Teradata. For example, tmode=ANSI.
Enable Metadata Quotification	Determines if a Teradata connection reads reserved words used in table or column names from the Teradata database. Select the <b>Enable Metadata Quotification</b> checkbox for the Secure Agent to read reserved words from Teradata.

## Database privileges

Before you use Teradata Connector, select privileges on specific Data Dictionary tables.

Verify that you have the following database privileges:

- Select privileges on DBC.Tables, DBC.Columns, DBC.UDTInfo, and DBC.Databases.  
For information about select privileges, see the Teradata JDBC Driver documentation.



## CHAPTER 220

# UKGPro V2 connection properties

When you set up a UKGPro V2 connection, you must configure the connection properties.

The following table describes the UKGPro V2 connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	The user name of the UKGPro service account. Specify one of the following user names: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the user name of the service account in UKGPro.</li><li>- To read Time Management data, specify the ODataService user name associated with UKG support.</li></ul>
Password	The password of the UKGPro service account. Specify one of the following passwords: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the password of the service account in UKGPro.</li><li>- To read Time Management data, specify the ODataService password associated with UKG support.</li></ul>
Service Host Name	The organization domain of UKGPro to read data from the HR, Payroll, Talent, Benefits, or the Integration Events module. To get the service host name, navigate to <b>UKGPro &gt; Menu &gt; System Configuration &gt; Security &gt; Web Services</b> . Specify the service host name in the following format: <code>service\$.ultipro.com,</code> where \$ is a numeric value. To read the Time Management data, specify the clock server URL provided by UKG support.
User API Key	The User API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module. To get the user API key, navigate to <b>UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio Dashboard &gt; Service Accounts graphic tile</b> To read the Time Management data, specify None as the value of the user API key.

Property	Description
Customer API Key	<p>The Customer API key to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the customer API key, navigate to <b>Dashboard &gt; Service Accounts graphic tile &gt; UKGPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio</b>.</p>
Application Module	<p>Determines the type of objects that you can access through the connection.</p> <p>You can select from the following modules to access data from UKGPro:</p> <p><b>HR, Payroll, Talent, and Benefits</b></p> <p>Access HR, Payroll, Talent, and Benefits objects.</p> <p><b>Integration Events</b></p> <p>Access the Integration Events object to read subscribed Integration Events, such as the date and time of the completed events.</p> <p><b>Other</b></p> <p>Access Time Management objects.</p>

## CHAPTER 221

# UltiPro connection properties

When you set up an UltiPro connection, you must configure the connection properties.

The following table describes the UltiPro connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Password	The password of the UltiPro service account. Specify one of the following passwords: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the password of the service account in UltiPro.</li><li>- To read Time Management data, specify the ODataService password associated with UKG support.</li></ul>
Username	The user name of the UltiPro service account. Specify one of the following user names: <ul style="list-style-type: none"><li>- To read HR, Payroll, Talent, and Benefits or Integration Events data, specify the user name of the service account in UltiPro.</li><li>- To read Time Management data, specify the ODataService user name associated with UKG support.</li></ul>
Service Host Name	The organization domain of UltiPro to read data from the HR, Payroll, Talent, Benefits, or the Integration Events module. To get the service host name, navigate to <b>UltiPro &gt; Menu &gt; System Configuration &gt; Security &gt; Web Services</b> . Specify the service host name in the following format: <code>service\$.ultipro.com</code> , where \$ is a numeric value. To read the Time Management data, specify the clock server URL provided by UKG support.
Customer API Key	The Customer API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module. To get the customer API key, navigate to <b>Dashboard &gt; Service Accounts graphic tile &gt; UltiPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio</b> .

Property	Description
User API Key	<p>The User API key when you want to read data from the HR, Payroll, Talent, Benefits, or Integration Events module.</p> <p>To get the user API key, navigate to <b>UltiPro &gt; Menu &gt; Administration &gt; Integration Studio &gt; Integration Studio Dashboard &gt; Service Accounts graphic tile</b></p> <p>To read the Time Management data, specify None as the value of the user API key.</p>
Application Module	<p>Determines the type of objects that you can access through the connection.</p> <p>You can select from the following modules to access data from Ultipro:</p> <p><b>HR, Payroll, Talent, and Benefits</b></p> <p>Access HR, Payroll, Talent, and Benefits objects.</p> <p><b>Integration Events</b></p> <p>Access the Integration Events object to read subscribed Integration Events, such as the date and time of the completed events.</p> <p><b>Other</b></p> <p>Access Time Management objects.</p>

## CHAPTER 222

# VSAM CDC connection properties

When you configure a VSAM CDC connection, you must set the connection properties.

The following table describes VSAM CDC connection properties:

Property	Description
Connection Name	A name for the VSAM CDC connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the VSAM CDC connection. Maximum length is 4000 characters.
Type	Type of connection. For VSAM CDC, the type must be <b>VSAM CDC</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where both the PowerExchange Listener that processes PWX CDC Reader requests for VSAM change data and the PowerExchange Logger for Linux, UNIX, and Windows run. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  CDC1A:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Collection Name	The instance name that is specified in the <b>Collection Identifier</b> field of the registration group that contains the capture registrations for the VSAM source data sets. This value is used to filter the extraction-map metadata that the PWX CDC Metadata Adapter imports when using this connection.
CAPI Connection Name	Name of a CAPX CAPI_CONNECTION statement that is defined in the PowerExchange dbmover configuration file. This statement includes parameters that the PWX CDC Reader uses to extract change data from PowerExchange Logger for Linux, UNIX, and Windows log files. The PWX CDC Reader requires this property value and ignores any default CAPI_CONNECTION statement that is defined in the dbmover configuration file.

Property	Description
Connection Retry Period	Number of seconds that the PWX CDC Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.
Compression	Controls whether the PowerExchange Listener compresses change data before sending the data over the network to the PWX CDC Reader. Select this property to compress the data. By default, this property is not selected.
Encryption	Controls whether the PowerExchange Listener encrypts change data before sending it over the network to the PWX CDC Reader. Also specifies the type of encryption to use. Select one of the following options: <ul style="list-style-type: none"> <li>- <b>None</b>. Do not use encryption.</li> <li>- <b>AES 128-bit</b>. Use a 128-bit encryption key.</li> <li>- <b>AES 192-bit</b>. Use a 192-bit encryption key.</li> <li>- <b>AES 256-bit</b>. Use a 256 encryption key.</li> </ul> The default is <b>None</b> .
Pacing Size	Amount of data, in rows or kilobytes, that the source system passes to the PowerExchange Listener before pausing to wait for another PWX CDC Reader request for more data. Decrease this value to improve session performance. Use 0 for maximum performance. The default and minimum value is 0.
Pacing Units	Type of units to use with the <b>Pacing Size</b> property. Select either <b>Rows</b> or <b>Kilobytes</b> .
Map Location	Host name or IP address of the system where the extraction maps reside. Also include the port number.  This value is required when the PowerExchange Listener runs on a PowerExchange Logger for Linux, UNIX, and Windows machine that is remote from the extraction maps. The Listener requires access to the extraction maps to process change data extraction requests.  Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  CDC01:25100  <b>Note:</b> The <b>Map Location</b> value takes precedence over the <b>Listener Location</b> value for testing connections and importing extraction-map metadata.
Map Location User	A user name that can access the PowerExchange Listener at the location that is specified in the <b>Map Location</b> property.
Map Location Password	Password associated with the user name that is specified in <b>Map Location User</b> property.
Event Table	If you created an event table to stop change data extraction based on user-defined events, enter the name of the PowerExchange extraction map for the event table. The VSAM event table must reside on the CDC source system.

