Informatica®

Informatica® Cloud Data Integration for PowerCenter

April 2024

Security Guide

Informatica Cloud Data Integration for PowerCenter Security Guide
April 2024
April 2024

Publication Date: 2024-04-21

Table of Contents

Preface 9

Chapter 1: Introduction to Informatica Security 10

Overview of Informatica Security 10

Infrastructure Security 11

Authentication 11

Secure Domain Communication 12

Secure Data Storage 12

Operational Security 13

Domain Configuration Repository 13

Security Domain 14

Chapter 2: User Authentication 15

User Authentication Overview 15

Native User Authentication 16

LDAP User Authentication 16

Kerberos Authentication 17

SAML Authentication 17

SAML Authentication for Informatica Web Applications 17

Chapter 3: LDAP Authentication 19

Overview 19

LDAP Security Domains 19

User Account Synchronization 20

LDAP Directory Services 20

Azure Active Directory for Secure LDAP Authentication 21

Prepare to Import Active Directory User Accounts 21

Creating an LDAP Configuration 22

Create the LDAP Configuration and Configure the LDAP Server Connection 23

Configure the Security Domain 24

Configure the Synchronization Schedule 25

Using Nested Groups in the LDAP Directory Service 26

Using a Self-Signed SSL Certificate 27

Deleting an LDAP Configuration 27

Chapter 4: Kerberos authentication 28

How Kerberos Works in the CDI-PC domain 29

Kerberos Cross Realm Authentication 30

Converting a Domain From Kerberos Single Realm Authentication to Kerberos Cross Realm Authentication 30

Preparing to Enable Kerberos Authentication. . . . 31
Determine the Kerberos Service Principal Level. . . . 31
Configure the Kerberos Configuration File. . . . 32
Create Kerberos Principal Accounts in Active Directory. . . . 35
Generate the Service Principal Name and Keytab File Name Formats. . . . 36
Generate the Keytab Files. . . . 40
Enabling Kerberos Authentication. . . . 44
Enable Kerberos Authentication in the Domain. . . . 44
Update the Nodes in the Domain. . . . 46
Enabling Kerberos on CDI-PC Nodes. . . . 47
Copy the Keytab Files to the CDI-PC Nodes. . . . 48
Enable Kerberos Authentication for CDI-PC Client. . . . 49
Enabling User Accounts to Use Kerberos Authentication. . . . 50
Import User Accounts from Active Directory into LDAP Security Domains. . . . 50
Migrate Native User Privileges and Permissions to the Kerberos Security Domain. . . . 53
Kerberos Delegation. . . . 55
Types of Kerberos Delegation. . . . 55
Service for User (S4U) Extension. . . . 55
Enable Resource-based Constrained Delegation with S4U2Self. . . . 55
Enable Full Delegation for the Kerberos Principal User Accounts in Active Directory. . . . 56
Switch from Full Delegation to Constrained Delegation. . . . 56

Chapter 5: SAML Authentication for Informatica Web Applications. . . . 57

SAML Authentication Overview. . . . 57
Default Keystore and Truststore Directory. . . . 58
Supported Identity Providers. . . . 58
SAML Authentication Process. . . . 59
Enable SAML Authentication in a Domain. . . . 60
Create an LDAP Configuration for the Identity Provider or LDAP Store. . . . 60
Export the Assertion Signing Certificate. . . . 60
Import the Certificate into the Truststore Used for SAML Authentication. . . . 61
Configure the Identity Provider. . . . 61
Add Informatica Web Application URLs to the Identity Provider. . . . 61
Set Up SAML Authentication in the Domain. . . . 61
Enable SAML Authentication on the Nodes. . . . 62
Enhanced Authentication Security. . . . 62
Request Signing. . . . 63
Signed Response. . . . 64
Encrypted Assertion. . . . 64
Configuring Web Applications to Use Different Identity Providers. . . . 65
Prepare to Use an Identity Provider. . . . 66
Configure Informatica Administrator to Use an Identity Provider. . . . 66

Chapter 6: Domain Security 68

Domain Security Overview 68
Secure Communication Within the Domain 69
Secure Communication for Services and the Service Manager 69
Secure Domain Configuration Repository Database 75
Secure CDI-PC repository Database 78
Secure Connections to a Web Application Service 78
Requirements for Secure Connections to Web Application Services 78
Enabling Secure Connections to the Administrator Tool 78
Cipher Suites for the Informatica Domain 79
Create the Cipher Suite Lists 80
Configure the Informatica Domain with a New Effective List of Cipher Suites 81
Secure Sources and Targets 82
CDI-PC Sources and Targets 82
Secure Data Storage 83
Secure Directory on UNIX 83
Changing the Encryption Key from the Command Line 84
Application Services and Ports 86

Chapter 7: Security Management in Informatica Administrator 87

Using Informatica Administrator Overview 87
User Security 88
Encryption 88
Authentication 88
Authorization 89
Security Tab 89
Using the Search Section 89
Using the Security Navigator 90
Groups 90
Users 91
Roles 91
Operating System Profiles 92
LDAP Configuration 92
Account Management 92
Audit Reports 92
Password Management 93
Changing Your Password 93
Domain Security Management 94
User Security Management 94

Chapter 8: Users and Groups 95

Users and Groups Overview 95

Default Groups. . . . 96
Administrator Group. . . . 96
Everyone Group. . . . 96
Operator Group. . . . 96
Understanding User Accounts. . . . 97
Default Administrator. . . . 97
Domain Administrator. . . . 97
Application Client Administrator. . . . 98
User. . . . 98
Managing Users. . . . 98
Creating Native Users. . . . 98
Editing General Properties of Native Users. . . . 99
Assigning Native Users to Native Groups. . . . 100
Assigning LDAP Users to Native Groups. . . . 100
Enabling and Disabling User Accounts. . . . 100
Deleting Native Users. . . . 101
LDAP Users. . . . 101
Unlocking a User Account. . . . 101
Increasing System Memory for Many Users. . . . 102
Viewing User Activity. . . . 103
Managing Groups. . . . 106
Adding a Native Group. . . . 106
Editing Properties of a Native Group. . . . 107
Moving a Native Group to Another Native Group. . . . 107
Deleting a Native Group. . . . 107
LDAP Groups. . . . 108
Managing operating system profiles. . . . 108
Operating System Profile Properties for the CDI-PC Integration Service 108
Creating an Operating System Profile. . . . 110
Editing an Operating System Profile. . . . 111
Assigning a Default Operating System Profile to a User or Group. . . . 111
Deleting an Operating System Profile 111
Working with Operating System Profiles in a Secure Domain. . . . 112
Working with Operating System Profiles in a Domain with Kerberos Authentication. . . . 112
Account Lockout. . . . 113
Configuring Account Lockout. . . . 113
Rules and Guidelines for Account Lockout. . . . 114

Chapter 9: Privileges and Roles. . . . 115

Privileges. . . . 115
Privilege Groups. . . . 115
Roles. . . . 116
Domain Privileges. . . . 116

Security Administration Privilege Group. . . . 116
Domain Administration Privilege Group. . . . 117
Tools Privilege Group. . . . 121
Cloud Administration Privilege Group. . . . 121
CDI-PC Repository Service Privileges. . . . 122
Tools Privilege Group. . . . 122
Folders Privilege Group. . . . 123
Design Objects Privilege Group. . . . 124
Sources and Targets Privilege Group. . . . 127
Run-time Objects Privilege Group. . . . 129
Global Objects Privilege Group. . . . 133
Managing Roles. . . . 135
System-Defined Roles. . . . 135
Custom Roles. . . . 136
Assigning Privileges and Roles to Users and Groups. . . . 138
Inherited Privileges. . . . 138
Assigning Privileges and Roles to a User or Group by Navigation. . . . 139
Viewing Users with Privileges for a Service. . . . 139
Troubleshooting Privileges and Roles. . . . 140

Chapter 10: Permissions. . . . 142

Permissions Overview. . . . 142
Types of Permissions. . . . 143
Permission Search Filters. . . . 143
Domain Object Permissions. . . . 144
Permissions by Domain Object. . . . 144
Permissions by User or Group. . . . 146
Operating System Profile Permissions. . . . 146
Connection Permissions. . . . 148
Types of Connection Permissions. . . . 148
Default Connection Permissions. . . . 148
Assigning Permissions on a Connection. . . . 148
Viewing Permission Details on a Connection. . . . 149
Editing Permissions on a Connection. . . . 149
Application and Application Object Permissions. . . . 150
Types of Application and Application Object Permissions. . . . 150
Assigning Permissions on an Application or Application Object. . . . 150
Viewing Permission Details on an Application or Application Object. . . . 151
Editing Permissions on an Application or Application Object. . . . 151
Denying Permissions on an Application or Application Object. . . . 151

Chapter 11: Audit Reports. . . . 152

Audit Reports Overview. . . . 152

User Personal Information. 153
User Group Association. 153
Privileges. 154
Roles Association. 155
Domain Object Permission. 155
Selecting Users for an Audit Report. 156
Selecting Groups for an Audit Report 156
Selecting Roles for an Audit Report. 157

Appendix A: Command Line Privileges and Permissions. 158

infacmd dp Commands. 158
infacmd es commands. 158
infacmd isp Commands. 159
infacmd ms Commands. 167
infacmd rms Commands. 167
infacmd sch commands. 167
infacmd wfs Commands. 168
pmcmd Commands. 168
pmrep Commands. 171

Appendix B: Custom Roles. 176

CDI-PC Repository Service Custom Roles. 176

Index. 178

Preface

Use the *Security Guide* to learn how to enable security in an Informatica domain. Understand how to configure and manage various authentication protocols, including Lightweight Directory Access Protocol, Kerberos, and Security Assertion Markup Language. Learn how to manage users and groups, and how to use permissions, privileges, and roles to manage user security.

CHAPTER 1

Introduction to Informatica Security

This chapter includes the following topics:

- Overview of Informatica Security, 10
- Infrastructure Security, 11
- Operational Security, 13
- Domain Configuration Repository, 13
- Security Domain, 14

Overview of Informatica Security

You can secure the CDI-PC domain to protect from threats from inside and outside the network on which the domain runs.

Security for the CDI-PC domain includes the following types of security:

Infrastructure Security

Infrastructure security protects the CDI-PC domain against unauthorized access to or modification of services and resources in the CDI-PC domain. Infrastructure security includes the following aspects:

- Protection of data transmitted and stored within the CDI-PC domain.
- Authentication of users and services connecting to the CDI-PC domain.
- Security of connections for external components, including client applications and relational databases for repositories, sources, and targets.

Operational Security

Operational security controls access to the data and services in the CDI-PC domain. Operational security includes the following aspects:

- Setting restrictions to user access to data and metadata based on the role of the user in the organization.
- Setting restrictions to user ability to perform operations within the CDI-PC domain based on the user role in the organization.

CDI-PC stores the domain configuration information and the list of users authorized to access the domain in the domain configuration repository. The domain configuration repository also contains the groups, roles, privileges, and permissions that are assigned to each user in the Informatica domain.

CDI-PC organizes the list of users by security domains. A security domain contains a collection of user accounts. A domain can have multiple security domains.

Infrastructure Security

Infrastructure security includes user and service authentication, secure communication within the domain, and secure data storage.

Authentication

The Service Manager authenticates the services that run in the domain and the users who log in to the CDI-PC Client tools.

You can configure the CDI-PC domain to use the following types of authentication:

Native Authentication

Native authentication is a mode of authentication available only for user accounts in the CDI-PC domain. When the CDI-PC domain uses native authentication, the Service Manager stores user credentials and privileges in the domain configuration repository and performs all user authentication within the CDI-PC domain.

If the CDI-PC domain uses native authentication, by default, the domain has a native security domain and all user accounts belong to the native security domain.

Informatica uses user name and passwords to authenticate users and services in the CDI-PC domain.

Lightweight Directory Access Protocol (LDAP) Authentication

LDAP is a software protocol for accessing users and resources on a network. If the CDI-PC domain uses LDAP authentication, the user accounts and credentials are stored in the LDAP directory service. The user privileges and permissions are stored in the domain configuration repository. You must periodically synchronize the user accounts in the domain configuration repository with the user accounts in the LDAP directory service.

Informatica uses user name and passwords to authenticate Informatica users and services in the CDI-PC domain.

Kerberos Authentication

Kerberos is a network authentication protocol which uses tickets to authenticate users and services in a network. When the CDI-PC domain uses Kerberos authentication, the user accounts and credentials are stored in the Kerberos principal database, which can be an LDAP directory service. The user privileges and permissions are stored in the domain configuration repository. You must periodically synchronize the user accounts in the domain configuration repository with the user accounts in the Kerberos principal database.

Informatica uses the Kerberos tickets to authenticate Informatica users and services in the CDI-PC domain.

SAML-based Single Sign-on

Security Assertion Markup Language (SAML) is an XML-based data format for exchanging authentication and authorization information between a service provider and an identity provider. You can configure SAML-based single sign-on for the Administrator tool.

In CDI-PC domain, the Informatica web application is the service provider, and Microsoft Active Directory Federation Services (AD FS) is the identity provider. The accounts and credentials for Informatica web application users are stored in Microsoft Active Directory. You import accounts from Active Directory into a security domain within the CDI-PC domain. You must periodically synchronize the user accounts in the security domain with the user accounts in the Active Directory directory service.

Note: You cannot enable SAML-based single sign-on in CDI-PC domain configured to use Kerberos authentication.

Secure Domain Communication

The CDI-PC domain has various options to secure the data and metadata that are transmitted between the Service Manager and services in the domain and the client applications. CDI-PC uses the TCP/IP and HTTP protocols to communicate between components in the domain and uses SSL certificates to secure the communication between services and the Service Manager in the domain.

The SSL/TLS protocol uses public key cryptography to encrypt and decrypt network traffic. The public key used to encrypt and decrypt traffic is stored in an SSL certificate that can be self-signed or signed. A self-signed certificate is signed by the creator of the certificate. Because the identity of the signer is not verified, a self-signed certificate is less secure than a signed certificate. A signed certificate is an SSL certificate that has the identity of the person who requested the certificate verified by a certificate authority (CA). CDI-PC recommends CA signed certificates for a higher level of security.

A keystore contains private keys and certificates. It is used to provide a credential. A truststore contains the certificate of trusted SSL/TLS servers. It is used to verify a credential.

To secure connections in the domain, CDI-PC requires keystores and truststores in PEM and JKS formats. You can use the following programs to create the required files:

keytool

You can use the Java keytool key and certificate management utility to create an SSL certificate or a certificate signing request (CSR) as well as keystores and truststores in JKS format.

The keytool utility is available in the following directory on domain nodes:

```
<CDI-PC installation directory>\java\bin
```

OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website:

https://www.openssl.org/docs/

The type of connection that you secure determines the files required.

Secure Data Storage

CDI-PC encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the domain configuration repository. CDI-PC also saves sensitive files, such as configuration files, in a secure directory.

Operational Security

You can assign privileges, roles, and permissions to users or groups of users to manage the level of access users and groups can have and the scope of the actions that users and groups can perform in the domain.

You can use the following methods to manage user and group access in the domain:

Privileges

Privileges determine the actions that users can perform in the CDI-PC Client tools. You can assign a set of privileges to a user to restrict access to the services available in the domain. You can also assign privileges to a group to allow all users in the group the same access to services.

Roles

A role is a set of privileges that you can assign to users or groups. You can use roles to more easily manage assignments of privileges to users. You can create a role with limited privileges and assign it to users and groups that have restricted access to domain services. Or you can create roles with related privileges to assign to users and groups that require the same level of access.

Permissions

Permissions define the level of access that users have to an object. A user who has the privilege to perform a certain action might require permission to perform the action on a particular object. For example, to manage an application service, a user must have the privilege to manage services and permission on the specific application service.

Default Administrator Group

The CDI-PC domain has a system-defined Administrator group that includes all privileges and permissions for a service. Any user account that you add to the Administrator group has privileges and permissions on all services and objects in the domain. When you install CDI-PC services, the installer creates a user account that belongs to the Administrator group. You can use the default Administrator account to initially log in to the Administrator tool.

Domain Configuration Repository

The domain configuration repository contains information about the domain configuration and user privileges and permissions.

If the CDI-PC domain uses native user authentication, the domain configuration repository also contains the user credentials. If the domain uses LDAP or Kerberos authentication, the domain configuration repository does not contain the user credentials. All LDAP and Kerberos user credentials are stored outside the CDI-PC domain, in the LDAP directory service or Kerberos principal database.

When you create the CDI-PC domain during installation, the installer creates a domain configuration repository in a relational database. You must specify the database in which to create the domain configuration repository. You can create the repository on a database secured with the SSL protocol.

Security Domain

A security domain is a collection of user accounts and groups in the CDI-PC domain.

The CDI-PC domain can have the following types of security domains:

Native Security Domain

The Native security domain contains the users and groups created and managed in the Administrator tool. CDI-PC stores all credentials for user accounts in the Native security domain in the domain configuration repository. By default, the native security domain is created during installation. After installation, you cannot create additional Native security domains or delete the Native security domain.

If the CDI-PC domain uses Kerberos authentication, the domain does not use the Native security domain.

LDAP Security Domain

An LDAP security domain contains users and groups imported from an LDAP directory service. If the CDI-PC domain uses LDAP or Kerberos authentication, you can create an LDAP security domain and add users and groups that you import from the LDAP directory service.

When you install CDI-PC services and create a domain that uses native or LDAP authentication, the installer creates the Native security domain but does not create an LDAP security domain. You can create LDAP security domains after installation.

When you install CDI-PC services and create a domain that uses Kerberos authentication, the installer creates the following LDAP security domains:

- Internal security domain. The installer creates an LDAP security domain with the name *_infaInternalNamespace*. The _infaInternalNamespace security domain contains the default administrator user account that you create during installation. After installation, you cannot add users to the _infaInternalNamespace security domain or delete the security domain.
- User realm security domain. The installer creates an empty LDAP security domain gives it the same name as the Kerberos user realm you specify during installation. After installation, you can import users from the Kerberos principal database into the user realm security domain. You cannot delete the user realm security domain.
  When you run command line programs in a domain that uses Kerberos authentication, the security domain option defaults to the user realm security domain created during installation.

You create and manage LDAP security domains the same way, whether the CDI-PC domain uses LDAP authentication or Kerberos authentication.

CHAPTER 2

User Authentication

This chapter includes the following topics:

- User Authentication Overview, 15
- Native User Authentication, 16
- LDAP User Authentication, 16
- Kerberos Authentication, 17
- SAML Authentication, 17

User Authentication Overview

User authentication in the Informatica domain depends on the type of authentication that you configure when you install the Informatica services.

The CDI-PC domain can use the following types of authentication to authenticate users in the CDI-PC domain:

- Native user authentication
- LDAP user authentication
- Kerberos network authentication
- Security Assertion Markup Language (SAML)-based single sign-on

Native user accounts are stored in the CDI-PC domain and can only be used within the CDI-PC domain.

LDAP and Kerberos and user accounts are stored in an LDAP directory service and are shared by applications within the enterprise.

SAML-based single sign-on authenticates users against account credentials stored in Microsoft Active Directory. Accounts are imported from Active Directory into a security domain within the Informatica domain.

You can select the type of authentication to use in the Informatica domain during installation. If you enable Kerberos authentication during installation, you must configure the CDI-PC domain to work with the Kerberos key distribution center (KDC). You must create the service principal names (SPN) required by the CDI-PC domain in the Kerberos principal database. The Kerberos principal database can be an LDAP directory service. You must also create keytab files for the SPNs and store it in the Informatica directory as required by the CDI-PC domain.

If you do not enable Kerberos authentication during installation, the installer configures the Informatica domain to use native authentication. After installation, you can set up a connection to an LDAP server and configure the CDI-PC domain to use LDAP authentication in addition to native authentication.

You can use native authentication and LDAP authentication together in the CDI-PC domain. The Service Manager authenticates the users based on the security domain. If a user belongs to the native security domain, the Service Manager authenticates the user in the domain configuration repository. If the user belongs to an LDAP security domain, the Service Manager passes the user name and password to the LDAP server for authentication.

You cannot use native authentication with Kerberos authentication. If the CDI-PC domain uses Kerberos authentication, all user accounts must be in LDAP security domains. The Kerberos server authenticates a user account when the user logs in to the network. The CDI-PC Client applications use the credentials from the network login to authenticate users in the CDI-PC domain. Native groups and roles are still supported.

You can enable SAML-based single sign-on for Informatica web applications during installation, or after installation. However, you must complete all required set up tasks before enabling SAML-based single sign-on. You cannot enable SAML-based single sign-on in an Informatica domain configured to use Kerberos authentication.

When the CDI-PC domain resides on-premises and not on an AWS EC2 instance, you cannot use the EMRFS authentication protocol in integration with Amazon EMR.

You can encrypt the user-credential token with the unique site key. To encrypt the user-credential token, set the environment variable `infaEnableAdvancedEncryptionSchemeForCredential` to *true*. In case of native and LDAP user authentication, after successful user authentication, the encrypted credential token is used instead of user password.

Native User Authentication

If the CDI-PC domain uses native authentication, the Service Manager stores all user account information and performs all user authentication within the CDI-PC domain. When a user logs in, the Service Manager uses the native security domain to authenticate the user name and password.

If you do not configure the Informatica domain to use Kerberos network authentication, the CDI-PC domain contains a native security domain by default. The native security domain is created at installation and cannot be deleted. The CDI-PC domain can have only one native security domain. You create and maintain user accounts in the native security domain in the Administrator tool. The Service Manager stores details about the user accounts, including the user credentials and privileges, in the domain configuration repository.

LDAP User Authentication

You can configure an Informatica domain to enable users in an LDAP directory service to log in to Informatica client applications. You can create multiple LDAP configurations for a domain, each connecting to a different LDAP server. A domain can use LDAP user authentication in addition to native user authentication.

To enable the Informatica domain to use LDAP user authentication, you must set up a connection to an LDAP server and specify the users and groups from the LDAP directory service that can have access to the Informatica domain. You can use the Administrator tool to set up the connection to the LDAP server.

When you synchronize the LDAP security domains with the LDAP directory service, the Service Manager imports the list of LDAP user accounts with access to the Informatica domain into the LDAP security domains. When you assign privileges and permissions to users in LDAP security domains, the Service

Manager stores the information in the domain configuration repository. The Service Manager does not store the user credentials in the domain configuration repository.

When a user logs in, the Service Manager passes the user name and password to the LDAP server for authentication.

Note: The Service Manager requires that LDAP users log in to a client application with a password even though an LDAP directory service may allow a blank password for anonymous login mode.

Kerberos Authentication

You can configure the CDI-PC domain to use Kerberos network authentication to authenticate users and services on a network.

Kerberos is a network authentication protocol which uses tickets to authenticate access to services and nodes in a network. Kerberos uses a Key Distribution Center (KDC) to validate the identities of users and services and to grant tickets to authenticated user and service accounts. In the Kerberos protocol, users and services are known as principals. The KDC has a database of principals and their associated secret keys that are used as proof of identity. Kerberos can use an LDAP directory service as a principal database.

To use Kerberos authentication, you must install and run the Informatica domain on a network that uses Kerberos network authentication. Informatica can run on a network that uses Kerberos authentication with Microsoft Active Directory service as the principal database.

You can configure the CDI-PC domain to use Kerberos cross realm authentication. Kerberos cross realm authentication enables Informatica clients that belong to one Kerberos realm to authenticate with nodes and application services that belong to another Kerberos realm.

The Informatica domain requires keytab files to authenticate nodes and services in the domain without transmitting passwords over the network. The keytab files contain the service principal names (SPN) and associated encrypted keys. Create the keytab files before you create nodes and services in the Informatica domain.

SAML Authentication

You can configure an Informatica domain to allow users to use Security Assertion Markup Language (SAML) authentication to log into the Administrator tool.

SAML is an XML-based data format for exchanging authentication and authorization information between a service provider and an identity provider.

SAML Authentication for Informatica Web Applications

In an Informatica domain, the Informatica web application is the service provider. Microsoft Active Directory Federation Services (ADFS) is the identity provider which authenticates web application users with your organization's Active Directory identity store.

To enable the Informatica domain to use SAML-based single sign-on, you must create an LDAP security domain for Informatica web application user accounts and then import the users into the domain from Active Directory. You can use the Administrator tool to set up the connection to the Active Directory server and then import users into the security domain.

When a user logs into an Informatica web application, the application sends a SAML authentication request to ADFS. ADFS authenticates the user's credentials against the user account information in Active Directory and then returns a SAML assertion token containing security-related information about the user to the web application.

You configure ADFS to issue SAML tokens to authenticate Informatica web application users. You must also export the Identity Provider Assertion Signing Certificate from ADFS and then import the certificate into the Informatica default truststore file on each gateway node in the domain.

CHAPTER 3

LDAP Authentication

This chapter includes the following topics:

- Overview, 19
- LDAP Security Domains, 19
- User Account Synchronization, 20
- LDAP Directory Services, 20
- Azure Active Directory for Secure LDAP Authentication, 21
- Creating an LDAP Configuration, 22
- Deleting an LDAP Configuration, 27

Overview

You can configure an Informatica domain to enable users imported from one or more LDAP directory services to log in to Informatica nodes and services.

An LDAP directory service stores account user names and passwords. Using LDAP authentication enables you to consolidate the credentials for all of your Informatica users in a single identity store, simplifying the task of creating and updating account credentials.

You can use native authentication and LDAP authentication together in an Informatica domain. The Service Manager running on the master gateway node within the domain authenticates users based on the security domain the users belong to. If a user belongs to the default native security domain, the Service Manager authenticates the user against account information in the domain configuration repository. If the user belongs to an LDAP security domain, the Service Manager passes the user's credentials to the LDAP server for authentication.

LDAP Security Domains

An LDAP security domain contains users and groups imported from an LDAP directory service. You can define multiple LDAP security domains within the CDI-PC domain. You can then import accounts from LDAP directory services into the security domains.

You must create an LDAP security domain if you configure an CDI-PC domain to use Kerberos authentication. When you install CDI-PC services and enable Kerberos authentication, the CDI-PC installer creates an LDAP security domain with the name of the Kerberos realm that you specify during installation.

When you create an LDAP security domain, you configure search bases and filters that define the set of LDAP user accounts and groups to include in the security domain. The Service Manager uses the security domain configuration to import or synchronize users and groups in the security domain with users and groups in the LDAP directory service.

The Service Manager uses the following criteria when it imports or synchronizes users and groups within an LDAP security domain:

- The Service Manager uses the user search bases and filters to import user accounts.
- The Service Manager uses the group search bases and filters to import groups.
- The Service Manager imports the groups that are included in the group filter and the user accounts that are included in the user filter.

User Account Synchronization

The Service Manager updates the security domain with the users and groups in an LDAP directory service on a scheduled basis. You can set up the synchronization schedule when you configure LDAP authentication.

The Service Manager performs the following steps during synchronization:

- Retrieves an updated list of users and groups from the LDAP directory service, based on the search base and filters you configured for the security domain.
- Updates the list of LDAP users and groups in the security domain. If an LDAP user in the security domain has been deleted in the LDAP directory service, the Service Manager transfers ownership of the user's objects to the domain administrator account.

LDAP Directory Services

You can import user accounts into CDI-PC security domains from LDAP directory services.

You can import users from the following LDAP directory services:

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP
- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Sun Java System Directory Server

Note: If you use Kerberos authentication, you can import users only from Microsoft Active Directory.

The Service Manager requires a particular unique ID (UID) to identify users in each LDAP directory service. The following table lists the default UID for each LDAP directory service:

LDAP Directory Service	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid
OpenLDAP	uid
Oracle Directory Server (ODSEE)	uid
Oracle Unified Directory (OUD)	uid
Sun Java System Directory Server	uid

Azure Active Directory for Secure LDAP Authentication

You can import users from Azure Active Directory (Azure AD) into an LDAP security domain.

Azure Active Directory Domain Services provide a secure LDAP public IP address that you use to import user accounts from Azure Active Directory into an LDAP security domain. Users you import can use their LDAP credentials to log in to Informatica nodes, services, and applications that run on virtual machines in an Azure Active Directory managed domain.

To see supported versions of Active Directory, see the Product Availability Matrix on Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices.

You must enable Secure Lightweight Directory Access Protocol (secure LDAP) authentication in Azure Active Directory Domain Services to authenticate Informatica users.

Prepare to Import Active Directory User Accounts

Complete the following steps to prepare to import user accounts from Azure Active Directory into an Informatica domain:

1. Verify that port 636, which is the Azure Active Directory secure LDAP port, is accessible through your firewall.
2. Enable secure LDAP authentication in Azure Active Directory Domain Services.

   You use the Azure portal to enable secure LDAP in Azure Active Directory Domain Services. For information about configuring secure LDAP in Azure Active Directory Domain Services, see the following link:

   https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap

3. When you configure the secure LDAP certificate in Azure Active Directory Domain Services, ensure that the Subject name on the certificate is the Fully Qualified Domain Name (FQDN) of Azure Active Directory.
4. Convert the secure LDAP certificate from the PFX format to the PEM format. Java requires that the certificate is in the PEM format.
5. Import the certificates used by all domain nodes into the Java `cacerts` truststore file in the following directory on a single gateway node in the domain:

   ```
   <Informatica installation directory>/java/jre/lib/security/
   ```
6. Copy the `cacerts` file that contains the imported certificates to the same directory on every other gateway node in the domain.
7. Add the Azure Active Directory public IP address and the Fully Qualified Domain Name (FQDN) of Azure Active Directory to the /etc/hosts file on each gateway node in the domain. Use the following format:

   ```
   <Azure Active Directory host IP address> ldaps.<FDQN of Azure Active Directory>
   ```

Creating an LDAP Configuration

You can create one or more LDAP configurations to enable user accounts and user groups that you import from LDAP directory services to authenticate with an Informatica domain.

You create and manage LDAP users and groups in the LDAP directory service. You set up a connection to the LDAP directory server and use search filters to specify the users and groups that you want to have access to the Informatica domain. You then import the user accounts into an LDAP security domain. If the LDAP server uses the SSL protocol, you must also specify the location of the SSL certificate.

After you import users into an LDAP security domain, you can assign roles, privileges, and permissions to the users. You can assign LDAP user accounts to native groups to organize the accounts based on their roles in the Informatica domain.

You cannot use the Administrator tool to create, edit, or delete users and groups in an LDAP security domain. You must make changes to LDAP users and groups in the LDAP directory service, and then synchronize the LDAP security domain with the LDAP directory service.

Use the LDAP Configuration dialog box to set up the connection to the LDAP directory service and create the LDAP security domain into which to import user accounts. You can also use the LDAP Configuration dialog box to set up a synchronization schedule.

To create an LDAP configuration, perform the following steps:

1. Configure the connection to the LDAP server that contains the directory service from which you want to import user accounts and groups.
2. Create an LDAP security domain for each set of user accounts and groups you want to import from the LDAP directory service.
3. Set up a schedule for the Service Manager to update the LDAP security domains with new or changed users and groups in the LDAP directory service.

Create the LDAP Configuration and Configure the LDAP Server Connection

Create the LDAP configuration and configure the connection to the LDAP server that contains the directory service from which you want to import the user accounts.

When you configure the connection to the LDAP server, indicate that the Service Manager must ignore the case sensitivity of the distinguished name attributes of the LDAP user accounts when it assigns users to groups in the Informatica domain. If the Service Manager does not ignore case sensitivity, the Service Manager might not assign all the users that belong to a group.

If the LDAP server uses SSL, you must import the certificate used by each domain node into the `cacerts` truststore file on a gateway node domain. You then copy the `cacerts` file that contains the imported certificates to the same directory on every node in the domain. For more information, see "Using a Self-Signed SSL Certificate" on page 27.

To set up a connection to the LDAP directory service, perform the following tasks:

1. In the Administrator tool, click the **Security** tab.
2. Click the **LDAP Configuration** tab.
3. Click the **Actions** menu, and then and select **Create LDAP Configuration**.
4. In the **Create LDAP Configuration** dialog box, click the **LDAP Connectivity** tab.
5. Configure the connection properties for the LDAP server.

   You might need to consult the LDAP administrator to get the information needed to connect to the LDAP server.

   The following table describes the LDAP server configuration properties:

Property	Description
LDAP Configuration Name	Name of the LDAP configuration.
Server Name	Host name or IP address of the machine hosting the LDAP directory service.
Port	Listening port for the LDAP server. This is the port number to communicate with the LDAP directory service. Typically, the LDAP server port number is 389. If the LDAP server uses SSL, the LDAP server port number is 636. The maximum port number is 65535.
LDAP Directory Service	Type of LDAP directory service.
Name	Distinguished name (DN) for the principal user. The user name often consists of a common name (CN), an organization (O), and a country (C). The principal user name is an administrative user with access to the directory. Specify a user that has permission to read other user entries in the LDAP directory service. To connect to Azure Active Directory, specify the User Principal Name (UPN) for the principal user.
Password	Password for the principal user. Leave blank for anonymous log in.
Use SSL Certificate	Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol.

Property	Description
Trust LDAP Certificate	Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.
Not Case Sensitive	Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups.
Group Membership Attribute	Name of the attribute that contains group membership information for a user. This is the attribute in the LDAP group object that contains the DNs of the users or groups who are members of a group. For example, *member* or *memberof*.
Maximum Size	Maximum number of user accounts to import into a security domain. For example, if the value is set to 100, you can import a maximum of 100 user accounts into the security domain. If the number of user to be imported exceeds the value for this property, the Service Manager generates an error message and does not import any user. Set this property to a higher value if you have many users to import. Default is 1000.

