Informatica

Informatica®

10.1

Security Guide

Informatica Security Guide
10.1
June 2016

Publication Date: 2018-07-02

Table of Contents

Preface

The Informatica Security Guide contains information about security in the Informatica domain. It contains information that you need to manage security for the Informatica domain and the Informatica clients that connect to the domain. This book assumes that you have knowledge of the Informatica domain and the Informatica Administrator. It also assumes that you are familiar with the authentication servers and processes for your network.

Informatica Resources

Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit https://network.informatica.com.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- Review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com.

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access Informatica Velocity resources at http://velocity.informatica.com.

If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that augment, extend, or enhance your Informatica implementations. By leveraging any of the hundreds of solutions from Informatica developers and partners, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link: http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.

CHAPTER 1

Introduction to Informatica Security

This chapter includes the following topics:

Overview of Informatica Security

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

Security for the Informatica domain includes the following types of security:

Infrastructure Security

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

- Protection of data transmitted and stored within the Informatica domain
- Authentication of users and services connecting to the Informatica 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 Informatica 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 Informatica domain based on the user role in the organization

Informatica 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.

Informatica 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 Informatica client tools.

You can configure the Informatica domain to use the following types of authentication:

Native Authentication

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

If the Informatica 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 Informatica domain.

Lightweight Directory Access Protocol (LDAP) Authentication

LDAP is a software protocol for accessing users and resources on a network. If the Informatica 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 Informatica domain.

Kerberos Authentication

Kerberos is a network authentication protocol which uses tickets to authenticate users and services in a network. When the Informatica 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 Informatica domain.

Secure Domain Communication

The Informatica 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. Informatica 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). Informatica 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, Informatica requires keystores and truststores in PEM and JKS formats. You can use the following programs to create the required files:

keytool

Use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

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

http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

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

Informatica encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the domain configuration repository. Informatica 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 Informatica 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 Informatica 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 Informatica 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 Informatica 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 Informatica domain, in the LDAP directory service or Kerberos principal database.

When you create the Informatica 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 Informatica domain.

The Informatica 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. Informatica 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 Informatica 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 Informatica 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 Informatica 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 Informatica 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 Informatica domain uses LDAP authentication or Kerberos authentication.

CHAPTER 2

User Authentication

This chapter includes the following topics:

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 Informatica domain can use the following types of authentication to authenticate users in the Informatica domain:

- Native user authentication
- LDAP user authentication
- Kerberos network authentication

Native user accounts are stored in the Informatica domain and can only be used within the Informatica domain. Kerberos and LDAP user accounts are stored in an LDAP directory service and are shared by applications within the enterprise.

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 Informatica domain to work with the Kerberos key distribution center (KDC). You must create the service principal names (SPN) required by the Informatica 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 Informatica 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 Informatica domain to use LDAP authentication in addition to native authentication.

You can use native authentication and LDAP authentication together in the Informatica 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 Informatica 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 Informatica client applications use the credentials from the network login to authenticate users in the Informatica domain. Native groups and roles are still supported.

Native User Authentication

If the Informatica domain uses native authentication, the Service Manager stores all user account information and performs all user authentication within the Informatica 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 Informatica domain contains a native security domain by default. The native security domain is created at installation and cannot be deleted. An Informatica 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 the Informatica domain to allow users in an LDAP directory service to log in to Informatica client applications. The Informatica 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 Informatica 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.

Informatica does not support cross or multi-realm Kerberos authentication. The server host, client machines, and Kerberos authentication server must be in the same 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.

CHAPTER 3

LDAP Security Domains

This chapter includes the following topics:

LDAP Security Domains Overview

An LDAP security domain contains a set of users and groups that are imported from an LDAP directory service. You must create an LDAP security domain if you use LDAP user authentication or Kerberos network authentication.

Configure the LDAP security domains to store the list of users from an LDAP directory service that you want to allow access to the Informatica domain and client applications. The LDAP security domain does not store user account credentials. When a user logs in to an Informatica client, the Service Manager verifies that the user account is in a security domain. If the user account belongs to an LDAP security domain, the Service Manager authenticates the user with the LDAP directory service.