Property	Description
Replace Low Values with Spaces	Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator or you can specify a parameter to specify connection property overrides through a parameter file.</p> <p>For example:</p> <pre data-bbox="508 590 963 615">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>In most cases, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PowerCenter (PWXPC) CDC connections in PowerCenter.</p> <p>To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$(ParameterName)</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="508 905 1406 1010" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the "Connection overrides reference" chapter.</p>

## CHAPTER 223

# VSAM connection properties

When you configure a VSAM connection, you must set the connection properties.

The following table describes the VSAM connection properties:

Property	Description
Connection Name	A name for the VSAM connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	Description of the VSAM connection. Maximum length is 4000 characters.
Type	Type of connection. For VSAM, the type must be <b>VSAM</b> .
Runtime Environment	Name of the runtime environment that contains the Secure Agent that you want to use to run mapping tasks.
Listener Location	Host name or IP address of the system where the PowerExchange Listener that processes requests for VSAM runs. Also include the Listener port number. Enter the value in the following format, where <i>host_name</i> can be a host name or IP address:  <i>host_name:port_number</i>  For example:  LSNR1:1467
User Name	A user name that can be used to access the PowerExchange Listener when PowerExchange Listener security is enabled. For more information, see the SECURITY statement in the <i>PowerExchange Reference Manual</i> .
Password	Password that is associated with the user name that is specified in the <b>User Name</b> property.
Schema Name	The schema name of the data map.
Code Page	The code page that the Secure Agent for the Data Integration Service uses to extract data from the source file.
Offload Processing	Controls whether to use offload processing. Offload processes transfers bulk data processing from the source system to the target system. Options are: <ul style="list-style-type: none"><li>- <b>Auto</b>. Cloud Data Integration determines whether to use offload processing.</li><li>- <b>Filter After</b>. Offloads the bulk data processing to the target, including the filtering of data.</li><li>- <b>Filter Before</b>. Offloads processing to the target but continues to filter data on the source system.</li><li>- <b>No</b>. Disables offload processing.</li></ul> Default is No.



Property	Description
Offload Threads	<p>The number of threads that Cloud Data Integration uses to process bulk data.</p> <p>For optimal performance, this value should not exceed the number of installed or available processors on the machine where the secure agent runs.</p> <p>Valid values are 1 through 64.</p> <p>Default is 0, which disables multithreading.</p> <p>Not all connection types support offload threads. If the <b>Offload Threads</b> connection attribute for one of these connections is set to a nonzero value, processing continues without threads.</p>
Array Size	<p>For VSAM data sets and sequential files, the size of the storage array, in number of records, that is used for partitioned or multithreaded sessions.</p> <p>For partitioned sessions, this array size is shared across the partitions. For multithreaded sessions, each thread has this array size.</p> <p>Valid values are from 1 through 5000. Default is 25.</p> <p>To tune partitioned sessions, particularly when the <b>Write Mode</b> attribute specifies <b>Confirm Write On</b>, increase the array size.</p>
Replace Low Values with Spaces	<p>Controls whether to replace embedded nulls in character data with spaces. Select this property to replace embedded nulls. By default, this property is selected.</p>
Connection Retry Period	<p>Number of seconds that the PowerExchange Bulk Reader tries to reconnect to the PowerExchange Listener after the initial connection attempt fails. If a connection cannot be established within the retry period, the mapping task fails. The default is 0, which disables connection retries.</p>
Custom Properties	<p>Custom properties or connection property overrides. Custom properties are properties that you can specify to override PowerExchange default settings. You can enter multiple properties by using a semicolon (;) as the separator.</p> <p>For example:</p> <pre data-bbox="500 1167 954 1192">&lt;property&gt;=&lt;value&gt;;&lt;property&gt;=&lt;value&gt;</pre> <p>Normally, you set custom properties only at the direction of Informatica Global Customer Support.</p> <p><b>Note:</b> These properties are equivalent to the <b>PWX Override</b> options for the PowerExchange Client for PWX NRDB Batch connections in PowerCenter.</p> <p>You can also specify connection property overrides in this field or through a parameter file. To specify connection property overrides through a parameter file, you set a parameter in the form of <code>\$&lt;ParameterName&gt;</code>, where you prefix a user-defined parameter name with a dollar sign character (\$). Then configure a mapping task for the mapping to use a parameter file that contains the user-defined parameter definition by specifying the parameter file name in the <b>Parameter File Name</b> field on the <b>Runtime Options</b> tab.</p> <p><b>Note:</b></p> <ul data-bbox="500 1482 1398 1587" style="list-style-type: none"> <li>- If you enter the same parameter for both the mapping and connection, the connection custom property takes precedence.</li> <li>- If you have a parameter file, the parameter name you specify in this field must match an entry defined in the parameter file.</li> </ul> <p>For more information, see the “Connection overrides reference” chapter.</p>
Write Properties	<p>Write Mode. Options are:</p> <ul data-bbox="500 1682 1406 1808" style="list-style-type: none"> <li>- <b>Confirm Write On.</b> Sends data to the PowerExchange Listener and waits for a success or no success response before sending more data. This mode sends data synchronously to the PowerExchange Listener rather than buffering the data.</li> <li>- <b>Confirm Write Off.</b> Sends data asynchronously to the PowerExchange Listener by buffering the data. This mode does not wait for a success or no success response.</li> </ul>

## CHAPTER 224

# Web Service Consumer connection properties

When you configure a Web Service Consumer connection, you must configure the connection properties.

The following table describes the Web Service Consumer connection properties:

Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select Web Service Consumer from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
Authentication	You can configure the connection to use the following types of authentication: <b>Username Token</b> Use the user name token and the password to authenticate the web services. <b>Other Authentication</b> Use the WSDL URL and endpoint URL to authenticate the web services. <b>NTLM Authentication</b> Use NTLM V2 authentication to authenticate the web services.
WSDL URL	The URL provided by the web service.
Endpoint URL	Endpoint URL for the web service. The WSDL file specifies this URL in the location element.
Username	Applicable if you use Username Token or NTLM authentication. User name to authenticate the web service.
Password	Applicable if you use Username Token or NTLM authentication. Password to authenticate the web service.
DOMAIN NAME	Applicable if you use NTLM authentication. Name of the domain that authenticates the accounts.

<b>Property</b>	<b>Description</b>
Encrypt Password	Applicable if you use Username Token authentication. Enables the PasswordDigest property which combines the password with a nonce and a time stamp. The mapping task applies a SHA hash on the password, encodes it in base64 encoding, and uses the encoded password in the SOAP header.
Must Understand	Applicable if you use Username Token authentication. Specifies whether to process a header entry or not.
HTTP Username	User name to access the web service.
HTTP Password	Password to access the web service.

## CHAPTER 225

# WebServices V2 connection properties

When you set up a WebServices V2 connection, you must configure the connection properties.

**Important:** WebServices V2 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Web Service Consumer Connector to access web services applications.

The following table describes the WebServices V2 connection properties:

Connection Property	Description
Connection Name	Enter a unique name for the connection.
Description	Provide a relevant description for the connection.
Type	Select Web Services from the list.
Secure Agent	Select the appropriate Secure Agent from the list.
WSDL URL	Enter the WSDL URI or URL. <b>Note:</b> The length of the WSDL URL fields in Connection tab is increased to 500 characters.
Header CSV path	Enter the Secure Agent server path where header* CSV Files are created.
Body CSV path	Enter the Secure Agent server path where body* CSV Files are created.
Endpoint URL	Enter the Web Service endpoint URL, where the request are served. <b>Note:</b> The length of the Endpoint URL fields in Connection tab is increased to 500 characters.