6. Click **Test Connection** to verify that the connection to the LDAP server is valid.
7. Click **OK** to save the LDAP configuration.

Configure the Security Domain

Create an LDAP security domain for each set of user accounts and groups you want to import from the LDAP directory service. Set up search bases and filters to define the set of user accounts and groups to include in a security domain.

The names of users and groups to be imported from the LDAP directory service must conform to the same rules as the names of native users and groups. The Service Manager does not import LDAP users or groups if names do not conform to the rules of native user and group names. Note that unlike native user names, LDAP user names can be case sensitive.

The Service Manager uses the user search bases and filters to import user accounts and the group search bases and filters to import groups. The Service Manager uses the filters to imports groups and the list of users that belong to each group.

If you modify the LDAP connection properties to connect to a different LDAP server, the Service Manager does not delete the existing security domains. You must ensure that the LDAP security domains are correct for the new LDAP server. Modify the user and group filters in the security domains or create additional security domains so that the Service Manager correctly imports the users and groups that you want to use in the Informatica domain.

To configure an LDAP security domain, perform the following steps:

1. In the Administrator tool, click the **Security** tab.
2. Click the **Actions** menu, and then select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **Security Domains** tab.
4. Click **Add**.

The following table describes the filter properties that you can set for a security domain:

Property	Description
Security Domain	Name of the LDAP security domain. The name is not case sensitive and must be unique within the domain. The string cannot exceed 128 characters or contain the following special characters: , + / < > @ ; \ % ? The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.
User search base	Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The search finds an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName, where the series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.
User filter	An LDAP query string that specifies the criteria for searching for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: `(objectclass=*)` searches all objects. `(&(objectClass=user)(!(cn=susan)))` searches all user objects except "susan". For more information about search filters, see the documentation for the LDAP directory service.
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

5. Click **Preview** to view a subset of the list of users and groups that fall within the filter parameters.

   If the preview does not display the correct set of users and groups, modify the user and group filters and search bases to get the correct users and groups.

6. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, click **Synchronize Now**.

   The Service Manager synchronizes the users in all the LDAP security domains with the users in the LDAP directory service. The time it takes for the synchronization process to complete depends on the number of users and groups to be imported.

7. Click **OK** to save the security domain.

Configure the Synchronization Schedule

You can set up a daily schedule for the Service Manager to update the LDAP security domains with new or changed users and groups in the LDAP directory service.

When the Service Manager synchronizes the LDAP security domains with the LDAP directory service, it imports all users that match the user filter settings from the LDAP directory service into the security domain. The Service Manager then imports all groups that match the group filter settings, and associates users with their corresponding groups. The Service Manager also deletes any user or group not found in the LDAP directory service from the security domain.

By default, the Service Manager is not scheduled time to synchronize with the LDAP directory service. To ensure that the list of users and groups in the LDAP security domains is accurate, schedule when the Service

Manager synchronizes the LDAP security domains with the LDAP directory service. The Service Manager synchronizes the LDAP security domains with the LDAP directory service every day at the times you set.

To ensure that synchronization succeeds, consider the following recommendations before set up the synchronization schedule:

Verify that the /etc/hosts file contains an entry for the LDAP server.

Verify that the `/etc/hosts` file on each node gateway in the domain contains an entry with the host name and IP address of the LDAP server. If the Service Manager cannot resolve the host name for the LDAP server, synchronization can fail.

Enable paging in LDAP if you are synchronizing more than 100 users or groups.

Enable paging on the LDAP directory service before you synchronize more than 100 users or groups. If you do not enable paging on the LDAP directory service, synchronization can fail.

Synchronize security domains during times when most users are not logged in to Informatica applications.

During synchronization, the Service Manager locks each user account it synchronizes. Users might not be able to log in to the Informatica application clients during synchronization. Users logged in to an application client when synchronization starts might not be able to perform certain tasks.

To set up a schedule that synchronizes LDAP security domains with the LDAP directory service, perform the following steps:

1. In the Administrator tool, click the **Security** tab.
2. Click the **Actions** menu and select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **Schedule** tab.
4. Click the **Add** button (+) to add a time.

   The synchronization schedule uses a 24-hour time format.
5. To immediately synchronize the users and groups in the LDAP security domains with the users and groups in the LDAP directory service, click **Synchronize Now**.
6. Click **OK** to save the synchronization schedule.

   Note: Wait until the Service Manager synchronizes with the LDAP directory service before restarting the Informatica domain to avoid losing the synchronization times that you set in the schedule.

Using Nested Groups in the LDAP Directory Service

An LDAP security domain can contain nested LDAP groups. The Service Manager can import nested groups that are created in the following manner:

- Create the groups under the same organizational units (OU).
- Set the relationship between the groups.

For example, you want to create a nested grouping where GroupB is a member of GroupA and GroupD is a member of GroupC.

1. Create GroupA, GroupB, GroupC, and GroupD within the same OU.
2. Edit GroupA, and add GroupB as a member.
3. Edit GroupC, and add GroupD as a member.

You cannot import nested LDAP groups into an LDAP security domain that are created in a different way.

Using a Self-Signed SSL Certificate

You can connect to an LDAP server that uses an SSL certificate signed by a certificate authority (CA). By default, the Service Manager does not connect to an LDAP server that uses a self-signed certificate.

To connect to an LDAP server that uses an SSL certificate, use the Java keytool key and certificate management utility to import the certificates used by all domain nodes into the Java `cacerts` truststore file on a single gateway node in the domain. You then copy the `cacerts` keystore file that contains the imported certificates to the other nodes in the domain.

The `cacerts` truststore file is in the following directory on each node:

```
<Informatica installation directory>\java\jre\lib\security
```

The keytool utility is available in the following directory on each node:

```
<Informatica installation directory>\java\bin
```

Restart the node after you import the certificate.

Deleting an LDAP Configuration

You can delete an LDAP configuration and the associated security domains to permanently prohibit users from accessing the domain.

When you delete an LDAP configuration, you must first delete the security domains associated with the LDAP configuration. The Service Manager deletes all user accounts and groups in each deleted LDAP security domain from the domain configuration database.

1. In the Administrator tool, click the **Security** tab.
2. Click the **LDAP Configuration** tab.
3. Click the **Security Domains** tab, and then click the **Edit** button.
4. Select a security domain in the **Edit LDAP Configuration** dialog, and then click **Delete**.
5. Select the LDAP configuration to delete in the LDAP Configuration navigator.
6. Click the **Actions** menu, and then and select **Delete LDAP Configuration**.
7. Click **OK** to confirm that you want to delete the LDAP configuration.

CHAPTER 4

Kerberos authentication

Kerberos is a computer network authentication protocol that enables CDI-PC Client, nodes, and services communicating over a network to connect to one another in a secure manner.

Kerberos authentication eliminates Informatica native accounts and removes the need for the domain to pass user credentials to an LDAP server. After you enable Kerberos authentication in a domain, Informatica clients use the Kerberos tickets created during the Windows authentication process to log in to the Informatica services running in the domain.

You can enable Kerberos authentication in a domain that runs on a Windows network. The network must use Microsoft Active Directory Domain Services (AD DS) as the Kerberos principal database.

To enable Kerberos authentication in CDI-PC domain, perform the following steps:

Prepare to enable Kerberos authentication.

You must complete multiple tasks before you enable Kerberos authentication. The tasks you must complete include the following tasks:

- Create the Kerberos configuration file.
- Create accounts for Kerberos principal users in Active Directory.
- Generate the service principal name (SPN) and keytab formats.
- Create the keytab files used to authenticate users and services in the network.

Enable Kerberos authentication in the CDI-PC domain.

You can enable Kerberos authentication in CDI-PC domain when you install the Informatica services, or you can enable Kerberos authentication after you install the services. If you do not enable Kerberos authentication during installation, you can use the Informatica command line programs to configure the domain to use Kerberos authentication.

Enable Kerberos authentication on CDI-PC nodes and client hosts.

After you enable Kerberos in the domain, copy the Kerberos configuration file to each node in the domain and to each CDI-PC Client host. You also configure web browsers to access the Informatica web applications.

Enable Informatica users to use Kerberos authentication.

After you enable Kerberos authentication, import Informatica users from Active Directory into an LDAP security domain that contains the Kerberos user accounts. You must also migrate the groups, roles, privileges, and permissions of the native user accounts to the user accounts in the LDAP security domain.

How Kerberos Works in the CDI-PC domain

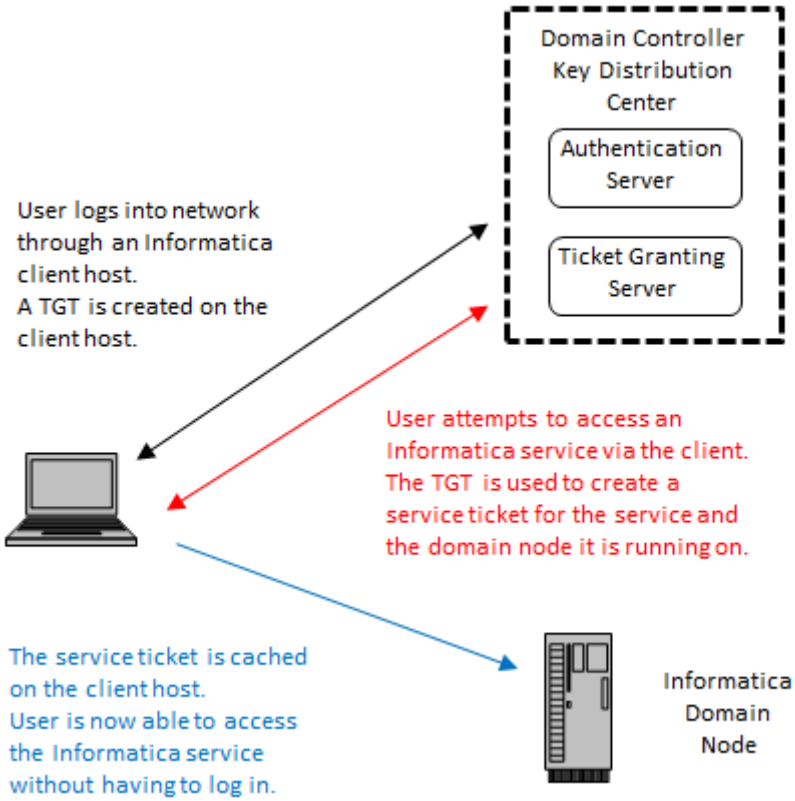
In a domain configured to use Kerberos authentication, CDI-PC Client authenticates with nodes and application services within the domain, without requiring passwords.

In a domain that uses Kerberos authentication, services that run within the domain, including node processes, web application processes, and CDI-PC application services, are Kerberos *principals*. The Active Directory principal database the Kerberos realm uses contains a user account for each principal.

The Kerberos authentication protocol uses *keytabs* to authenticate CDI-PC Client with services that run within the domain. The keytab for a principal is stored on the node on which the service runs. The keytab contains the *service principal name (SPN)* that identifies the service within the Kerberos realm, and the key assigned to the SPN in Active Directory.

When the KDC gives a service ticket to a client, it encrypts the ticket with the key assigned to the SPN. The requested service uses the key to decrypt the service ticket.

The following image illustrates the basic Kerberos authentication flow:



The following outline describes the basic Kerberos authentication flow:

1. CDI-PC Client user logs in to a network computer hosting the CDI-PC Client.
2. The login request is directed to the *Authentication Server*, a component of the *Kerberos Key Distribution Center (KDC)*. The KDC is a network service with access to user account information that runs on each domain controller within the Active Directory domain.
3. The Authentication Server verifies that the user exists in the principal database, and then creates a Kerberos token called a *ticket-granting-ticket (TGT)* on the user's computer.

4. The user attempts to access a process or service within the CDI-PC domain through CDI-PC Client.
5. Informatica and the Kerberos libraries use the TGT to request a *service ticket* and *session key* for the requested service from the *Ticket Granting Server*, which also runs within the KDC.
6. Kerberos uses the service ticket to authenticates the client with the requested service.
   The service ticket is cached on the computer hosting the CDI-PC Client, enabling the client to use the ticket while it remains valid. If the user shuts down and then restarts the Informatica client, the client reuses the same ticket to access processes and services within the CDI-PC domain.

Kerberos Cross Realm Authentication

You can configure the CDI-PC domain to use Kerberos cross realm authentication. Kerberos cross realm authentication enables CDI-PC Clients that belong to one Kerberos realm to authenticate with nodes and application services that belong to another Kerberos realm.

When you configure a domain to use Kerberos cross-realm authentication, you add properties for each Kerberos realm to the Kerberos configuration file. You also include the name of each realm when you run `infasetup` commands to enable Kerberos authentication in the domain and on domain nodes.

The Active Directory servers that the domain uses for Kerberos cross realm authentication must belong to the same Active Directory forest. An Active Directory forest is a group of Active Directory domains that share a common global catalog, directory schema, logical structure, and directory configuration. You connect to the global catalog to import users from the Active Directory servers into LDAP security domains.

To use Kerberos cross domain authentication, two-way trust must be enabled between the Active Directory servers in the forest.

Converting a Domain From Kerberos Single Realm Authentication to Kerberos Cross Realm Authentication

You can convert CDI-PC domain that uses a single Kerberos realm to authenticate users to use Kerberos cross realm authentication.

You must also import user and group accounts from the Active Directory global catalog into an LDAP security domain. When you import accounts, existing accounts in the LDAP security domain, which use the samAccount name attribute, are deleted and are replaced with new accounts that use the user principal name attribute.

Users log in to CDI-PC Clients with the fully qualified user principal name, which is in the following format:

```
<user name>@<KERBEROS REALM NAME>
```

After you import the user and group accounts, assign privileges, roles, and permissions to the accounts.

1. Add the required properties for each Kerberos realm to the Kerberos configuration file.

   Set the properties for each realm in the `krb5.conf` configuration file on each node in the domain. Restart the domain after you update the file on all of the nodes in the domain.

   For more information about configuring the `krb5.conf` configuration file for Kerberos cross realm authentication, see "Configure the Kerberos Configuration File" on page 32.
2. Copy the updated `krb5.conf` file to the following directory on each computer that hosts an Informatica client:

   ```
   <Informatica installation directory>\clients\shared\security
   ```

3. Run the `infasetup UpdateGatewayNode` and `infasetup UpdateWorkerNode` commands on the domain nodes.

   Specify the name of each Kerberos realm that the domain uses to authenticate users as the values for the -srn and -urn options, separated by a comma.

   For more information about running the infasetup commands, see the "infasetup Command Reference" chapter in the *Command Reference Guide*.
4. Run the UpdateKerberosConfig command on a gateway node within the domain.

   Specify the name of each Kerberos realm that the domain uses to authenticate users as the values for the -srn and -urn options, separated by a comma.
5. Run the UpdateKerberosAdminUser command on a gateway node within the domain.

   Specify the fully qualified user principal name for the domain administrator user account.
6. Import user and group accounts into LDAP security domains.

   Connect to the Active Directory global catalog. When you connect to the global catalog, you import users from the Active Directory server used by each Kerberos realm.

   For more information about connecting to the global catalog and importing accounts, see "Import User Accounts from Active Directory into LDAP Security Domains" on page 50.
7. Assign privileges, roles, and permissions to the user and group accounts you imported into an LDAP security domain.

   For more information about assigning privileges and roles, see Chapter 9, "Privileges and Roles" on page 115.

   For more information about assigning permissions, see Chapter 10, "Permissions" on page 142.

Preparing to Enable Kerberos Authentication

You must complete multiple tasks to prepare to enable Kerberos authentication in the CDI-PC domain. The procedures you follow for each task depend on the service principal level at which you enable Kerberos.

Note: You cannot disable Kerberos authentication in a domain after you enable it. You also cannot switch the service principal level between the node level and the process level.

Determine the Kerberos Service Principal Level

When you prepare to enable Kerberos authentication, you must determine the required service principal level. The required service principal level determines the procedures you must follow to prepare to enable Kerberos authentication in the domain.

You can enable Kerberos authentication at one of the following levels:

Node Level

If you use the domain for testing or development, and the domain does not require a high level of security, you can enable Kerberos at the node level. You can use a single service principal name and a single keytab file for the node and for all of the processes and services that run on the node. You must also create a an SPN and a keytab file for the HTTP processes that run on the node.

Process Level

If you use the domain for production, and the domain requires a high level of security, you can set the service principal at the process level. You create a unique SPN and keytab file for each node and each

process on the node. You must also create a an SPN and a keytab file for the HTTP processes that run on the node.

Kerberos enabled at the process level provides the highest level of security, but might be difficult to manage in the CDI-PC domain that contains many nodes or has many services. In this scenario, you might want to enable Kerberos at the node level.

Configure the Kerberos Configuration File

Set the properties required by Informatica in the Kerberos configuration file, and then copy the file to each node in the CDI-PC domain.

Kerberos stores configuration information in a file named *krb5.conf*. You must set the properties in the krb5.conf configuration file and then copy the file to every node in the CDI-PC domain.

If the domain uses Kerberos cross realm authentication, enter the required properties for each Kerberos realm.

1. Configure the following Kerberos library properties in the *libdefaults* section of the file.

   The following table describes the properties to enter:

Property	Description
default_realm	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. If the domain uses a single Kerberos realm for authentication, the service realm name and the user realm name must be the same.
forwardable	Allows a service to delegate client user credentials to another service. The CDI-PC domain requires application services to authenticate the client user credentials with other services. Set to true.
default_tkt_enctypes	Encryption types for the session key included in ticket-granting tickets (TGT). Set this property only if session keys must use specific encryption types. Ensure that the Kerberos Key Distribution Center (KDC) supports the encryption type that you specify. Do not set this property to allow the Kerberos protocol to select the encryption type to use. If the node hosts or CDI-PC Client hosts use 256-bit encryption, install the Java Cryptography Extension (JCE) unlimited strength policy files on all node hosts and CDI-PC Client hosts to avoid authentication issues.
rdns	Determines whether reverse name lookup is used in addition to forward name lookup to canonicalize host names for use in service principal names. Set to false.
renew_lifetime	The default renewable lifetime for initial ticket requests.
ticket_lifetime	The default lifetime for initial ticket requests.
udp_preference_limit	Determines the protocol that Kerberos uses when it sends a message to the KDC. Set to 1 to use the TCP protocol if the domain experiences intermittent Kerberos authentication failures.

Property	Description
dns_lookup_kdc	Indicates whether the Kerberos client uses DNS SRV records to locate the KDCs and other servers for a realm, if they are not listed in the information for the realm. DNS uses SRV records to identify computers that host specific services. Required when the domain is Kerberos-enabled. Requires you to set the admin_server realm property. Set to true.
dns_lookup_realm	Indicates whether the Kerberos client uses DNS TXT records to determine the Kerberos realm of a host. DNS uses text or TXT records to associate arbitrary text with a host or other name, such as human readable information about a server, network, data center, or other accounting information. Required when the domain is Kerberos-enabled. Set to true.

2. Define each Kerberos realm in the *realms* section of the file.

   The following example shows the entry for a Kerberos realm named COMPANY.COM:

   ```
   [realms]
   COMPANY.COM = {...}
   ```

3. Enter the following realm properties inside the brackets for each Kerberos realm in the *realms* section of the file.

   The following table describes the properties to enter:

Property	Description
admin_server	The name or IP address of the Kerberos administration server host. You can include an optional port number, separated from the host name by a colon. Default is 749. Required if you configure dns_lookup_kdc in the *libdefaults* section.
kdc	The name or IP address of a host running the Key Distribution Center (KDC) for the realm. You can include an optional port number, separated from the host name by a colon. Default is 88.

   The following example shows the entries for each Kerberos realm in a Kerberos cross realm configuration:

   ```
   [realms]
   COMPANY.COM = {
   admin_server = KDC01.COMPANY.COM:749
   kdc = KDC01.COMPANY.COM:88
   }
   EAST.COMPANY.COM = {
   kdc = 10.75.141.193
   admin_server = 10.75.141.193
   }
   WEST.COMPANY.COM = {
   kdc = 10.78.140.111
   admin_server = 10.78.140.111
   }
   ```

4. In the *domain_realms* section, map the domain name or host name to a Kerberos realm name. The domain name is prefixed by a period (.).

The following example shows the parameters for the Hadoop domain_realm if the CDI-PC domain does not use Kerberos authentication:

```
[domain_realm]
 .hadoop_realm.com = HADOOP-REALM
  hadoop_realm.com = HADOOP-REALM
```

The following example shows the parameters for the Hadoop domain_realm if the CDI-PC domain uses Kerberos authentication:

```
[domain_realm]
.infa_ad_realm.com = INFA-AD-REALM
  infa_ad_realm.com = INFA-AD-REALM
.hadoop_realm.com = HADOOP-REALM
  hadoop_realm.com = HADOOP-REALM
```

The following example shows the content of a Kerberos configuration file with the required properties for a single Kerberos realm configuration:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
```

The following example shows the content of a Kerberos configuration file with the required properties for a Kerberos cross realm configuration:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
admin_server = 10.78.140.111

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
```

```
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM
```

For more information about the Kerberos configuration file, see the Kerberos network authentication documentation.

Create Kerberos Principal Accounts in Active Directory

Create LDAP user accounts for the Kerberos principals in Active Directory. A Kerberos principal is a process, service, or user within the Kerberos realm.

If you set the default_tkt_enctypes property in the krb5.conf configuration file to the 128-bit or 256-bit AES encryption types, configure each account to use the corresponding encryption type in Active Directory.

The accounts that you create depend on whether you enable Kerberos at the node level or at the process level.

Note: Account names can be a maximum of 20 characters in length.

Accounts Required at Node Level

Create the LDAP user accounts required to enable Kerberos authentication at the node level in Active Directory.

Create the following Kerberos principal accounts in Active Directory if you enable Kerberos at the node level:

Node processes

Create an account for each node that runs in the domain.

HTTP process

Create an account for the Informatica web applications that run on a node in the domain. Web applications that run on a node might include the Administrator tool.

Bind User Distinguished Name (DN)

Create an LDAP bind user account that you use to synchronize the LDAP security domain that contains Kerberos user accounts with Active Directory.

Accounts Required at Process Level

Create the LDAP user accounts required to enable Kerberos authentication at the process level in Active Directory.

Create the following Kerberos principal accounts in Active Directory if you enable Kerberos at the process level:

Node processes

Create an account for each node that runs in the domain.

HTTP processes

Create an account for the Informatica web applications that run on a node in the domain.

Informatica Administrator service

Create an account for the Administrator tool on each gateway node in the domain.

Informatica application services

Create an account for every Informatica application service that runs on each node in the domain.

Bind User Distinguished Name (DN)

Create an LDAP user account that you use to synchronize the LDAP security domain that contains Kerberos user accounts with Active Directory.

Generate the Service Principal Name and Keytab File Name Formats

Use the Informatica Kerberos SPN Format Generator utility to generate the service principal name (SPN) and keytab file name formats required to use Kerberos authentication. The Kerberos SPN Format Generator utility generates a text file named SPNKeytabFormat.txt that contains the correct format for the SPNs and keytab file names.

The SPN and keytab file name formats you generate depend on whether you enable Kerberos at the node level or at the process level.

Generate the Service Principal Name and Keytab File Name Formats at Node Level

Generate the formats for the SPNs and keytab file names required to enable Kerberos authentication at the node level.

The CDI-PC domain requires SPNs and keytab files for the following processes when you enable Kerberos authentication at the node level:

Node processes

Informatica requires an SPN and keytab file for every node in the domain. Kerberos uses the same service principal name and keytab to authenticate the CDI-PC application services that run on the node.

HTTP processes

Informatica requires an SPN and keytab file for the web applications that run on each node in the domain. Web applications that run on a node might include the Administrator tool. Kerberos uses the same service principal name to authenticate all of the web applications that run on the node.

1. On a Windows Informatica node host, go to the directory that contains the SPNFormatGenerator.bat batch file:

   ```
   <Informatica installation directory>\tools\Kerberos
   ```

   On a UNIX Informatica node host, go to the directory that contains the SPNFormatGenerator.sh shell file:

   ```
   <Informatica installation directory>/tools/Kerberos
   ```

2. Run SPNFormatGenerator.bat or SPNFormatGenerator.sh.
3. Click **Next**.
4. Select **Node Level**.
5. Click **Next**.
6. Enter the properties required to generate the SPN and keytab file formats.

The following table describes the properties:

Prompt	Description
Domain Name	Name of the Informatica domain. The name must not exceed 128 characters and must be 7-bit ASCII. It can't contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Service Realm Name	Name of the Kerberos realm. The realm name must be in uppercase.
Node Name	Name of the Informatica node.
Node Host Name	Fully qualified name of the node host. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the host.

7. To generate the SPN format for an additional node, click **+Node** and specify the node name and host name.
8. Click **Next**.

   The SPN Format Generator utility displays the path and file name of the file that contains the list of service principal names and keytab file names.
9. Click **Done** to exit the SPN Format Generator utility.

Generate the Service Principal Name and Keytab File Name Formats at Process Level

Generate the formats for the SPNs and keytab file names required to enable Kerberos authentication at the process level.

The CDI-PC domain requires SPNs and keytab files for the following processes and services when you enable Kerberos authentication at the process level:

Node processes

Informatica requires an SPN and keytab file for every node in the domain.

Informatica Administrator

Informatica requires an SPN and keytab file for the Administrator tool for every gateway node in the domain.

HTTP processes

Informatica requires an SPN and keytab file for the web applications that run on a node in the domain.

Informatica application service processes

Informatica requires an SPN and keytab file for each Informatica application service that runs on every node in the domain.

1. On a Windows Informatica node host, go to the directory that contains the SPNFormatGenerator.bat batch file:

   ```
   <CDI-PC installation directory>/tools/Kerberos
   ```

   On a UNIX Informatica node host, go to the directory that contains the SPNFormatGenerator.sh shell file:

   ```
   <Informatica installation directory>/tools/Kerberos
   ```
2. Run SPNFormatGenerator.bat or SPNFormatGenerator.sh.

3. Click **Next**.
4. Select **Process Level**.
5. Click **Next**.
6. Enter the properties required to generate the SPN and keytab file formats.

   The following table describes the properties:

Prompt	Description
Domain Name	Name of the CDI-PC domain. The name must not exceed 128 characters and must be 7-bit ASCII. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Service Realm Name	Name of the Kerberos realm. The realm name must be in uppercase.
Node Name	Name of the CDI-PC node.
Node Host Name	Fully qualified name or the IP address of the node host. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the host.

7. To generate the SPN format for an Informatica application service that runs on a node, click **Service** after entering the node details.

   Enter the name of the CDI-PC application service as shown in the Administrator tool. Complete this step for each CDI-PC application service that runs on each node in the domain.
8. To generate the SPN format for an additional node, click **+Node** and specify the node name and host name.
9. Click **Next**.

   The SPN Format Generator utility displays the path and file name of the file that contains the list of service principal names and keytab file names.
10. Click **Done** to exit the SPN Format Generator utility.

Review the Service Principal Name and Keytab File Name Format Text File

After you generate the SPNKeytabFormat.txt file, you can review the file.

You use the information in the file to generate the keytab files, and to associate each SPN with the corresponding principal user account in Active Directory.

The SPNKeytabFormat.txt file contains the following information:

Entity Name

Identifies the node or service associated with the process.

Service Principal Name

Format for the SPN. The SPN is case sensitive.

Note: If you enter a string containing multiple Kerberos domain names, or add an asterisk before a realm suffix to include all realms that include the suffix, the SPN format does not include the realm name.

The following table describes the SPN formats:

Keytab type	SPN Format
NODE_SPN	isp/<node name>/<domain name>@<REALM NAME>
NODE_AC_SPN	_AdminConsole/<node name>/<domain name>@<REALM NAME>
NODE_HTTP_SPN	HTTP/<node host name>@<REALM NAME> **Note:** The Kerberos SPN Format Generator validates the node host name. If the node host name is not valid, the utility does not generate an SPN. Instead, it displays the following message: Unable to resolve host name.
SERVICE_PROCESS_SPN	<application service name>/<node name>/<domain name>@<REALM NAME>

Keytab File Name

Format for the name of the keytab file to be created for the associated SPN. The keytab file name is case sensitive.

The following table describes the keytab file name formats:

Keytab Type	Keytab File Name
NODE_SPN	<node name>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<application service name>.keytab

Service Principals at Node Level

The following image shows the contents of the SPNKeytabFormat.txt file generated for service principals at the node level:

```
ENTITY_NAME     SPN                                        KEY_TAB_NAME          KEY_TAB_TYPE
node01          isp/node01/InfaDomain@COMPANY.COM          node01.keytab         NODE_SPN
node01          HTTP/US001DEV.company.com@COMPANY.COM      webapp_http.keytab    NODE_HTTP_SPN
node02          isp/node02/InfaDomain@COMPANY.COM          node02.keytab         NODE_SPN
node02          HTTP/US005DEV.company.com@COMPANY.COM      webapp_http.keytab    NODE_HTTP_SPN
```

Service Principals at Process Level

The following image shows the contents of the SPNKeytabFormat.txt file generated for service principals at the process level:

```
ENTITY_NAME     SPN                                        KEY_TAB_NAME          KEY_TAB_TYPE
node01          isp/node01/InfaDomain@COMPANY.COM          node01.keytab         NODE_SPN
node01          _AdminConsole/node01/InfaDomain@COMPANY.COM _AdminConsole.keytab  NODE_AC_SPN
node01          HTTP/US001DEV.company.com@COMPANY.COM      webapp_http.keytab    NODE_HTTP_SPN
node02          isp/node02/InfaDomain@COMPANY.COM          node02.keytab         NODE_SPN
node02          _AdminConsole/node02/InfaDomain@COMPANY.COM _AdminConsole.keytab  NODE_AC_SPN
node02          HTTP/US005DEV.company.com@COMPANY.COM      webapp_http.keytab    NODE_HTTP_SPN
MRS_dev:node01  MRS_dev/node01/InfaDomain@COMPANY.COM      MRS_dev.keytab        SERVICE_PROCESS_SPN
DIS_dev:node01  DIS_dev/node01/InfaDomain@COMPANY.COM      DIS_dev.keytab        SERVICE_PROCESS_SPN
CAT_dev:node02  CAT_dev/node02/InfaDomain@COMPANY.COM      CAT_dev.keytab        SERVICE_PROCESS_SPN
```

Generate the Keytab Files

Generate the keytab files used to authenticate Informatica users and services.

You use the Microsoft Windows Server ktpass utility to generate a keytab file for each user account you created in Active Directory. You must generate the keytab files on a member server or on a domain controller within the Active Directory domain. You cannot generate keytab files on a workstation operating system such as Microsoft Windows 7.

To use ktpass to generate a keytab file, run the following command:

```
ktpass.exe -out  <keytab filename> -princ <service principal name> -mapuser <user
account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-
target <realm name>]
```

The following table describes the command options:

Option	Description
-out	The file name of the Kerberos keytab file to generate as shown under the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file.
-princ	The service principal name displayed under the `SPN` column in the SPNKeytabFormat.txt file. If the domain uses Kerberos cross realm authentication, the service principal name must be unique across all Kerberos realms.
-mapuser	The Active Directory user account to associate with the SPN. The account name can be a maximum of 20 characters.
-pass	The password set in Active Directory for the Active Directory user account, if applicable.
-crypto	Specifies the key types generated in the keytab file. Set to all to use all supported cryptographic types.
-ptype	The principal type. Set to KRB5_NT_PRINCIPAL.
-target	The name of the realm to which the Active Directory server belongs. Include this option if the following error occurs when you run the utility: DsCrackNames returned 0x2 in the name

The keytab files you generate depends on whether you enable Kerberos at the node level or at the process level.

Generate the Keytab Files at Node Level

When you run ktpass to generate the keytab files at the node level, you associate each Kerberos principal user account with the corresponding SPN in Active Directory.

The following table shows the association between the Kerberos principal user accounts and the SPNs shown in the example SPNKeytabFormat.txt file:

User Account	Keytab Type	Service Principal Name
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM

User Account	Keytab Type	Service Principal Name
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

You also create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

1. Create a keytab file for the Kerberos principal user account that you created for each node in Active Directory.

   Copy the keytab file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named nodeuser0:

   ```
   ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser
   nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

2. Create a keytab file for each HTTP process Kerberos principal user account that you created in Active Directory.

   If the domain uses Kerberos cross realm authentication, the principal user account can exist in any Kerberos realm the domain uses.

   Copy the keytab file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named httpuser01:

   ```
   ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
   httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

3. Create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

   Structure the value for the -princ option as <principal name>@<KERBEROS REALM>. Include the name of the LDAP configuration for the Active Directory server in the keytab file name. Structure the keytab file name as follows: <Active Directory LDAP configuration_name>.keytab.