When you install Informatica services and you do not enable Kerberos authentication, the Informatica installer creates the native security domain by default. After installation, you can add users and groups to the native security domain. If you have users in an LDAP directory service that you want to give access to Informatica client applications, you can set up LDAP security domains in addition to the native security domain. Configure a connection to the LDAP server and import the users and groups into the LDAP security domains.

When you install Informatica services and enable Kerberos authentication, the Informatica installer creates an LDAP security domain with the name of the Kerberos realm that you specify during installation. After installation, you can configure a connection to the LDAP server and import users and groups from the LDAP directory service into the LDAP security domain. If you use Kerberos authentication, you cannot use the Native security domain.

Setting Up an LDAP Security Domain

You can create an LDAP security domain for user accounts that you import from an LDAP directory service. To organize different groups of users, you can create multiple LDAP security domains.

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

You can import users from the following LDAP directory services:

- Microsoft Active Directory Service

  Note: If you use Kerberos authentication, you can import users only from a Microsoft Active Directory (AD) directory service.
- Sun Java System Directory Service
- Novell e-Directory Service
- IBM Tivoli Directory Service
- Open LDAP Directory Service

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 them 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.

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

To set up the LDAP security domain, perform the following steps:

1. Set up the connection to the LDAP directory service.
2. Configure a security domain.
3. Schedule the synchronization times.

Step 1. Set Up the Connection to the LDAP Server

Configure the connection to the LDAP server that contains the directory service from which you want to import the user accounts for the Informatica domain.

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 you modify the LDAP connection properties to connect to a different LDAP directory service, ensure that the user and group filters in the LDAP security domains are correct for the new LDAP directory service. Verify that the filters include the users and groups that you want to use in the Informatica domain.

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 **Actions** menu and select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **LDAP Connectivity** tab.

4. Configure the connection properties for the LDAP server.

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

   The following table describes the LDAP server configuration properties:

Property	Description
Server name	Name 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. Select from the following directory services: - Microsoft Active Directory Service - Sun Java System Directory Service - Novell e-Directory Service - IBM Tivoli Directory Service - Open LDAP Directory Service **Note:** If you use Kerberos authentication, you must select Microsoft Active 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. Leave blank for anonymous login. For more information, see the documentation for the LDAP directory service.
Password	Password for the principal user. Leave blank for anonymous login. Not available if you use Kerberos authentication.
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. To enable the Service Manager to recognize a self-signed certificate as valid, specify the truststore file and password to use.
Not Case Sensitive	Indicates that the Service Manager must ignore case-sensitivity for distinguished name attributes when assigning users to groups. Enable this option.

Property	Description
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 of100 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.

5. Click Test Connection to verify that the connection to the LDAP server is valid.

Step 2. Configure a Security Domain

Create a 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 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 imports groups and the list of users that belong to the groups. It imports the groups that are included in the group filter and the user accounts that are included in the user filter.

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: Unlike native user names, LDAP user names can be case-sensitive.

When you set up the LDAP directory service, you can use different attributes for the unique ID (UID). The Service Manager requires a particular UID to identify users in each LDAP directory service. Before you configure the security domain, verify that the LDAP directory service uses the required UID.

The following table lists the required UID for each LDAP directory service:

LDAP Directory Service	UID
IBMTivoliDirectory	uid
Microsoft Active Directory	sAMAccountName
NovellE	uid
OpenLDAP	uid
SunJavaSystemDirectory	uid

The Service Manager does not import the LDAP attribute that indicates that a user account is enabled or disabled. You must enable or disable an LDAP user account in the Administrator tool. The status of the user account in the LDAP directory service affects user authentication in application clients. For example, a user account is enabled in the Informatica domain but disabled in the LDAP directory service. If the LDAP directory service allows disabled user accounts to log in, then the user can log in to application clients. If the

LDAP directory service does not allow disabled user accounts to log in, then the user cannot log in to application clients.

Note: 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 select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **Security Domains** tab.
4. Click **Add**.
5. Use LDAP query syntax to create filters to specify the users and groups to be included in the security domain you are creating.

   You might need to consult the LDAP administrator to get the information about the users and groups available in the LDAP directory service.