Connection Property	Description
Authentication Type	Select the type of authentication from the list of authentication available: <b>None</b> No Authentication required. <b>Basic Authentication</b> Basic Authentication required. <b>WSSE UserToken Authentication</b> User token authentication required. <b>WSSE Digital Signature Authentication</b> SSL certificate based authentication required.
User Name	Enter the username required for authentication.
Password	Enter the password.
Certificate Path	Enter the certificate path only when you use WSSE Digital Signature Authentication.
Auto CSV file creation	Select Auto Creation of Body/Header CSV files (Automatic creation of CSV files) or Manual Creation of Body/Header CSV files (You manually create the CSV files).
Download path for attachment	Enter the local directory path in which all the files will be downloaded.
Upload path for attachment	Enter the local directory path from which all the files will be uploaded.
Enable Logging	Select the checkbox to enable logging.
Allow Empty Tags	Select to allow empty tags in the SOAP requests.

## CHAPTER 226

# Workday connection properties

When you set up a Workday connection, you must configure the connection properties.

**Important:** Workday Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Workday V2 Connector to access Workday.

The following table describes the Workday connection properties:

Connection property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks.
Username	The username in <b>Username@Tenant</b> format, where tenant represents the <b>Tenant Name</b> field value.
Password	The relevant password.
Domain Name	The Workday domain name. For example, impl-cc.workday.com.
Tenant Name	The Workday tenant name. For example, informatica_gms1.
Module Name	The module for which you want to connect to.
Enable Logging	Enables logging. Select the checkbox to enable logging.

## CHAPTER 227

# Workday Mass Ingestion connection properties

When you set up a Workday Mass Ingestion connection, you must configure the connection properties.

The properties of a Workday Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **Basic:** Authenticates the connection by validating the login credentials of the Workday account.
- **OAuth 2.0 Refresh Token Flow:** Authenticates the connection by using an application that is registered in Workday. To use this method, you must register an application in Workday and then specify the client ID and client secret of the application in the connection properties. For more information about registering an application in Workday, see the [Workday documentation](#).

### Connection properties for Basic authentication

The following table describes the connection properties for a Workday Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Workday Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	Identifier of the Workday tenant that you want to access.

Connection property	Description
Version	Optional. Web Service Description Language (WSDL) version for the endpoints that the connection must use to retrieve Workday data. The list of operations supported for a web service depends on the WSDL version that you specify in this field. <b>Note:</b> Informatica recommends that you use WSDL v37.0 because Workday Mass Ingestion connections might not read data from the services that are not part of WSDL v37.0. For more information on the WSDL versions, see the <a href="#">Workday Web Services (WWS) documentation</a> .
User Name	User name of the Workday account.
Password	Password for the Workday account.

**Note:** If you configure a connection with the Basic authentication method and then test the connection, the test is always successful even if the connection property values that you specified are incorrect. Therefore, ensure that you specify correct values for the connection properties before you save the connection.

### Connection properties for OAuth 2.0 Refresh Token Flow authentication

The following table describes the connection properties for a Workday Mass Ingestion connection configured with OAuth 2.0 Refresh Token Flow authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Workday Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	Identifier of the Workday tenant that you want to access.
Version	Optional. Web Service Description Language (WSDL) version for the endpoints that the connection must use to retrieve Workday data. The list of operations supported for a web service depends on the WSDL version that you specify in this field. <b>Note:</b> Informatica recommends that you use WSDL v37.0 because Workday Mass Ingestion connections might not read data from the services that are not part of WSDL v37.0. For more information on the WSDL versions, see the <a href="#">Workday Web Services (WWS) documentation</a> .
User Name	Optional. User name of the Workday account.
Client ID	Client ID of the application registered in Workday.



<b>Connection property</b>	<b>Description</b>
Client Secret	Private key of the application registered in Workday.
Refresh Token	Refresh token string that Workday generates for the registered application.
Token Endpoint	OAuth token endpoint of the Workday instance. The registered application sends the access token requests to this endpoint.

## CHAPTER 228

# Workday V2 connection properties

Create a Workday V2 connection to securely read data from or write data to Workday.

## Connect to Workday

Let's configure the Workday V2 connection properties to connect to Workday.

### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Workday V2
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure agent, Hosted Agent, or serverless runtime environment.

Property	Description
Authentication	Authentication by Workday service to access Workday modules. Select Workday.
Username	User name of the Workday tenant to log in to the Workday service. You can enter the user name with the tenant name in the following format: <username>@<tenant name> For example, jjoe@informatica_pt1. If you do not specify the tenant name, the Secure Agent appends the tenant name to the specified user name.
Password	Password to log in to the Workday service.
Domain Name	Name of the Workday domain that contains the resources that you want to access.
Tenant Name	The Workday tenant ID that you want to access. For example, informatica_pt1
Module Name	The Workday service that you want to access. For example, Human_Resources, Financial_Management, and Staffing. For more information about the available modules for the web services, see the following link: <a href="#">Modules for the web services.</a>
Version	The Web Service Description Language (WSDL) version for a service that you want to fetch from Workday. The list of operations supported for a service depends on the WSDL version that you select. For more information about the supported versions, see the following link: <a href="#">Supported WSDL versions.</a>

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Customized	The standard or custom WSDL to fetch Workday object fields. Select to fetch Workday custom object fields. Deselect to fetch the Workdaystandard object fields. Default is disabled.

## Xactly connection properties

When you set up an Xactly connection, configure the connection properties.

**Important:** Xactly Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Xactly connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Xactly.
Runtime Environment	Name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment.
UserID	The UserID for accessing the Xactly portal.
PassKey	The password for accessing the Xactly portal.
Xactly App Name	The application name to sign in to Xactly.
WSDL URL	The WSDL URL.
Endpoint URL	The endpoint URL where you want to send the request.
Enable Logging	Enables logging for the task. Select to log SOAP request and response in the session log file.

## CHAPTER 230

# Xero connection properties

When you create a Xero connection, configure the connection properties.

The following table describes the Xero connection properties:

Connection property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	Xero
Runtime Environment	The name of the runtime environment where you want to run tasks. Specify a Secure Agent or a Hosted Agent.
Authentication	The authentication method that Xero Connector must use to log in to Xero. Default is <b>AuthorizationCode</b> .
Authorization URL	The authorization server endpoint from where you retrieve the authorization code. The authorization URL is <a href="https://login.xero.com/identity/connect/authorize">https://login.xero.com/identity/connect/authorize</a> .
Access Token URL	The Xero access token URL required to exchange the authorization code for an access token. The access token URL is <a href="https://identity.xero.com/connect/token">https://identity.xero.com/connect/token</a> .
Client ID	The client identifier issued to the client during the application registration process.
Client Secret	The client secret key issued to the client during the application registration process.
Scope	The scope of the access request.
Access Token Parameters	Additional parameters to use with the access token URL.
Authorization Code Parameters	Additional parameters to use with the authorization URL.

Connection property	Description
Access Token	The access token granted by Xero to access data. Click <b>Generate Token</b> to populate the access token. <b>Note:</b> Do not manually enter the access token. If you manually enter the access token, the connection fails when the access token expires.
Refresh Token	The refresh token to fetch a new access token. Click <b>Generate Token</b> to populate the refresh token. If the access token expires, the agent fetches a new access token with the help of the refresh token.
Xero Tenant ID	The tenant identifier for Xero. You can get the tenant ID from the Xero administrator.

## CHAPTER 231

# XML Source connection properties

When you create an XML Source connection, you must configure the connection properties.

**Important:** XML Source Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the XML Source connection properties:

Connection property	Description
Connection Name	Name of the XML Source connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Type	Type of connection. Select XML Source from the list.
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Sample XML File Name	Enter the XML file path.
Sample XSD Schema Name	Enter the XSD file path.

# XML Target connection properties

When you create an XML Target connection, you must configure the connection properties.