   The following example creates a keytab file for a service principal user account named ldapuser:

   ```
   ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser
   ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

Generate the Keytab Files at Process Level

When you run ktpass to generate the keytab files at the process level, you associate each Kerberos principal user account with the corresponding SPN in Active Directory.

The following table shows the association between the Kerberos principal user accounts and the SPNs shown in the example SPNKeytabFormat.txt file:

User Account	Keytab Type	Service Principal Name
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/InfaDomain@COMPANY.COM

User Account	Keytab Type	Service Principal Name
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/InfaDomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/InfaDomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/InfaDomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/InfaDomain@COMPANY.COM

You also create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

1. Create a keytab file for the Kerberos principal user account that you created for each node in Active Directory.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named nodeuser01:

   ```
   ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser
   nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

2. Create a keytab file for each HTTP process Kerberos principal user account that you created.

   If the domain uses Kerberos cross realm authentication, the principal user account can exist in any Kerberos realm the domain uses.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named httpuser01:

   ```
   ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
   httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

3. Create a keytab file for each Administrator tool Kerberos principal user account that you created.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named admintooluser01:

   ```
   ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/InfaDomain@COMPANY.COM -
   mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

4. Create a keytab file for each Informatica application service Kerberos principal user account that you created.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a service Kerberos principal user account named MRSdevuser01:

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

5. Create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

   Structure the value for the -princ option as <principal name>@<KERBEROS REALM>. Include the name of the LDAP configuration for the Active Directory server in the keytab file name. Structure the keytab file name as follows: <Active Directory LDAP configuration_name>.keytab.

   The following example creates a keytab file for a service principal user account named ldapuser:

   ```
   ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser
   ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

Verify the Service Principal Names and Keytab Files

You can use Kerberos utilities to verify that the SPNs and the keytab files are valid. You can also use the utilities to determine the status of the Kerberos Key Distribution Center (KDC).

You can use Kerberos utilities such as *kinit* and *klist* to view and verify the SPNs and keytab files. To use the utilities, ensure that the KRB5_CONFIG environment variable contains the path and file name of the Kerberos configuration file. For more information about running the Kerberos utilities, see the Kerberos documentation.

Use the following utilities to verify the SPNs and keytab files:

kinit

You can use the *kinit* utility to request a ticket-granting ticket (TGT) from the KDC and verify that a keytab file can be used to establish a Kerberos connection. If the keytab and specified SPN are valid, the command obtains a ticket, and then caches the ticket in the specified cache.

The kinit utility is available in the following directory on an Informatica node:

```
<CDI-PC installation directory>\java\jre\bin
```

To request a ticket-granting ticket for an SPN, run the following command:

```
kinit -c <cache name> -k -t <keytab file name> <service principal name>
```

The following output example shows the ticket-granting ticket created in the default cache for a specified keytab file and SPN:

```
Cache: \temp\krb
Using principal: isp/node01/InfaDomain/COMPANY.COM
Using keytab: node01.keytab
Authenticated to Kerberos v5
```

klist

You can use the *klist* utility to list the Kerberos principals and keys in a keytab file. To list the keys in the keytab file and the time stamp for the keytab entry, run the following command:

```
klist -k -t <keytab file name>
```

The following output example shows the principals in a keytab file:

```
Keytab name: FILE:node01.keytab
KVNO Timestamp         Principal
---- ----------------- --------------------------------------------------------
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
```

Enabling Kerberos Authentication

You can enable Kerberos authentication in an CDI-PC domain when you install the CDI-PC services, or you can enable Kerberos authentication after you install the services.

If you do not enable Kerberos authentication during installation, follow the steps in this section to use the Informatica command line programs to enable Kerberos authentication after you install the services.

Enable Kerberos Authentication in the Domain

Enable Kerberos on a gateway node within the domain.

Run the infasetup switchToKerberosMode command on a gateway node within the domain to change the authentication to Kerberos network authentication.

1. Shut down the domain and all CDI-PC services. Shut down the services in the following order:
   - CDI-PC Integration Service
   - CDI-PC Repository Service
2. At the command prompt on a gateway node, switch to the directory where the infasetup executable is located:

   ```
   <CDI-PC installation directory>\isp\bin
   ```
3. Run the following command:

   ```
   infasetup switchToKerberosMode -ad <administrator name> -srn <Kerberos realm names> -
   urn <Kerberos realm names> -spnSL <service principal level>
   ```

The following table describes the options and arguments for the infasetup switchToKerberosMode command:

Option	Argument	Description
-administratorName -ad	user_name	User name for the domain administrator account that is created when you configure Kerberos authentication. Specify the name of an account that exists in Active Directory. After you configure Kerberos authentication, this user is included in the *_infaInternalNamespace* security domain that the command creates. If the domain uses a single Kerberos realm to authenticate users, specify the samAccount name of the account you want to use as the administrator account. If the domain uses Kerberos cross realm authentication, specify the fully qualified user principal name of the account you want to use as the administrator account, including the realm name. For example: sysadmin@COMPANY.COM
-ServiceRealmName -srn	Kerberos_realm_name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
-SPNShareLevel -spnSL	NODE|PROCESS	Service principal level for the domain. Set to NODE to enable Kerberos at the node level. Set to PROCESS to enable Kerberos at the process level.

The following example changes the domain authentication to Kerberos and sets the sysadmin user account as the administrator account in a domain that uses a single Kerberos realm to authenticate users:

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL
NODE
```

The following example changes the domain authentication to Kerberos and sets the sysadmin user account as the administrator account in a domain that uses Kerberos cross realm authentication:

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -spnSL NODE
```

Update the Nodes in the Domain

Update all gateway and worker nodes with the Kerberos authentication server information except the gateway nodes on which you ran the infasetup switchToKerberosMode command.

Use the following commands to update the gateway and worker nodes:

infasetup UpdateGatewayNode

Use the UpdateGatewayNode command to set the Kerberos authentication parameters on a gateway node in the domain. If the domain has multiple gateway nodes, run the UpdateGatewayNode command on each gateway node.

infasetup UpdateWorkerNode

Use the UpdateWorkerNode command to set the Kerberos authentication parameters on a worker node in the domain. If the domain has multiple worker nodes, run the UpdateWorkerNode command on each worker node.

1. At the command prompt on a node, switch to the directory where the infasetup executable is located:

   ```
   <Informatica installation directory>\isp\bin
   ```

2. To set the Kerberos authentication parameters on a gateway node, run the following command:

   ```
   infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn
   <Kerberos realm names>
   ```

   To set the Kerberos authentication parameters on a worker node, run the following command:

   ```
   infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn
   <Kerberos realm names>
   ```

The following table describes the options and arguments required to enable Kerberos authentication on a node:

Option	Argument	Description
-EnableKerberos -krb	true|false	Configures the CDI-PC domain to use Kerberos authentication. Set to true to enable Kerberos authentication. Default is false.
-ServiceRealmName -srn	Kerberos_realm_name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM

The following example updates a worker node to use Kerberos authentication:

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

The following example updates a worker node to use Kerberos cross realm authentication:

```
infasetup updateWorkerNode -krb true -srn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

Enabling Kerberos on CDI-PC Nodes

After you enable Kerberos in the domain, you must copy the Kerberos configuration file to each node in the domain. You must also configure web browsers to access the CDI-PC web applications.

Copy the keytab files to the following directory on each node:

```
<CDI-PC installation directory>\isp\config\keys
```

The keytab files you copy depends on whether you enable Kerberos authentication at the node level or at the process level.

Keytab Files at Node Level

Copy each keytab file generated at the node level to the corresponding node.

The following table shows the node to which to copy each keytab file:

Keytab File	Location on Node
<node name>.keytab	Copy each file to the corresponding node.
webapp_http.keytab	Copy each file to the corresponding gateway node.
ldapuser.keytab	Copy the file to each gateway node.

Keytab Files at Process Level

Copy each keytab file generated at the process level to the corresponding node.

The following table shows the node to which to copy each keytab file:

Keytab File	Location on Node
<node name>.keytab	Copy each file to the corresponding node.
webapp_http.keytab	Copy each file to the corresponding gateway node.
_AdminConsole.keytab	Copy each file to the corresponding gateway node.
<application service name>.keytab	Copy each file to the corresponding node on which the CDI-PC application service runs.
ldapuser.keytab	Copy the file to each gateway node.

Configure web browsers to access CDI-PC web applications.

In Microsoft Internet Explorer and Google Chrome, add the URL of the CDI-PC web applications to the list of trusted sites.

If you are using Chrome version 41 or later, you must also set the AuthServerWhitelist and AuthNegotiateDelegateWhitelist policies.

Copy the Keytab Files to the CDI-PC Nodes

After you create the keytab files, copy each keytab file to the corresponding node.

Copy the keytab files to the following directory on each node:

```
<CDI-PC installation directory>\isp\config\keys
```

The keytab files you copy depends on whether you enable Kerberos authentication at the node level or at the process level.

Keytab Files at Node Level

Copy each keytab file generated at the node level to the corresponding node.

The following table shows the node to which to copy each keytab file:

Keytab File	Location on Node
<node name>.keytab	Copy each file to the corresponding node.
webapp_http.keytab	Copy each file to the corresponding node.
ldapuser.keytab	Copy the file to each gateway node.

Keytab Files at Process Level

Copy each keytab file generated at the process level to the corresponding node.

The following table shows the node to which to copy each keytab file:

Keytab File	Location on Node
<node name>.keytab	Copy each file to the corresponding node.
webapp_http.keytab	Copy each file to the corresponding node.
_AdminConsole.keytab	Copy each file to the corresponding node.
<application service name>.keytab	Copy each file to the corresponding node on which the CDI-PC application service runs.
ldapuser.keytab	Copy the file to each node.

Enable Kerberos Authentication for CDI-PC Client

Copy the Kerberos configuration file to each computer that hosts an Informatica client, and then set an environment variable to point to the configuration file. You must also enable client browsers to access the CDI-PC web applications.

After you configure the Informatica domain to run with Kerberos authentication, perform the following tasks on the CDI-PC Client tools:

Copy the Kerberos configuration file to each CDI-PC Client host.

Copy the `krb5.conf` file to each computer that hosts a Informatica client such as the CDI-PC Client. Copy the file to the following directory on each host:

```
<CDI-PC installation directory>\clients\shared\security
```

Set the KRB5_CONFIG environment variable on each CDI-PC Client host.

Set the KRB5_CONFIG environment variable to the path and file name of the Kerberos configuration file on each computer that hosts Informatica clients such as the CDI-PC Client.

Configure web browsers to access CDI-PC web applications.

In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web applications to the list of trusted sites.

If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

Register the CDI-PC domain.

After you convert the non-Kerberos CDI-PC domain to Kerberos CDI-PC domain, the domain appears offline in Informatica Intelligent Cloud Services. You must register the domain again.

If a domain appears offline, you can try to reestablish a connection with the domain. If the status is offline because the domain is shut down, you first need to start the domain. After the domain is started, you can reestablish a connection with the domain.

Enabling User Accounts to Use Kerberos Authentication

After you enable Kerberos authentication in the domain, import Informatica user accounts from Active Directory into the LDAP security domain that contains Kerberos user accounts. You must also migrate the groups, roles, privileges, and permissions from the native security domain to the corresponding Active Directory user accounts in the LDAP security domain that contains Kerberos user accounts.

Import User Accounts from Active Directory into LDAP Security Domains

Import user accounts from Active Directory into LDAP security domains.

When you enable Kerberos authentication in the domain, Informatica creates an empty LDAP security domain with the same name as the Kerberos realm. You can import user accounts from Active Directory into this LDAP security domain, or you can import the user accounts into a different LDAP security domain.

You use the Administrator tool to import the user accounts that use Kerberos authentication from Active Directory into an LDAP security domain.

To configure Kerberos cross realm authentication, connect to the Active Directory global catalog. When you connect to the global catalog, you import users from the Active Directory server used by each Kerberos realm.

1. Start the domain and all Informatica services.
2. Log in to Windows with the administrator account you specified when you enabled Kerberos authentication in the domain.
3. Log in to the Administrator tool. Select _infaInternalNamespace as the security domain.
4. In the Administrator tool, click the **Security** tab.
5. Click the **Actions** menu and select **LDAP Configuration**.
6. In the **LDAP Configuration** dialog box, click the **LDAP Connectivity** tab.
7. Configure the connection properties for the Active Directory.

   You might need to consult the LDAP administrator to get the information needed to connect to the LDAP server.

The following table describes the LDAP server configuration properties:

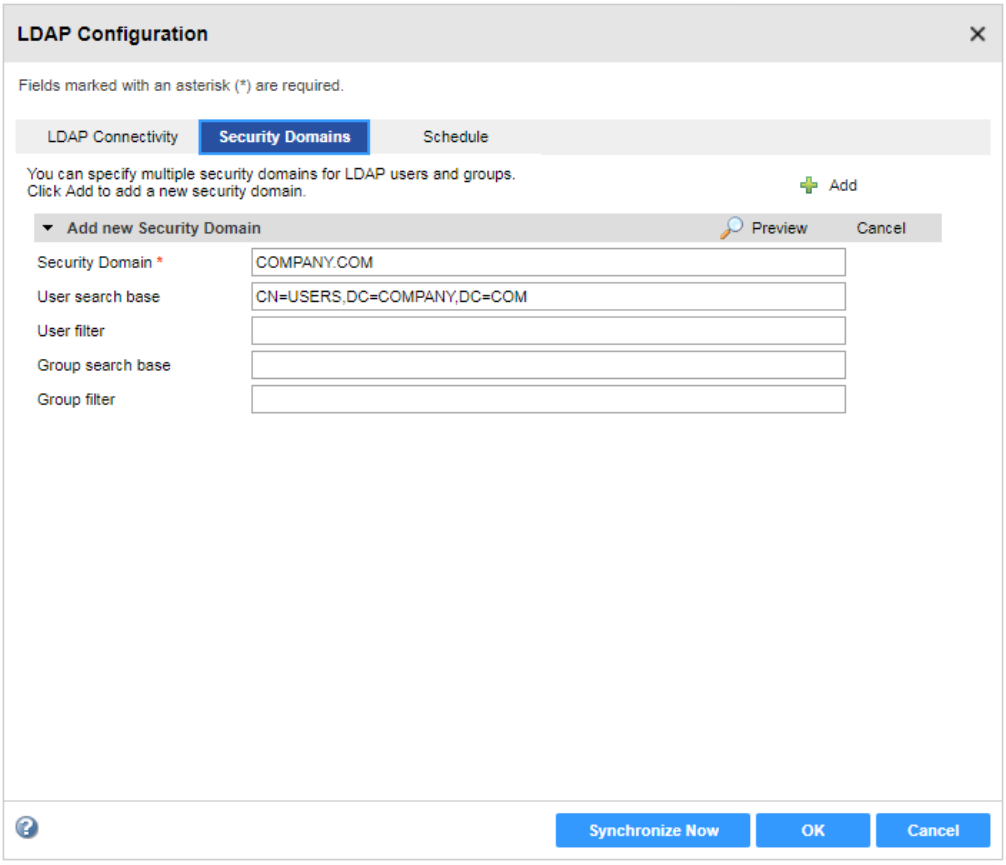
Property	Description
Server name	Host name or IP address of the Active Directory server. To configure Kerberos cross realm authentication, connect to the Active Directory global catalog host. Specify the fully qualified hostname. For example: host.company.local
Port	Listening port for the Active Directory server. The default is 389. The default SSL port is 636. To configure Kerberos cross realm authentication, connect to the Active Directory global catalog port. The default is 3268. The default SSL port is 3269.
LDAP Directory Service	Select **Microsoft Active Directory Service**.
Name	Specify the bind user account you created in Active Directory to synchronize accounts in Active Directory with the LDAP security domain. Because the domain is enabled for Kerberos authentication, you do not have the option to provide a password for the account. If the domain uses Kerberos cross realm authentication, include the name of the realm to which the Active Directory principal database belongs.
Use SSL Certificate	Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol.
Trust LDAP Certificate	Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.
Not Case Sensitive	Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups.
Group Membership Attribute	Name of the attribute that contains group membership information for a user. This is the attribute in the LDAP group object that contains the DNs of the users or groups who are members of a group. For example, *member* or *memberof*.
Maximum Size	Maximum number of user accounts to import into a security domain. For example, if the value is set to 100, you can import a maximum of 100 user accounts into the security domain. If the number of user to be imported exceeds the value for this property, the Service Manager generates an error message and does not import any user. Set this property to a higher value if you have many users to import. Default is 1000.

8. In the **LDAP Configuration** dialog box, click the **Security Domains** tab.
9. Click **Add**.

The following table describes the filter properties that you can set for a security domain:

Property	Description
Security Domain	Name of the LDAP security domain into which you want to import user accounts from Active Directory.
User search base	Distinguished name (DN) of the entry that serves as the starting point to search for user names in Active Directory. The search finds an object in the directory according to the path in the distinguished name of the object. For example, to search the USERS container that contains Informatica user accounts in the example.com Windows domain, specify CN=USERS,DC=EXAMPLE,DC=COM.
User filter	An LDAP query string that specifies the criteria for searching for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: `(objectclass=*)` searches all objects. `(&(objectClass=user)(!(cn=susan)))` searches all user objects except “susan”. For more information about search filters, see the documentation for the LDAP directory service.
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

The following image shows the information required to import LDAP users from Active Directory into the LDAP security domain created when you enabled Kerberos in the domain:



10. Click **Synchronize Now**.

    The Service Manager synchronizes the users in all the LDAP security domains with the users in the LDAP directory service. The time it takes for the synchronization process to complete depends on the number of users and groups to be imported.

11. Click **OK** to save the LDAP security domain.

Migrate Native User Privileges and Permissions to the Kerberos Security Domain

If the Informatica domain has user accounts in the native security domain, the corresponding Active Directory user accounts in the Kerberos security domain must have the same groups, roles, privileges, and permissions. Migrate the groups, roles, privileges, and permissions of the native users to the corresponding user accounts in the Kerberos LDAP security domain.

1. Review the list of native user accounts and determine the accounts that you want to migrate to the LDAP security domain for Kerberos authentication.

   To list the user accounts in the Informatica domain, run the following command:

   ```
   infacmd isp ListAllUsers
   ```

   Each native user account that you want to migrate to the Kerberos security domain must have a corresponding account in the Active Directory service that you use for Kerberos authentication.

2. Create the user migration file.

   The user migration file is a plain text file that contains the list of native users and the corresponding Kerberos users that require the same groups, roles, privileges, and permissions.

   Use the following format to list entries in the user migration file:

   ```
   Native/<source user name>,<LDAP security domain>/<target user name>
   ```

   The following example shows a user migration file containing the following list of users to migrate to the COMPANY.COM security domain:

   ```
   Native/User1,COMPANY.COM/User1
   Native/User2,COMPANY.COM/User2
   Native/User3,COMPANY.COM/User3
   ```

3. Run the infacmd isp migrateUsers command to migrate account privileges and permissions in the native security domain to the accounts in the Kerberos security domain.

   To migrate the groups, roles, privileges, and permissions for users, run the following command:

   ```
   infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd
   <administrator password> -sdn <security domain> -umf <user migration file>
   ```

   The following table describes the options for the command:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain. Specify the user name of the administrator account you specified in the infasetup switchToKerberosMode command.
-Password -pd	Password for the administrator account.
-SecurityDomain -sdn	LDAP security domain of the administrator account used to connect to the domain. Specify _infaInternalNamespace.
-UserMigrationFile -umf	Path and file name of the user migration file. The command skips entries with a duplicate source user name or target user name.

   The following example migrates the groups, roles, privileges, and permissions for users based on the `um_s.txt` user migration file:

   ```
   infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
   _infaInternalNamespace -umf C:\Infa\um_s.txt
   ```

   The command overwrites the connection object permissions assigned to the LDAP user with the connection object permissions for the native user. The command merges the groups, roles, privileges, and domain object permissions for native users and corresponding LDAP users.

   The migrateUsers command creates a detailed log file named `infacmd_umt_<date>_<time>.txt` in the directory where you run the command.

Kerberos Delegation

Kerberos delegation enables a Kerberos service to impersonate a Kerberos client user and get a service ticket for another service on behalf of the client user.

The services in the CDI-PC domain need to connect to other services to complete an operation. You can connect to other services through delegated authentication. In delegated authentication, when a user is authenticated by a service, the service uses those credentials to connect to another service. For example, when a pmcmd user accesses CDI-PC Integration Service, the service acts as the pmcmd user to authenticate with CDI-PC Repository Service.

Types of Kerberos Delegation

When you use delegated authentication, you can choose one of the following types of delegation:

Full delegation

Full delegation is the initial implementation of Kerberos delegation. In this delegation method, a client forwards its Ticket Granting Ticket (TGT) to a service after Kerberos authentication. The service uses the TGT to get service tickets to access any other service in the network. This type of delegation is not considered secure because an administrator cannot control the services that the server can access using the client identity. Full delegation is also known as unconstrained delegation.

Resource-based constrained delegation

With resource-based constrained delegation, administrators can restrict the usage of the client identity by the services. In this delegation method, the client does not forward TGT to the server. In this method, the services specify who they trust and who can delegate authentication to them.

Constrained delegation uses Kerberos protocol extensions called Service for User (S4U) that allow a service to obtain a Kerberos service ticket on behalf of a user.

Note: You cannot use both constrained delegation and full delegation in a single domain. You can configure the domain to use either full delegation or constrained delegation.

Service for User (S4U) Extension

Service for User (S4U) extensions allow a service to obtain a Kerberos service ticket on behalf of a user. Following are the two types of S4U extensions:

- Service for user to self (S4U2Self). This extension allows a service to get a service ticket to itself on behalf of a client user.
- Service for user to proxy (S4U2Proxy). This extension allows a service to obtain a service ticket to another service on behalf of a client user. To perform S4U2proxy, a service needs a service ticket to itself. The service ticket can be presented by the client user or obtained through S4U2Self extension.

For more information on the S4U extensions, see the Microsoft documentation.

Enable Resource-based Constrained Delegation with S4U2Self

Make sure that the forwardable flag is set to true in libdefaults section of krb5.conf file.

You can configure Resource-based Constrained Delegation only through powershell commands. Make sure powershell is started by a user with required privileges to change the properties of KDC accounts, preferably a KDC administrator.

To enable Resource-based Constrained Delegation with S4U2Self, perform the following steps every Informatica keytab account on the KDC server:

1. Right-click the user account and select **Properties**.

   The **Properties** dialog box appears.
2. On the **Delegation** tab, select **Do not trust this computer for delegation**.
3. Click **Apply**.
4. Run the following command to set the `PrincipalsAllowedToDelegateToAccount` attribute:

   ```
   $IntermediateService = Get-ADUser -Identity <Intermediate server account's samAccountName> -Properties *
   ```

   ```
   Set-ADUser -Identity <Targer server account's samAccountName> -PrincipalsAllowedToDelegateToAccount $IntermediateService1, $IntermediateService2, $IntermediateService3
   ```

   Note: You can use comma separated values to add multiple accounts in the `PrincipalsAllowedToDelegateToAccount` attribute.
5. If you want to unset the `PrincipalsAllowedToDelegateToAccount` attribute, run the following command:

   ```
   Set-ADUser -Identity <Targer server account's samAccountName> PrincipalsAllowedToDelegateToAccount $null
   ```
6. To view existing principals in `PrincipalsAllowedToDelegateToAccount` list, run following commands:

   ```
   $FormatEnumerationLimit=-1
   Get-ADUser -Identity <sam account name> -properties
   ```

   ```
   PrincipalsAllowedToDelegateToAccount
   ```

   Note: By default, powershell command output shows four values in the service principal list in the output. Set this parameter to -1 to show the complete list of principals.

Enable Full Delegation for the Kerberos Principal User Accounts in Active Directory

Create the keytab files using the `ktpass` command.

To use full delegation, you must enable delegation for all of the accounts you created, except for the LDAP bind user account that you use to access and search Active Directory during LDAP synchronization.

To enable full delegation, perform the following steps for each user account:

1. Right-click the user account and select **Properties**.

   The **Properties** dialog box appears.
2. On the **Delegation** tab, select **Trust this user for delegation to any service (Kerberos only)**.
3. Click **Apply**.

   Full delegation is enabled.

Switch from Full Delegation to Constrained Delegation

If you are using Full Delegation and want to use Constrained Delegation, perform the following steps.

1. Shut down the domain.
2. "Enable Resource-based Constrained Delegation with S4U2Self" on page 55 for existing active directory users associated with keytab account on the KDC server.
3. Start up the domain.

CHAPTER 5

SAML Authentication for Informatica Web Applications

This chapter includes the following topics:

- SAML Authentication Overview, 57
- SAML Authentication Process, 59
- Enable SAML Authentication in a Domain, 60
- Enhanced Authentication Security, 62
- Configuring Web Applications to Use Different Identity Providers, 65

SAML Authentication Overview

You can configure Security Assertion Markup Language (SAML) authentication for Informatica web applications.

Security Assertion Markup Language is an XML-based data format for exchanging authentication information between a service provider and an identity provider. In an Informatica domain, the Informatica web application is the service provider.

You can configure the following Informatica web applications to use SAML authentication:

- Informatica Administrator
- Data Privacy Management

Note: SAML authentication cannot be used in an Informatica domain configured to use Kerberos authentication.

If you enable a domain to use SAML authentication, all web applications that run in the domain use the identity provider you configure in the domain by default. However, you can configure web applications that run in a domain to use different identity providers. For example, you might configure Informatica Administrator to use AD FS as the identity provider.

For more information about configuring web applications to use different identity providers, see "Configuring Web Applications to Use Different Identity Providers" on page 65.

Default Keystore and Truststore Directory

The Informatica deployment includes default keystore and truststore files in the directory `<Informatica installation directory>\services\shared\security`.

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases. To secure a production environment, use the following guidelines:

- Configure a custom keystore and truststore for SAML authentication in a location other than the default directory:
  `<Informatica installation directory>\services\shared\security`
- You cannot use the default keystore and truststore to configure other services or clients.
- When you enable SAML authentication, you import keystore or truststore certificate files and private keys into the default directory:
  `<Informatica installation directory>\services\shared\security`
- When you assign an alias to the keystore or truststore, do not use "Informatica LLC," which Informatica uses for private key authentication and certificate signing.
- Modifying the default SAML keystore or truststore is allowed only when the default directory is configured as the SAML keystore and truststore directory and you want to import private key and certificate entries in the default keystore or truststore.

  You cannot use "Informatica LLC" as the alias for new entries in default keystore and truststore. You can use "Informatica LLC" as the alias for custom keystore-truststore entries.

  No other operation is allowed for the default keystore and truststore files, including deleting or replacing the files, changing the password of the keystore or truststore, or modifying, removing or replacing the Informatica-generated private key and signing certificate.
- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

Supported Identity Providers

Use a supported identity provider to manage SAML authentication on the domain for web applications.

Informatica supports the following identity providers. Click the How-to Library (H2L) article link to get instructions for integration between each identity provider and the domain.

Identity Provider	How-to Library (H2L) article
Microsoft Active Directory Federation Services (AD FS)	SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
PingFederate	SAML Authentication with PingFederate in Informatica 10.4.0
F5 Big-IP	SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1
NetScaler	SAML Authentication with NetScaler for Web Applications
Oracle Access Manager (OAM)	SAML Authentication with Oracle Access Manager for Web Applications

Identity Provider	How-to Library (H2L) article
Okta SSO	SAML Authentication with Okta SSO for Web Applications
Azure Active Directory	SAML Authentication with Azure Active Directory for Web Applications

For information about supported versions of these identity providers, see the Product Availability Matrix on Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices.

SAML Authentication Process

Informatica web applications and the identity provider exchange authentication information to enable SAML authentication in an Informatica domain.

The following steps describe the basic SAML authentication flow:

1. A user accesses an Informatica web application.
2. The user selects the security domain containing LDAP user accounts used for SAML authentication on the application log in page, and then clicks the log in button.

   If the user selects the native security domain, the user provides a user name and password and logs in to the application.
3. Based on the identity provider configuration, the user is prompted to provide the credentials required for first time authentication.
4. The identity provider validates the user's credentials and creates a session for the user.

   The identity provider also validates the target web application URL, and then redirects the user to the web application with a SAML token containing the user's identity information.
5. The application validates the SAML token and user identity information, creates a user session, and then completes the user log in process.

The existing user session in the browser is used for subsequent authentication. To access another Informatica web application configured to use SAML authentication, the user selects the LDAP security domain on the application log in page. The user does not need to supply a user name or password.

The user remains logged in to all Informatica web applications that are running in the same browser session. However, if the user logs out of an Informatica web application, the user is also logged out of other Informatica web applications running in the same browser session.

Enable SAML Authentication in a Domain

Configure the identity provider, the Informatica domain, and the nodes within the domain to use SAML authentication.

To configure SAML authentication for supported Informatica web applications that run in a domain, perform the following tasks:

1. Create an LDAP configuration to connect to the LDAP identity store that contains Informatica web application user accounts. You also create an LDAP security domain, and then import the user accounts into the security domain.
2. Export the assertion signing certificate from the identity provider.
3. Import the assertion signing certificate into a truststore file on each gateway node in the domain. You can import the certificate into the Informatica default truststore file, or into a custom truststore file.
4. Add one or more relying party trusts or service providers in the identity provider.
5. Add the URL for each Informatica web application to the identity provider.
6. Enable SAML authentication in the domain.
7. Enable SAML authentication on every node in the domain.

Note: For several of the SAML identity providers that Informatica supports, you can follow detailed integration steps in a How-To Library (H2L) article. See "Supported Identity Providers" on page 58 for links to the articles.

Create an LDAP Configuration for the Identity Provider or LDAP Store

Use the Administrator tool to create an LDAP configuration for the identity provider or LDAP store that contains the web application user accounts that use SAML authentication.

When you create an LDAP configuration, you create a security domain for the user accounts, and then import the accounts into the security domain. After you import the accounts into the security domain, assign the appropriate Informatica domain roles, privileges and permissions to the accounts in the security domain.

For more information about creating an LDAP configuration, see "Creating an LDAP Configuration" on page 22.

Export the Assertion Signing Certificate

The identity provider sends assertions of authenticity to service providers in the form of an assertion signing certificate.

A signed assertion contains a signature that the identity provider creates, using an algorithm chosen by the identity provider administrator. Informatica then verifies the signature using the corresponding public certificate that the domain administrator imported to the SAML truststore.

Informatica recommends that you enable the signed assertion.

Export the assertion signing certificate from the identity provider to enable the signed assertion.

Import the Certificate into the Truststore Used for SAML Authentication

Import the assertion signing certificate used by the identity provider into the truststore file used for SAML authentication on every gateway node within the Informatica domain.

You can import the certificate into the default Informatica truststore file, or into a custom truststore file.

Configure the Identity Provider

Configure the identity provider to issue SAML tokens to Informatica web applications.

Perform the following tasks to configure the identity provider:

- Add a relying party trust for the domain in the identity provider. The relying party trust definition enables the identity provider to accept authentication requests from Informatica web applications that run in the domain.
- Edit the Send LDAP Attributes as Claims rule to map LDAP attributes in your identity store to the corresponding types used in SAML tokens issued by the identity provider.

You provide the name of the relying party trust when you enable SAML authentication in a domain. Depending on your security requirements, you might create multiple relying party trusts in the identity provider to enable domains used by different organizations within the enterprise to use SAML authentication.

Informatica recognizes "Informatica" as the default relying party trust name. If you create a single relying party trust with "Informatica" as the relying party trust name, you do not need to provide the relying party trust name when you enable SAML authentication in a domain.

Note: All strings are case sensitive in the identity provider, including URLs.

Add Informatica Web Application URLs to the Identity Provider

Add the URL for each Informatica web application using SAML authentication to the identity provider.

You provide the URL for an Informatica web application to enable the identity provider to accept authentication requests sent by the application. Providing the URL also enables the identity provider to send the SAML token to the application after authenticating the user.

Set Up SAML Authentication in the Domain

You can set up SAML authentication in an existing Informatica domain, or you can enable it when you create a domain.

When you enable a domain to use SAML authentication, all web applications that run in the domain use the default identity provider you specify when you enable SAML authentication in the domain.

Select one of the following options:

Enable SAML authentication when you run Informatica installer.

You can enable SAML authentication and specify the identity provider URL when you configure the domain as part of the installation process.

Enable SAML authentication in an existing domain.

Use the infasetup updateDomainSamlConfig command to enable SAML authentication in an existing Informatica domain. You can run the command on any gateway node within the domain.

Enable SAML authentication when you create a domain.

Use the infasetup defineDomain command to enable SAML authentication when you create a domain.

See the *Informatica Command Reference* for instructions on using the commands.

Enable SAML Authentication on the Nodes

You must configure SAML authentication on every gateway and worker node in the Informatica domain.

Select one of the following options to configure SAML authentication on a gateway node:

Enable SAML authentication when you define a gateway node on a machine.

Use the infasetup DefineGatewayNode command to enable SAML authentication on the gateway node.

Enable SAML authentication when you configure a gateway node to join a domain that uses SAML authentication.

Use the infasetup UpdateGatewayNode command to enable SAML authentication on the gateway node.

Enable SAML authentication when you convert a worker node to a gateway node.

Use the isp SwitchToGatewayNode command to enable SAML authentication on the node.

Select one of the following options to configure SAML authentication on a worker node:

Enable SAML authentication when you define a worker node on a machine.

Use the infasetup DefineWorkerNode command to enable SAML authentication on the worker node.

Enable SAML authentication when you configure a worker node to join a domain that uses SAML authentication.

Use the infasetup UpdateWorkerNode command to enable SAML authentication on the worker node.