   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. It 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.

6. 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.
7. To add another LDAP security domain, repeat steps 4 through 6.

8. 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.
9. Click **OK** to save the security domains.

Step 3. Schedule the Synchronization Times

You can set up a schedule for the Service Manager to periodically synchronize the list of users and groups in the LDAP security domain with the list of users and groups in the LDAP directory service.

Important: Before you start the synchronization process, verify that the /etc/hosts file contains an entry for the host name of the LDAP server. If the Service Manager cannot resolve the host name for the LDAP server, the user synchronization can fail.

During synchronization, the Service Manager imports users and groups from the LDAP directory service. The Service Manager deletes any user or group from the LDAP security domain that is no longer included in the search filters used for the import.

By default, the Service Manager does not have a 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, you can schedule the times during the day when the Service Manager synchronizes the LDAP security domains. The Service Manager synchronizes the LDAP security domains with the LDAP directory service every day at the times you set.

Note: During synchronization, the Service Manager locks the user account that it synchronizes. When the user account is locked, the Service Manager cannot authenticate the user account. Users might not be able to log in to application clients. If users are logged in to application clients when synchronization starts, the users might not be able to perform tasks. The duration of the synchronization process depends on the number of users and groups to be synchronized. To avoid usage disruption, synchronize the security domains during times when most users are not logged in. To synchronize more than 100 users or groups, enable paging on the LDAP directory service before you run the synchronization. If you do not enable paging on the LDAP directory service, the synchronization can fail.

To set up a schedule to synchronize the 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.

   You can add as many synchronization times in the day as you require. If the list of users and groups in the LDAP directory service changes often, you can schedule the Service Manager to synchronize multiple times a day.
5. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, click **Synchronize Now**.
6. Click **OK** to save the synchronization schedule.

   Note: If you restart the Informatica domain before the Service Manager synchronizes with the LDAP directory service, the synchronization times that you added are lost.

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 use a self-signed certificate, import the self-signed certificate into a truststore file and use the INFA_JAVA_OPTS environment variable to specify the truststore file and password:

```
setenv INFA_JAVA_OPTS -Djavax.net.ssl.trustStore=<TrustStoreFile>
-Djavax.net.ssl.trustStorePassword=<TrustStorePassword>
```

On Windows, configure INFA_JAVA_OPTS as a system variable.

Restart the node for the change to take effect. The Service Manager uses the truststore file to verify the SSL certificate.

keytool is a key and certificate management utility that allows you to generate and administer keys and certificates for use with the SSL security protocol. You can use keytool to create a truststore file or to import a certificate to an existing truststore file. You can find the keytool utility in the following directory:

```
<PowerCenterClientDir>\CMD_Utilities\PC\java\bin
```

For more information about using keytool, see the documentation on the following web site: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Deleting an LDAP Security Domain

To permanently prohibit users in an LDAP security domain from accessing application clients, you can delete the LDAP security domain. When you delete an LDAP security domain, the Service Manager deletes all user accounts and groups in the LDAP security domain from the domain configuration database.

1. In the LDAP Configuration dialog box, click the Security Domains tab.

   The LDAP Configuration dialog box displays the list of security domains.

2. To ensure that you are deleting the correct security domain, click the security domain name to view the filter used to import the users and groups and verify that it is the security domain you want to delete.
3. Click the Delete button next to a security domain to delete the security domain.
4. Click OK to confirm that you want to delete the security domain.

CHAPTER 4

Kerberos Authentication Setup

This chapter includes the following topics:

Kerberos Authentication Setup Overview

When you create the Informatica domain during installation, you can select the option to enable Kerberos authentication. 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.

To configure Kerberos authentication for the Informatica domain on the command line, perform the following steps:

1. Create an LDAP User Domain with Users from Microsoft Active Directory.
2. Migrate native users to an LDAP security domain.
3. Set up the Kerberos configuration and copy the configuration file to the Informatica directory.
4. Generate the SPN and keytab file name in the format required by the Informatica domain.
5. Review the SPN and keytab file format text file.
6. Create the SPNs and keytab files.
7. Configure Kerberos authentication for the Informatica domain.
8. Update the nodes in the Informatica domain.
9. Update the client machines.