**Important:** XML Target Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the XML Target connection properties:

Connection property	Description
Connection Name	Enter a name for the connection.
Description	Provide a description for the connection.
Type	Select XML Target from the list.
Secure Agent	Select the secure agent from the list.
Sample XML/XSD Schema Name	Enter XSD file path or XML file path.
XML Working Directory	Enter the file path for XML working directory.
Final XML File Name	Enter final XML file path with the file name.

**Note:** The XML target Connector will create other files in XML working directory for its internal processing, which you can delete after generating the final XML to save the space.



## CHAPTER 233

# Yellowbrick Data Warehouse connection properties

When you set up a Yellowbrick Data Warehouse connection, you must configure the connection properties.

The following table describes the Yellowbrick Data Warehouse connection properties:

Connection property	Description
Connection Name	Name of the connection.
Description	Optional. Description that you use to identify the connection.
Type	Select Yellowbrick as the connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks.
Database	Name of the Yellowbrick Data Warehouse that you want to connect to.
Host Name	Hostname or IP address of the Yellowbrick server.
Password	Password for the Yellowbrick Data Warehouse.
Port No	Port number of the Yellowbrick Data Warehouse.
Schema Name	Name of the schema. Required if you select Specified for Schema Policy.
Schema Policy	Policy for naming the schemas for tables. Select one of the following options: <ul style="list-style-type: none"><li>- None</li><li>- Specified</li><li>- FromImport: Not applicable</li></ul>
User Name	User name for the Yellowbrick Data Warehouse.
Secure Connection	Select this option to use TLS to secure the communication with Yellowbrick. Default is false.

Connection property	Description
Secure CA Cert	<p>Use the name of the custom PEM-encoded certificate file or the name and password of the JKS keystore file to customize trust with secure communications. The name and password of the JKS keystore file must be in the following format:  FILENAME:PASSWORD</p> <p>If a file name is not specified, use the following fallback root CA certificate file:  Windows: %APPDATA%\postgresql\root.crt</p> <p>If the file exists, it will be treated the same as a specified Secure CA Certificate file. For more information, see the Yellowbrick Documentation Library.</p>
Secure Disable Trust	<p>Select this option to disable the SSL and TLS trust when you use a secured connection.</p> <p>Default is false.</p>

## CHAPTER 234

# Zendesk connection properties

When you set up a Zendesk connection, you must configure the connection properties.

**Important:** Zendesk Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Zendesk V2 Connector to access Zendesk.

The following table describes the Zendesk connection properties:

Connection property	Description
Secure Agent	The Secure Agent that you want to run the tasks.
Username	Username of the Zendesk account.
Password	Password of the Zendesk account.
URL	URL of the Zendesk account. Specify the complete URL.
Custom Field	<p>Specify custom fields for Zendesk objects.</p> <p>Specify the custom fields in Zendesk using the following format, where FieldKey is value of the custom field key in Zendesk:</p> <pre>Object1="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldKey2,DataType,Size,Filterable,Pr Object2="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldID2,DataType,Size,Filterable,Pr</pre> <p><b>For example:</b></p> <pre>Organizations="support_description,String,255,true,false"; Users="fixes,String,255,true,false";age,Double,255,true,false";"required,Boolean,255,true,fals ing,255,true,false";"support_description,String,255,true,false";"reg_ex,String,255,true,false"</pre> <p><b>Note:</b> When you specify a custom field for Tickets object, you must specify the custom fields in the following format:</p> <pre>Tickets="CF_FieldKey1,DataType,Size,Filterable,PrimaryKey";"CF_FieldID2,DataType,Size,Filterab</pre> <p><b>For example:</b></p> <pre>Tickets="CF_360003199614,String,255,true,false";"CF_360003373654,String,255,true,false"</pre>

## CHAPTER 235

# Zendesk Mass Ingestion connection properties

When you set up a Zendesk Mass Ingestion connection, you must configure the connection properties.

The properties of a Zendesk Mass Ingestion connection vary based on the authentication method that you specify for the connection. When you create a connection, you can select one of the following authentication methods:

- **Basic:** Authenticates the connection by using the login credentials and subdomain associated with the Zendesk account. The Basic authentication method does not use any encrypted access token to connect to the data source, which results in quick and easy access to Zendesk data.

**Note:** You can use the Basic authentication method only if your Zendesk account is not configured with two-factor authentication. If the account is configured with two-factor authentication, you must use the OAuth 2.0 authentication method for the connection.

- **OAuth 2.0:** Authenticates the connection by using an application that is registered in Zendesk along with the login credentials and subdomain associated with the Zendesk account. To use this method, you must register an application in Zendesk and then specify the client ID and client secret of the application in the connection properties. For more information about registering an application in Zendesk, see the [Zendesk documentation](#).

### Connection properties for Basic authentication

The following table describes the connection properties for a Zendesk Mass Ingestion connection configured with Basic authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + - Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Zendesk Mass Ingestion</b> .

Connection property	Description
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the Zendesk account. The user name is an email address.
Password	Password for the Zendesk account.
Subdomain	URL of the Zendesk help center that you want to access.

**Note:** For more information about the Basic authentication method, see the Zendesk documentation.

### Connection properties for OAuth 2.0 authentication

The following table describes the connection properties for a Zendesk Mass Ingestion connection configured with OAuth 2.0 authentication:

Connection property	Description
Connection Name	A name for the connection. This name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -  Spaces at the beginning or end of the name are trimmed and are not saved as part of the name. Maximum length is 100 characters. Connection names are not case sensitive.
Description	An optional description for the connection. Maximum length is 255 characters.
Type	The type of connection. For an Oracle Database Ingestion connection, the type must be <b>Zendesk Mass Ingestion</b> .
Runtime Environment	Name of the runtime environment where you want to run the ingestion tasks. You must specify a Secure Agent as the runtime environment. <b>Note:</b> You cannot run application ingestion and replication tasks on a Hosted Agent or serverless runtime environment.
Email ID	User name of the Zendesk account. The user name is an email address.
Password	Password for the Zendesk account.
Subdomain	URL of the Zendesk help center that you want the connection to access.
Client ID	Client ID of the application registered in Zendesk.
Client Secret	Client secret of the application registered in Zendesk.
Grant Type	OAuth 2.0 grant type to be used by the connection. By default, Zendesk Mass Ingestion connections are configured to use the password grant type to exchange user names and passwords for access tokens.

**Note:** For more information about the OAuth 2.0 authentication method, see the Zendesk documentation.

## CHAPTER 236

# Zendesk V2 connection properties

When you set up a Zendesk V2 connection, configure the connection properties.

The following table describes the Zendesk V2 connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	
Type	The Zendesk V2 connection type.
Runtime Environment	Name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Username	Username of the Zendesk account.
Password	Password of the Zendesk account.
URL	URL of the Zendesk account. Specify the complete URL. For example, <a href="https://informaticabusinesssolution13.zendesk.com/api/v2">https://informaticabusinesssolution13.zendesk.com/api/v2</a> .
Enable Logging	Select the checkbox to enable logging.
Use Proxy	Connects to Zendesk through proxy server. Select the checkbox to use proxy server.
Custom Field	Specify custom fields for Zendesk objects.