See the *Informatica Command Reference* for instructions on using the commands.

Enhanced Authentication Security

You can enable request signing, signed response, or encrypted assertion to enhance authentication security:

Request signing

A signed authentication request contains a signature to verify the authenticity of the request itself. Informatica, acting as a service provider, sends an authentication request to the identity provider. To maintain the integrity of the request, the authentication request can be signed.

Informatica signs a SAML request using a private key, and the identity provider verifies the signature using the corresponding public certificate.

Informatica sends SAML authentication requests via HTTP-Redirect. The requests use deflate encoding, which puts the signature in a URL parameter.

Signed response

The identity provider responds to authentication requests from a service provider. A signed response contains a signature that the identity provider creates, using an algorithm chosen by the identity provider administrator. Informatica then verifies the signature using the corresponding public certificate that the domain administrator imported to the SAML truststore.

Signed assertion and encrypted assertion

The identity provider sends assertions of authenticity to service providers.

A signed assertion contains a signature that the identity provider creates, using an algorithm chosen by the identity provider administrator. Informatica then verifies the signature using the corresponding public certificate that the domain administrator imported to the SAML truststore. Informatica recommends that you enable the signed assertion.

The Informatica administrator generates an asymmetric key (public-private key).

The assertion can be encrypted by the identity provider using an assertion encryption key, which is a symmetric key generated by the identity provider.

When you enable encrypted assertion, the identity provider also encrypts the symmetric key using the public certificate that the security administrator imported into the identity provider. The SAML response will contain the encrypted assertion and an encrypted symmetric key. Acting as a service provider, Informatica decrypts the encrypted symmetric key using the corresponding private key that the Informatica administrator imports into the SAML keystore. After obtaining the symmetric key, Informatica decrypts the encrypted assertion.

Follow the steps in this section to enable request signing, encrypted assertion, or signed response.

Request Signing

You can enable request signing during the install-upgrade process or after install-upgrade by using infasetup.

During the installation or upgrade process, check the **Signed request** option in the installer utility.

After the installation or upgrade process, set up request signing using infasetup.

You can also configure request signing for the web applications using the Administrator tool or the web application user interface.

infasetup

To use infasetup, use the following options with the `infasetup updateDomainSamlConfig` command:

```
[<-SignSamlRequest|-ssr> sign_smal_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
```

For details about these commands, see the *Informatica Command Reference*.

Administrator Tool

Configure request signing in the Administrator tool.

1. In the Domain Navigator, select the domain node.
2. In the node properties, click the **Edit** icon in the **SAML Configuration** section.
3. Select **Enable Signing Request**.
4. Populate the following properties:
   - Signing Private Key Alias
   - Signin Private Key Password
   - Signing Algorithm
5. Click **OK**.
6. Restart the domain.

Signed Response

Enable signed response to allow the identity provider to sign the authentication request responses from the service provider.

You can enable signed response during the install-upgrade process or after install-upgrade by using infasetup.

During the installation or upgrade process, check the **Signed response** option in the installer utility.

After the installation or upgrade process, set up response signing using infasetup.

You can also configure signed response for the web applications using the Administrator tool or the web application user interface.

Note: The Okta SSO identity provider does not support signed response.

infasetup

To use infasetup, use the following options with the `infasetup updateDomainSamlConfig` command:

```
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

For details about these commands, see the *Informatica Command Reference*.

Administrator Tool

Configure response signing in the Administrator tool.

1. In the Domain Navigator, select the domain node.
2. In the node properties, click the **Edit** icon in the **SAML Configuration** section.
3. Select **Enable Response Signing**.
4. Populate the Response Signing Certificate Alias property.
5. Click **OK**.
6. Restart the domain.

Encrypted Assertion

Enable encrypted assertion to allow the identity provider to encrypt assertions of authenticity using a symmetric key.

You can enable assertion signing or encrypted assertion during the install-upgrade process or after install-upgrade by using infasetup.

During the installation or upgrade process, check the **Encrypt assertion** option in the installer utility.

After the installation or upgrade process, set up encrypted assertion using infasetup.

You can also configure signed response for the web applications using the Administrator tool or the web application user interface.

infasetup

To use infasetup, use the following options with the `infasetup updateDomainSamlConfig` command:

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
```

For details about these commands, see the *Informatica Command Reference*.

Administrator Tool

Configure encrypted assertion in the Administrator tool.

1. In the Domain Navigator, select the domain node.
2. In the node properties, click the **Edit** icon in the **SAML Configuration** section.
3. Select **Enable Assertion Encryption**.
4. Populate the following properties:
   - Encryption Assertion Private Key Alias
   - Encryption Assertion Private Key Password
5. Click **OK**.
6. Restart the domain.

Configuring Web Applications to Use Different Identity Providers

You can configure Informatica web applications that run in a domain to use different identity providers. For example, you might configure Informatica Administrator to use AD FS as the identity provider.

When you enable a domain to use SAML authentication, all web applications that run in the domain use the default identity provider you specify when you enable SAML authentication in the domain. For example, if you configure AD FS as the identity provider, all web applications use AD FS as the identity provider, unless you configure a web application to use a different identity provider.

You specify the default identity provider when you use one of the following options to enable SAML authentication:

- When you create the domain and install the Informatica services.
- When you run the infasetup defineDomain command to create the domain.
- When you run the infasetup updateDomainSamlConfig command to enable SAML authentication in an existing domain.

You use the Administrator tool to configure a web application to use a different identify provider. To configure the Administrator tool or the monitoring application to use a different identity provider, you modify the SAML configuration on the node where the application runs. To configure other web applications to use a different identity provider, you modify the SAML configuration within the application process.

Prepare to Use an Identity Provider

Complete the following tasks to prepare an Informatica web application to use an identity provider.

1. Create an LDAP configuration for the identity provider store that contains Informatica web application user accounts. You also create an LDAP security domain, and then import the user accounts into the security domain.
2. Export the identity provider assertion signing certificate from the identity provider.
3. Import the identity provider assertion signing certificate into a truststore file on each gateway node in the domain. You can import the certificate into the Informatica default truststore file, or into a custom truststore file.

   If you change the alias name, import the corresponding certificate into the truststore file on each gateway node, and then restart the node.
4. Add one or more relying party trusts in the identity provider, and map LDAP attributes to the corresponding types used in security tokens issued by the identity provider.
5. Add the URL for the Informatica web application to the identity provider.

Configure Informatica Administrator to Use an Identity Provider

Use the Administrator tool to configure the Administrator tool or the monitoring application to use a SAML identity provider. You configure the Administrator tool or the monitoring application to use an identity provider on the node where the application runs.

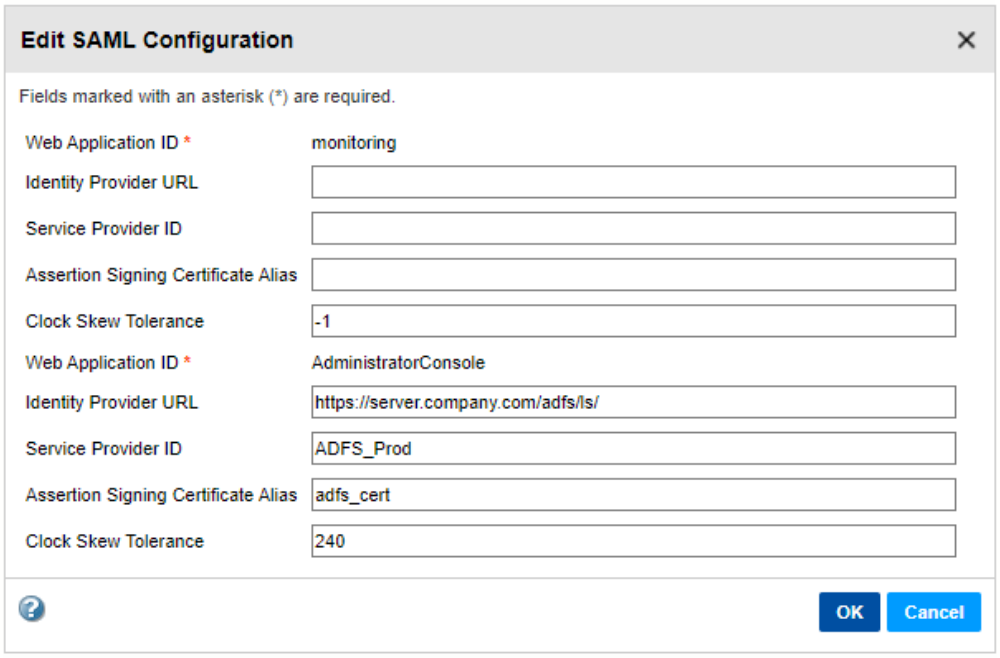
1. In the Administrator tool, click the **Services and Nodes** tab.
2. Select the gateway node where the Administrator tool and the monitoring application run in the Domain Navigator.
3. Click the edit icon next to SAML Configuration.
4. Enter the properties required to enable the application to use an identity provider.

   The following table describes the properties you enter:

Property	Description
Identity Provider URL	Optional. The URL for the identity provider server. You must specify the complete URL string.
Service Provider ID	Optional. The relying party trust name or the service provider identifier for the domain as defined in the identity provider.

Property	Description
Assertion Signing Certificate Alias	Optional. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication. If you change the alias name, import the corresponding certificate into the truststore file on each gateway node, and then restart the node.
Clock Skew Tolerance	Optional. The allowed time difference between the identity provider host system clock and the system clock on the master gateway node. Optional. The lifetime of SAML tokens issued by the identity provider by is set according to the identity provider host system clock. The lifetime of a SAML token issued by the identity provider is valid if the start time or end time set in the token is within the specified number seconds of the system clock on the master gateway node. Values must be from 0 to 600 seconds. Set to -1 to use the value configured for the domain. Default is 120 seconds.

The following image shows the configuration to enable the Administrator tool to use AD FS as the identity provider. If you do not specify a value for a property, the domain uses the value set in the default SAML configuration.



5. Click **OK**.
6. Restart the application.

CHAPTER 6

Domain Security

This chapter includes the following topics:

- Domain Security Overview, 68
- Secure Communication Within the Domain, 69
- Secure Connections to a Web Application Service, 78
- Cipher Suites for the Informatica Domain, 79
- Secure Sources and Targets, 82
- Secure Data Storage, 83
- Application Services and Ports, 86

Domain Security Overview

You can enable options in the Informatica domain to configure secure communication between the components in the domain and between the domain and client components.

You can enable different options to secure specific components in the domain. You do not have to secure all components in the domain.

Informatica uses the TCP/IP and HTTP protocols to communicate between components in the domain. The domain uses SSL certificates to secure communication between components.

When you install the Informatica services, you can enable secure communication for the services in the domain and for the Administrator tool. After installation, you can configure secure communication in the domain in the Administrator tool or from the command line.

During installation, the installer generates an encryption key to encrypt sensitive data, such as passwords, that are stored in the domain. After installation, you can change the encryption key for sensitive data. You must upgrade the content of repositories to update the encrypted data.

You can enable secure communication in the following areas:

Domain

Within the domain, you can select options to enable secure communication for the following components:

- Between the Service Manager, the services in the domain, and the Informatica client tools
- Between the domain and the domain configuration repository
- Between the repository services and repository databases

Data storage

Informatica encrypts sensitive data, such as passwords, when it stores data in the domain. Informatica generates an encryption key during installation. Informatica uses the encryption key to encrypt and decrypt sensitive data that are stored in the domain.

Secure Communication Within the Domain

You can use the Secure Communication option to secure the connection between services and between services and the service managers in the domain. Additionally, you can enable security for workflows and use secure databases for the repositories that you create in the domain.

After you secure the domain, configure the Informatica client applications to work with a secure domain.

Default Directory for Keystore and Truststore

The Informatica deployment includes default keystore and truststore files in the following default directory:

```
<Informatica installation directory>\services\shared\security
```

Informatica recommends that you use the default keystore and truststore only for setup and proof-of-concept use cases.

To secure a production environment, use the following guidelines:

- When you configure secure communication, do not modify, replace, or delete files in the default directory: `<Informatica installation directory>\services\shared\security`
- You cannot use the default keystore and truststore to configure other services or clients.
- Configure a custom keystore and truststore for secure communication in a location other than the default directory.
- If you replaced the default Informatica keystore and truststore files with custom keystore and truststore files in the previous Informatica installation directory structure, you must run the `infasetup UpdateGatewayNode` command to update the locations of the custom keystore and truststore for the domain.

Secure Communication for Services and the Service Manager

You can configure secure communication within the domain during installation. After installation, you can configure secure communication for the domain on the Administrator tool or from the command line.

Informatica provides an SSL certificate that you can use to secure the domain. However, you should provide a custom SSL certificate for domains that require a higher level of security, such as a domain in a production environment. Specify the keystore and truststore files that contain the SSL certificates you want to use.

Note: Informatica provides SSL certificates for evaluation purposes. If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. The security of your domain could be compromised. Provide an SSL certificate to ensure a high level of security for the domain. The certificate that you provide can be self-signed or from a certificate authority (CA).

When you configure secure communication for the domain, you secure the connections between the following components:

- The Service Manager and all services running in the domain
- The CDI-PC Integration Service and the CDI-PC Repository Service

- The domain services and the Informatica client tools and command line programs

Requirements for Secure Communication within the Domain

Before you enable secure communication within the domain, ensure that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

Note: The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

You imported the certificate into truststores.

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

The keystores and truststores are in the correct directory.

If you enable secure communication during installation, the keystore and truststore must be in a directory that is accessible to the installer.

If you enable secure communication after installation, the keystore and truststore must be in a directory that is accessible to the command line programs.

You enforced the HTTP Strict Transport Security (HSTS) response header.

You can choose to enable HSTS response header in your domain to prevent man-in-the-middle (MITM) security threats. If you enable HSTS response header, you can stop HTTP redirects to HTTPS and ensure that only secured URLs (HTTPS) are accessed.

Important: Informatica supports multiple applications and services running on both HTTP and HTTPS. If you enable this option, you cannot access the applications or services with HTTP URL.

To enable this option, set the `INFA_HSTS_HEADER_ENABLED` environment variable to `true` and import the certificates from `infa_truststore` and Informatica Administrator keystore to your browser.

Guidelines for Using Default and Custom Truststore Files

The installer places the default infa_truststore.jks and keystore files in the `<Informatica installation directory>/services/shared/security` directory on each node. You can use the default truststore for setup and proof-of-concept, but the default truststore and keystore files provide limited security. For production, Informatica recommends using custom truststore and keystore files for more secure communication and SAML authentication.

Place custom truststore and keystore files in a custom directory. The truststore file name must be `infa_truststore.jks`.

Do not overwrite, delete or move the default truststore and keystore files. Do not place custom truststore and keystore files in the `<Informatica installation directory>/services/shared/security` directory

When you create an alias for new certificates and private keys, do not use the default "Informatica LLC" name, which is used by the default truststore and keystore files.

Guidelines for Creating Certificates and Custom Truststore and Keystore Files

You can use the Java keytool key and certificate management utility to create an SSL certificate or a certificate signing request (CSR) as well as keystores and truststores in JKS format.

The keytool is available in the following directory on domain nodes:

```
<Informatica installation directory>\java\bin
```

If the domain nodes run on AIX, you can use the keytool provided with the IBM JDK to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores:

1. Copy the certificate files to a local folder on a gateway node within the Informatica domain.
2. From the command line, go to the location of the keytool utility on the node.
3. Run the keytool utility to import the certificate.
4. Restart the node.

Next Steps

For more information about how to create a custom keystore and truststore and import certificates in your browser, see the Informatica How-To Library article How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain: https://docs.informatica.com/data-quality-and-governance/data-quality/h2l/0700-how-to-create-keystore-and-truststore-files-for-secure-comm/abstract.html

After you secure the domain, configure the Informatica client applications to work with a secure domain.

Enabling Secure Communication for the Domain from the Command Line

Use the infacmd and infasetup commands to enable secure communication for the domain. After you enable secure communication, you must restart the domain for the change to take effect.

To use your SSL certificate files, specify the keystore files when you run the infasetup command.

To configure secure domain communication from the command line, use the following commands:

infacmd isp UpdateDomainOptions

Use the UpdateDomainOptions command to set the secure communication mode for the domain.

infasetup UpdateGatewayNode

Use the UpdateGatewayNode command to enable secure communication for the Service Manager on a gateway node in a domain. If the domain has multiple gateway nodes, run the UpdateGatewayNode command on each gateway node.

infasetup UpdateWorkerNode

Use the UpdateWorkerNode command to enable secure communication for the Service Manager on a worker node in a domain. If the domain has multiple worker nodes, run the UpdateWorkerNode command on each worker node.

1. Verify that the domain you want to secure is running.
2. Update the domain.

Run the following command with the required options and arguments:

- Windows: `infacmd isp UpdateDomainOptions`
- UNIX: `infacmd.sh isp UpdateDomainOptions`

To configure secure communication for the domain, include the following option when you run the infacmd command:

Option	Argument	Description
-DomainOptions -do	option_name=value	Set the following option to configure secure communication for the domain: TLSMode=True

3. Shut down the domain.

   The domain must be shut down before you run the infasetup commands.

4. Run infasetup with the required options and arguments.

   Enter the following command:

   - Windows: `infasetup UpdateGatewayNode` or `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` or `infasetup.sh UpdateWorkerNode`

   To configure secure communication on the nodes, run the commands with the following options:

Option	Argument	Description
-EnableTLS -tls	enable_tls	Configures secure communication for the services in the Informatica domain.
-NodeKeystore -nk	node_keystore_directory	Optional if you use the default SSL certificate from Informatica. Required if you use your SSL certificate. Directory that contains the keystore files. The Informatica domain requires the SSL certificate in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem You can use the same keystore file for multiple nodes.
-NodeKeystorePass -nkp	node_keystore_password	Optional if you use the default SSL certificate from Informatica. Required if you use your SSL certificate. Password for the infa_keystore.jks file.
-NodeTruststore -nt	node_truststore_directory	Optional if you use the default SSL certificate from Informatica. Directory that contains the truststore files. You can use the same truststore file for multiple nodes.
-NodeTruststorePass -ntp	node_truststore_password	Optional if you use the default SSL certificate from Informatica. Password for the infa_truststore.jks file.

5. Run the infasetup command on each node in the domain.

If you have multiple gateway nodes in the domain, run infasetup UpdateGatewayNode on each gateway node. If you have multiple worker nodes, run infasetup UpdateWorkerNode on each worker node. You must use the same keystore files for all nodes in the domain.

6. Restart the domain.

Enabling Secure Communication for the Domain in the Administrator Tool

You can use the Administrator tool to enable secure communication for the domain. When you enable secure communication in the Administrator tool, you must also run infasetup commands to update the nodes.

When you enable the Secure Communication option in the Administrator tool, you also need to run the infasetup command to update Informatica configuration files on each node. To specify the SSL certificate files to use, specify the keystore files when you run the infasetup command.

To update the Informatica configuration files on each node, use the following commands:

infasetup UpdateGatewayNode

Use the UpdateGatewayNode command to enable secure communication for the Service Manager on a gateway node in a domain. If the domain has multiple gateway nodes, run the UpdateGatewayNode command on each gateway node.

infasetup UpdateWorkerNode

Use the UpdateWorkerNode command to enable secure communication for the Service Manager on a worker node in a domain. If the domain has multiple worker nodes, run the UpdateWorkerNode command on each worker node.

To enable secure domain communication from the Administrator tool, perform the following steps:

1. On the Administrator tool, select the domain.
2. In the contents panel, click the **Properties** view.
3. Go to the **General Properties** section and click **Edit**.
4. On the **Edit General Properties** window, select **Enable Secure Communication**.
5. Click **OK**
6. Shut down the domain.

   The domain must be shut down before you run the infasetup commands.
7. Run infasetup with the required options and arguments.

   Enter the following command:

   - Windows: `infasetup UpdateGatewayNode` or `infasetup UpdateWorkerNode`
   - UNIX: `infasetup.sh UpdateGatewayNode` or `infasetup.sh UpdateWorkerNode`

To configure secure communication on the nodes, run the commands with the following options:

Option	Argument	Description
-EnableTLS -tls	enable_tls	Configures secure communication for the services in the Informatica domain.
-NodeKeystore -nk	node_keystore_directory	Optional if you use the default SSL certificate from Informatica. Required if you use your SSL certificate. Directory that contains the keystore files. The Informatica domain requires the SSL certificate in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem You can use the same keystore file for multiple nodes.
-NodeKeystorePass -nkp	node_keystore_password	Optional if you use the default SSL certificate from Informatica. Required if you use your SSL certificate. Password for the infa_keystore.jks file.
-NodeTruststore -nt	node_truststore_directory	Optional if you use the default SSL certificate from Informatica. Directory that contains the truststore files. You can use the same truststore file for multiple nodes.
-NodeTruststorePass -ntp	node_truststore_password	Optional if you use the default SSL certificate from Informatica. Password for the infa_truststore.jks file.

8. Run the infasetup command on each node in the domain.

   If you have multiple gateway nodes in the domain, run infasetup UpdateGatewayNode on each gateway node. If you have multiple worker nodes, run infasetup UpdateWorkerNode on each worker node. You must use the same keystore files for all nodes in the domain.

9. Restart the domain.

Configuring the Informatica Client Applications to Work with a Secure Domain

When you enable secure communication within the domain, you also secure connections between the domain and Informatica client applications. You might need to specify the location and password for the truststore files that you use to secure the domain in environment variables. You set the environment variables on machines hosting client applications that access services within the domain.

SSL certificates that are used to secure an Informatica domain are contained in truststore files named `infa_truststore.jks` and `infa_truststore.pem`. The truststore files must be available on each client host.

You might need to set the following environment variables on each client host:

INFA_TRUSTSTORE

Set this variable to the directory that contains the `infa_truststore.jks` and `infa_truststore.pem` truststore files.

INFA_TRUSTSTORE_PASSWORD

Set this variable to the password for the truststore. The password must be encrypted. Use the command line program pmpasswd to encrypt the password.

Note: INFA_TRUSTSTORE_PASSWORD is optional if you use any PowerCenter thick client, or commands such as pmcmd or pmrep. Enter a password only for the infacmd commands.

Informatica provides an SSL certificate in default truststore files that you can use to secure the domain. When you install the Informatica clients, the installer sets the environment variables and installs the truststore files in the following directory by default: `<Informatica installation directory>\clients\shared\security`

If you use the default Informatica SSL certificate, and the `infa_truststore.jks` and `infa_truststore.pem` files are in the default directory, you do not need to set the INFA_TRUSTSTORE or INFA_TRUSTSTORE_PASSWORD environment variables.

You must set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on each client host in the following scenarios:

You use a custom SSL certificate to secure the domain.

If you provide an SSL certificate to use to secure the domain, import the certificate into truststore files named `infa_truststore.jks` and `infa_truststore.pem`, and then copy the truststore files to each client host. You must specify the location of the files and the truststore password.

Secure Domain Configuration Repository Database

The Informatica domain configuration repository stores configuration information and user account privileges and permissions. When you create an Informatica domain, you must create a domain configuration repository.

You can create a domain configuration repository on a database that is secured with the SSL protocol. The SSL protocol uses SSL certificates stored in a truststore file. Access to the secure database access requires a truststore that contains the certificates for the database.

You can create a secure domain configuration repository database when you install the Informatica services and create a domain. For more information about configuring a secure domain configuration repository during installation, see the Informatica installation guides.

After installation, you can configure a secure domain configuration repository database from the command line.

Note: Before you configure a secure domain configuration repository database after installation, you must enable secure communication for the domain.

You can create a secure domain configuration repository on the following databases:

- Oracle
- Microsoft SQL Server
- IBM DB2

Configuring a Secure Domain Configuration Repository Database

After installation, you can change the domain configuration repository to a secure database. You can use a secure domain configuration repository database only if you enable secure communication for the domain.

You must shut down the domain before you change the domain configuration repository database. Use the infasetup command to back up the domain configuration repository database and to restore it in a secure

database. When you restore the domain configuration repository in the secure database, specify the security parameters for the secure database. Then update the gateway node with the domain configuration repository information.

To back up and restore the repository database and update the gateway node, use the following commands:

infasetup BackupDomain

Use the BackupDomain option to back up data from the domain configuration repository database.

infasetup RestoreDomain

Use the RestoreDomain option to restore domain configuration repository data to a secure database.

infasetup UpdateGatewayNode

Use the UpdateGatewayNode option update the domain configuration repository settings in the gateway nodes of the domain.

To change the domain configuration repository to a secure database, complete the following steps:

1. Verify that secure communication is enabled for the domain.

   The domain must be secure before you can use a secure database for the domain configuration repository.
2. Shut down the domain.
3. Run the infasetup BackupDomain command and specify the database connection information.

   When you run the BackupDomain command, infasetup backs up most of the domain configuration database tables to the file name you specify.

   Note: If the infasetup backup or restore command fails with a Java memory error, increase the system memory available for infasetup. To increase system memory, set the -Xmx value in the INFA_JAVA_CMD_OPTS environment variable.
4. Use the database backup utility to manually back up additional repository tables that the infasetup command does not back up.

   Back up the contents of the following table:

   - ISP_RUN_LOG
5. To restore the domain configuration repository in the secure database, run the infasetup RestoreDomain command and specify the database connection information.

   In addition to the connection information, specify the following options required for the secure database:

Option	Argument	Description
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Required. Indicates whether the database into which the domain configuration repository will be restored is a secure database. Set this option to True.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Required. Path and file name of the truststore file that contains the SSL certificate for the database.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Required. Password for the database truststore file for the secure database.

   In the connection string, include the following security parameters:

EncryptionMethod

Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to `SSL`.

ValidateServerCertificate

Optional. Indicates whether Informatica validates the certificate that the database server sends.

If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate.

If this parameter is set to False, Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify.

Default is True.

HostNameInCertificate

Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.

cryptoProtocolVersion

Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server.

6. Use the database restore utility to restore the repository tables that you manually backed up.

   Restore the following table:

   - ISP_RUN_LOG

7. To update the nodes in the domain with information about the secure domain configuration repository, run the infasetup UpdateGatewayNode command and specify the secure database connection information.

   In addition to the node options, specify the following options required for the secure database:

Option	Argument	Description
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Required. Indicates the database used for the domain configuration repository is a secure database. Set this option to True.
-DatabaseConnectionString -cs	database_connection_string	Required. Connection string to use to connect to the secure database. The connection string must include the security parameters that you included in the connection string when you ran the infasetup RestoreDomain command in step 5
-DatabaseTruststorePassword -dbtp	database_truststore_password	Required. Password for the database truststore file for the secure database.

   If you have multiple gateway nodes in the domain, run infasetup UpdateGatewayNode on each gateway node.

8. Restart the domain.

Secure CDI-PC repository Database

When you create a CDI-PC Repository Service, you can create the associated CDI-PC repository on a database secured with the SSL protocol.

The CDI-PC Repository Service connects to the CDI-PC repository database through native connectivity.

When you create a CDI-PC repository on a secure database, verify that the database client files contain the secure connection information for the database. For example, if you create a CDI-PC repository on a secure Oracle database, configure the Oracle database tnsnames.ora and sqlnet.ora client files with the secure connection information.

Secure Connections to a Web Application Service

To protect data that is transmitted between a web application service and the browser, secure the connection between the web application service and the browser.

You can secure the following connections:

Connections to the Administrator tool

You can secure the connection between the Administrator tool and the browser.

Requirements for Secure Connections to Web Application Services

Before you secure the connection to a web application service, ensure that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

The keystore is in an accessible directory.

The keystore must be in a directory that is accessible to the Administrator tool and the command line programs.

Enabling Secure Connections to the Administrator Tool

After installation, you can configure secure connections to the Administrator tool from the command line.

You must update the gateway nodes in the domain with the properties for a secure connection between the browser and the Informatica Administrator service.

To update the gateway node with secure connection properties, run the following command: `infasetup UpdateGatewayNode`

Include the following options:

Option	Argument	Description
-HttpsPort -hs	AdminConsole_https_port	Port number to use for a secure connection to the Informatica Administrator service.
-KeystoreFile -kf	AdminConsole_Keystore_File	Path and file name of the keystore file to use for the HTTPS connection to the Informatica Administrator service.
-KeystorePass -kp	AdminConsole_Keystore_Password	Password for the keystore file.

If you have multiple gateway nodes in the domain, run the command on each gateway node.

Cipher Suites for the Informatica Domain

You can configure the cipher suites that the Informatica domain uses when it encrypts connections within the Informatica domain. Connections from the Informatica domain to resources outside of the domain are not affected by the cipher suite configuration.

When you enable secure communication for the Informatica domain or secure connections to web application services, the Informatica domain uses cipher suites to encrypt traffic.

Informatica creates the effective list of cipher suites that it uses based on the following lists:

Blacklist

List of cipher suites that you want the Informatica domain to block. When you blacklist a cipher suite, the Informatica domain removes the cipher suite from the effective list. You can add cipher suites that are on the default list to the blacklist.

Default list

List of cipher suites that Informatica domain supports by default. If you do not configure a whitelist or blacklist, the Informatica domain uses the default list as the effective list.

For more information, see "Default List of Cipher Suites" on page 80

Whitelist

List of cipher suites that you want the Informatica domain to support. When you add a cipher suite to the whitelist, the Informatica domain adds the cipher suite to the effective list. You do not need to add cipher suites that are on the default list to the whitelist.

Informatica creates the effective list by adding cipher suites from the whitelist to the default list and removing cipher suites on the blacklist from the default list.

Consider the following guidelines for effective lists:

- To use a custom effective list for secure connections to web clients, the Informatica domain must use secure communication within the domain. If the domain does not use secure communication, Informatica uses the default list as the effective list.

- The effective list only governs connections within the Informatica domain. Connections to data sources do not use the effective list.
- The effective list must contain at least one cipher suite that TLS v1.1 or 1.2 supports.
- The effective list must be a valid cipher suite for Windows, the Java Runtime Environment, and OpenSSL.

Create the Cipher Suite Lists

To configure the Informatica domain to use specific cipher suites, create a whitelist specifying the additional cipher suites to support. You can also create a blacklist specifying the cipher suites to block.

Work with your network security administrator to determine the cipher suites that are suitable for the Informatica domain.

The list of cipher suites must be a comma-separated list. Use the Internet Assigned Numbers Authority (IANA) names for the cipher suites in the list. Alternatively, you can use a regular Java expression.

You configure the whitelist and blacklist with infasetup. You can provide the lists directly in command parameters or specify plain-text files that contain comma-separated lists.

The following sample text shows a list with two cipher suites:

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

You can configure the whitelist and blacklist of cipher suites for the Informatica domain when you create the domain. Use infasetup to create the Informatica domain, gateway nodes, and worker nodes. For more information about infasetup commands, see the *Informatica Command Reference*.

Alternatively, you can configure the whitelist and blacklist for an existing Informatica domain.

Default List of Cipher Suites

By default, the Informatica domain uses the following cipher suites for secure communication within the domain and secure client connections:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Configure the Informatica Domain with a New Effective List of Cipher Suites

To configure the cipher suites that the Informatica domain uses, you must update the Informatica domain, all gateway nodes, and all worker nodes with the same whitelist and blacklist.

Note: Changes to the blacklist, whitelist, and effective list are not cumulative. Informatica creates a new effective list based on the blacklist, default list, and whitelist when you run the command. The new effective list overwrites the previous list.

To configure an existing Informatica domain with a new effective list of cipher suites, perform the following steps:

1. Shutdown the Informatica domain.
2. Optionally, run the infasetup listDomainCiphers command to view the lists of cipher suites that a domain or node supports or blocks.

   For example, run the following command to view all the cipher suite lists:

   ```
   infasetup listDomainCiphers -l ALL -dc true
   ```
3. Run the infasetup updateDomainCiphers command on a gateway node and specify a whitelist, blacklist, or both.

For example, run the following command to add one cipher suite to the effective list and remove two cipher suites from the effective list:

```
infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

4. Run the infasetup updateGatewayNode command on each gateway node and specify a whitelist, blacklist, or both.

   Use the same whitelist and blacklist as the domain.

   For example, run the following command:

   ```
   infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

5. Update each worker node with the same set of cipher suites as the Informatica domain.

   Use the same whitelist and blacklist as the domain.

   For example, run the following command:

   ```
   infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl
   TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
   ```

6. Start the Informatica domain.

7. Optionally, run the infacmd isp listDomainCiphers command to view the lists of cipher suites that a domain or node uses.

   For example, run the following command to view the effective list of cipher suites that the domain uses:

   ```
   infacmd isp listDomainCiphers -l EFFECTIVE
   ```

Secure Sources and Targets

Informatica uses connection objects to connect to relational databases as source or target. You can create a connection object to a relational database that is secured with an SSL certificate.

You create CDI-PC connection objects in the Workflow Manager.

You can create a connection to a secure source or target on the following databases:

- Oracle
- Microsoft SQL Server
- IBM DB2

CDI-PC Sources and Targets

When you create a connection object for a CDI-PC session, you can define a connection to a database secured with the SSL protocol.

You can connect to relational CDI-PC sources and targets through native connectivity or ODBC drivers.

If you connect to a secure relational source or target through native connectivity, verify that the database client contains the connection information for the secure database. For example, if you connect to a CDI-PC target on a secure Oracle database, configure the Oracle database client file *tnsnames.ora* with the connection information for the secure database.