10. Start the Informatica domain and run the Administrator tool.

After you configure Kerberos authentication and the LDAP security domains, verify that the user accounts have the correct privileges and permissions. Verify that the services in the domain perform as expected and the users can log in with single sign-on.

Note: The steps provided are based on the assumption that you installed the Informatica services without enabling Kerberos authentication. If you enable Kerberos authentication during installation, follow the steps in the Informatica installation guides.

Step 1. Create an LDAP User Domain with Users from Microsoft Active Directory

Before you configure the Informatica domain to use Kerberos authentication, review the domain user accounts. Verify that they are in LDAP security domains and that the accounts are imported from the Microsoft Active Directory service.

If the domain has user accounts in an LDAP security domain that does not use Microsoft Active Directory, migrate the users to an LDAP security domain that uses Microsoft Active Directory. For more information about migrating user accounts to Microsoft Active Directory, see the documentation for your LDAP implementation.

If the domain has user accounts in the native security domain, migrate the users to an LDAP security domain that uses Microsoft Active Directory.

Set up an LDAP security domain and configure the connection to the Microsoft Active Directory service. Then set up the filters for the users and groups and synchronize the domain user accounts.

For more information about setting up an LDAP domain and synchronizing the user accounts, see "Setting Up an LDAP Security Domain" on page 22

Step 2. Migrate Native User Privileges and Permissions to an LDAP Security Domain

After you configure the domain to use Kerberos authentication, you cannot modify user accounts in the native security domain. Migrate the native user groups, roles, privileges, and permissions to an LDAP security domain before you configure Kerberos authentication

If the domain has user accounts in the native security domain, the corresponding user accounts in the LDAP security domain must have the same groups, roles, privileges, and permissions. Migrate the groups, roles, privileges, and permissions of the native users to the Active Directory users in the LDAP security domain. Then, verify that the groups, roles, privileges, and permissions migrated correctly.

If the domain does not have user accounts in the native security domain, you can continue to "Step 3. Set Up the Kerberos Configuration File" on page 34.

To migrate the groups, roles, privileges, and permissions of native users to the users in the LDAP security domain, perform the following steps:

1. Verify the user accounts for Kerberos Authentication.

2. Create the user migration file.
3. Run the infacmd isp migrateusers command.
4. Verify the groups, roles, privileges, and permissions for the user accounts.

Note: To avoid problems when you migrate user groups roles, privileges, and permissions, do not run workflows or modify user groups, roles, privileges, or permissions during the migration process.

Verify the User Accounts for Kerberos Authentication

View the list of native user accounts and determine the accounts that you want to migrate to an 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 LDAP security domain must have a corresponding account in the Microsoft Active Directory service that you use for Kerberos authentication.

If the accounts are not in the Microsoft Active Directory service, add the user accounts to the directory service. For more information about adding user accounts to the Microsoft Active Directory service, see the Microsoft Active Directory documentation.

Note: The user name for user accounts in the LDAP security domain has a maximum length of 20 characters. When you add the user accounts to the Microsoft Active Directory service, ensure that the length of the user name does not exceed 20 characters.

Create the User Migration File

The infacmd isp migrateUsers command uses a user migration file to determine what groups, roles, privileges, and permissions to assign LDAP users. The user migration file is a plain text file that contains the list of native users and the corresponding LDAP users that require the same groups, roles, privileges, and permissions.

When you create the user migration file, you must specify the security domain for the user account. A forward slash (/) separates the security domain from the user name. A comma (,) separates the native user from the corresponding LDAP user. Security domains are case sensitive. User names are not case sensitive.

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

```
Native/<SourceUserName>,LDAP/<TargetUserName>
```

You can migrate the groups, roles, privileges, and permissions of native users to users in different LDAP security domains. For example, the user migration file contains the following list of users:

```
Native/User1,LDAPSecurityDomain/User1
Native/User2,LDAPSecurityDomain/User2
Native/User3,newLDAPSecDomain/User3
```

The migrateUser command assigns User1 and User2 in LDAPSecurityDomain the same groups, roles, privileges, and permissions as User1 and User2 in the native security domain. The command assigns User3 in newLDAPSecDomain the same groups, roles, privileges, and permissions as User3 in the native security domain.