### Rules and guidelines for custom fields

Consider the following rules and guidelines when you configure a custom field:

- Specify the custom fields in Zendesk using the following format, where FieldKey is value of the **Field key** in Zendesk:

```
Object1="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldKey2,DataType,Size,Filterable,PrimaryKey"  
Object2="FieldKey1,DataType,Size,Filterable,PrimaryKey";"FieldKey2,DataType,Size,Filterable,PrimaryKey"
```

For example, you can specify the following custom fields for Organizations and Users objects:

```
Organizations="support_description,String,255,true,false"
Users="problems,String,255,true,false";age,Double,0,true,false";"required,Boolean,0,true,false";"select,String,255,true,false";"support_description,String,255,true,false";"reg_ex,String,255,true,false"
```

- When you specify a custom field for Tickets object, you must specify the custom fields in the following format:

```
Tickets="CF_FieldID1,DataType,Size,Filterable,PrimaryKey";"CF_FieldID2,DataType,Size,Filterable,PrimaryKey"
```

For example:

```
Tickets="CF_360003199614,String,255,true,false;"CF_360003373654,String,255,true,false"
```

- Specify the custom fields for different objects in a new line.
- When you specify multiple custom fields for an object, you must separate each custom field with a semicolon (;).
- If you specify a size for a custom field, the agent considers the size of only the string data type. You must set the size for custom fields of other data types as zero.
- The field key in a custom field must not contain special characters.
- To find the field key for Tickets object in the Zendesk website, go to **Settings > Manage Ticket Fields**.

## CHAPTER 237

# Zuora AQuA Connection properties

Create a Zuora connection to securely read data from Zuora. You can create a Zuora AQuA connection on the **Connections** page.

Use the Zuora AQuA connection when you create a synchronization task or a mapping task.

## Connect to Zuora

Let's configure the Zuora AQuA connection properties to connect to Zuora.

### Before you begin

Before you configure the connection properties, you'll need to get information from your Zuora account. The following video shows you how to get information from your Zuora account:



### Connection details

The following table describes the basic connection properties:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	



Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>This property is not supported by Data Ingestion and Replication.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Type	Zuora AQUA
Runtime Environment	<p>The name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent runtime environment.</p>
Endpoint URL	<p>The URL of the Zuora server.</p> <p>For example, you can specify the URL as <code>https://www.zuora.com/apps/api/</code>.</p>
Username	User name for the Zuora account.
Password	Password for the Zuora account.
WSDL Version	Zuora WSDL version number.

## Advanced settings

The following table describes the advanced connection properties:

Property	Description
Entity ID	The entity ID to connect to a specific entity in a tenant that contains multiple entities.
Entity Name	The entity name to connect to a specific entity in a tenant that contains multiple entities.
Retrieve Deleted Rows	<p>Optional. Retrieves the deleted rows in an incremental mode.</p> <p>Default is false.</p>
UTC Offset	<p>The difference in hours from the Coordinated Universal Time (UTC) for a particular place and date.</p> <p>You can use the UTC offset value when you use the <code>lastruntime</code> data filter field to read data from Zuora based on the specified time zone.</p>

## CHAPTER 238

# Zuora connection properties

When you create a Zuora connection, you must configure the connection properties.

**Important:** Zuora Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release. Informatica recommends that you use Zuora REST V2 Connector to access Zuora.

The following table describes the Zuora connection properties:

Property	Description
Runtime Environment	Runtime environment that contains Secure Agent used to access Zuora.
Username	User name for the Zuora portal login.
Password	Password for the Zuora portal login.
WSDL Url	Path of the Zuora WSDL Url.
EndPoint Url	Path of the Zuora Endpoint Url.
UTC Offset	The difference in hours from the Coordinated Universal Time (UTC) for a particular place and date. You can use the UTC offset value when you use the \$LastRuntime data filter field to read data from Zuora based on the specified time zone. By default, the UTC value is 0.
No of Records for Batch	Number of the records that the Secure Agent reads in batches.
No of records for Batch Write	Number of the records that the Secure Agent writes to the end point in batches. By default, the value of the field is 100.
Enable Debug logger	Determines whether to print the SOAP request and response in the session log.

## CHAPTER 239

# Zuora Multi-Entity connection properties

When you create a Zuora Multi-Entity connection, you must configure the connection properties.

The following table describes the Zuora Multi-Entity connection properties:

Property	Description
Runtime Environment	Runtime environment that contains the Secure Agent used to access Zuora.
Username	User name for the Zuora portal login.
Password	Password for the Zuora portal login.
WSDL Url	Path of the Zuora WSDL Url.
EndPoint Url	Path of the Zuora Endpoint Url.
UTC Offset	The difference in hours from the Coordinated Universal Time (UTC) for a particular place and date. You can use the UTC offset value when you use the \$LastRuntime data filter field to read data from Zuora Multi-Entity based on the specified time zone. By default, the UTC value is 0.
No of Records for Batch	Number of the records that the Secure Agent reads in batches.
No of records for Batch Write	Number of the records that the Secure Agent writes to the end point in batches. By default, the value of the field is 100.
Enable Debug logger	Determines whether to print the SOAP request and response in the session log.
Entity Id	When you have multiple entities in a single tenant, specify the entity ID to connect to a particular entity.
Entity Name	When you have multiple entities in a single tenant, specify the entity name to connect to a particular entity.

## CHAPTER 240

# Zuora REST V2 connection properties

When you create a Zuora REST V2 connection, you must configure the connection properties.

**Important:** Zuora REST V2 Connector is deprecated and has been moved to maintenance mode. Informatica intends to drop support in a future release.

The following table describes the Zuora REST V2 connection properties:

Property	Description
Runtime Environment	Runtime environment that contains Secure Agent used to access Zuora.
Authentication	Select <b>ZuoraRESTV2</b> .
Base Url	Endpoint URL of REST API to which you want to make calls. Do not specify the query parameters with the Base URL. For example, <a href="https://rest.apisandbox.zuora.com/">https://rest.apisandbox.zuora.com/</a>
Authentication Type	The type of user authentication to connect to the Zuora portal login. Select authentication method that the connector must use to login to the Zuora portal login. You can select the following authentication types: <ul style="list-style-type: none"><li>- Basic Auth</li><li>- OAuth 2.0</li></ul> Default is OAuth 2.0.
Username	User name for the Zuora portal login. You must enter the username if you select <b>Basic Auth</b> as the <b>Authentication Type</b> .
Password	Password for the Zuora portal login. You must enter the password if you select <b>Basic Auth</b> as the <b>Authentication Type</b> .
Client ID	The client ID to complete the OAuth 2.0 authentication to connect to Zuora. You must enter the client ID if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Client Secret	The client secret key to complete the OAuth 2.0 authentication to connect to Zuora. You must enter the client secret key if you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> .
Grant Type	The type of authentication used to obtain the token. Use <b>client_credentials</b> .

Property	Description
Entity ID	<p>When you have multiple entities in a single tenant, specify the entity ID to connect to a particular entity.</p> <p>You can also specify the entity ID in the Request Message Editor. If you specify the entity ID in connection properties and Request Message Editor, entity ID specified in the connection properties takes precedence</p> <p><b>Note: Entity ID</b> is mandatory when you select <b>OAuth 2.0</b> as the <b>Authentication Type</b> and specify custom fields in the <b>Custom Field Config</b> property.</p>
Zuora API Version	<p>Swagger file that you want to use for the Zuora REST V2 connection.</p> <p>You can select the <b>Zuora Swagger API V1_2017_09_06</b> or <b>Zuora Swagger API V1_2018_08_23</b> swagger file.</p>
Custom Field Config	<p>Specify the name of the Zuora objects for which you want to configure custom fields as comma-separated values.</p> <p>You can specify the following Zuora objects that support custom fields:</p> <ul style="list-style-type: none"> <li>- Account</li> <li>- Accounting Code</li> <li>- Accounting Period</li> <li>- Amendment</li> <li>- Contact</li> <li>- CreditBalanceAdjustment</li> <li>- CreditMemoItem</li> <li>- CreditMemo</li> <li>- DebitMemoItem</li> <li>- DebitMemo</li> <li>- Feature</li> <li>- InvoiceAdjustment</li> <li>- InvoiceItemAdjustment</li> <li>- InvoiceItem</li> <li>- Invoice</li> <li>- JournalEntryItem</li> <li>- JournalEntry</li> <li>- OrderAction</li> <li>- Order</li> <li>- Payment</li> <li>- ProductFeature</li> <li>- Product</li> <li>- ProductRatePlanCharge</li> <li>- ProductRatePlan</li> <li>- RatePlanCharge</li> <li>- RatePlan</li> <li>- Refund</li> <li>- RevenueEventItem</li> <li>- RevenueEvent</li> <li>- RevenueScheduleItem</li> <li>- RevenueSchedule</li> <li>- Subscription</li> <li>- SubscriptionProductFeature</li> <li>- TaxationItem</li> <li>- Usage</li> </ul> <p><b>Note:</b> Applies only when you select the value of the <b>Zuora API Version</b> as <b>Zuora Swagger API V1_2018_08_23</b>.</p> <p>For more information about Zuora objects that support custom fields, visit <a href="https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Manage_Custom_Fields/Objects_that_Support_Custom_Fields_in_Zuora">https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Manage_Custom_Fields/Objects_that_Support_Custom_Fields_in_Zuora</a>.</p>