If you connect to a secure relational source or target through ODBC drivers, verify that the database client contains the connection information for the secure database and the ODBC data source correctly defines the connection to the secure database.

Secure Data Storage

Informatica encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the domain configuration repository. Informatica uses an encryption key to encrypt sensitive data.

During installation, the installer generates the encryption key for the domain. All nodes in a domain must use the same encryption key. If you install on multiple nodes, the installer uses the same encryption key for all nodes in the domain. For more information about generating an encryption key for the domain during installation, see the Informatica installation guides.

After installation, you can change the encryption key for the domain. Run the infasetup command to generate an encryption key and change the encryption key for the domain. After you change the encryption key for the domain, you must upgrade the content of the repositories in the domain to update the encrypted data.

Note: You must keep the encryption key file in a secure location. The encryption key is required when you change the encryption key for the domain or move a repository to another domain.

Secure Directory on UNIX

When you install Informatica, the installer creates a directory to store Informatica files that require restricted access, such as the domain encryption key file. On UNIX, the installer assigns different permissions for the directory and the files in the directory.

By default, the installer creates the following directory within the Informatica installation directory to store the encryption key: `<INFA_HOME>/isp/config/keys`

The /keys directory contains the encryption key file for the node. If you configure the domain to use Kerberos authentication, the directory also contains the Kerberos keytab files.

During installation, you can specify a different directory in which to store the encryption file. The installer assigns the same permissions to the specified directory as the default directory.

The /keys directory and the files in the directory have the following permissions:

Directory Permissions

The owner of the directory has `-wx` permissions to the directory but no `r` permission. The owner of the directory is the user account used to run the installer. The group to which the owner belongs also has `-wx` permissions to the directory but no `r` permission.

For example, the user account *ediqa* owns the directory and belongs to the *infaadmin* group. The *ediqa* user account and the *infaadmin* group have the following permissions: `-wx-wx---`

The *ediqa* user account and the *infaadmin* group can write to and run files in the directory. They cannot display the list of files in directory but they can list a specific file by name.

If you know the name of a file in the directory, you can copy the file from the directory to another location. If you do not know the name of the file, you must change the permission for the directory to include the read permission before you can copy the file. You can use the command `chmod 730` to give read permission to the owner of the directory and subdirectories.

For example, you need to copy the encryption key file named *siteKey* to a temporary directory to make it accessible to another node in the domain. Run the command `chmod 730` on the `<Informatica installation directory>/isp/config` directory to assign the following permissions: rwx-wx---. You can then copy the encryption key file from the /keys subdirectory to another directory.

After you complete copying the files, change the permissions for the directory back to write and execute permissions. You can use the command `chmod 330` to remove the read permission.

Note: Do not use the -R option to recursively change the permissions for the directory and files. The directory and the files in the directory have different permissions.

File Permissions

The owner of the files in the directory has `rwx` permissions to the files. The owner of the files in the directory is the user account used to run the installer. The group to which the owner belongs also has `rwx` permissions to the files in the directory.

The owner and group have full access to the file and can display or edit the file in the directory.

Note: You must know the name of the file to be able to list or edit the file.

Changing the Encryption Key from the Command Line

After installation, you can change the encryption key for the domain from the command line. You must shut down the domain before you change the encryption key.

Use the infasetup command to generate an encryption key and configure the domain to use the new encryption key.

The following infasetup commands generate and change the encryption key:

generateEncryptionKey

Generates an encryption key in a file named *sitekey*. If the directory specified for the encryption key contains a file named *sitekey*, Informatica renames the file to *siteKey_old*.

migrateEncryptionKey

Changes the encryption key used to store sensitive data in the Informatica domain.

To change the encryption key for a domain, complete the following steps:

1. Shut down the domain.
2. Back up the domain before you change the encryption key.

   To ensure that you can recover the domain if you encounter problems when you change the encryption key, back up the domain before you run the infasetup commands.
3. To generate an encryption key for the domain, run the infasetup generateEncryptionKey command.

   Specify the encryptionKeyLocation option to generate an encryption key:

Option	Argument	Description
-encryptionKeyLocation -kl	encryption_key_location	Directory that contains the current encryption key. The name of the encryption file is *sitekey*. Informatica renames the current *sitekey* file to *sitekey_old* and generates an encryption key in a new file named *sitekey* in the same directory.

   Note: The installer creates an encryption key during installation and upgrade. You do not need the keyword and domain name options while generating the encryption file sitekey. Make sure that you save a copy of the unique site key. If you lose the site key, you cannot generate the site key again. Do not share the unique site key with others.
4. To change the encryption key for the domain, run the infasetup migrateEncryptionKey command and specify the location of the old and new encryption key.

Specify the following options required to change the encryption key for the domain:

Option	Argument	Description
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	Directory in which the old encryption key file named *siteKey_old* and the new encryption key file named *siteKey* are stored. The directory must contain the old and new encryption key files. If the old and new encryption key files are stored in different directories, copy the encryption key files to the same directory. If the domain has multiple nodes, this directory must be accessible to any node in the domain where you run the migrateEncryptionKey command. When you migrate a multinode domain, all the nodes in the domain must use the same encryption key. To change the encryption key for the domain, run the infasetup migrateEncryptionKey command on all nodes in the domain. **Note:** On UNIX, the file name *siteKey_old* is case-sensitive. If you manually rename the previous encryption key file, verify that the file name has the correct letter case.
-IsDomainMigrated -mig	is_domain_migrated	Indicates whether the domain has been updated to use the latest encryption key. When you run the migrateEncryptionKey command for the first time, set this option to False to indicate that the domain uses the old encryption key. After the first time, when you run the migrateEncryptionKey command to update other nodes in the domain, set this option to True to indicate that the domain has been updated to use the latest encryption key. Or, you can run the migrateEncryptionKey command without this option. Default is True.

5. Run the infasetup command on each node in the domain.

   If the domain has multiple nodes, run infasetup migrateEncryptionKey on each node. Run the command on the gateway nodes before you run the command on the worker nodes. You can omit the IsDomainMigrated option after the first time you run the command.

6. Restart the domain.

   You must upgrade all repository services in the domain to update and encrypt sensitive data in the repositories with the new encryption key. You must also migrate the site key after you upgrade the domain.

7. Upgrade CDI-PC Repository Service.

   You can upgrade a CDI-PC Repository Service in the Administrator tool or at the command prompt.

   To upgrade a service in the Administrator tool, select **Manage** > **Upgrade** in the header area. If you select multiple services, the Administrator tool upgrades the services in the correct order.

To upgrade a service at the command prompt, use the following commands:

Repository Service Type	Command
CDI-PC Repository Service	`pmrep Upgrade`

Application Services and Ports

Informatica domain services and application services in the Informatica domain have unique ports.

Informatica Domain

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

CHAPTER 7

Security Management in Informatica Administrator

This chapter includes the following topics:

- Using Informatica Administrator Overview, 87
- User Security, 88
- Security Tab, 89
- Password Management, 93
- Domain Security Management, 94
- User Security Management, 94

Using Informatica Administrator Overview

Informatica Administrator is the tool that you use to manage the Informatica domain and Informatica security.

The Administrator tool has the following tabs:

- **Manage**. View and edit the properties of the domain and objects within the domain.
- **Logs**. View log events for the domain and services within the domain.
- **Reports**. Run a Web Services Report or License Management Report.
- **Security**. Manage users, groups, roles, and privileges.
- **Cloud**. View information about your Informatica Cloud® organization.

The Administrator tool has the following header items:

- **Log out**. Log out of the Administrator tool.
- **Manage**. Manage your account.
- **Help**. Access help for the current tab and determine the Informatica version.

User Security

The Service Manager and some application services control user security in application clients. Application clients include Informatica Administrator and PowerCenter Client.

The Service Manager and application services control user security by performing the following functions:

Encryption

When you log in to an application client, the Service Manager encrypts the password.

Authentication

When you log in to an application client, the Service Manager authenticates your user account based on your user name and password or on your user authentication token.

Authorization

When you request an object in an application client, the Service Manager and some application services authorize the request based on your privileges, roles, and permissions.

Encryption

Informatica encrypts passwords sent from application clients to the Service Manager. Informatica uses AES encryption with multiple 128-bit or 256-bit keys to encrypt passwords and stores the encrypted passwords in the domain configuration database. Configure HTTPS to encrypt passwords sent to the Service Manager from application clients.

Authentication

The Service Manager authenticates users who log in to application clients.

The first time you log in to an application client, you enter a user name, password, and security domain. A security domain is a collection of user accounts and groups in an Informatica domain.

The security domain that you select determines the authentication method that the Service Manager uses to authenticate your user account:

- Native. When you log in to an application client as a native user, the Service Manager authenticates your user name and password against the user accounts in the domain configuration database.
- Lightweight Directory Access Protocol (LDAP). When you log in to an application client as an LDAP user, the Service Manager passes your user name and password to the external LDAP directory service for authentication.

Single Sign-On

After you log in to an application client, the Service Manager allows you to launch another application client or to access multiple repositories within the application client. You do not need to log in to the additional application client or repository.

The first time the Service Manager authenticates your user account, it creates an encrypted authentication token for your account and returns the authentication token to the application client. The authentication token contains your user name, security domain, and an expiration time. The Service Manager periodically renews the authentication token before the expiration time.

When you access multiple repositories within an application client, the application client sends the authentication token to the Service Manager for user authentication.

When you launch one web application client from another one, the application client passes the authentication token to the next application client. The next web application client sends the authentication token to the Service Manager for user authentication. You must log out of each web application client separately.

Note: To use single sign-on between the Administrator tool you must add their fully qualified domain names to the host file for every node.

You cannot use single sign-on to connect to a web application client from a client tool.

Authorization

The Service Manager authorizes user requests for domain objects. Requests can come from the Administrator tool. The following application services authorize user requests for other objects:

- CDI-PC Repository Service

When you create native users and groups or import LDAP users and groups, the Service Manager stores the information in the domain configuration database into the following repositories:

- CDI-PC repository

The Service Manager synchronizes the user and group information between the repositories and the domain configuration database when the following events occur:

- You restart the CDI-PC Repository Service.
- You add or remove native users or groups.
- The Service Manager synchronizes the list of LDAP users and groups in the domain configuration database with the list of users and groups in the LDAP directory service.

When you assign permissions to users and groups in an application client, the application service stores the permission assignments with the user and group information in the appropriate repository.

When you request an object in an application client, the appropriate application service authorizes your request.

Security Tab

You administer Informatica security on the Security tab of the Administrator tool.

The Security tab has the following components:

- Search section. Search for users, groups, or roles by name.
- Navigator. The Navigator appears in the left pane and displays groups, users, and roles.
- Contents panel. The contents panel displays properties and options based on the object selected in the Navigator and the tab selected in the contents panel.
- Security Actions menu. Contains options to create or delete a group, user, or role. You can manage LDAP configurations and operating system profiles. You can also view users that have privileges for a service.

Using the Search Section

Use the Search section to search for users, groups, and roles by name. Search is not case sensitive.

1. In the Search section, select whether you want to search for users, groups, or roles.

2. Enter the name or partial name to search for.

   You can include an asterisk (*) in a name to use a wildcard character in the search. For example, enter “ad*” to search for all objects starting with “ad”. Enter “*ad” to search for all objects ending with “ad”.

3. Click Go.

   The Search Results section appears and displays a maximum of 100 objects. If your search returns more than 100 objects, narrow your search criteria to refine the search results.

4. Select an object in the Search Results section to display information about the object in the contents panel.

Using the Security Navigator

The Navigator appears in the contents panel of the Security tab. When you select an object in the Navigator, the contents panel displays information about the object.

The Navigator on the Security tab displays one of the following sections based on what you are viewing:

- Groups section. Select a group to view the properties of the group, the users assigned to the group, and the roles and privileges assigned to the group.
- Users section. Select a user to view the properties of the user, the groups the user belongs to, and the roles and privileges assigned to the user.
- Roles section. Select a role to view the properties of the role, the users and groups that have the role assigned to them, and the privileges assigned to the role.
- Operating Profiles section. Select an operating profile to view the properties of the operating system profile, and the permissions assigned to users and groups that use the operating system profile.
- LDAP Configuration section. Select a configuration to view the LDAP server connection details, the LDAP security domain that contains users and groups imported from the LDAP directory service, and the LDAP synchronization schedule.

The Navigator provides different ways to complete a task. You can use any of the following methods to manage groups, users, and roles:

- Click the **Actions** menu. Each section of the Navigator includes an Actions menu to manage groups, users, roles, operating system profiles, or LDAP configurations.
- Right-click an object. Right-click an object in the Navigator to display the options available in the Actions menu.
- Use keyboard shortcuts. Use keyboard shortcuts to move to different sections of the Navigator.

Groups

A group is a collection of users and groups that can have the same privileges, roles, and permissions.

The Groups section of the Navigator organizes groups into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Groups section of the Navigator, the contents panel displays all groups belonging to the security domain.

When you select a group in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the group and users assigned to the group.

- Privileges. Displays the privileges and roles assigned to the group for the domain and for application services in the domain.
- Permissions. Displays the level of access that users within the group have perform tasks on domain objects, including nodes, grids and application services . Also displays the level of access that users within the group have to perform tasks on connection objects and operating system profiles.

Users

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator
- CDI-PC Client

The Users section of the Navigator organizes users into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Users section of the Navigator, the contents panel displays all users belonging to the security domain.

When you select a user in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the user and all groups to which the user belongs.
- Privileges. Displays the privileges and roles assigned to the user for the domain and for application services in the domain.
- Permissions. Displays the level of access that the user has to perform tasks on domain objects, including nodes, grids and application services . Also displays the level of access that the user has to perform tasks on connection objects and operating system profiles.

Roles

A role is a collection of privileges that you assign to a user or group. Privileges determine the actions that users can perform. You assign a role to users and groups for the domain and for application services in the domain.

The Roles section of the Navigator organizes roles into the following folders:

- System-defined Roles. Contains roles that you cannot edit or delete. The Administrator role is a system-defined role.
- Custom Roles. Contains roles that you can create, edit, and delete. The Administrator tool includes some custom roles that you can edit and assign to users and groups.

When you select a folder in the Roles section of the Navigator, the contents panel displays all roles belonging to the folder.

When you select a role in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the role and the users and groups that have the role assigned for the domain and application services.
- Privileges. Displays the privileges assigned to the role for the domain and application services.

Operating System Profiles

An operating system profile is a security mechanism that the CDI-PC Integration Service use to run mappings, workflows, and profiling jobs.

The Operating System Profiles section of the Navigator lists the operating system profiles configured in the domain.

When you select an operating system profile in the Navigator, the contents panel displays the following tabs:

- Properties. Displays general properties of the operating system profile configured for the CDI-PC Integration Service.
- Permissions. Displays the permissions assigned to users and groups that use the operating system profile. Also indicates whether the operating system profile is the default profile assigned to a user or group.

LDAP Configuration

You can configure an Informatica domain to enable users and groups imported from one or more LDAP directory services to log in to Informatica nodes, services, and application clients.

The LDAP Configuration section of the Navigator lists the LDAP configurations the domain uses.

When you select an LDAP configuration, the following tabs appear under the LDAP Configuration tab:

- Overview. Lists the connection details for the LDAP server that contains the directory service from which you want to import users and groups.
- Security Domains. Lists the details for the LDAP security domain that contains users and groups imported from the LDAP directory service.
- Schedule. Lists the details for the synchronization schedule specifying when the Service Manager updates the security domain with the users and groups in the LDAP directory service.

Account Management

To improve security in the Informatica domain, you can enforce lockout of user and administrator accounts after a specified number of failed login attempts.

The Account Lockout Configuration section of the Account Management page displays whether account lockout is enabled for user accounts and administrator accounts. The section also indicates the maximum number of failed login attempts allowed.

The Locked Out Native Users section of the page lists locked out user accounts in the native security domain. You can unlock a user account in the native security domain.

The Locked Out LDAP Users section of the page lists locked out user accounts in an LDAP security domain. You can unlock a user account in the Informatica domain. However, the LDAP administrator must unlock the user account in the LDAP server. The user cannot log in to the Informatica domain until the LDAP administrator unlocks the user account.

Audit Reports

Audit reports provide information about users and groups in the Informatica domain, and about the privileges, roles, and permissions assigned to each user or group.

You select the audit report to generate from the Select Report Type menu. You can generate the following audit reports:

User Personal Information

Displays contact information and status details of user accounts in the domain. You can select the users or groups for which you want to generate the report.

User Group Association

Displays information about users and the groups to which they belong. You can select the users or groups for which you want to generate the report.

Privileges

Displays information about privileges assigned to the users and groups in the domain. You can select the users or groups for which you want to generate the report.

Roles

Displays information about the roles assigned to the users and groups in the domain. You can select the roles for which you want to generate the report.

Domain Object Permissions

Displays information about the domain objects for which users and groups have permission. You can select the users or groups for which you want to generate the report.

Password Management

You can change the password through the Change Password application.

You can open the Change Password application from the Administrator tool or with the following URL:
`http://<fully qualified host name>:<port>/passwordchange/`

The Service Manager uses the user password associated with a worker node to authenticate the domain user. If you change a user password that is associated with one or more worker nodes, the Service Manager updates the password for each worker node. The Service Manager cannot update nodes that are not running. For nodes that are not running, the Service Manager updates the password when the nodes restart.

Note: For an LDAP user account, change the password in the LDAP directory service.

For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password:

- The length of the password must be at least eight characters.
- It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as:
  `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~`

When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Changing Your Password

Change the password for a native user account at any time. For a user account created by someone else, change the password the first time you log in to the Administrator tool.

1. In the Administrator tool header area, click **Manage** > **Change Password**.

   The Change Password application opens in a new browser window.

2. Enter the current password in the **Password** box, and the new password in the **New Password** and **Confirm Password** boxes.
3. Click **Update**.

Domain Security Management

You can configure Informatica domain components to use the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to encrypt connections with other components. When you enable SSL or TLS for domain components, you ensure secure communication.

You can configure secure communication in the following ways:

Between services within the domain

You can configure secure communication between services within the domain.

Between the domain and external components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

Each method of configuring secure communication is independent of the other methods. When you configure secure communication for one set of components, you do not need to configure secure communication for any other set.

Note: If you change a non-secure domain to a secure domain, you must delete the domain configuration in the CDI-PC Client tools and configure the domain again in the client.

User Security Management

You manage user security within the domain with privileges and permissions.

Privileges determine the actions that users can complete on domain objects. Permissions define the level of access a user has to a domain object. Domain objects include the domain, folders, nodes, grids, licenses, database connections, operating system profiles, and application services.

Even if a user has the domain privilege to complete certain actions, the user might also require permission to complete the action on a particular object. For example, a user has the Manage Services domain privilege which grants the user the ability to edit application services. However, the user also must have permission on the application service. A user with the Manage Services domain privilege and permission on the Development Repository Service but not on the Production Repository Service can edit the Development Repository Service but not the Production Repository Service.

To log in to the Administrator tool, a user must have the Access Informatica Administrator domain privilege. If a user has the Access Informatica Administrator privilege and permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can view the object. For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties but cannot configure, shut down, or remove the node.

If a user does not have permission on a selected object in the Navigator, the contents panel displays a message indicating that permission on the object is denied.

CHAPTER 8

Users and Groups

This chapter includes the following topics:

- Users and Groups Overview, 95
- Default Groups, 96
- Understanding User Accounts, 97
- Managing Users, 98
- Managing Groups, 106
- Managing operating system profiles, 108
- Account Lockout, 113

Users and Groups Overview

To access the application services and objects in the Informatica domain and to use the application clients, you must have a user account.

During installation, a default administrator user account is created. Use the default administrator account to log in to the Informatica domain and manage application services, domain objects, and other user accounts. When you log in to the Informatica domain after installation, change the password to ensure security for the Informatica domain and applications.

User account management in Informatica involves the following key components:

- Users. You can set up different types of user accounts in the Informatica domain. Users can perform tasks based on the roles, privileges, and permissions assigned to them.
- Authentication. When a user logs in to an application client, the Service Manager authenticates the user account in the Informatica domain and verifies that the user can use the application client. The Informatica domain can use native or LDAP authentication to authenticate users. The Service Manager organizes user accounts and groups by security domain. It authenticates users based on the security domain the user belongs to.
- Groups. You can set up groups of users and assign different roles, privileges, and permissions to each group. The roles, privileges, and permissions assigned to the group determines the tasks that users in the group can perform within the Informatica domain.
- Privileges and roles. Privileges determine the actions that users can perform in application clients. A role is a collection of privileges that you can assign to users and groups. You assign roles or privileges to users and groups for the domain and for application services in the domain.

- Operating system profiles. If you run the Integration Service on UNIX or Linux, you can configure the Integration Service to use operating system profiles. Use operating system profiles to increase security and to isolate the run-time environment for users. You can create and manage operating system profiles on the Security tab of the Administrator tool.
- Account lockout. You can configure account lockout to lock a user account when the user specifies an incorrect login in the Administrator tool or any application clients. You can also unlock a user account.

Default Groups

The Informatica domain has a set of user groups that are created during installation.

By default, the Informatica domain has the following user groups after installation:

- Administrator
- Everyone
- Operator

Administrator Group

The Informatica domain includes a default group named Administrator. The default administrator account created during installation belongs to this group.

The Administrator group has administrator permissions and privileges on the domain and all application services. You can add users to or remove users from the Administrator group. All users in the Administrator group have the same permissions and privileges as the default administrator created during installation.

You cannot delete the default administrator account from the Administrator group and you cannot delete the Administrator group.

Everyone Group

The Informatica domain includes a default group named Everyone. All users in the domain belong to the group.

By default, the Everyone group does not have any privileges. You can assign privileges, roles, and permissions to the Everyone group to grant the same access to all users.

You cannot perform the following tasks on the Everyone group:

- Edit or delete the Everyone group.
- Add users to or remove users from the Everyone group.
- Move a group to the Everyone group.

Operator Group

The Informatica domain includes a default group named Operator.

By default, the Operator group has permission on all of the objects in the domain. You can assign the Operator role to the Operator group and use it to manage the Operator users in the domain.

You can perform the following tasks on the Operator group:

- Assign privileges and roles to the group.
- Add users to or remove users from the group.
- Move a group to the group.
- Edit or delete the group.

Understanding User Accounts

An Informatica domain can have the following types of accounts:

- Default administrator
- Domain administrator
- Application client administrator
- User

Default Administrator

When you install Informatica services, the installer creates the default administrator with a user name and password you provide. You can use the default administrator account to initially log in to the Administrator tool.

The default administrator has administrator permissions and privileges on the domain and all application services.

The default administrator can perform the following tasks:

- Create, configure, and manage all objects in the domain, including nodes, application services, and administrator and user accounts.
- Configure and manage all objects and user accounts created by other domain administrators and application client administrators.
- Log in to any application client.

You cannot disable or modify the user name or privileges of the default administrator. You can change the default administrator password.

Domain Administrator

A domain administrator can create and manage objects in the domain.

The domain administrator can log in to the Administrator tool and create and configure application services in the domain. However, by default, the domain administrator cannot log in to application clients. The default administrator must explicitly give a domain administrator full permissions and privileges to the application services so that they can log in and perform administrative tasks in the application clients.

To create a domain administrator, assign a user the Administrator role for a domain.

Application Client Administrator

An application client administrator can create and manage objects in an application client. You must create administrator accounts for the application clients. To limit administrator privileges and keep application clients secure, create a separate administrator account for each application client.

By default, the application client administrator does not have permissions or privileges on the domain. Without permissions or privileges on the domain, the application client administrator cannot log in to the Administrator tool to manage the application service.

You can set up the following application client administrators:

CDI-PC Client administrator

Has full permissions and privileges on all objects in the CDI-PC Client. The CDI-PC Client administrator can log in to the CDI-PC Client to manage the CDI-PC repository objects and perform all tasks in the CDI-PC Client. The CDI-PC Client administrator can also perform all tasks in the pmrep and pmcmd command line programs.

To create a CDI-PC Client administrator, assign a user the Administrator role for a CDI-PC Repository Service.

User

A user with an account in the Informatica domain can perform tasks in the application clients.

Typically, the default administrator or a domain administrator creates and manages user accounts and assigns roles, permissions, and privileges in the Informatica domain. However, any user with the required domain privileges and permissions can create a user account and assign roles, permissions, and privileges.

Users can perform tasks in application clients based on the privileges and permissions assigned to them.

Managing Users

You can create, edit, and delete users in the native security domain. You cannot delete or modify the properties of user accounts in the LDAP security domains. You cannot modify the user assignments to LDAP groups.

You can assign roles, permissions, and privileges to a user account in the native security domain or an LDAP security domain. The roles, permissions, and privileges assigned to the user determines the tasks the user can perform within the Informatica domain.

You can also unlock a user account.

Creating Native Users

Add, edit, or delete native users on the Security tab.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create User.

3. Enter the following details for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > “
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > “
Email	Email address for the user. The email address cannot include the following special characters: < > “ Enter the email address in the format UserName@Domain.
Phone	Telephone number for the user. The telephone number cannot include the following special characters: < > “

4. Click OK to save the user account.

   After you create a user account, the details panel displays the properties of the user account and the groups that the user is assigned to.

Editing General Properties of Native Users

You cannot change the login name of a native user. You can change the password and other details for a native user account.

1. In the Administrator tool, click the Security tab.
2. In the Users section of the Navigator, select a native user account and click Edit.
3. To change the password, select Change Password.

   The Security tab clears the Password and Confirm Password fields.
4. Enter a new password and confirm.
5. Modify the full name, description, email, and phone as necessary.
6. Click OK to save the changes.

Assigning Native Users to Native Groups

Assign native users to native groups on the Security tab.

1. In the Administrator tool, click the Security tab.
2. In the Users section of the Navigator, select a native user account and click **Edit**.
3. Click the Groups tab.
4. To assign a native user to a group, select a group name in the All Groups column and click **Add**.

   If nested groups do not display in the All Groups column, expand each group to show all nested groups.

   You can assign a native user to more than one group. Use the Ctrl or Shift keys to select multiple groups at the same time.
5. To remove a native user from a group, select a group in the Assigned Groups column and click **Remove**.
6. Click **OK** to save the group assignments.

Assigning LDAP Users to Native Groups

You can assign LDAP user accounts to native groups. You cannot change the assignment of LDAP user accounts to LDAP groups.

1. In the Administrator tool, click the **Security** tab.
2. In the Groups section of the Navigator, select a native group, and then click **Edit**.
3. Click the **Users** tab.
4. To assign an LDAP user to a group, select an LDAP user in the All Users column, and then click **Add**.
5. To remove an LDAP user from a group, select an LDAP user in the Assigned Users column, and then click **Remove**.
6. Click **OK** to save the user assignments.

Enabling and Disabling User Accounts

Users with active accounts can log in to application clients and perform tasks based on their permissions and privileges. If you do not want users to access application clients temporarily, you can disable their accounts. You can enable or disable user accounts in the native or an LDAP security domain. When you disable a user account, the user cannot log in to the application clients.

To disable a user account, select a user account in the Users section of the Navigator and click Disable. When you select a disabled user account, the Security tab displays a message that the user account is disabled. When a user account is disabled, the Enable button is available. To enable the user account, click Enable.

You cannot disable the default administrator account.

Note: When the Service Manager imports a user account from the LDAP directory service, it does not import the LDAP attribute that indicates that a user account is enabled or disabled. The Service Manager imports all user accounts as enabled user accounts. You must disable an LDAP user account in the Administrator tool if you do not want the user to access application clients. During subsequent synchronization with the LDAP server, the user account retains the enabled or disabled status set in the Administrator tool.

Deleting Native Users

To delete a native user account, right-click the user account name in the Users section of the Navigator and select Delete User. Confirm that you want to delete the user account.

You cannot delete the default administrator account. When you log in to the Administrator tool, you cannot delete your user account.

Deleting Users of CDI-PC

When you delete a user who owns objects in the CDI-PC repository, you remove any ownership that the user has over folders, connection objects, deployment groups, labels, or queries. After you delete a user, the default administrator becomes the owner of all objects owned by the deleted user.

When you view the history of a versioned object previously owned by a deleted user, the name of the deleted user appears prefixed by the word "deleted."

LDAP Users

You cannot add, edit, or delete LDAP users in the Administrator tool. You must manage the LDAP user accounts in the LDAP directory service.

Unlocking a User Account

The domain administrator can unlock a user account that is locked out of the domain. If the user is a native user, the administrator can request that the user reset their password before logging back into the domain.

The user must have a valid email address configured in the domain to receive notifications when their account password has been reset.

If the user is locked out of the LDAP authentication server, the LDAP administrator must unlock the user account in the LDAP server.

1. In the Administrator tool, click the **Security** tab.
2. Click **Account Management**.

   The Account Management page displays the following lists of locked-out users:

   Locked Out Native Users

   Includes user accounts in the Native security domain that are locked out.

   Locked Out LDAP Users

   Includes user accounts in LDAP security domains that are locked out.
3. Select the users that you want to unlock.
4. Select **Unlock user and reset password** to generate a new password for the user after you unlock the account.

   The user receives the new password in an email.
5. Click the **Unlock selected users** button.

Increasing System Memory for Many Users

Processing time for an Informatica domain restart, LDAP user synchronization, and some infacmd and infasetup commands increases proportionally with the number of users in the Informatica domain.

The number of users affects the processing time of the following commands:

- infasetup BackupDomain, DeleteDomain, and RestoreDomain
- infacmd isp ExportDomainObjects, ExportUsersandGroups, ImportDomainObjects, and ImportUsersandGroups
- infacmd tools ExportObjects and ImportObjects

You may need to increase the system memory used by Informatica Services, infasetup, and infacmd when you have a large number of users in the domain. To increase the maximum heap size, configure the following environment variables and specify the value in megabytes:

- INFA_JAVA_OPTS. Determines the maximum heap size used by Informatica Services. Configure on each node where Informatica Services is installed.
- ICMD_JAVA_OPTS. Determines the maximum heap size used by infacmd. Configure on each machine where you run infacmd.
- INFA_JAVA_CMD_OPTS. Determines the maximum heap size used by infasetup. Configure on each machine where you run infasetup.

For example, to configure 2048 MB of system memory on UNIX for the INFA_JAVA_OPTS environment variable, use the following command:

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

On Windows, configure the variables as system variables.

The following table lists the minimum requirement for the maximum heap size settings, based on the number of users and services in the domain:

Number of Domain Users	Maximum Heap Size (1-5 Services)	Maximum Heap Size (6-10 Services)
1,000 or less	512 MB (default)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

Note: The maximum heap size settings in the table are based on the number of application services in the domain.

After you configure these environment variables, restart the node for the changes to take effect.

Viewing User Activity

Use the Logs tab of the Administrator tool to view user activity logs. View user activity logs to review login attempts from Informatica client applications. You can also view the logs to determine when a user created, updated, or removed services, nodes, users, groups, or roles.

You can also use the infacmd isp getUserActivityLog command to view user activity log data. The infacmd isp getUserActivityLog command uses the following syntax:

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

The infacmd isp getUserActivityLog command requires the Administrator role or membership in the Administrator group. For more information about the isp getUserActivityLog command, see the *Command Reference*.

The user activity log data includes successful and unsuccessful user login attempts from Informatica clients. If the client sets custom properties on login requests, the log data includes the custom properties.

Note: The user activity logs do not include user login attempts in a domain configured to use Kerberos authentication.

The user activity data includes the following properties for each login attempt from an Informatica client:

- Application name
- Application version
- Host name or IP address of the application host

You can view log events based on the following optional filters:

- User name
- Security domain
- Date and time
- Chronological order
- Activity code
- Activity text

You can display the log events at the command prompt or write the events to a file in one the following formats:

- Binary
- Text
- XML

If you print a log in binary format, you can use the infacmd isp convertUserActivityLog command to convert it to text or XML format. See the *Command Reference* for more information on using the infacmd isp convertUserActivityLog command.

User Activity Codes

User activity logs include codes that indicate the success or failure of each activity.

Valid activity codes include the following:

- CCM_10437. Indicates that an activity succeeded.
- CCM_10438. Indicates that an activity failed.
- CCM_10778. Indicates that a login attempt with custom properties succeeded.
- CCM_10779. Indicates that a login attempt with custom properties failed.

- CCM_10786. Indicates that a login attempt without custom properties succeeded.
- CCM_10787. Indicates that a login attempt without custom properties failed.

User Activity Log Filters

Use one or more filters to retrieve log events for specific users, dates, or events.

Use one or more of the following parameters for the infacmd isp getUserActivityLog command to filter log events:

Users and security domains

Optional. The list of users that you want to get log events for. Separate multiple users with a space. Use the wildcard symbol (*) to view logs for multiple users on a single security domain or all security domains. For example, the following strings are valid values for the option:

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

Add the following parameter to the getUserActivityLog command to filter log events based on user or security domain:

```
-usrs <UserName>:<SecurityDomain>
```

For example, add the following parameter to retrieve user activity for a user named User1 on all security domains:

```
-usrs "User1:*"
```

Date and time

Optional. The range of dates you want to view log events for.

If you enter an end date that is before the start date, the command returns no log events.