# INDEX

## A

- ActiveCampaign
  - connection properties [35](#)
- activities or custom fields
  - configuration [232](#)
- Adabas
  - connection properties [39](#)
- Adabas CDC
  - connection properties [36](#)
- Adaptive Insights
  - connection properties [41](#)
- add-on connectors
  - building [29](#)
  - installing [29](#)
  - purpose [29](#)
- Adobe Analytics
  - connection properties [42](#)
- Adobe Analytics Mass Ingestion connections
  - connection properties [43](#)
- Adobe Experience Platform
  - connection properties [45](#)
- Advanced FTP Connections
  - properties [46](#)
- Advanced FTP V2 connections
  - properties [48](#)
- Advanced FTPS connections
  - properties [50](#)
- Advanced FTPS V2 connections
  - properties [52](#)
- Advanced SFTP connections
  - properties [55](#)
- Advanced SFTP V2 connections
  - properties [56](#)
- Amazon Aurora
  - connection properties [63](#)
- Amazon DynamoDB
  - connection properties [65](#)
- Amazon DynamoDB V2
  - connection properties [66](#)
- Amazon Kinesis connection
  - overview [68](#)
- Amazon Redshift
  - connection properties [72](#)
- Amazon Redshift V2
  - connection properties [85](#)
- Amazon Redshift V2 connections
  - overview [74](#)
- Amazon S3
  - connection properties [101](#)
- Amplitude
  - connection properties [124](#)
- Anaplan V2
  - connection properties [127](#)
- Ariba V2
  - connection properties [129](#)

- AS2
  - properties [131](#)
- authentication
  - OAuth 2.0 authorization code [476](#), [585](#)
  - OAuth 2.0 client credentials [478](#), [588](#)

## B

- BigMachines
  - connection properties [136](#)
- Birst Cloud Connect
  - connection properties [138](#)
- Business 360
  - connection properties [143](#)
- Business 360 FEP
  - connection properties [145](#)

## C

- CallidusCloud Commissions
  - connection properties [146](#)
- CallidusCloud File Processor
  - connection properties [148](#)
- Cassandra V2 connections
  - properties [150](#)
- Chatter
  - connection properties [152](#)
- Cloud Application Integration community
  - URL [27](#)
- Cloud Developer community
  - URL [27](#)
- Cloud Integration Hub connections
  - connection properties [153](#)
- Concur
  - connection properties [155](#)
- Concur V2
  - connection properties [157](#)
- configuring
  - TLS authentication [579](#), [580](#)
- connection
  - Amazon Kinesis Firehose
    - connection properties [68](#)
  - Amazon Kinesis Streams
    - connection properties [70](#)
  - properties [144](#)
- connection dependencies [34](#)
- connection properties
  - company name [400](#)
  - Domo [226](#)
  - language [400](#)
  - overview [518](#)
  - SAP BAPI [628](#)
  - SuccessFactors ODATA Connector [750](#)
  - WSDL URI [400](#)

## connections

- SAP ADSO Writer [622](#)
- ActiveCampaign [35](#)
- Adabas CDC connection properties [36](#)
- Adabas connection properties [39](#)
- Adaptive Insights [41](#)
- add-on connectors [29](#)
- Adobe Analytics [42](#)
- Adobe Analytics Mass Ingestion [43](#)
- Adobe Experience Platform [45](#)
- Amazon Aurora [63](#)
- Amazon DynamoDB [65](#)
- Amazon DynamoDB V2 [66](#)
- Amazon Redshift [72](#)
- Amazon Redshift V2 [85](#)
- Amazon S3 [101](#)
- Amplitude [124](#)
  - AMQP
    - connection properties [125](#)
- Anaplan V2 [127](#)
- Ariba V2 [129](#)
- AS2 [131](#)
  - Azure Event Hub
    - connection properties [362](#)
- BigMachines [136](#)
- Birst Cloud Connect [138](#)
- Business 360 [143](#)
- Business 360 FEP [145](#)
- CallidusCloud Commissions [146](#)
- CallidusCloud File Processor [148](#)
- Chatter [152](#)
- Cloud Integration Hub [153](#)
- Concur [155](#)
- Concur V2 [157](#)
- configuring properties [32](#)
- Coupa [161](#)
- creating [32](#)
- Datacom CDC connection properties [188](#)
- Datacom connection properties [191](#)
- Db2 Data Map connection properties [193](#)
- Db2 for i CDC connection properties [195](#)
- Db2 for i connection properties [198](#)
- Db2 for i Database Ingestion [200](#)
- Db2 for LUW CDC connection properties [202](#)
- Db2 for LUW Database Ingestion connection [205](#)
- Db2 for z/OS Bulk Load connection properties [206](#)
- Db2 for z/OS CDC connection properties [208](#)
- Db2 for z/OS connection properties [211](#)
- Db2 for z/OS Image Copy connection properties [216](#)
- Db2 for z/OS Unload File connection properties [218](#)
- Db2 for zOS Database Ingestion [214](#)
- DB2 Loader [221](#)
- Db2 Warehouse on Cloud connection properties [225](#)
- Dropbox [227](#)
- Eloqua REST [241](#)
- FHIR connection properties [242](#)
- File List [247](#)
- File Processor [249](#)
- FileIO [250](#)
- flat file [251](#)
- FTP/SFTP [255](#)
- Google Ads [258](#)
- Google Analytics [260](#)
- Google Analytics Mass Ingestion [263](#)
- Google BigQuery [264](#)
- Google Bigtable [276](#)
- Google Cloud Storage [277](#)
- Google Cloud Storage V2 [278](#)

## connections (continued)

- Google Drive [280](#)
- Google PubSub [281–283](#)
- Google Sheets [284](#)
- Google Sheets V2 [286](#)
- Greenplum [290](#)
- guidelines for [31](#)
- Hadoop [294](#)
- Hadoop Files [297](#)
- Hive [302](#)
- HubSpot [304](#)
- IBM MQ [305](#)
- IDMS CDC connection properties [307](#)
- IDMS connection properties [310](#)
- IMS CDC connection properties [312](#)
- IMS connection properties [315](#)
- JD Edwards EnterpriseOne [317](#)
- JDBC [319](#)
- JDBC V2 [321](#)
- JIRA [327](#)
- JIRA Cloud [326](#)
  - JMS
    - connection properties [329](#)
- JSON Target [331](#)
  - Kafka
    - connection properties [332](#)
- Klaviyo [336](#)
- LDAP [337](#)
- Magento V1 [339](#)
- Mailchimp [340](#)
- Microsoft Access [344](#)
- Microsoft Azure Blob Storage [345](#)
- Microsoft Azure Blob Storage V2 [346](#)
- Microsoft Azure Blob Storage V3 [349](#)
- Microsoft Azure Cosmos DB SQL API [353](#)
- Microsoft Azure Data Lake Storage Gen2 [356](#)
- Microsoft Azure SQL Data Warehouse [366](#)
- Microsoft Azure SQL Data Warehouse - Database Ingestion [364](#)
- Microsoft Azure SQL Data Warehouse V2 [367](#)
- Microsoft Azure Synapse Analytics Database Ingestion [368](#)
- Microsoft Azure Synapse SQL [373](#)
- Microsoft CDM Folders V2 [381](#)
- Microsoft Dynamics 365 Mass Ingestion [396](#)
- Microsoft Dynamics NAV [403](#)
- Microsoft Excel [404](#)
- Microsoft Power BI [409](#)
- Microsoft SharePoint [411](#)
- Microsoft SQL Server [426](#)
- Microsoft SQL Server CDC connection properties [421](#)
- Mixpanel [434](#)
- MLLP connection properties [435](#)
- MongoDB Mass Ingestion [437](#)
  - MQTT
    - connection properties [445](#)
- MRI Software [447](#)
- MySQL [451](#)
- MySQL CDC connection properties [448](#)
- Netezza [456](#)
- NetSuite [467](#)
- NetSuite Mass Ingestion [465](#)
- NICE Satmetrix [469](#)
- OData V2 Protocol Reader [475](#)
- OData V2 Protocol Writer [479](#)
- ODBC [486](#)
- Open Table [497](#)
- OpenAir [494](#)
- Oracle [502](#)
- Oracle CDC connection properties [515](#)

connections (*continued*)

- Oracle CRM Cloud V1 [523](#)
- Oracle CRM On Demand [524](#)
- Oracle Database Ingestion [525](#)
- Oracle Financials Cloud V1 [535](#)
- Oracle Fusion Cloud Mass Ingestion [539](#)
- Oracle HCM Cloud V1 [541](#)
- overview [31](#)
- PostgreSQL [557](#)
- PostgreSQL CDC connection properties [552](#)
- Power BI [562](#)
- purpose [29](#)
- QuickBooks V2 [563](#)
- REST API [566](#)
- REST V2 [567](#)
- REST V3 [584](#)
- rules for [31](#)
- rules for FTP/SFTP [257](#)
- Salesforce [594](#)
- Salesforce Analytics [591](#)
- Salesforce Commerce Cloud [592](#)
- Salesforce Data Cloud [599](#)
- Salesforce Marketing Cloud [601](#)
- Salesforce Mass Ingestion [603](#)
- Salesforce Pardot [607](#)
- SAP BW [637](#)
- SAP HANA [657](#)
- SAP HANA CDC connection properties [653](#)
- SAP HANA Database Ingestion [661](#)
- SAP IDoc Reader [618](#)
- SAP IDoc Writer [619](#)
- SAP IQ [665](#)
- SAP Mass Ingestion [667](#)
- SAP ODP Extractor [690](#)
- SAP RFC/BAPI Interface [620](#)
- SAP Table [703](#)
- Satmetrix [716](#)
- Sequential connection properties [717](#)
- ServiceNow Mass Ingestion [725](#)
- Snowflake [729](#)
- Stripe [746](#)
- SurveyMonkey [754](#)
- Tableau V2 [756](#)
- Tableau V3 [757](#)
- Teradata [761](#)
- testing [32](#)
- UKGPro V2 [765](#)
- UltiPro [767](#)
- using sample data [33](#)
- VSAM CDC connection properties [769](#)
- VSAM connection properties [772](#)
- Web Service Consumer [774](#)
- WebServices V2 [776](#)
- Workday [778](#)
- Workday Mass Ingestion [779](#)
- Xactly [784](#)
- Xero [785](#)
- XML Source [787](#)
- XML Target [788](#)
- Yellowbrick [789](#)
- Zendesk [791](#)
- Zendesk Mass Ingestion [792](#)
- Zuora [798](#)
- Zuora Multi-Entity [799](#)
- Zuora REST V2 [800](#)

connections Hadoop Files V2 [299](#)

Couchbase connections  
properties [159](#)

Coupa

- connection properties [161](#)

## D

- Data Integration community  
URL [27](#)
- Datacom  
connection properties [191](#)
- Datacom CDC  
connection properties [188](#)
- Db2 Data Map  
connection properties [193](#)
- Db2 for i  
connection properties [198](#)
- Db2 for i CDC  
connection properties [195](#)
- Db2 for i Database Ingestion connections  
connection properties [200](#)
- Db2 for LUW CDC  
connection properties [202](#)
- Db2 for LUW Database Ingestion connection  
connection properties [205](#)
- Db2 for z/OS  
connection properties [211](#)
- Db2 for z/OS Bulk Load  
connection properties [206](#)
- Db2 for z/OS CDC  
connection properties [208](#)
- Db2 for z/OS Image Copy  
connection properties [216](#)
- Db2 for z/OS Unload File  
connection properties [218](#)
- Db2 for zOS Database Ingestion connections  
connection properties [214](#)
- DB2 Loader  
connection properties [221](#)
- Db2 Warehouse on Cloud  
connection properties [225](#)
- dependencies  
connections [34](#)
- Domo Connection  
properties [226](#)
- Dropbox  
connection properties [227](#)

## E

- Elasticsearch connections  
properties [229](#)
- Eloqua REST  
connection properties [241](#)
- environment variables  
Kerberos authentication [425, 502](#)

## F

- FHIR  
connection properties [242](#)
- File List  
connection properties [247](#)
- File Processor  
connection properties [249](#)
- FileIO  
connection properties [250](#)



- flat file
  - connection properties [251](#)
- FTP/SFTP
  - connection properties [255](#)
- FTP/SFTP connections
  - local directory [255](#)
  - overview [255](#)
  - remote directory [255](#)
  - rules and guidelines [257](#)

## G

- generating
  - OAuth access token [142](#)
- Google Ads
  - connection properties [258](#)
- Google Analytics
  - connection properties [260](#)
- Google Analytics Mass Ingestion connections
  - connection properties [263](#)
- Google BigQuery
  - connection properties [264](#)
- Google Bigtable
  - connection properties [276](#)
- Google Cloud Storage
  - connection properties [277](#)
- Google Cloud Storage V2
  - connection properties [278](#)
- Google Drive
  - connection properties [280](#)
- Google PubSub
  - connection properties [281–283](#)
- Google Sheets
  - connection properties [284](#)
- Google Sheets V2
  - connection properties [286](#)
- Greenplum
  - connection properties [290](#)

## H

- Hadoop
  - connection properties [294](#)
- Hadoop Connector
  - JDBC driver class [296](#)
  - JDBC URL [295](#)
- Hadoop Files
  - connection properties [297](#)
- Hadoop Files V2
  - connection properties [299](#)
- Hive
  - connection properties [302](#)
- HubSpot
  - connection properties [304](#)

## I

- IBM MQ
  - connection properties [305](#)
- IDMS
  - connection properties [310](#)
- IDMS CDC
  - connection properties [307](#)
- IMS
  - connection properties [315](#)

- IMS CDC
  - connection properties [312](#)
- Informatica Global Customer Support
  - contact information [28](#)
- Informatica Intelligent Cloud Services
  - web site [27](#)

## J

- JD Edwards EnterpriseOne
  - connection properties [317](#)
- JDBC
  - connection properties [319](#), [657](#)
- JDBC V2
  - connection properties [321](#)
- JIRA
  - connection properties [327](#)
- JIRA Cloud connection [326](#)
- JSON Target connection
  - properties [331](#)