Enter the date and time in one of the following formats:

- MM/dd/yyyy
- MM/dd/yyyy HH:mm:ss
- yyyy-MM-dd
- yyyy-MM-dd HH:mm:ss

Add the following parameter to the getUserActivityLog command to filter the log by start date or end date:

```
-sd <start_date> -ed <end_date>
```

For example, add the following parameter to retrieve user activity between January 1, 2014 and February 3, 2014:

```
-sd 01/01/2014 -ed 02/03/2014
```

Activity code

Optional. Returns log events based on the activity code.

Use the wildcard symbol (*) to retrieve log events for multiple activity codes. Valid activity codes include:

- CCM_10437. Indicates that an activity succeeded.
- CCM_10438. Indicates that an activity failed.
- CCM_10778. Indicates that a login attempt with custom properties succeeded.

- CCM_10779. Indicates that a login attempt with custom properties failed.
- CCM_10786. Indicates that a login attempt without custom properties succeeded.
- CCM_10787. Indicates that a login attempt without custom properties failed.

Add the following parameter to the getUserActivityLog command to filter by activity code:

```
-ac <activity_code>
```

For example, add the following parameter to retrieve log events that succeeded:

```
-ac CCM_10437
```

If you use the wildcard symbol, enclose the argument in quotation marks.

Activity text

Optional. Returns log events based on a string found in the activity text.

Add the following parameter to the getUserActivityLog command to filter by activity text:

```
-atxt <activity_text>
```

Use the wildcard symbol (*) to retrieve logs for multiple events. For example, the following parameter returns all log events that contain the phrase "Enabling service" in their description:

```
-atxt "*Enabling service*"
```

If you use the wildcard symbol, enclose the argument in quotation marks.

Chronological order

Optional. Prints log events in reverse chronological order. If you do not specify this parameter, the command displays log events in chronological order.

Add the following parameter to the getUserActivityLog command to print the most recent event first:

```
-ro true
```

Writing and Viewing User Activity Log Events

You can write user activity log events to a file or display it in the command line when you use the infacmd isp getUserActivityLog command. Write the user activity log events to the format based on how you plan to use the exported log events file.

Writing and Viewing Log Files

To write the user activity log events to a file, run the command with the output file parameter -lo:

```
-lo output_file_name
```

If you do not specify an output format, the command writes the log events to a text file. For example, run the following command to write log events to a file named `log.txt`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo
log.txt
```

To specify an output format, run the command with the format parameter -fm:

```
-fm output_format_BIN_TEXT_XML
```

Valid formats include:

- Bin (binary). Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support
- Text. Use text format if you want to analyze the log events in a text editor.

- XML. Use XML format if you want to analyze log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.

If you specify text or XML as the output format, but you do not specify an output file, the command displays the text or XML log on the command line.

If you specify binary as the output format, you must provide an output file name.

For example, run the following command to print log events to a file named `log.xml`:

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm
xml -lo log.xml
```

Converting Log Files

If you use the getUserActivity command to write log events to a binary file, you can convert the file to text or XML format.

Run the following command to convert a binary log you retrieved to text or XML format:

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm
output_format_TEXT_XML -lo output_file_name
```

For example, run the following command to convert a binary input file named `log.bin` to XML format and output it to a file named `convertedLog.xml`:

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

To display the log on the command line, omit the output file name.

If you omit the format, the command uses the text format.

Managing Groups

You can create, edit, and delete groups in the native security domain.

You can assign roles, permissions, and privileges to a group in the native or an LDAP security domain. You cannot delete or modify the properties of group accounts in the LDAP security domains. The roles, permissions, and privileges assigned to the group determines the tasks that users in the group can perform within the Informatica domain.

Adding a Native Group

Add, edit, or remove native groups on the Security tab.

A native group can contain native or LDAP user accounts or other native groups. You can create multiple levels of native groups. For example, the Finance group contains the AccountsPayable group which contains the OfficeSupplies group. The Finance group is the parent group of the AccountsPayable group and the AccountsPayable group is the parent group of the OfficeSupplies group. Each group can contain other native groups.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create Group.

3. Enter the following information for the group:

Property	Description
Name	Name of the group. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Parent Group	Group to which the new group belongs. If you select a native group before you click Create Group, the selected group is the parent group. Otherwise, Parent Group field displays Native indicating that the new group does not belong to a group.
Description	Description of the group. The group description cannot exceed 765 characters or include the following special characters: < > “

4. Click Browse to select a different parent group.

   You can create more than one level of groups and subgroups.
5. Click OK to save the group.

Editing Properties of a Native Group

After you create a group, you can change the description of the group and the list of users in the group. You cannot change the name of the group or the parent of the group. To change the parent of the group, you must move the group to another group.

1. In the Administrator tool, click the Security tab.
2. In the Groups section of the Navigator, select a native group and click Edit.
3. Change the description of the group.
4. To change the list of users in the group, click the Users tab.

   The Users tab displays the list of users in the domain and the list of users assigned to the group.
5. To assign users to the group, select a user account in the All Users column and click Add.
6. To remove a user from a group, select a user account in the Assigned Users column and click Remove.
7. Click OK to save the changes.

Moving a Native Group to Another Native Group

To organize the groups of users in the native security domain, you can set up nested groups and move a group to another group.

To move a native group to another native group, right-click the name of a native group in the Groups section of the Navigator and select Move Group.

Deleting a Native Group

To delete a native group, right-click the group name in the Groups section of the Navigator and select Delete Group.

When you delete a group, the users in the group lose their membership in the group and all permissions or privileges inherited from group.

When you delete a group, the Service Manager deletes all groups and subgroups that belong to the group.

LDAP Groups

You cannot add, edit, or delete LDAP groups or modify user assignments to LDAP groups in the Administrator tool. You must manage groups and user assignments in the LDAP directory service.

Managing operating system profiles

Create and manage operating system profiles on the Security tab of the Administrator tool or from the command line. You can create, edit, and delete operating system profiles. You can assign or change the default operating system profile to users and groups.

If the CDI-PC Integration Service is configured to use operating system profiles, it runs workflows with the operating system profile.

Create, edit, and delete operating system profiles in the **Operating System Profiles** view of the **Security** tab.

Complete the following steps to create an operating system profile:

1. Enter an operating system profile name and a system user name.
2. Select the Integration Services and configure the operating system profile properties.
3. Optionally, assign permissions on the operating system profile.

   You can assign users and groups to operating system profiles and assign a default profile to users and groups after you create an operating system profile.

Operating System Profile Properties for the CDI-PC Integration Service

Service process variables that are set in session properties and parameter files override the operating system profile settings.

The following table describes the operating system profile properties for the CDI-PC Integration Service:

Property	Description
Name	Read-only name of the operating system profile. The name cannot exceed 128 characters. It cannot include spaces or the following special characters: \ / : * ? " < > | [ ] = + ; ,
System User Name	Read-only name of an operating system user that exists on the machines where the CDI-PC Integration Service runs. The CDI-PC Integration Service runs workflows using the system access of the system user defined for the operating system profile.
$PMRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters: * ? < > " | ,

Property	Description
$PMSessionLogDir	Directory for session logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SessLogs.
$PMBadFileDir	Directory for reject files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/BadFiles.
$PMCacheDir	Directory for index and data cache files. You can increase performance when the cache directory is a drive local to the CDI-PC Integration Service process. Do not use a mapped or mounted drive for cache files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Cache.
$PMTargetFileDir	Directory for target files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/TgtFiles.
$PMSourceFileDir	Directory for source files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SrcFiles.
$PmExtProcDir	Directory for external procedures. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/ExtProc.
$PMTempDir	Directory for temporary files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Temp.
$PMLookupFileDir	Directory for lookup files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/LkpFiles.
$PMStorageDir	Directory for run-time files. Workflow recovery files save to the $PMStorageDir configured in the CDI-PC Integration Service properties. Session recovery files save to the $PMStorageDir configured in the operating system profile. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Storage.
Environment Variables	Name and value of environment variables used by the Integration Service at run time. If you specify the LD_LIBRARY_PATH environment variable in the operating system profile properties, the Integration Service appends the value of this variable to its LD_LIBRARY_PATH environment variable. The Integration Service uses the value of its LD_LIBRARY_PATH environment variable to set the environment variables of the child processes generated for the operating system profile. If you do not specify the LD_LIBRARY_PATH environment variable in the operating system profile properties, the Integration Service uses its LD_LIBRARY_PATH environment variable.

Creating an Operating System Profile

Create an operating system profile and assign it to users and groups to increase security and to isolate the run-time user environment. You can create one or more operating system profiles. The CDI-PC Integration Service uses the operating system profile to run workflows.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create Operating System Profile**.

   The **Create Operating System Profile - Step 1 of 3** dialog box appears.
3. Enter the following general properties for the operating system profile:

Property	Description
Name	Name of the operating system profile. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain the following special characters: % * + \ / ? ; < > The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.
System User Name	Name of an operating system user that exists on the machines where the Integration Service runs. The Integration Service runs workflows or jobs using the system access of the system user defined for the operating system profile. **Note:** When you create operating system profiles, you cannot specify the system user name as root or use a non-root user with uid==0.

4. Click **Next**.

   The **Configure Operating System Profile - Step 2 of 3** dialog box appears.
5. Select the service that will use the operating system profile.
   - CDI-PC Integration Service
6. Configure the operating system profile properties for the selected services.
7. Optionally, configure the environment variables.
8. Click **Next**.

   The **Assign Groups and Users to Operating System Profile - Step 3 of 3** dialog box appears.
9. In the **Groups** tab, assign groups to the operating system profile as follows:
   a. To assign specific groups to the operating system profile, select one or more groups and click **Add**.
   b. To assign all available groups to the operating system profile, click **Add All**.
10. Optionally, assign the operating system profile as the default profile to one or more groups. To assign a default profile, select **Default Profile** for the group in the Selected Group(s) list.
11. In the **Users** tab, assign users to the operating system profile as follows:
    a. To assign specific users to the operating system profile, select one or more users and click **Add**.
    b. To assign all available users to the operating system profile, click **Add All**.
12. Optionally, assign the operating system profile as the default profile to one or more users. To assign a default profile, select **Default Profile** for the user in the Selected User(s) list.
13. Click **Finish**.

    After you create the operating system profile, the details panel displays the properties of the operating system profile and the groups and users that the profile is assigned to.

Editing an Operating System Profile

You can edit an operating system profile to change the operating system profile properties.

You cannot edit the name or the system user name after you create an operating system profile. If you do not want to use the operating system user specified in the operating system profile, delete the operating system profile.

1. In the Administrator tool, click the **Security** tab.
2. Select the **Operating System Profiles** view.
3. Select the operating system profile.
4. In the **Properties** tab, click **Edit**.

   The **Edit Properties** dialog box appears.
5. Select the CDI-PC Integration Service that you want to configure.
6. Edit the service properties.
7. Click **OK**.

Assigning a Default Operating System Profile to a User or Group

When a user or group has access to more than one operating system profile, assign a default operating system profile that the Integration Service uses to run jobs and workflows. You can assign any operating system profile with direct permission as the default profile to a user or group. A user or group can have only one default operating system profile. However, you can assign the same operating system profile as the default profile to more than one user or group.

1. On the Security tab, select the **Users** or **Groups** view.
2. In the Navigator, select the user or group.
3. In the content panel, select the **Permissions** view.
4. Click the **Operating System Profiles** tab.
5. Click the **Assign or Change the Default Operating System Profile** button.

   The **Assign or Change the Default Operating System Profile** dialog box appears.
6. Select a profile from the **Default Operating System Profile** list. Or, select **Do not assign a default operating system profile** from the list to remove the default profile that is assigned to a user or group.
7. Click **OK**.

   In the details panel, the **Default Profile** column displays **Yes (Direct)** for the operating system profile.

Deleting an Operating System Profile

To delete an operating system profile, right-click the operating system profile name in the Operating System Profile section of the Navigator and select **Delete Profile**.

After you delete an operating system profile, assign another operating system profile to the users and groups that the operating system profile was assigned to as the default profile. If the CDI-PC Integration Service uses operating system profiles, assign another operating system profile to the repository folders and workflows that the operating system profile was assigned to.

Working with Operating System Profiles in a Secure Domain

You can use operating system profiles in an Informatica domain that has secure communication enabled.

Consider the following rules and guidelines when you use operating system profiles in a domain that has secure communication enabled:

You must set the following environment variable for the operating system profile:
INFA_TRUSTSTORE

Set the value to the directory that contains the truststore files for the SSL certificates for the secure domain. The directory must contain a truststore file named infa_truststore.pem.

INFA_TRUSTSTORE_PASSWORD

If you use a custom truststore, set the value to the password for the infa_truststore.pem that contains the SSL certificate for the secure domain. The password must be encrypted. Use the command line program pmpasswd to encrypt the password.

Additionally, if the PowerCenter Integration Service uses the Session on Grid option, you must set the following environment variable for the operating system profile:
INFA_KEYSTORE

Set the value to the directory that contains the keystore files for the SSL certificates for the secure domain. The directory must contain a keystore file named infa_keystore.pem.

You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security** > **Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

Working with Operating System Profiles in a Domain with Kerberos Authentication

You can use operating system profiles in an Informatica domain that runs on a network with Kerberos authentication.

Consider the following rules and guidelines when you use operating system profiles in a domain that runs on a network with Kerberos authentication:

- The user account for the operating system profile must be a principal in the Active Directory service used for Kerberos authentication and imported into an LDAP security domain in the Informatica domain.
- The user account must have a Kerberos credentials cache file that is accessible to the operating system profile user account. Each operating system profile user account must have a separate credentials cache file.
- The credentials cache file for the operating system profile user account must be forwardable. For example, if you use the *kinit* utility to create the credentials cache file, you must include the *-f* option.
- The credentials cache file for the operating system profile user account must be available when you run a workflow that uses an operating system profile.
- The credentials cache file for the operating system profile user account must always have the latest credentials. You can run a job scheduler utility, such as *cron*, to regularly update the user credentials in the credentials cache file.

- You must set the following environment variables for the operating system profile:
  INFA_OSPI_SECURITY_DOMAIN

  Set the value to the name of the security domain that contains the user account for the operating system profile. If the user account is in the user realm security domain for Kerberos, you do not need to set this variable. The user realm security domain for Kerberos is the security domain created during installation which has the same name as the Kerberos user realm.

  KRB5_CONFIG

  Set the value to the path and file name of the Kerberos configuration file. The name of the Kerberos configuration file is *krb5.conf*.

  KRB5CCNAME

  Set the value to the path and file name of the Kerberos credentials cache file for the operating system profile user account.

  You can set the environment variables for the operating system profile in the Administrator tool. To set the environment variables for the operating system profile, click **Security** > **Operating System Profiles**. Edit the properties of the operating system profile and set the environment variables.

Account Lockout

To improve security in the Informatica domain, an administrator can enforce lockout of domain user accounts, including other administrator users, after multiple failed logins.

The administrator can specify the number of failed login attempts a user can make before the user account is locked. If an account is locked out, the administrator can unlock the account in the Informatica domain.

When the administrator unlocks a user account, the administrator can select the "Unlock user and reset password" option to reset the user password. The administrator can send an email to the user to request that the user change the password before logging back into the domain. To enable the domain to send emails to users when their passwords are reset, configure the email server settings for the domain.

If the user is locked out of the Informatica domain and the LDAP server, the Informatica administrator can unlock the user account in the Informatica domain. The user cannot log in to the Informatica domain until the LDAP administrator also unlocks the user account in the LDAP server.

Note: If the Informatica domain uses Kerberos network authentication, you cannot configure lockout for user accounts. The **Account Management** view is not available in the **Security** tab of the Administrator tool.

Configuring Account Lockout

Select the account lockout options to lock out user accounts in the Informatica domain after multiple failed logins.

1. In the Administrator tool, click **Security** > **Account Management**.
2. In **Account Lockout Configuration** section, click **Edit**.

3. Set the following properties:

Property	Description
Enable Account Lockout	Enforces lockout of an Informatica domain user account after a specified number of failed logins. By default, this option does not enforce lockout of administrator user accounts. You must select the **Enable Admin Account Lockout** option to enforce lockout for administrator user accounts.
Enable Admin Account Lockout	Enforces lockout of an Informatica domain administrator user account after a specified number of failed logins. You must select the **Enable Account Lockout** option before you can enforce lockout for administrator user accounts.
Maximum Login Attempts	Specifies the maximum number of consecutive login failures allowed before a user account is locked out of the Informatica domain.

Rules and Guidelines for Account Lockout

Consider the following rules and guidelines when you enforce account lockout for Informatica users:

- If an application service runs under a user account and the wrong password is provided for the application service, the user account can become locked when the application service tries to start.
- If an LDAP user account is locked out of the Informatica domain and the LDAP authentication server, the Informatica domain administrator can unlock the account in the Informatica domain. The LDAP administrator can unlock the user account in the LDAP server.
- If you enable account lockout in the Informatica domain and in the LDAP server, configure the same threshold for login failures in the Informatica domain and in the LDAP server to avoid confusion about the account lockout policy.
- If account lockout is not enabled in the Informatica domain but a user is locked out, verify that the user is not locked out in the LDAP server.

CHAPTER 9

Privileges and Roles

This chapter includes the following topics:

- Privileges, 115
- Roles, 116
- Domain Privileges, 116
- CDI-PC Repository Service Privileges, 122
- Managing Roles, 135
- Assigning Privileges and Roles to Users and Groups, 138
- Viewing Users with Privileges for a Service, 139
- Troubleshooting Privileges and Roles, 140

Privileges

Privileges determine the actions that users can perform in application clients. Informatica includes the following privileges:

- Domain privileges. Determine actions that users can perform on the Informatica domain using the Administrator tool and the infacmd and pmrep command line programs.
- CDI-PC Repository Service privileges. Determine CDI-PC repository actions that users can perform using the Repository Manager, Designer, Workflow Manager, Workflow Monitor, and the pmrep and pmcmd command line programs.

You assign privileges to users and groups for application services. You can assign different privileges to a user for each application service of the same service type.

You assign privileges to users and groups on the **Security tab** of the Administrator tool.

The Administrator tool organizes privileges into levels. A privilege is listed below the privilege that it includes. Some privileges include other privileges. When you assign a privilege to users and groups, the Administrator tool also assigns any included privileges.

Privilege Groups

The domain and application service privileges are organized into privilege groups. A privilege group is an organization of privileges that define common user actions. For example, the domain privileges include the following privilege groups:

- Tools. Includes privileges to log in to the Administrator tool.

- Security Administration. Includes privileges to manage users, groups, roles, and privileges.
- Domain Administration. Includes privileges to manage the domain, folders, nodes, grids, licenses, and application services.

Tip: When you assign privileges to users and user groups, you can select a privilege group to assign all privileges in the group.

Roles

A role is a collection of privileges that you assign to a user or group. Each user within an organization has a specific role, whether the user is a developer, administrator, basic user, or advanced user.

You assign a role to users and groups for the domain and for application services in the domain.

Tip: If you organize users into groups and then assign roles and permissions to the groups, you can simplify user administration tasks. For example, if a user changes positions within the organization, move the user to another group. If a new user joins the organization, add the user to a group. The users inherit the roles and permissions assigned to the group. You do not need to reassign privileges, roles, and permissions. For more information, see the following Informatica How-To Library article:Using Groups and Roles to Manage Access Controls.

Domain Privileges

Domain privileges determine the actions that users can perform using the Administrator tool and the infacmd and pmrep command line programs.

The following table describes each domain privilege group:

Privilege Group	Description
Security Administration	Includes privileges to manage users, groups, roles, and privileges.
Domain Administration	Includes privileges to manage the domain, folders, nodes, grids, licenses, application services, connections, and cluster configurations.
Monitoring	Includes privileges to configure monitoring statistics and reports, view monitoring for integration objects, and access monitoring.
Tools	Includes privileges to log in to the Administrator tool.
Cloud Administration	Includes privileges to add Informatica Cloud organizations in the Administrator tool and view them.

Security Administration Privilege Group

Privileges in the Security Administration privilege group and domain object permissions determine the security management actions users can perform.

Some security management tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the domain can complete the following tasks:

- Create, edit, and delete operating system profiles.
- Grant permission on operating system profiles.

Note: To complete security management tasks in the Administrator tool, users must also have the Access Informatica Administrator privilege.

Grant Privileges and Roles Privilege

Users assigned the Grant Privileges and Roles privilege can assign privileges and roles to users and groups.

The following table lists the required permissions and the actions that users can perform with the Grant Privileges and Roles privilege:

Permission On	Description
Domain or application service	User is able to perform the following actions: - Assign privileges and roles to users and groups for the domain or application service. - Edit and remove the privileges and roles assigned to users and groups.

Manage Users, Groups, and Roles Privilege

Users assigned the Manage Users, Groups, and Roles privilege can configure LDAP authentication and manage users, groups, and roles.

The Manage Users, Groups, and Roles privilege includes the Grant Privileges and Roles privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Users, Groups, and Roles privilege:

Permission On	Description
-	User is able to perform the following actions: - Configure LDAP authentication for the domain. - Create, edit, and delete users, groups, and roles. - Import LDAP users and groups.
Operating system profile	User is able to edit operating system profile properties.

Domain Administration Privilege Group

Domain management actions that users can perform depend on privileges in the Domain Administration group and permissions on domain objects.

Some domain management tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the domain can complete the following tasks:

- Configure domain properties.
- Configure cluster configurations.
- Grant permission on the domain.
- Manage and purge log events.

- Receive domain alerts.
- Run the License Report.
- View user activity log events.
- Shut down the domain.
- Access the service upgrade wizard.

Users who are assigned domain object permissions but not privileges can complete some domain management tasks. The following table lists the actions that users can perform when they are assigned domain object permissions only:

Permission On	Description
Domain	User can perform the following actions: - View domain properties and log events. - Configure monitoring settings.
Folder	User can view folder properties.
Application service	User can view application service properties and log events.
License object	User can view license object properties.
Grid	User can view grid properties.
Node	User can view node properties.

Note: To complete domain management tasks in the Administrator tool, users must also have the Access Informatica Administrator privilege.

Manage Service Execution Privilege

Users assigned the Manage Service Execution privilege can enable and disable application services and receive application service alerts.

The following table lists the required permissions and the actions that users can perform with the Manage Service Execution privilege:

Permission On	Description
Application service	User is able to perform the following actions: - Enable and disable application services and service processes. - Receive application service alerts.

Manage Services Privilege

Users assigned the Manage Services privilege can create, configure, move, remove, and grant permission on application services and license objects.

The Manage Services privilege includes the Manage Service Execution privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Services privilege:

Permission On	Description
Domain or parent folder	User is able to create license objects.
Domain or parent folder, node or grid where application service runs, license object, and any associated application service	User is able to create application services.
Application service	User is able to perform the following actions: - Configure application services. - Grant permission on application services.
Original and destination folders	User is able to move application services or license objects from one folder to another.
Domain or parent folder and application service	User is able to remove application services.
CDI-PC Integration Service	User is able to run the CDI-PC Integration Service in safe mode.
CDI-PC Repository Service	User is able to perform the following actions: - Back up, restore, and upgrade the CDI-PC repository. - Configure data lineage for the CDI-PC repository. - Copy content from another CDI-PC repository. - Close user connections and release CDI-PC repository locks. - Create and delete CDI-PC repository content. - Create, edit, and delete reusable metadata extensions in the CDI-PC repository Manager. - Enable version control for the CDI-PC repository. - Manage a CDI-PC repository domain. - Perform an advanced purge of object versions at the repository level in the CDI-PC repository Manager. - Register and unregister CDI-PC repository plug-ins. - Run the CDI-PC repository in exclusive mode. - Send CDI-PC repository notifications to users. - Update CDI-PC repository statistics. - Upgrade the content of the CDI-PC Repository Service.
License object	User is able to perform the following actions: - Edit license objects. - Grant permission on license objects.
License object and application service	User is able to assign a license to an application service.
Domain or parent folder and license object	User is able to remove license objects.

Manage Nodes and Grids Privilege

Users assigned the Manage Nodes and Grids privilege can create, configure, move, remove, shut down, and grant permission on nodes and grids.

The following table lists the required permissions and the actions that users can perform with the Manage Nodes and Grids privilege:

Permission On	Description
Domain or parent folder	User is able to create nodes.
Domain or parent folder and nodes assigned to the grid	User is able to create grids.
Node or grid	User is able to perform the following actions: - Configure and shut down nodes and grids. - Grant permission on nodes and grids.
Original and destination folders	User is able to move nodes and grids from one folder to another.
Domain or parent folder and node or grid	User is able to remove nodes and grids.

Manage Domain Folders Privilege

Users assigned the Manage Domain Folders privilege can create, edit, move, remove, and grant permission on domain folders.

The following table lists the required permissions and the actions that users can perform with the Manage Domain Folders privilege:

Permission On	Description
Domain or parent folder	User is able to create folders.
Folder	User is able to perform the following actions: - Edit folders. - Grant permission on folders.
Original and destination folders	User is able to move folders from one parent folder to another.
Domain or parent folder and folder being removed	User is able to remove folders.

Manage Connections Privilege

Users assigned the Manage Connections privilege can create, edit, and delete connections in the Administrator tool and infacmd command line program.

Users assigned the Manage Connections privilege can also create, refresh, and delete cluster configurations and set and clear configuration properties in the Administrator tool and the infacmd command line program.

Users assigned connection permissions but not the Manage Connections privilege can perform the following connection management actions:

- View all connection metadata, except passwords. Requires read permission on connection.
- Preview data or run a mapping, scorecard, or profile. Requires execute permission on connection.

The following table lists the required permissions and the actions that users can perform with the Manage Connections privilege:

Permission	Description
-	User is able to create connections and cluster configurations.
Write on connection	User is able to copy, edit, and delete connections.
Grant on connection	User is able to grant and revoke permissions on connections.
Write on cluster configuration	User is able to create, refresh, and delete cluster configurations. User is able to set and clear cluster configuration properties.

Tools Privilege Group

The privilege in the domain Tools group determines which users can access the Administrator tool.

The following table lists the required permissions and the actions that users can perform with the privilege in the Tools group:

Privilege	Description
Access Informatica Administrator	User is able to perform the following actions: - Log in to the Administrator tool. - Manage their own user account in the Administrator tool. - Export log events.

Users must have the Access Informatica Administrator privilege in order to complete tasks in the Administrator tool. Users do not need the Access Informatica Administrator privilege to run infacmd commands.

Cloud Administration Privilege Group

The privileges in the Cloud Administration group determine which users can view and configure Informatica Cloud organizations.

The following table lists the required permissions and the actions that users can perform with the privileges in the Cloud Administration group:

Privilege	Permission On	Description
View Organization	Domain	User can view the Informatica Cloud organizations and the associated Secure Agents and cloud connections.
Manage Organization	Domain	User can add Informatica Cloud organizations in the Administrator tool.

CDI-PC Repository Service Privileges

CDI-PC Repository Service privileges determine CDI-PC repository actions that users can perform using the CDI-PC repository Manager, Designer, Workflow Manager, Workflow Monitor, and the pmrep and pmcmd command line programs.

The following table describes each privilege group for the CDI-PC Repository Service:

Privilege Group	Description
Tools	Includes privileges to access CDI-PC Client tools and command line programs.
Folders	Includes privileges to manage repository folders.
Design Objects	Includes privileges to manage business components, mapping parameters and variables, mappings, mapplets, transformations, and user-defined functions.
Sources and Targets	Includes privileges to manage cubes, dimensions, source definitions, and target definitions.
Run-time Objects	Includes privileges to manage session configuration objects, tasks, workflows, and worklets.
Global Objects	Includes privileges to manage connection objects, deployment groups, labels, and queries.

Users must have the Manage Services domain privilege and permission on the CDI-PC Repository Service to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the CDI-PC repository level.
- Create, edit, and delete reusable metadata extensions.

Tools Privilege Group

The privileges in the CDI-PC Repository Service Tools privilege group determine the CDI-PC Client tools and command line programs that users can access.

The following table lists the actions that users can perform for the privileges in the Tools group:

Privilege	Permission	Description
Access Designer	-	User is able to connect to the CDI-PC repository using the Designer.
Access Repository Manager	-	User is able to perform the following actions: - Connect to the CDI-PC repository using the Repository Manager. - Run *pmrep* commands.
Access Workflow Manager	-	User is able to perform the following actions: - Connect to the CDI-PC repository using the Workflow Manager. - Remove a CDI-PC Integration Service from the Workflow Manager.
Access Workflow Monitor	-	User is able to perform the following actions: - Connect to the CDI-PC repository using the Workflow Monitor. - Connect to the CDI-PC Integration Service in the Workflow Monitor.

Note: When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

The appropriate privilege in the Tools privilege group is required for all users completing tasks in CDI-PC Client tools and command line programs. For example, to create folders in the Repository Manager, a user must have the Create Folders and Access Repository Manager privileges.

If users have a privilege in the Tools privilege group and permission on a CDI-PC repository object but not the privilege to modify the object type, they can still perform some actions on the object. For example, a user has the Access Repository Manager privilege and read permission on some folders. The user does not have any of the privileges in the Folders privilege group. The user can view objects in the folders and compare the folders.

Folders Privilege Group

Folder management actions are determined by privileges in the Folders privilege group, CDI-PC repository object permissions, and domain object permissions. Users perform folder management actions in the Repository Manager and with the pmrep command line program.

Some folder management tasks are determined by folder ownership and the Administrator role, not by privileges or permissions. The folder owner or a user assigned the Administrator role for the CDI-PC Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the CDI-PC Integration Service uses operating system profiles. Requires permission on the operating system profile.
- Change the folder owner.
- Configure folder permissions.
- Delete the folder.
- Designate the folder to be shared.
- Edit the folder name and description.

Users assigned folder permissions but no privileges can perform some folder management actions. The following table lists the actions that users can perform when they are assigned folder permissions only:

Permission	Description
Read on folder	User is able to perform the following actions: - Compare folders. - View objects in folders.

Note: To perform actions on folders, users must also have the Access Repository Manager privilege.

Create Folders Privilege

Users assigned the Create Folders privilege can create CDI-PC repository folders.

The following table lists the required permissions and the actions that users can perform with the Create Folders privilege:

Permission	Description
-	User is able to create folders.

Copy Folders Privilege

Users assigned the Copy Folders privilege can copy folders within a CDI-PC repository or to another CDI-PC repository.

The following table lists the required permissions and the actions that users can perform with the Copy Folders privilege:

Permission	Description
Read on folder	User is able to copy folders within the same CDI-PC repository or to another CDI-PC repository. Users must also have the Create Folders privilege in the destination repository.

Manage Folder Versions

If you have a team-based development option, assign users the Manage Folder Versions privilege in a versioned CDI-PC repository. Users can change the status of folders and perform an advanced purge of object versions at the folder level.

The following table lists the required permissions and the actions that users can perform with the Manage Folder Versions privilege:

Permission	Description
Read and Write on folder	User is able to perform the following actions: - Change the status of folders. - Perform an advanced purge of object versions at the folder level.

Design Objects Privilege Group

Privileges in the Design Objects privilege group and CDI-PC repository object permissions determine actions users can perform on the following design objects:

- Business components
- Mapping parameters and variables
- Mappings
- Mapplets
- Transformations
- User-defined functions

Users assigned permissions but no privileges can perform some actions for design objects. The following table lists the actions that users can perform when they are assigned permissions only:

Permission	Description
Read on folder	User is able to perform the following actions: - Compare design objects. - Copy design objects as an image. - Export design objects. - Generate code for Custom transformation and external procedures. - Receive CDI-PC repository notification messages. - Search for design objects. - View design objects, design object dependencies, and design object history.
Read on shared folder Read and Write on destination folder	User is able to create shortcuts.

Note: To perform actions on design objects, users must also have the appropriate privilege in the Tools privilege group.

Create, Edit, and Delete Design Objects Privilege

Users assigned the Create, Edit, and Delete Design Objects privilege can create, edit, and delete business components, mapping parameters, mapping variables, mappings, mapplets, transformations, and user-defined functions.

The following table lists the required permissions and the actions that users can perform with the Create, Edit, and Delete Design Objects privilege:

Permission	Description
Read on original folder Read and Write on destination folder	User is able to perform the following actions: - Copy design objects from one folder to another. - Copy design objects to another CDI-PC repository. Users must also have the Create, Edit, and Delete Design Objects privilege in the destination repository.
Read and Write on folder	User is able to perform the following actions: - Change comments for a versioned design object. - Check in and undo a checkout of design objects checked out by their own user account. - Check out design objects. - Copy and paste design objects in the same folder. - Create, edit, and delete data profiles and launch the Profile Manager. Users must also have the Create, Edit, and Delete Run-time Objects privilege. - Create, edit, and delete design objects. - Generate and clean SAP ABAP programs. - Generate business content integration mappings. Users must also have the Create, Edit, and Delete Sources and Targets privilege. - Import design objects using the Designer. Users must also have the Create, Edit, and Delete Sources and Targets privilege. - Import design objects using the Repository Manager. Users must also have the Create, Edit, and Delete Run-time Objects and Create, Edit, and Delete Sources and Targets privileges. - Revert to a previous design object version. - Validate mappings, mapplets, and user-defined functions.

Manage Design Object Versions

If you have a team-based development option, assign users the Manage Design Object Versions privilege in a versioned CDI-PC repository. Users can change the status, recover, and purge design object versions. Users can also check in and undo checkouts made by other users.

The Manage Design Object Versions privilege includes the Create, Edit, and Delete Design Objects privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Design Object Versions privilege:

Permission	Description
Read and Write on folder	User is able to perform the following actions: - Change the status of design objects. - Check in and undo checkouts of design objects checked out by other users. - Purge versions of design objects. - Recover deleted design objects.

Sources and Targets Privilege Group

Privileges in the Sources and Targets privilege group and CDI-PC repository object permissions determine actions users can perform on the following source and target objects:

- Cubes
- Dimensions
- Source definitions
- Target definitions

Users assigned permissions but no privileges can perform some actions for source and target objects. The following table lists the actions that users can perform when they are assigned permissions only:

Permission	Description
Read on folder	User is able to perform the following actions: - Compare source and target objects. - Export source and target objects. - Preview source and target data. - Receive CDI-PC repository notification messages. - Search for source and target objects. - View source and target objects, source and target object dependencies, and source and target object history.
Read on shared folder Read and Write on destination folder	Create shortcuts.

Note: To perform actions on source and target objects, users must also have the appropriate privilege in the Tools privilege group.

Create, Edit, and Delete Sources and Targets Privilege

Users assigned the Create, Edit, and Delete Sources and Targets privilege can create, edit, and delete cubes, dimensions, source definitions, and target definitions.

The following table lists the required permissions and the actions that users can perform with the Create, Edit, and Delete Sources and Targets privilege:

Permission	Description
Read on original folder Read and Write on destination folder	User is able to perform the following actions: - Copy source and target objects to another folder. - Copy source and target objects to another CDI-PC repository. Users must also have the Create, Edit, and Delete Sources and Targets privilege in the destination repository.
Read and Write on folder	User is able to perform the following actions: - Change comments for a versioned source or target object. - Check in and undo a checkout of source and target objects checked out by their own user account. - Check out source and target objects. - Copy and paste source and target objects in the same folder. - Create, edit, and delete source and target objects. - Import SAP functions. - Import source and target objects using the Designer. Users must also have the Create, Edit, and Delete Design Objects privilege. - Import source and target objects using the Repository Manager. Users must also have the Create, Edit, and Delete Design Objects and Create, Edit, and Delete Run-time Objects privileges. - Generate and execute SQL to create targets in a relational database. - Revert to a previous source or target object version.

Manage Source and Target Versions Privilege

If you have a team-based development option, assign users the Manage Source and Target Versions privilege in a versioned CDI-PC repository. Users can change the status, recover, and purge versions of source and target objects. Users can also check in and undo checkouts made by other users.

The Manage Source and Target Versions privilege includes the Create, Edit, and Delete Sources and Targets privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Source and Target Versions privilege:

Permission	Description
Read and Write on folder	User is able to perform the following actions: - Change the status of source and target objects. - Check in and undo checkouts of source and target objects checked out by other users. - Purge versions of source and target objects. - Recover deleted source and target objects.

Run-time Objects Privilege Group

Privileges in the Run-time Objects privilege group, CDI-PC repository object permissions, and domain object permissions determine actions users can perform on the following run-time objects:

- Session configuration objects
- Tasks
- Workflows
- Worklets

Some run-time object tasks are determined by the Administrator role, not by privileges or permissions. A user assigned the Administrator role for the PowerCenter Repository Service can delete a CDI-PC Integration Service from the Navigator of the Workflow Manager.

Users assigned permissions but no privileges can perform some actions for run-time objects. The following table lists the actions that users can perform when they are assigned permissions only:

Permission	Description
Read on folder	User is able to perform the following actions: - Compare run-time objects. - Export run-time objects. - Receive CDI-PC repository notification messages. - Search for run-time objects. - Use mapping parameters and variables in a session. - View run-time objects, run-time object dependencies, and run-time object history.
Read and Execute on folder	Stop and abort tasks and workflows started by their own user account. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

Note: To perform actions on run-time objects, users must also have the appropriate privilege in the Tools privilege group.

Create, Edit, and Delete Run-time Objects Privilege

Users assigned the Create, Edit, and Delete Run-time Objects privilege can create, edit, and delete session configuration objects, tasks, workflows, and worklets.

The following table lists the required permissions and the actions that users can perform with the Create, Edit, and Delete Run-time Objects privilege:

Permission	Description
Read on original folder Read and Write on destination folder	User is able to perform the following actions: - Copy tasks, workflows, or worklets from one folder to another. - Copy tasks, workflows, or worklets to another CDI-PC repository. Users must also have the Create, Edit, and Delete Run-time Objects privilege in the destination repository.
Read and Write on folder	User is able to perform the following actions: - Assign a CDI-PC Integration Service to a workflow in the workflow properties. - Assign a service level to a workflow. - Change comments for a versioned run-time object. - Check in and undo a checkout of run-time objects checked out by their own user account. - Check out run-time objects. - Copy and paste tasks, workflows, and worklets in the same folder. - Create, edit, and delete data profiles and launch the Profile Manager. Users must also have the Create, Edit, and Delete Design Objects privilege. - Create, edit, and delete session configuration objects. - Delete and validate tasks, workflows, and worklets. - Import run-time objects using the Repository Manager. Users must also have the Create, Edit, and Delete Design Objects and Create, Edit, and Delete Sources and Targets privileges. - Import run-time objects using the Workflow Manager. - Revert to a previous object version.
Read and Write on folder Read on connection object	User is able to perform the following actions: - Create and edit tasks, workflows, and worklets. - Replace a relational database connection for all sessions that use the connection.

Manage Run-time Object Versions Privilege

If you have a team-based development option, assign users the Manage Run-time Object Versions privilege in a versioned CDI-PC repository. Users can change the status, recover, and purge run-time object versions. Users can also check in and undo checkouts made by other users.

The Manage Run-time Object Versions privilege includes the Create, Edit, and Delete Run-time Objects privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Run-time Object Versions privilege:

Permission	Description
Read and Write on folder	User is able to perform the following actions: - Change the status of run-time objects. - Check in and undo checkouts of run-time objects checked out by other users. - Purge versions of run-time objects. - Recover deleted run-time objects.

Monitor Run-time Objects Privilege

Users assigned the Monitor Run-time Objects privilege can Monitor workflows and tasks in the Workflow Monitor.

The following table lists the required permissions and the actions that users can perform with the Monitor Run-time Objects privilege:

Permission	Grants Users the Ability To
Read on folder	User is able to perform the following actions: - View properties of run-time objects in the Workflow Monitor. - View session and workflow logs in the Workflow Monitor. - View run-time object and performance details in the Workflow Monitor. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

Execute Run-time Objects Privilege

Users assigned the Execute Run-time Objects privilege can start, cold start, and recover tasks and workflows.

The Execute Run-time Objects privilege includes the Monitor Run-time Objects privilege.

The following table lists the required permissions and the actions that users can perform with the Execute Run-time Objects privilege:

Permission	Description
Read and Execute on folder	User is able to assign a CDI-PC Integration Service to a workflow using the Service menu or the Navigator.
Read, Write, and Execute on folder Read and Execute on connection object	User is able to debug a mapping by creating a debug session instance or by using an existing reusable session. Users must also have the Create, Edit, and Delete Run-time Objects privilege. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

Permission	Description
Read and Execute on folder Read and Execute on connection object	User is able to debug a mapping by using an existing non-reusable session. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.
Read and Execute on folder Read and Execute on connection object	User is able to perform the following actions: - Start, cold start, and restart tasks and workflows. - Recover tasks and workflows started by their own user account. If the CDI-PC Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

Manage Run-time Object Execution Privilege

Users assigned the Manage Run-time Object Execution privilege can schedule and unschedule workflows. Users can also stop, abort, and recover tasks and workflows started by other users.

The Manage Run-time Object Execution privilege includes the Execute Run-time Objects privilege and the Monitor Run-time Objects privilege.

The following table lists the required permissions and the actions that users can perform with the Manage Run-time Object Execution privilege:

Permission	Description
Read and Execute on folder	User is able to truncate workflow and session log entries.
Read and Execute on folder	User is able to perform the following actions: - Stop and abort tasks and workflows started by other users. - Stop and abort tasks that were recovered automatically. - Unschedule workflows. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.
Read and Execute on folder Read and Execute on connection object	User is able to perform the following actions: - Recover tasks and workflows started by other users. - Recover tasks that were recovered automatically. If the CDI-PC Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.
Read, Write, and Execute on folder Read and Execute on connection object	User is able to perform the following actions: - Create and edit a reusable scheduler from the Workflows > Schedulers menu. - Edit a non-reusable scheduler from the workflow properties. - Edit a reusable scheduler from the workflow properties. Users must also have the Create, Edit, and Delete Run-time Objects privilege. If the CDI-PC Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service.

Global Objects Privilege Group

Privileges in the Global Objects privilege group and CDI-PC repository object permissions determine actions users can perform on the following global objects:

- Connection objects
- Deployment groups
- Labels
- Queries

Some global object tasks are determined by global object ownership and the Administrator role, not by privileges or permissions. The global object owner or a user assigned the Administrator role for the CDI-PC Repository Service can complete the following global object tasks:

- Configure global object permissions.
- Change the global object owner.
- Delete the global object.

Users assigned permissions but no privileges can perform some actions for global objects. The following table lists the actions that users can perform when they are assigned permissions only:

Permission	Description
Read on connection object	User is able to view connection objects.
Read on deployment group	User is able to view deployment groups.
Read on label	User is able to view labels.
Read on query	User is able to view object queries.
Read and Write on connection object	User is able to edit connection objects.
Read and Write on label	User is able to edit and lock labels.
Read and Write on query	User is able to edit and validate object queries.
Read and Execute on query	User is able to run object queries.
Read on folder Read and Execute on label	User is able to apply labels and remove label references.

Note: To perform actions on global objects, users must also have the appropriate privilege in the Tools privilege group.

Create Connections Privilege

Users assigned the Create Connections privilege can create connection objects.

The following table lists the required permissions and the actions that users can perform with the Create Connections privilege:

Permission	Description
-	User is able to create and copy connection objects.

Manage Deployment Groups Privilege

If you have a team-based development option, users assigned the Manage Deployment Groups privilege in a versioned CDI-PC repository can create, edit, copy, and roll back deployment groups. In a non-versioned repository, users can create, edit, and copy deployment groups.

The following table lists the required permissions and the actions that users can perform with the Manage Deployment Groups privilege:

Permission	Description
-	User is able to create deployment groups.
Read and Write on deployment group	User is able to perform the following actions: - Edit deployment groups. - Remove objects from a deployment group.
Read on original folder Read and Write on deployment group	User is able to add objects to a deployment group.
Read on original folder Read and Write on destination folder Read and Execute on deployment group	User is able to copy deployment groups.
Read and Write on destination folder	User is able to roll back deployment groups.

Execute Deployment Groups Privilege

Users assigned the Execute Deployment Groups privilege can copy a deployment group without write permission on target folders.

The following table lists the required permissions and the actions that users can perform with the Execute Deployment Groups privilege:

Permission	Description
Read on original folder Execute on deployment group	User is able to copy deployment groups.

Create Labels Privilege

If you have a team-based development option, users assigned the Create Labels privilege in a versioned CDI-PC repository can create labels.

The following table lists the required permissions and the actions that users can perform with the Create Labels privilege:

Permission	Description
-	User is able to create labels.

Create Queries Privilege

Users assigned the Create Queries privilege can create object queries.

The following table lists the required permissions and the actions that users can perform with the Create Queries privilege:

Permission	Description
-	User is able to create object queries.

Managing Roles

A role is a collection of privileges that you can assign to users and groups. You can assign the following types of roles:

- System-defined. Roles that you cannot edit or delete.
- Custom. Roles that you can create, edit, and delete.

A role includes privileges for the domain or an application service type. You assign roles to users or groups for the domain or for each application service in the domain. For example, you can create a Developer role that includes privileges for the CDI-PC Repository Service. A domain can contain multiple CDI-PC Repository Services. You can assign the Developer role to a user for the Development CDI-PC Repository Service. You can assign a different role to that user for the Production CDI-PC Repository Service.

When you select a role in the Roles section of the Navigator, you can view all users and groups that have been directly assigned the role for the domain and application services. You can view the role assignments by users and groups or by services. To navigate to a user or group listed in the Assignments section, right-click the user or group and select Navigate to Item.

You can search for system-defined and custom roles.

System-Defined Roles

A system-defined role is a role that you cannot edit or delete. The Administrator role is a system-defined role.

When you assign the Administrator role to a user or group for the domain CDI-PC Repository Service, the user or group is granted all privileges for the service. The Administrator role bypasses permission checking. Users with the Administrator role can access all objects managed by the service.

Administrator Role

When you assign the Administrator role to a user or group for the domain CDI-PC Repository Service, the user or group can complete some tasks that are determined by the Administrator role, not by privileges or permissions.

You can assign a user or group all privileges for the domain CDI-PC Repository Service and then grant the user or group full permissions on all domain or CDI-PC repository objects. However, this user or group cannot complete the tasks determined by the Administrator role.

For example, a user assigned the Administrator role for the domain can configure domain properties in the Administrator tool. A user assigned all domain privileges and permission on the domain cannot configure domain properties.

The following table lists the tasks determined by the Administrator role for the domain CDI-PC Repository Service:

Service	Tasks
Domain	- Configure domain properties. - Configure cluster configurations. - Create operating system profiles. - Delete operating system profiles. - Grant permission on the domain and operating system profiles. - Manage and purge log events. - Receive domain alerts. - Run the License Report. - View user activity log events. - Shut down the domain. - Access the service upgrade wizard.
CDI-PC Repository Service	- Assign operating system profiles to repository folders if the CDI-PC Integration Service uses operating system profiles.* - Change the owner of folders and global objects.* - Configure folder and global object permissions.* - Connect to the CDI-PC Integration Service from the CDI-PC Client when running the CDI-PC Integration Service in safe mode. - Delete a CDI-PC Integration Service from the Navigator of the Workflow Manager. - Delete folders and global objects.* - Designate folders to be shared.* - Edit the name and description of folders.* *The CDI-PC repository folder owner or global object owner can also complete these tasks.

Custom Roles

A custom role is a role that you can edit or delete.

By default, the Administrator tool includes the following custom roles:

- Operator custom role
- CDI-PC Repository Service custom roles

You can edit the privileges for these roles, or delete the roles. You can also create your own custom roles.

Creating Custom Roles

When you create a custom role, you assign privileges to the role for the domain or for an application service type. A role can include privileges for one or more services.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Create Role.

   The Create Role dialog box appears.
3. Enter the following properties for the role:

Property	Description
Name	Name of the role. The role name is case insensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Description	Description of the role. The description cannot exceed 765 characters or include a tab, newline character, or the following special characters: < > "

4. Click the Privileges tab.
5. Expand the domain or an application service type.
6. Select the privileges to assign to the role for the domain or application service type.
7. Click OK.

Editing Properties for Custom Roles

When you edit a custom role, you can change the description of the role. You cannot change the name of the role.

1. In the Administrator tool, click the Security tab.
2. In the Roles section of the Navigator, select a role.
3. Click Edit.
4. Change the description of the role and click OK.

Editing Privileges Assigned to Custom Roles

You can change the privileges assigned to a custom role for the domain and for each application service type.

1. In the Administrator tool, click the Security tab.
2. In the Roles section of the Navigator, select a role.
3. Click the Privileges tab.
4. Click Edit.

   The Edit Roles and Privileges dialog box appears.
5. Expand the domain or an application service type.
6. To assign privileges to the role, select the privileges for the domain or application service type.
7. To remove privileges from the role, clear the privileges for the domain or application service type.
8. Repeat the steps to change the privileges for each service type.

9. Click OK.

Deleting Custom Roles

When you delete a custom role, the custom role and all privileges that it included are removed from any user or group assigned the role.

To delete a custom role, right-click the role in the Roles section of the Navigator and select Delete Role. Confirm that you want to delete the role.

Assigning Privileges and Roles to Users and Groups

You determine the actions that users can perform by assigning the following items to users and groups:

- Privileges. A privilege determines the actions that users can perform in application clients.
- Roles. A role is a collection of privileges. When you assign a role to a user or group, you assign the collection of privileges belonging to the role.

Use the following rules and guidelines when you assign privileges and roles to users and groups:

- You assign privileges and roles to users and groups for the domain and for each application service that is running in the domain.

  You cannot assign privileges and roles to users and groups for a CDI-PC Repository Service in the following situations:

  - The application service is disabled.
  - The CDI-PC Repository Service is running in exclusive mode.
- You can assign different privileges and roles to a user or group for each application service of the same service type.
- A role can include privileges for the domain and multiple application service types. When you assign the role to a user or group for one application service, privileges for that application service type are assigned to the user or group.

If you change the privileges or roles assigned to a user, the changed privileges or roles take effect the next time that the user logs in.

Note: You cannot edit the privileges or roles assigned to the default Administrator user account.