## K

- Kerberos authentication
  - Microsoft SQL Server [424](#)
  - Oracle [501](#)
- Key [361](#)
- key exchange algorithms
  - SFTP connections [256](#)
- keystore certificate
  - creation [500](#)
- Klaviyo
  - connection properties [336](#)

## L

- LDAP
  - connection properties [337](#)

## M

- Magento V1
  - connection properties [339](#)
- Mailchimp
  - connection properties [340](#)
- maintenance outages [28](#)
- Microsoft Access
  - connection properties [344](#)
- Microsoft Azure Blob Storage
  - connection properties [345](#)
- Microsoft Azure Blob Storage V2
  - connection properties [346](#)
- Microsoft Azure Blob Storage V3
  - connection properties [349](#)
- Microsoft Azure Cosmos DB SQL API
  - connection properties [353](#)
- Microsoft Azure Data Lake Storage Gen2
  - connection properties [356](#)
- Microsoft Azure SQL Data Warehouse
  - connection properties [366](#)
- Microsoft Azure SQL Data Warehouse - Database Ingestion
  - connections
  - connection properties [364](#)

- Microsoft Azure SQL Data Warehouse V2
  - connection properties [367](#)
- Microsoft Azure Synapse Analytics Database Ingestion connections
  - connection properties [368](#)
- Microsoft Azure Synapse SQL
  - connection properties [373](#)
- Microsoft CDM Folders V2
  - connection properties [381](#)
- Microsoft Dynamics 365 for Sales connection
  - overview [387](#)
- Microsoft Dynamics 365 Mass Ingestion connections
  - connection properties [396](#)
- Microsoft Dynamics AX V3
  - connection properties [400](#)
- Microsoft Dynamics AX V3 connections
  - properties [400](#)
- Microsoft Dynamics CRM connection
  - connection properties [401](#)
- Microsoft Dynamics NAV
  - connection properties [403](#)
- Microsoft Excel
  - connection properties [404](#)
- Microsoft Fabric Data Warehouse
  - connection properties [405](#)
- Microsoft Fabric Lakehouse
  - connection properties [406](#)
- Microsoft Fabric OneLake
  - connection properties [407](#)
- Microsoft Power BI
  - connection properties [409](#)
- Microsoft SharePoint
  - connection properties [411](#)
- Microsoft SQL Server
  - connection properties [426](#)
- Microsoft SQL Server CDC
  - connection properties [421](#)
- Microsoft SQL Server Connector
  - administration [432](#)
- Mixpanel
  - connection properties [434](#)
- MLLP
  - connection properties [435](#)
- mock connectors [33](#)
- MongoDB connections
  - properties [439](#)
- MongoDB Mass Ingestion
  - connection properties [437](#)
- MongoDB V2 connections
  - properties [441](#)
- MongoDB V2 Connector
  - administration [444](#)
- MRI Software
  - connection properties [447](#)
- MySQL
  - connection properties [451](#)
- MySQL CDC
  - connection properties [448](#)

## N

- Netezza
  - connection properties [456](#)
- NetSuite
  - connection properties [467](#)
- NetSuite Mass Ingestion connections
  - connection properties [465](#)

- NICE Satmetrix
  - connection properties [469](#)

## O

- OAuth access token
  - generating [142](#)
- OData V2 Applications
  - connection properties [479](#)
- OData V2 Protocol Reader
  - connection properties [475](#)
- ODBC
  - connection properties [486](#)
- Open Table
  - connection properties [497](#)
- OpenAir
  - connection properties [494](#)
- Oracle
  - connection properties [502](#)
- Oracle CDC
  - connection properties [515](#)
- Oracle Cloud Object Storage connections
  - properties [520](#)
- Oracle CRM Cloud V1
  - connection properties [523](#)
- Oracle CRM On Demand
  - connection properties [524](#)
- Oracle Database Ingestion connections
  - connection properties [525](#)
- Oracle Financials Cloud V1
  - connection properties [535](#)
- Oracle Fusion Cloud Mass Ingestion connections
  - connection properties [539](#)
- Oracle HCM Cloud V1
  - connection properties [541](#)

## P

- PostgreSQL
  - connection properties [557](#)
- PostgreSQL CDC
  - connection properties [552](#)
- Power BI
  - connection properties [562](#)
- primary and secondary key [361](#)

## Q

- QuickBooks V2
  - connection properties [563](#)

## R

- Redis connections
  - properties [564](#)
- REST API
  - connection properties [566](#)
- REST V2
  - connection properties [567](#)
- REST V3
  - authentication
    - standard [584](#)
  - connection properties [584](#)
- Runtime Environment [361](#)

## S

Salesforce  
connection properties [594](#)

Salesforce Analytics  
connection properties [591](#)

Salesforce Commerce Cloud  
connection properties [592](#)

Salesforce Data Cloud  
connection properties [599](#)

Salesforce Marketing Cloud  
connection properties [601](#)

Salesforce Mass Ingestion connections  
connection properties [603](#)

Salesforce Pardot  
connection properties [607](#)

SAP ADSO Writer  
connection properties [622](#)

SAP BAPI  
connection properties [628](#)

SAP BW  
connection properties [637](#)

SAP BW BEx query connection  
properties [647](#)

SAP connections  
IDoc and BAPI/RFC [617](#)

SAP HANA CDC  
connection properties [653](#)

SAP HANA Connector  
administration [659](#)

SAP HANA Database Ingestion connections  
connection properties [661](#)

SAP IDoc Reader  
connection properties [618](#)

SAP IDoc Writer  
connection properties [619](#)

SAP IQ  
connection properties [665](#)

SAP Mass Ingestion connections  
connection properties [667](#)

SAP OData V2 connections [674](#)

SAP OData V4 connection  
connection [683](#)

SAP OData V4 connections [683](#)

SAP RFC/BAPI Interface  
connection properties [620](#)

SAP Table  
connection properties [703](#)

SAS connections  
properties [715](#)

Satmetrix  
connection properties [716](#)

schema [361](#)

Secure Agent [361](#)

Sequential File  
connection properties [717](#)

ServiceNow Mass Ingestion connections  
connection properties [725](#)

SFTP connections  
key exchange algorithms [256](#)

Snowflake  
connection properties [729](#)

status  
Informatica Intelligent Cloud Services [28](#)

Stripe  
connection properties [746](#)

SuccessFactors connection  
overview [750](#)

SuccessFactors Connector  
connection properties [753](#)

SuccessFactors LMS connections  
properties [748](#)

SuccessFactors ODATA Connector  
connection properties [750](#)

SurveyMonkey  
connection properties [754](#)

system status [28](#)

## T

Tableau V2  
connection properties [756](#)

Tableau V3  
connection properties [757](#)

Teradata  
connection properties [761](#)

trust site  
description [28](#)

trust store certificate  
creation [499](#)

## U

UKGPro V2  
connection properties [765](#)

UltiPro  
connection properties [767](#)

upgrade notifications [28](#)

## V

viewing connection dependencies [34](#)

VSAM  
connection properties [772](#)

VSAM CDC  
connection properties [769](#)

## W

Web Service Consumer  
connection properties [774](#)

web site [27](#)

WebServices V2  
connection properties [776](#)

Workday  
connection properties [778](#)

Workday Mass Ingestion connections  
connection properties [779](#)

## X

Xactly  
connection properties [784](#)

Xero  
connection properties [785](#)

XML Source  
connection properties [787](#)

XML Target  
connection properties [788](#)

## Y

Yellowbrick  
connection properties [789](#)

## Z

Zendesk  
connection properties [791](#)

Zendesk Mass Ingestion connections  
connection properties [792](#)

Zendesk V2 connections  
properties [794](#)

Zuora  
connection properties [798](#)

Zuora Multi-Entity  
connection properties [799](#)

Zuora REST V2  
connection properties [800](#)