Inherited Privileges

A user or group can inherit privileges from the following objects:

- Group. When you assign privileges to a group, all subgroups and users belonging to the group inherit the privileges.
- Role. When you assign a role to a user, the user inherits the privileges belonging to the role. When you assign a role to a group, the group and all subgroups and users belonging to the group inherit the privileges belonging to the role. The subgroups and users do not inherit the role.

You cannot revoke privileges inherited from a group or role. You can assign additional privileges to a user or group that are not inherited from a group or role.

The Privileges tab for a user or group displays all the roles and privileges assigned to the user or group for the domain and for each application service. Expand the domain or application service to view the roles and

privileges assigned for the domain or service. Click the following items to display additional information about the assigned roles and privileges:

- Name of an assigned role. Displays the role details on the details panel.
- Information icon for an assigned role. Highlights all privileges inherited with that role.

Privileges that are inherited from a role or group display an inheritance icon. The tooltip for an inherited privilege displays which role or group the user inherited the privilege from.

Assigning Privileges and Roles to a User or Group by Navigation

1. In the Administrator tool, click the Security tab.
2. In the Navigator, select a user or group.
3. Click the Privileges tab.
4. Click Edit.

   The Edit Roles and Privileges dialog box appears.
5. To assign roles, expand the domain or an application service on the Roles tab.
6. To grant roles, select the roles to assign to the user or group for the domain or application service.

   You can select any role that includes privileges for the selected domain or application service type.
7. To revoke roles, clear the roles assigned to the user or group.
8. Repeat steps 5 through 7 to assign roles for another service.
9. To assign privileges, click the Privileges tab.
10. Expand the domain or an application service.
11. To grant privileges, select the privileges to assign to the user or group for the domain or application service.
12. To revoke privileges, clear the privileges assigned to the user or group.

    You cannot revoke privileges inherited from a role or group.
13. Repeat steps 10 through 12 to assign privileges for another service.
14. Click OK.

Viewing Users with Privileges for a Service

You can view all users that have privileges for the domain or an application service.

1. In the Administrator tool, click the Security tab.
2. On the Security Actions menu, click Service User Privileges.

   The Services dialog box appears.
3. Select the domain or an application service.

   The details panel displays all users that have privileges for the domain or application service.
4. Right-click a user name and click Navigate to Item to navigate to the user.

Troubleshooting Privileges and Roles

I cannot assign privileges or roles to users for an existing CDI-PC Repository Service.

You cannot assign privileges and roles to users and groups for an existing CDI-PC Repository Service in the following situations:

- The application service is disabled.
- The CDI-PC Repository Service is running in exclusive mode.

I removed a privilege from a group. Why do some users in the group still have that privilege?

You can use any of the following methods to assign privileges to a user:

- Assign a privilege directly to a user.
- Assign a role to a user.
- Assign a privilege or role to a group that the user belongs to.

If you remove a privilege from a group, users that belong to that group can be directly assigned the privilege or can inherit the privilege from an assigned role.

I am assigned all domain privileges and permission on all domain objects, but I cannot complete all tasks in the Administrator tool.

Some of the Administrator tool tasks are determined by the Administrator role, not by privileges or permissions. You can be assigned all privileges for the domain and granted full permissions on all domain objects. However, you cannot complete the tasks determined by the Administrator role.

I am assigned the Administrator role for an application service, but I cannot configure the application service in the Administrator tool.

When you have the Administrator role for an application service, you are an application client administrator. An application client administrator has full permissions and privileges in an application client.

However, an application client administrator does not have permissions or privileges on the Informatica domain. An application client administrator cannot log in to the Administrator tool to manage the service for the application client for which it has administrator privileges.

To manage an application service in the Administrator tool, you must have the appropriate domain privileges and permissions.

I am assigned the Administrator role for the CDI-PC Repository Service, but I cannot use the Repository Manager to perform an advanced purge of objects or to create reusable metadata extensions.

You must have the Manage Services domain privilege and permission on the CDI-PC Repository Service in the Administrator tool to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the CDI-PC repository level.
- Create, edit, and delete reusable metadata extensions.

My privileges indicate that I should be able to edit objects in an application client, but I cannot edit any metadata.

You might not have the required object permissions in the application client. Even if you have the privilege to perform certain actions, you may also require permission to perform the action on a particular object.

I cannot use pmrep to connect to a new CDI-PC Repository Service running in exclusive mode.

The Service Manager might not have synchronized the list of users and groups in the CDI-PC repository with the list in the domain configuration database. To synchronize the list of users and groups, restart the CDI-PC Repository Service.

I am assigned all privileges in the Folders privilege group for the CDI-PC Repository Service and have read, write, and execute permission on a folder. However, I cannot configure the permissions for the folder.

Only the folder owner or a user assigned the Administrator role for the CDI-PC Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the CDI-PC Integration Service uses operating system profiles. Requires permission on the operating system profile.
- Change the folder owner.
- Configure folder permissions.
- Delete the folder.
- Designate the folder to be shared.
- Edit the folder name and description.

CHAPTER 10

Permissions

This chapter includes the following topics:

- Permissions Overview, 142
- Domain Object Permissions, 144
- Connection Permissions, 148
- Application and Application Object Permissions, 150

Permissions Overview

You manage user security with privileges and permissions. Permissions define the level of access that users and groups have to an object.

Even if a user has the privilege to perform certain actions, the user may also require permission to perform the action on a particular object.

For example, a user has the Manage Services domain privilege and permission on the Development CDI-PC Repository Service, but not on the Production CDI-PC Repository Service. The user can edit or remove the Development CDI-PC Repository Service, but not the Production CDI-PC Repository Service. To manage an application service, a user must have the Manage Services domain privilege and permission on the application service.

You use different tools to configure permissions on the following objects:

Object Type	Tool	Description
Applications and application objects	Administrator tool	You can assign permissions on applications and application objects such as mappings and workflows.
Connection objects	Administrator tool	You can assign permissions on connections defined in the Administrator tool. These tools share the connection permissions.
Domain objects	Administrator tool	You can assign permissions on the following domain objects: domain, folders, nodes, grids, licenses, application services, and operating system profiles.
CDI-PC repository objects	CDI-PC Client	You can assign permissions on CDI-PC folders, deployment groups, labels, queries, and connection objects.

Types of Permissions

Users and groups can have the following types of permissions in a domain:

Direct permissions

Permissions that are assigned directly to a user or group. When users and groups have permission on an object, they can perform administrative tasks on that object if they also have the appropriate privilege. You can edit direct permissions.

Inherited permissions

Permissions that users inherit. When users have permission on a domain or a folder, they inherit permission on all objects in the domain or the folder. When groups have permission on a domain object, all subgroups and users belonging to the group inherit permission on the domain object. For example, a domain has a folder named Nodes that contains multiple nodes. If you assign a group permission on the folder, all subgroups and users belonging to the group inherit permission on the folder and on all nodes in the folder.

You cannot revoke inherited permissions. You also cannot revoke permissions from users or groups assigned the Administrator role. The Administrator role bypasses permission checking. Users with the Administrator role can access all objects.

You can deny inherited permissions on some object types. When you deny permissions, you configure exceptions to the permissions that users and groups might already have.

Effective permissions

Superset of all permissions for a user or group. Includes direct permissions and inherited permissions.

When you view permission details, you can view the origin of effective permissions. Permission details display direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.

Permission Search Filters

When you assign permissions, view permission details, or edit permissions for a user or group, you can use search filters to search for a user or group.

When you manage permissions for a user or group, you can use the following search filters:

Security domain

Select the security domain to search for users or groups.

Pattern string

Enter a string to search for users or groups. The Administrator tool returns all names that contain the search string. The string is not case sensitive. For example, the string "DA" can return "iasdaemon," "daphne," and "DA_AdminGroup."

You can also sort the list of users or groups. Right-click a column name to sort the column in ascending or descending order.

Domain Object Permissions

You configure privileges and permissions to manage user security within the domain. Permissions define the level of access a user has to a domain object. To log in to the Administrator tool, a user must have permission on at least one domain object. If a user has permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can only view the object.

For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties, but cannot configure, shut down, or remove the node.

You can configure permissions on the following types of domain objects:

Domain Object Type	Description of Permission
Domain	Enables Administrator tool users to access all objects in the domain. When users have permission on a domain, they inherit permission on all objects in the domain.
Folder	Enables Administrator tool users to access all objects in the folder in the Administrator tool. When users have permission on a folder, they inherit permission on all objects in the folder.
Node	Enables Administrator tool users to view and edit the node properties. Without permission, a user cannot use the node when defining an application service or creating a grid.
Grid	Enables Administrator tool users to view and edit the grid properties. Without permission, a user cannot assign the grid to a CDI-PC Integration Service.
License	Enables Administrator tool users to view and edit the license properties. Without permission, a user cannot use the license when creating an application service.
Application Service	Enables Administrator tool users to view and edit the application service properties.
Operating System Profile	Enables Informatica developers, analysts, and operators associated with the operating system profile to run mappings, profiles, and workflows. Enables CDI-PC users to run workflows associated with the operating system profile. If the user that runs a workflow does not have permission on the operating system profile assigned to the workflow, the workflow fails.

You can use the following methods to manage domain object permissions:

- Manage permissions by domain object. Use the Permissions view of a domain object to assign and edit permissions on the object for multiple users or groups.
- Manage permissions by user or group. Use the Manage Permissions dialog box to assign and edit permissions on domain objects for a specific user or group.

Note: You configure permissions on an operating system profile differently than you configure permissions on other domain objects.

Permissions by Domain Object

Use the **Permissions** view of a domain object to assign, view, and edit permissions on the domain object for multiple users or groups.

Assigning Permissions on a Domain Object

When you assign permissions on a domain object, you grant users and groups access to the object.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Click **Actions** > **Assign Permission**.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the object.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group, and click **Next**.
8. Select **Allow**, and click **Finish**.

Viewing Permission Details on a Domain Object

When you view permission details, you can view the origin of effective permissions.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **View Permission Details**.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
7. Click **Close**.
8. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on a Domain Object

You can edit direct permissions on a domain object for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select the domain object.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
7. To assign permission on the object, select **Allow**.

8. To revoke permission on the object, select **Revoke**.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.

9. Click **OK**.

Permissions by User or Group

Use the **Manage Permissions** dialog box to view, assign, and edit domain object permissions for a specific user or group.

Viewing Permission Details for a User or Group

When you view permission details, you can view the origin of effective permissions.

1. In the Administrator tool, click the **Security** tab.
2. Click the **Groups** tab or the **Users** tab.
3. Select a user or group.
4. Click the **Permissions** tab.

Assigning and Editing Permissions for a User or Group

When you edit domain object permissions for a user or group, you can assign permissions and edit existing direct permissions. You cannot revoke inherited permissions or your own permissions.

You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**. If you revoke a permission on the object, the user or group might still inherit the permission from a parent group or object.

1. In the Administrator tool, click the **Security** tab.
2. Click the **Groups** tab or the **Users** tab.
3. Select a user or group.
4. Click the **Permissions** tab.
5. Select a domain object, and then click **Edit Direct Permissions**.
6. To assign a permission on the object, select **Allow**.
7. To revoke permission on the object, select **Revoke**.
8. Click **OK**.

Operating System Profile Permissions

Assign, view, and edit permissions on operating system profiles in the Security page of the Administrator tool.

The Administrator group has permissions on all operating system profiles.

Assigning Permissions on an Operating System Profile

When you assign permissions on an operating system profile, Informatica users run mappings, profiles, and workflows with the operating system profile. CDI-PC users run workflows assigned to the operating system profile.

1. In the Administrator tool, click the **Security** tab.
2. Click the **Operating System Profiles** tab.
3. Select an operating system profile, and then click the **Permissions** tab.
4. Click the **Groups** tab or the **Users** tab, and then select **Edit Direct Permissions**.
5. Select a domain object, and then click **Edit Direct Permissions**.
6. To assign a permission on the object, select **Allow**.
7. To revoke permission on the object, select **Revoke**.
8. Click **OK**.

Viewing Permission Details on an Operating System Profile

When you view permission details, you can view the origin of effective permissions.

1. On the **Security** tab, select the **Operating System Profiles** view.
2. Select the operating system profile, and click the **Permissions** tab.
3. Select the **Groups** or **Users** view.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group and click **View Permission Details**.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
6. Click **Close**.
7. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on an Operating System Profile

You can edit direct permissions on an operating system profile for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the **Security** tab, select the **Operating System Profiles** view.
2. Select the operating system profile, and click the **Permissions** tab.
3. Select the **Groups** or **Users** view.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group and click **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
6. To assign permission on the operating system profile, select **Allow**.
7. To revoke permission on the operating system profile, select **Revoke**.

You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.

8. Click **OK**.

Connection Permissions

Permissions control the level of access that a user or group has on the connection.

You can configure permissions on a connection in the Administrator tool.

Any connection permission that is assigned to a user or group in one tool also applies in other tools.

The following Informatica components use the connection permissions:

- Administrator tool. Enforces read, write, and execute permissions on connections.
- Informatica command line interface. Enforces read, write, and grant permissions on connections.

Types of Connection Permissions

You can assign different permission types to users to perform the following actions:

Action	Permission Types
View all connection metadata, except passwords, such as connection name, type, description, connection strings, and user names.	Read
Edit all connection metadata, including passwords. Delete the connection. Users with Write permission inherit Read permission.	Write
Access the physical data in the underlying data source defined by the connection. Users can preview data, run a mapping, run a mapping in a workflow Mapping task, run a scorecard, or run a profile that uses the connection.	Execute
Grant and revoke permissions on connections.	Grant

Default Connection Permissions

The domain administrator has all permissions on all connections. The user that creates a connection has read, write, execute, and grant permission on the connection. By default, all users have permission to perform the following actions on connections:

- View basic connection metadata, such as connection name, type, and description.

Assigning Permissions on a Connection

When you assign permissions on a connection, you define the level of access a user or group has to the connection.

1. On the Manage tab, select the **Connections** view.
2. In the Navigator, select the connection.

3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Click **Actions** > **Assign Permission**.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the connection.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group, and click **Next**.
8. Select **Allow** for each permission type that you want to assign.
9. Click **Finish**.

Viewing Permission Details on a Connection

When you view permission details, you can view the origin of effective permissions.

1. On the Manage tab, select the **Connections** view.
2. In the Navigator, select the connection.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Select a user or group and click **Actions** > **View Permission Details**.

   The **View Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group and direct permissions assigned to parent groups. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses the permission check.
6. Click **Close**.
7. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on a Connection

You can edit direct permissions on a connection for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Manage tab, select the **Connections** view.
2. In the Navigator, select the connection.
3. In the contents panel, select the **Permissions** view.
4. Click the **Groups** or **Users** tab.
5. Enter the filter conditions to search for users and groups, and click the **Filter** button.
6. Select a user or group and click **Actions** > **Edit Direct Permissions**.

   The **Edit Direct Permissions** dialog box appears.
7. Choose to allow or revoke permissions.
   - Select **Allow** to assign a permission.
   - Clear **Allow** to revoke a single permission.
   - Select **Revoke** to revoke all permissions.

You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.

8. Click **OK**.

Application and Application Object Permissions

Permissions control the level of access that a user or group has on applications and application objects such as mappings and workflows.

You can configure application and application object permissions in the Administrator tool or from the command line.

Types of Application and Application Object Permissions

You can assign view, grant, and execute permissions to users and groups.

You can assign the following permissions to users and groups:

View permission

View applications and application objects.

Grant permission

Grant and revoke permissions on the applications and application objects.

Execute permission

Run applications and application objects.

Note: To perform application operations such as start, stop, or back up in the Administrator tool or from the command line, the user must have execute permission and the Manage Applications privilege on the application.

Assigning Permissions on an Application or Application Object

When you assign permissions on an application or application object, you define the level of access a user or group has to the application or the application object.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select an application, a mapping, or a workflow.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Click the **Assign Permission** button.

   The **Assign Permissions** dialog box displays all users or groups that do not have permission on the application or application object.
7. Enter the filter conditions to search for users and groups, and click the **Filter** button.
8. Select a user or group, and click **Next**.
9. Select **Allow** for each permission type that you want to assign.
10. Click **Finish**.

Viewing Permission Details on an Application or Application Object

When you view permission details, you can view the origin of effective permissions.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the application, mapping, or workflow.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **View Permission Details** button.

   The **Permission Details** dialog box appears. The dialog box displays direct permissions assigned to the user or group, direct permissions assigned to parent groups, and permissions inherited from parent objects. In addition, permission details display whether the user or group is assigned the Administrator role which bypasses permission checking.
8. Click **Close**.
9. Or, click **Edit Permissions** to edit direct permissions.

Editing Permissions on an Application or Application Object

You can edit direct permissions on an application or application object for a user or group. You cannot revoke inherited permissions or your own permissions.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. On the Manage tab, select the **Services and Nodes** view.
2. In the Navigator, select a Data Integration Service.
3. In the contents panel, select the **Applications** view.
4. Select the application or application object.
5. In the details panel, select the **Group Permissions** or **User Permissions** view.
6. Enter the filter conditions to search for users and groups, and click the **Filter** button.
7. Select a user or group and click the **Edit Direct Permissions** button.

   The **Edit Direct Permissions** dialog box appears.
8. Choose to allow or revoke permissions.
   - Select **Allow** to assign a permission.
   - Clear **Allow** to revoke a single permission.
   - Select **Revoke** to revoke all permissions.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
9. Click **OK**.

Denying Permissions on an Application or Application Object

You can explicitly deny permissions on application and application objects. When you deny a permission, you are applying an exception to the effective permission.

CHAPTER 11

Audit Reports

This chapter includes the following topics:

- Audit Reports Overview, 152
- User Personal Information, 153
- User Group Association, 153
- Privileges, 154
- Roles Association, 155
- Domain Object Permission, 155
- Selecting Users for an Audit Report, 156
- Selecting Groups for an Audit Report , 156
- Selecting Roles for an Audit Report, 157

Audit Reports Overview

Use the audit reports to view information about users and groups in the Informatica domain and the privileges and permissions assigned to them.

You can generate the following audit reports:

User Personal Information

Displays information about the user accounts in the domain, including the user status. You can select the users or groups for which you want to generate the report.

User Group Association

Displays information about users and the groups to which they belong. You can select the users or groups for which you want to generate the report.

Privileges

Displays information about privileges assigned to the users and groups in the domain. You can select the users or groups for which you want to generate the report.

Roles

Displays information about the roles assigned the users and groups in the domain. You can select the roles for which you want to generate the report.

Domain Object Permissions

Displays information about the domain objects for which users and groups have permission. You can select the users or groups for which you want to generate the report.

You can generate the audit reports in different formats, including CSV, text, or PDF files. You can also view the report on the screen.

You can generate the audit reports from the Administrator tool or from the command line. To run the audit reports from the command line, run the infacmd aud command line program.

User Personal Information

The User Personal Information report displays the contact information and status of user accounts in the domain.

If you run the report for groups, the report organizes the list of users by group and displays the group name and security domain for each group. The report displays nested groups separately.

The User Personal Information report displays the following information:

Login Name

Login name for the user account.

Full Name

Full name for the user account.

Security Domain

Security domain to which the user belongs.

Description

Description of the user account.

Email ID

Email address for the user account.

Phone

Telephone number for the user account.

Account Locked

Indicates whether the account is locked or not. The report displays Yes if the account is locked and No if the account is not locked.

Account Disabled

Indicates whether the account is disabled or not. The report displays Yes if the account is disabled and No if the account is enabled.

User Group Association

The User Group Association report displays information about users and their associated groups.

If you run the report for users, the report displays the list of users and the groups to which they belong.

The User Group Association report displays the following information:

Login Name

Login name for the user account.

Full Name

Full name for the user account.

Security Domain

Security domain to which the user account belongs.

Group Name

Name of the group to which the user belongs.

Group Path

If the group is a single group, the group path shows the group name. If the group is a nested group, the group path shows position of the group within the hierarchy of the nested groups.

Group Security Domain

Security domain for the group to which the user belongs.

If you run the report for groups, the report organizes the list of users by group and displays the group name and security domain for each group. The report displays nested groups separately. For each group, the report shows the list of users and child groups that belong to the group.

The User Group Association report displays the following information for the users that belong to the group:

Login Name

Login name for the user account.

Full Name

Full name for the user account.

Security Domain

Security domain to which the user account belongs.

The User Group Association report displays the following information for the child groups that belong to the group:

Group Name

Name of the group.

Security Domain

Security domain to which the group belongs.

Group Path

If the group is a single group, the group path shows the group name. If the group is a nested group, the group path shows position of the group within the hierarchy of the nested groups.

Privileges

The Privileges report displays the users and groups and the privileges assigned to the users and groups.

If you run the report for users, the report shows the list of users and the privileges assigned to each user. If you run the report for groups, the report shows the list of groups and the privileges assigned to each group.

The Privileges report displays the following information:

Privilege Name

Name of the privilege.

Privilege Path

The hierarchy of the privilege group that contains the privilege.

Object Name

Name of the object on which the privilege is allowed.

Object Type

Type of the object on which the privilege is allowed.

Roles Association

The Roles Association report displays a list of roles and the users and groups to which the roles are assigned.

The Roles Association report displays the following information:

Login Name

Login name for the user account to which the role is assigned. Displays for the list of users.

Full Name

Full name for the user account to which the role is assigned. Displays for the list of users.

Group Name

Name of the group to which the role is assigned. Displays for the list of groups.

Security Domain

Security domain to which the user or group belongs.

Object Name

Name of the object on which the set of privileges in the role are allowed.

Object Type

Type of the object on which the set of privileges in the role are allowed.

Domain Object Permission

The Domain Object Permission report displays the users and groups and the objects to which the users and groups have permission.

If you run the report for users, the report shows the list of users and the objects to which the users have permissions. If you run the report for groups, the report shows the list of groups and the objects to which the groups have permissions.

The Domain Object Permission report displays the following information:

Object Name

Name of the object to which the user or group has permission.

Object Type

Type of the object to which the user or group has permission.

Object Path

Location of the object in the repository.

Selecting Users for an Audit Report

You can generate an audit report for multiple users.

1. In the Administrator tool, click **Security** > **Audit Reports**.
2. From the **Select Report Type** list, select the type of audit report that you want to run.
3. From the **Generate Report For** list, select **Users** and click **Go**.

   The **Select Users** dialog box appears. By default, the **Users** icon is selected and the list of all available users display. The list shows the full name of the user and the security domain to which the user belongs.
4. From the **Available Users** list, select the users for which you want to run the report.

   Use the Shift key or Ctrl key to select multiple users.
5. To select users by group, click the **Groups** icon.

   The **Available Groups** list displays all groups in the domain and the **Members** list displays the users who are members of the groups. From the **Members** list, select the users for which you want to run the report. You can select users from multiple groups.
6. Click **Add**.

   To run the report for all users, click the **Users** icon and then click **Add All** without selecting a user.

   To run the report for all users in a group, click the **Groups** icon. Select a group and click **Add All** without selecting a user from the **Members** list.

   The selected users move to the **Selected Users** list.
7. From the **Report Output Format** list, select the format in which you want to view the report.

   By default, the report displays on the screen.
   You can also view an audit report in one of the following formats:
   - Text. Generates the audit report as a text file with values listed in columns.
   - CSV. Generates the audit report as a text file with values separated by commas.
   - PDF. Generates the audit report in .pdf format. You must install Acrobat Reader to view the report.
8. Click **Generate Report**.

Selecting Groups for an Audit Report

You can run audit reports for multiple groups.

1. In the Administrator tool, click **Security** > **Audit Reports**.
2. From the **Select Report Type** list, select the type of audit report that you want to run.
3. From the **Generate Report For** list, select **Groups** and click **Go**.

   The **Select Groups** dialog box appears. The list of groups are organized by security domain.

4. From the **Available Groups** list, select the groups for which you want to run the report.

   Use the Shift key or Ctrl key to select multiple groups.
5. Click **Add**.

   To run the report for all groups, do not select a group and click **Add All**.

   The selected groups move to the **Selected Groups** list.
6. From the **Report Output Format** list, select the format in which you want to view the report.

   By default, the reports displays on the screen.
   You can also run an audit report in one of the following formats:

   - Text. Generates the audit report as a text file with values listed in columns.
   - CSV. Generates the audit report as a text file with values separated by commas.
   - PDF. Generates the audit report in .pdf format. You must install Acrobat Reader to view the report.
7. Click **Generate Report**.

Selecting Roles for an Audit Report

When you run the Roles Association report, you must select the roles for which you want to run the report.

1. In the Administrator tool, click **Security** > **Audit Reports**.
2. From the **Select Report Type** list, select the **Roles Association** report.
3. From the **Generate Report For** list, select **Roles** and click **Go**.

   The **Select Roles** dialog box appears. The list of system-defined roles display separately from the list of custom roles.
4. From the **Available Roles** list, select the roles for which you want to run the report.

   Use the Shift key or Ctrl key to select multiple roles.
5. Click **Add**.

   To run the report for all roles, do not select a role and click **Add All**.

   The selected roles move to the **Selected Roles** list.
6. From the **Report Output Format** list, select the format in which you want to view the report.

   By default, the reports displays on the screen.
   You can also run an audit report in one of the following formats:

   - Text. Generates the audit report as a text file with values listed in columns.
   - CSV. Generates the audit report as a text file with values separated by commas.
   - PDF. Generates the audit report in .pdf format. You must install Acrobat Reader to view the report.
7. Click **Generate Report**.

APPENDIX A

Command Line Privileges and Permissions

This appendix includes the following topics:

- infacmd dp Commands, 158
- infacmd es commands, 158
- infacmd isp Commands, 159
- infacmd ms Commands, 167
- infacmd rms Commands, 167
- infacmd sch commands, 167
- infacmd wfs Commands, 168
- pmcmd Commands, 168
- pmrep Commands, 171

infacmd dp Commands

Users must be native users or be assigned the Administrator role to run the following infacmd dp commands:

- startSparkJobServer
- stopSparkJobServer

infacmd es commands

Users must be assigned the Administrator role for the domain to run the following infacmd es commands:

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd isp Commands

To run *infacmd isp* commands, users must have one of the listed sets of domain privileges, service privileges, domain object permissions, and connection permissions.

The following table lists the required privileges and permissions for *infacmd isp* commands:

infacmd isp Command	Privilege Group	Privilege Name	Permission On
AddAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-
AddAlertUser (for your user account)	-	-	-
AddConnectionPermissions	-	-	Grant on connection
AddDomainLink*	-	-	-
AddDomainNode	Domain Administration	Manage Nodes and Grids	Domain and node
AddGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain CDI-PC Repository Service.
AddLicense	Domain Administration	Manage Services	Domain or parent folder
AddNodeResource	Domain Administration	Manage Nodes and Grids	Node
AddRolePrivilege	Security Administration	Manage Users, Groups, and Roles	-
AddServiceLevel*	-	-	-
AddUserToGroup	Security Administration	Manage Users, Groups, and Roles	-
AssignGroupPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignGroupPermission (on domain)*	-	-	-
AssignGroupPermission (on folders)	Domain Administration	Manage Domain Folders	Folder
AssignGroupPermission (on nodes and grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignGroupPermission (on operating system profiles)*	-	-	-
AssignLicense	Domain Administration	Manage Services	License object and application service
AssignRSToWSHubService	Domain Administration	Manage Services	CDI-PC Repository Service

infacmd isp Command	Privilege Group	Privilege Name	Permission On
AssignRoleToGroup	Security Administration	Grant Privileges and Roles	Domain CDI-PC Repository Service.
AssignRoleToUser	Security Administration	Grant Privileges and Roles	Domain CDI-PC Repository Service.
AssignUserPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignUserPermission (on domain)*	-	-	-
AssignUserPermission (on folders)	Domain Administration	Manage Domain Folders	Folder
AssignUserPermission (on nodes or grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignUserPermission (on operating system profiles)*	-	-	-
AssignUserPrivilege	Security Administration	Grant Privileges and Roles	Domain CDI-PC Repository Service.
AssignedToLicense	Domain Administration	Manage Services	License object and application service
ConvertLogFile	-	-	Domain or application service
CreateConnection*	-	-	-
CreateFolder	Domain Administration	Manage Domain Folders	Domain or parent folder
CreateGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and nodes assigned to grid
CreateGroup	Security Administration	Manage Users, Groups, and Roles	-
CreateIntegrationService	Domain Administration	Manage Services	Domain or parent folder, node or grid where CDI-PC Integration Service runs, license object, and associated CDI-PC Repository Service.
CreateOSProfile*	-	-	-
CreateRepositoryService	Domain Administration	Manage Services	Domain or parent folder, node where CDI-PC Repository Service runs, and license object

infacmd isp Command	Privilege Group	Privilege Name	Permission On
CreateRole	Security Administration	Manage Users, Groups, and Roles	-
CreateSAPBWService	Domain Administration	Manage Services	Domain or parent folder, node or grid where SAP BW Service runs, license object, and associated CDI-PC Integration Service
CreateUser	Security Administration	Manage Users, Groups, and Roles	-
DisableNodeResource	Domain Administration	Manage Nodes and Grids	Node
DisableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
DisableServiceProcess	Domain Administration	Manage Service Execution	Application service
DisableUser	Security Administration	Manage Users, Groups, and Roles	-
EditUser	Security Administration	Manage Users, Groups, and Roles	-
EnableNodeResource	Domain Administration	Manage Nodes and Grids	Node
EnableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
EnableServiceProcess	Domain Administration	Manage Service Execution	Application service
EnableUser	Security Administration	Manage Users, Groups, and Roles	-
ExportDomainObjects (for connections)	Domain Administration	Manage Connections	Read on connections
ExportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ExportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
GetFolderInfo	-	-	Folder
GetLastError	-	-	Application service
GetLog	-	-	Domain or application service

infacmd isp Command	Privilege Group	Privilege Name	Permission On
GetNodeName	-	-	Node
GetServiceOption	-	-	Application service
GetServiceProcessOption	-	-	Application service
GetServiceProcessStatus	-	-	Application service
GetServiceStatus	-	-	Application service
GetSessionLog	Run-time Objects	Monitor	Read on repository folder
GetWorkflowLog	Run-time Objects	Monitor	Read on repository folder
Help	-	-	-
ImportDomainObjects (for connections)	Domain Administration	Manage Connections	Write on connections
ImportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ImportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
ListAlertUsers	-	-	Domain
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Read on connection
ListConnectionPermissions	-	-	-
ListConnectionPermissions by Group	-	-	-
ListConnectionPermissions by User	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	Domain
ListDomainOptions	-	-	Domain
ListFolders	-	-	Folders
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
ListGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
ListGroupsForUser	-	-	Domain
ListLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	-
ListLicenses	-	-	License objects
ListNodeOptions	-	-	Node
ListNodeResources	-	-	Node
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domain
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	Domain
ListSecurityDomains	Security Administration	Manage Users, Groups, and Roles	-
ListServiceLevels	-	-	Domain
ListServiceNodes	-	-	Application service
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListUserPermissions	-	-	-
ListUserPrivilege	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
MoveFolder	Domain Administration	Manage Domain Folders	Original and destination folders
MoveObject (for application services or license objects)	Domain Administration	Manage Services	Original and destination folders
MoveObject (for nodes or grids)	Domain Administration	Manage Nodes and Grids	Original and destination folders
Ping	-	-	-
PurgeLog*	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
RemoveAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-
RemoveAlertUser (for your user account)	-	-	-
RemoveConnection	-	-	Write on connection
RemoveConnectionPermissions	-	-	Grant on connection
RemoveDomainLink*	-	-	-
RemoveFolder	Domain Administration	Manage Domain Folders	Domain or parent folder and folder being removed
RemoveGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and grid
RemoveGroup	Security Administration	Manage Users, Groups, and Roles	-
RemoveGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
RemoveLicense	Domain Administration	Manage Services	Domain or parent folder and license object
RemoveNode	Domain Administration	Manage Nodes and Grids	Domain or parent folder and node
RemoveNodeResource	Domain Administration	Manage Nodes and Grids	Node
RemoveOSProfile*	-	-	-
RemoveRole	Security Administration	Manage Users, Groups, and Roles	-
RemoveRolePrivilege	Security Administration	Manage Users, Groups, and Roles	-
RemoveService	Domain Administration	Manage Services	Domain or parent folder and application service
RemoveServiceLevel*	-	-	-
RemoveUser	Security Administration	Manage Users, Groups, and Roles	-
RemoveUserFromGroup	Security Administration	Manage Users, Groups, and Roles	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
RemoveUserPrivilege	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
RenameConnection	-	-	Write on connection
ResetPassword (for other users)	Security Administration	Manage Users, Groups, and Roles	-
ResetPassword (for your user account)	-	-	-
RunCPUProfile	Domain Administration	Manage Nodes and Grids	Node
SetConnectionPermission	-	-	Grant on connection
SetLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	-
SetRepositoryLDAPConfiguration	-	-	Domain
ShowLicense	-	-	License object
ShutdownNode	Domain Administration	Manage Nodes and Grids	Node
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMService	Domain Administration	Manage Services	CDI-PC Integration Service
UnAssignRoleFromGroup	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
UnAssignRoleFromUser	Security Administration	Grant Privileges and Roles	Domain or CDI-PC Repository Service.
UnassignLicense	Domain Administration	Manage Services	License object and application service
UnassignRSWSHubService	Domain Administration	Manage Services	CDI-PC Repository Service and Web Services Hub
UnassociateDomainNode	Domain Administration	Manage Nodes and Grids	Node
UpdateConnection	-	-	Write on connection
UpdateDomainOptions*	-	-	-
UpdateFolder	Domain Administration	Manage Domain Folders	Folder

infacmd isp Command	Privilege Group	Privilege Name	Permission On
UpdateGatewayInfo*	-	-	-
UpdateGrid	Domain Administration	Manage Nodes and Grids	Grid and nodes
UpdateIntegrationService	Domain Administration	Manage Services	CDI-PC Integration Service
UpdateLicense	Domain Administration	Manage Services	License object
UpdateMMService	Domain Administration	Manage Services	Metadata Manager Service
UpdateNodeOptions	Domain Administration	Manage Nodes and Grids	Node
UpdateNodeRole	Domain Administration	Manage Nodes and Grids	Node
UpdateOSProfile	Security Administration	Manage Users, Groups, and Roles	Operating system profile
UpdateRepositoryService	Domain Administration	Manage Services	CDI-PC Repository Service
UpdateSAPBWService	Domain Administration	Manage Services	SAP BW Service
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	Domain Administration	Manage Services	CDI-PC Integration Service Each node added to the CDI-PC Integration Service
listMonitoringOptions	Monitoring	Monitoring Configuration	Domain
purgeMonitoringData	Monitoring	Monitoring Configuration	Domain
updateMonitoringOptions	Monitoring	Monitoring Configuration	Domain
**To run these commands, users must be assigned the Administrator role for the domain.*			

infacmd ms Commands

To run *infacmd ms* commands, users must have one of the listed sets of domain object permissions.

The following table lists the required privileges and permissions for *infacmd ms* commands:

infacmd ms Command	Privilege Group	Privilege Name	Permission On...
deleteMappingPersistedOutputs	-	-	Execute on the application
getRequestLog	-	-	-
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	View on the application
listMappings	-	-	-
runMapping	-	-	Execute on connection objects used by the mapping

infacmd rms Commands

To run *infacmd rms* commands, users must have one of the listed sets of domain privileges and permissions

The following table lists the required privileges and permissions for *infacmd rms* commands:

infacmd rms Command	Privilege Group	Privilege Name	Permission On
ListComputeNodeAttributes	Domain Administration	-	Resource Manager Service
ListServiceOptions	Domain Administration	-	Resource Manager Service
SetComputeNodeAttributes	Domain Administration	Manage Services	Resource Manager Service
UpdateServiceOptions	Domain Administration	Manage Services	Resource Manager Service

infacmd sch commands

To run infacmd sch commands, users must have one of the listed sets of privileges and permissions.

The following table lists the required privileges and permissions for infacmd sch commands:

infacmd sch Command	Privilege Group	Privilege Name	Permission On
CreateSchedule	Scheduler Privileges	Create Schedule	Scheduler Service
DeleteSchedule	Scheduler Privileges	Delete Schedule	Scheduler Service
ListSchedule	Scheduler Privileges	View Schedules	Scheduler Service
ListServiceOptions	Domain Privileges	Manage Services	Scheduler Service
ListServiceProcessOptions	Domain Privileges	Manage Services	Scheduler Service
PauseAll	Scheduler Privileges	Edit Schedule	Scheduler Service
PauseSchedule	Scheduler Privileges	Edit Schedule	Scheduler Service
ResumeAll	Scheduler Privileges	Edit Schedule	Scheduler Service
ResumeSchedule	Scheduler Privileges	Edit Schedule	Scheduler Service
UpdateSchedule	Scheduler Privileges	Edit Schedule	Scheduler Service
UpdateService	Domain Privileges	Manage Services	Scheduler Service
UpdateServiceProcess	Domain Privileges	Manage Services	Scheduler Service
Upgrade	Domain Privileges	Manage Services	Scheduler Service

infacmd wfs Commands

To run infacmd wfs commands, users do not require any privileges or permissions.

pmcmd Commands

To run *pmcmd* commands, users must have the listed sets of CDI-PC Repository Service privileges and CDI-PC repository object permissions.

When the CDI-PC Integration Service runs in safe mode, users must have the Administrator role for the associated CDI-PC Repository Service to run the following commands:

- aborttask
- abortworkflow
- getrunningsessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails

- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

The following table lists the required privileges and permissions for *pmcmd* commands:

pmcmd Command	Privilege Group	Privilege Name	Permission
aborttask (started by own user account)	-	-	Read and Execute on folder
aborttask (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
abortworkflow (started by own user account)	-	-	Read and Execute on folder
abortworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningsessionsdetails	Run-time Objects	Monitor	-
getservicedetails	Run-time Objects	Monitor	Read on folder
getserviceproperties	-	-	-
getsessionstatistics	Run-time Objects	Monitor	Read on folder
gettaskdetails	Run-time Objects	Monitor	Read on folder
getworkflowdetails	Run-time Objects	Monitor	Read on folder
help	-	-	-
pingservice	-	-	-
recoverworkflow (started by own user account)	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)

pmcmd Command	Privilege Group	Privilege Name	Permission
recoverworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
scheduleworkflow	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
setfolder	-	-	Read on folder
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
startworkflow	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
stoptask (started by own user account)	-	-	Read and Execute on folder
stoptask (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
stopworkflow (started by own user account)	-	-	Read and Execute on folder
stopworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
unscheduleworkflow	Run-time Objects	Manage Execution	Read and Execute on folder
unsetfolder	-	-	Read on folder
version	-	-	-

pmcmd Command	Privilege Group	Privilege Name	Permission
waittask	Run-time Objects	Monitor	Read on folder
waitworkflow	Run-time Objects	Monitor	Read on folder

pmrep Commands

Users must have the Access Repository Manager privilege to run all *pmrep* commands except for the following commands:

- Run
- Create
- Restore
- Upgrade
- Version
- Help

To run *pmrep* commands, users must have one of the listed sets of domain privileges, CDI-PC Repository Service privileges, domain object permissions, and CDI-PC repository object permissions.

Users must be the object owner or have the Administrator role for the CDI-PC Repository Service to run the following commands:

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder (to change owner, configure permissions, designate the folder as shared, or edit the folder name or description)

The following table lists the required privileges and permissions for *pmrep* commands:

pmrep Command	Privilege Group	Privilege Name	Permission
AddToDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on deployment group
ApplyLabel	-	-	Read on folder Read and Execute on label

pmrep Command	Privilege Group	Privilege Name	Permission
AssignPermission	-	-	-
BackUp	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ChangeOwner	-	-	-
CheckIn (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
CheckIn (for your own checkouts)	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
CheckIn (for your own checkouts)	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
CheckIn (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
CheckIn (for others' checkouts)	Sources and Targets	Manage Versions	Read and Write on folder
CheckIn (for others' checkouts)	Run-time Objects	Manage Versions	Read and Write on folder
CleanUp	-	-	-
ClearDeploymentGroup	Global Objects	Manage Deployment Groups	Read and Write on deployment group
Connect	-	-	-
Create	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
CreateConnection	Global Objects	Create Connections	-
CreateDeploymentGroup	Global Objects	Manage Deployment Groups	-
CreateFolder	Folders	Create	-
CreateLabel	Global Objects	Create Labels	-
CreateQuery	Global Objects	Create Queries	-
Delete	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-

pmrep Command	Privilege Group	Privilege Name	Permission
DeleteObject	Design Objects	Create, Edit, and Delete	Read and Write on folder
DeleteObject	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
DeleteObject	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
DeleteQuery	-	-	-
DeployDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on destination folder Read and Execute on deployment group
DeployFolder	Folders	Copy on original repository Create on destination repository	Read on folder
ExecuteQuery	-	-	Read and Execute on query
Exit	-	-	-
FindCheckout	-	-	Read on folder
GetConnectionDetails	-	-	Read on connection object
Help	-	-	-
KillUserConnection	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ListConnections	-	-	Read on connection object
ListObjectDependencies	-	-	Read on folder
ListObjects	-	-	Read on folder
ListTablesBySess	-	-	Read on folder
ListUserConnections	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ModifyFolder (to change owner, configure permissions, designate the folder as shared, or edit the folder name or description)	-	-	-
ModifyFolder (to change status)	Folders	Manage Versions	Read and Write on folder

pmrep Command	Privilege Group	Privilege Name	Permission
Notify	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
ObjectExport	-	-	Read on folder
ObjectImport	Design Objects	Create, Edit, and Delete	Read and Write on folder
ObjectImport	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
ObjectImport	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
PurgeVersion	Design Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
PurgeVersion	Sources and Targets	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
PurgeVersion	Run-time Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
PurgeVersion (to purge objects at the folder level)	Folders	Manage Versions	Read and Write on folder
PurgeVersion (to purge objects at the repository level)	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
Register	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
RegisterPlugin	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
Restore	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
RollbackDeployment	Global Objects	Manage Deployment Groups	Read and Write on destination folder
Run	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Run-time Objects	Create, Edit, and Delete	Read and Write on folder Read on connection object

pmrep Command	Privilege Group	Privilege Name	Permission
TruncateLog	Run-time Objects	Manage Execution	Read and Execute on folder
UndoCheckout (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for your own checkouts)	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for your own checkouts)	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
UndoCheckout (for others' checkouts)	Sources and Targets	Manage Versions	Read and Write on folder
UndoCheckout (for others' checkouts)	Run-time Objects	Manage Versions	Read and Write on folder
Unregister	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
UnregisterPlugin	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
UpdateConnection	-	-	Read and Write on connection object
UpdateEmailAddr	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSeqGenVals	Design Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSrcPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateStatistics	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
UpdateTargPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Upgrade	Domain Administration	Manage Services	Permission on CDI-PC Repository Service
Validate	Design Objects	Create, Edit, and Delete	Read and Write on folder
Validate	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Version	-	-	-

APPENDIX B

Custom Roles

This appendix includes the following topic:

- CDI-PC Repository Service Custom Roles, 176

CDI-PC Repository Service Custom Roles

The CDI-PC Repository Service custom roles include the CDI-PC Connection Administrator, CDI-PC Operator, and CDI-PC repository Folder Administrator.

CDI-PC Connection Administrator

The following table lists the default privileges assigned to the CDI-PC Connection Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Manager
Global Objects	Create Connections

CDI-PC Operator

The following table lists the default privileges assigned to the CDI-PC Operator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Monitor
Run-time Objects	- Execute - Manage Execution - Monitor

CDI-PC repository Folder Administrator

The following table lists the default privileges assigned to the CDI-PC repository Folder Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Repository Manager
Folders	- Copy - Create - Manage Versions
Global Objects	- Manage Deployment Groups - Execute Deployment Groups - Create Labels - Create Queries

INDEX

A

account management
  overview 92
accounts
  changing the password 93
Administrator
  role 135
administrators
  default 97
  domain 97
application
  permissions 150
audit reports
  description 152
  for groups 156
  for users 156, 157
  overview 92
authentication
  LDAP 16, 22, 88
  native 88
  Service Manager 88

C

cacerts truststore file 27
changing
  password for user account 93
cipher suites
  configuring 79
client configuration
  secure domain 74
Cloud Administration privilege group
  domain 121
command line programs
  privileges 158
connections
  default permissions 148
  permission types 148
  permissions 148
custom roles
  assigning to users and groups 138
  creating 137
  deleting 138
  description 135, 136
  editing 137
  privileges, assigning 137

D

default administrator
  description 97
  modifying 97
  passwords, changing 97
design objects
  description 124
  privileges 124
Design Objects privilege group
  description 124
direct permission
  description 143
domain
  administration privileges 117
  administrator 97
  privileges 116
  security administration privileges 116
  user security 94
  users with privileges 139
Domain Administration privilege group
  description 117
domain administrator
  description 97
domain permissions
  direct 143
  effective 143
  inherited 143

E

effective permission
  description 143
environment variables
  INFA_TRUSTSTORE 74
  INFA_TRUSTSTORE_PASSWORD 74
es
  permissions by command 158
  privileges by command 158
Everyone group
  description 96

F

filters
  getUserActivityLog 104
folders
  privileges 123
Folders privilege group
  description 123

G

getUserActivityLog
  filters 104
group description
  invalid characters 106
groups
  default Everyone 96

groups *(continued)*
invalid characters 106
managing 106
overview 90
parent group 106
privileges, assigning 138
roles, assigning 138
valid name 106

I

identity provider
configuring for single sign-on 61
Informatica Administrator
Navigator 90
overview 87
searching 89
tabs, viewing 87
Informatica domain
permissions 94
privileges 94
user security 94
users, managing 98
inherited permission
description 143
inherited privileges
description 138
isp
permissions by command 159
privileges by command 159

K

Kerberos authentication
keytab 36
LDAP synchronization 50
service principal accounts 35
service principal name 36
SPN keytab format file 38
keytool utility 27

L

LDAP authentication
Azure Active Directory 21
description 16, 88
directory services 22
nested groups 26
self-signed SSL certificate 27
setting up 22
LDAP configurations
deleting 27
LDAP directory service
nested groups 26
LDAP groups
importing 22
managing 106
LDAP security domain
description 16
LDAP users
assigning to groups 100
enabling 100
importing 22
managing 98

M

mapping
inherited permissions 150
permissions 150
Metadata Manager Service
users with privileges 139
Model Repository Service
users with privileges 139
ms
permissions by command 167
privileges by command 167

N

native authentication
description 88
native groups
adding 106
deleting 107
editing 107
managing 106
moving to another group 107
users, assigning 100
native users
adding 98
assigning to groups 100
deleting 101
editing 99
enabling 100
managing 98
passwords 98
Navigator
Security page 90
nested groups
LDAP authentication 26
LDAP directory service 26

O

operating system profile
creating 110
default 111
deleting 111
operating system profiles
overview 92
permissions 146

P

parent groups
description 106
password
changing for a user account 93
passwords
changing for default administrator 97
native users 98
requirements 98
permissions
application 150
connections 148
description 142
direct 143
effective 143
es commands 158

permissions *(continued)*
inherited 143
isp commands 159
mapping 150
ms commands 167
operating system profiles 146
pmcmd commands 168
pmrep commands 171
rms commands 167
sch commands 167
search filters 143
types 143
wfs commands 168
workflow 150
working with privileges 142
pmcmd
permissions by command 168
privileges by command 168
pmrep
permissions by command 171
privileges by command 171
PowerCenter Repository Service
users with privileges 139
privilege groups
description 115
Design Objects 124
Domain Administration 117
Folders 123
Informatica Cloud Administration 121
Run-time Objects 129
Security Administration 116
Sources and Targets 127
Tools 121
privileges
assigning 138
command line programs 158
description 115
design objects 124
domain 116
domain administration 117
domain tools 121
es commands 158
folders 123
Informatica Cloud Administration 121
inherited 138
isp commands 159
ms commands 167
pmcmd commands 168
pmrep commands 171
rms commands 167
run-time objects 129
sch commands 167
security administration 116
sources 127
targets 127
troubleshooting 140
wfs commands 168
working with permissions 142

R

rms
permissions by command 167
privileges by command 167
roles
Administrator 135
assigning 138
roles *(continued)*
custom 136
description 116
managing 135
overview 91
troubleshooting 140
run-time objects
description 129
privileges 129
Run-time Objects privilege group
description 129

S

sch
permissions by command 167
privileges by command 167
search filters
permissions 143
Search section
Informatica Administrator 89
secure domain
client configuration 74
security
passwords 98
permissions 94
privileges 94, 115, 116
roles 116
Security Administration privilege group
description 116
Security Assertion Markup Language (SAML)
assertion, signed or encrypted 62
enabling on gateway nodes 62
enabling on the domain 61
encrypted assertion 64
request signing 62, 63
signed response 62, 64
support for 57
security domains
deleting LDAP 27
LDAP 16
Security page
Navigator 90
Service Manager
authentication 88
single sign-on 88
single sign-on
configuring 60
description 88
overview 57
sources
privileges 127
Sources and Targets privilege group
description 127
SSL certificate
LDAP authentication 27
synchronization
LDAP users 22
system memory
increasing 102
system-defined roles
Administrator 135
assigning to users and groups 138
description 135

T

targets
  privileges 127
Tools privilege group
  domain 121

U

user accounts
  changing the password 93
  created during installation 97
  default 97
  enabling 100
  overview 97
user activity logs
  activity codes 103
user description
  invalid characters 98
user security
  description 88
users
  assigning to groups 100
  invalid characters 98
users *(continued)*
  large number of 102
  managing 98
  overview 91
  privileges, assigning 138
  roles, assigning 138
  system memory 102
  valid name 98

V

valid name
  groups 106
  user account 98

W

wfs
  permissions by command 168
  privileges by command 168
workflow
  inherited permissions 150
  permissions 150