The migrateUsers command skips any entry with a duplicate source user name or target user name.

Run the infacmd isp migrateUsers Command

To migrate groups, roles, privileges and permissions from the native security domain users to LDAP security domain users, run the infacmd migrateUsers command and specify the user migration file to use.

Before you run the infacmd isp migrateUsers command, ensure that all instances of the following services on the domain are running:

- Analyst Service
- Content Management Service
- Model Repository Service
- Metadata Manager Service
- PowerCenter Repository Service
- Reporting Service

Ensure that the PowerCenter Repository Service is running in normal mode.

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

```
infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd
<AdministratorPassword> -umf <UserMigrationFile>
```

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

```
infacmd isp migrateUsers -dn UMT_Domain -un Administrator -pd Admnistrator -umf C:\UMT
\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.

For more information about the command, see the *Informatica Command Reference*.

Troubleshooting the migrateUsers Command

How do I improve migration performance?

To improve migration performance, perform the following steps:

1. Create multiple unique user migration files with a limited number of users in each file.
2. Run multiple instances of the migrateUsers command concurrently.

For example, to migrate the groups, roles, privileges, and permissions for 150 users, create three user migration files that each contain 50 users. Then, run three instances of the migrateUsers command concurrently. Specify a unique user migration file for each instance of the command.

The migrateUsers command fails.

If the migrateUsers command fails, the following recovery paths are available:

- Run the migrateUsers command again.
- Modify the user migration file. Then, run the migrateUsers command.

When you run the command again, specify the same user migration file. 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.

To modify the user migration file, perform the following steps:

1. View the detailed log file that was created when you ran the migrateUsers command.
2. Delete users that the command successfully migrated from the user migration file.
3. Run the migrateUsers command.

Verify Privileges and Permissions for the User Accounts

Before you enable Kerberos authentication, verify that the users in the LDAP security domain have the correct groups, roles, privileges, and permissions. You can use infacmd to verify groups, roles, privileges, and permissions for the user accounts in the LDAP security domain.

Verify that the following objects migrated successfully:

Users and groups

To determine the groups that user accounts belong to, get a list of the users and associated groups. Run the following command:

```
infacmd aud getUserGroupAssociation
```

Roles

To get the list of roles associated with the domain users and groups, run the following command:

```
infacmd aud getUserGroupAssociationForRoles
```

Privileges

To get a list of the privileges assigned to the users and groups in the domain, run the following command:

```
infacmd aud getPrivilegeAssociation
```

Permissions

To get a list of the permissions assigned to the users and groups in the domain, run the following command:

```
infacmd aud getDomainObjectPermissions
```

Permissions on folders and global objects

If the domain contains a PowerCenter Repository Service, verify permissions for PowerCenter folders and global repository objects assigned to the user accounts. The PowerCenter repository can have the following objects:

- Folders
- Deployment groups
- Labels
- Queries
- Connections

After you configure the domain to use Kerberos authentication, you cannot modify the native user accounts.

After you confirm that the groups, roles, privileges, and permissions for the native user accounts have been successfully moved to the LDAP user accounts, delete the native user accounts. Use the Administrator tool to delete the user accounts. For more information, see “Deleting Native Users” on page 90.

Step 3. Set Up the Kerberos Configuration File

Kerberos stores configuration information in a file named *krb5.conf*. Informatica requires specific properties in the Kerberos configuration file to be set so that the Informatica domain can use Kerberos authentication correctly. You must set the properties in the krb5.conf configuration file and then copy the file to the Informatica directory.

The configuration file contains the information about the Kerberos server, including the Kerberos realm and the address of the KDC. You can request the Kerberos administrator to set the properties in the configuration file and send you a copy of the file.

1. Back up the krb5.conf file before you make any changes.
2. Edit the krb5.conf file.
3. In the *libdefaults* section, set or add the properties required by Informatica.

   The following table lists the values to which you must set properties In the libdefaults section:

Parameter	Value
default_realm	Name of the service realm for the Informatica domain.
forwardable	Allows a service to delegate client user credentials to another service. Set this parameter to True. The Informatica domain requires application services to authenticate the client user credentials with other services.
default_tkt_enctypes	Encryption type for the session key in the ticket-granting ticket (TGT). Set this parameter to *rc4-hmac*. Informatica supports only the *rc4-hmac* encryption type.
udp_preference_limit	Determines the protocol that Kerberos uses when it sends a message to the KDC. Set udp_preference_limit = 1 to always use TCP. The Informatica domain supports only the TCP protocol. If the udp_preference_limit is set to any other value, the Informatica domain can shut down unexpectedly.

4. In the *realms* section, include the port number in the address of the KDC separated by a colon.

   For example, if the KDC address is kerberos.example.com and the port number is 88, set the *kdc* parameter to the following:

   ```
   kdc = kerberos.example.com:88
   ```
5. Save the krb5.conf file.
6. Copy the configuration file to the Informatica directory.

   You must copy the krb5.conf to the following directory: `<INFA_HOME>/services/shared/security`
   If the domain has multiple nodes, copy the krb5.conf to the same directory on all the nodes in the domain.

The following example shows the content of a krb5.conf with the required properties:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
  admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
  kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
 }
```

```
[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

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

Step 4. Generate the Principal Name and Keytab Format

If you run the Informatica domain with Kerberos authentication, you must associate Kerberos service principal names (SPN) and keytab files with the nodes and processes in the Informatica domain. Informatica requires keytab files to authenticate services in the network without requests for passwords.

Based on the security requirements for the domain, you can set the service principal level to one of the following levels:

Node Level

If the domain is used for testing or development and does not require a high level of security, you can set the service principal at the node level. You can use one SPN and keytab file for the node and all the service processes on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

Process Level

If the domain is used for production and requires a high level of security, you can set the service principal at the process level. Create a unique SPN and keytab file for each node and each process on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

The Informatica domain requires the service principal and keytab file names to follow a specific format. To ensure that you follow the correct format for the service principal and keytab file names, use the Informatica Kerberos SPN Format Generator to generate a list of the service principal and keytab file names in the format required by the Informatica domain.

Service Principal Requirements at Node Level

If the Informatica domain does not require a high level of security, the node and service processes can share the same SPNs and keytab files. The domain does not require a separate SPN for each service process in a node.

The Informatica domain requires SPNs and keytab files for the following components at node level:

Principal distinguished name (DN) for the LDAP directory service

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

Node process

Principal name for the Informatica node that initiates or accepts authentication calls. The same principal name is used to authenticate the services in the node. Each gateway node in the domain requires a separate principal name.

HTTP processes in the domain

Principal name for all web application services in the Informatica domain, including Informatica Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

Service Principal Requirements at Process Level

If the Informatica domain requires a high level of security, create a separate SPN and keytab file for each node and each service in the node.

The Informatica domain requires SPNs and keytab files for the following components at process level:

Principal distinguished name (DN) for the LDAP directory service

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

Node process

Principal name for the Informatica node that initiates or accepts authentication calls.

Informatica Administrator service

Principal name for the Informatica Administrator service that authenticates the service with other services in the Informatica domain. The name of the keytab file must be *_AdminConsole.keytab*.

HTTP processes in the domain

Principal name for all web application services in the Informatica domain, including Informatica Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

Service process

Principal name for the application service that runs on a node in the Informatica domain. Each application service requires a unique service principal and keytab file name.

Running the Informatica Kerberos SPN Format Generator on Windows

You can run the Informatica Kerberos SPN Format Generator to generate a file that shows the correct format for the SPNs and keytab file names required in the Informatica domain.

1. On a machine that hosts the Informatica node, go to the following Informatica directory:
   `<InformaticaDirectory>/Tools/Kerberos`
2. Run the SPNFormatGenerator.bat file.

   The Informatica Kerberos SPN Format Generator **Welcome** page appears.
3. Click **Next**.

   The **Service Principal Level** page appears.
4. Select the level at which to set the Kerberos service principals for the domain.

The following table describes the levels you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

5. Click **Next**.

   The **Authentication Parameters - Kerberos Authentication** page appears.

6. Enter the domain and node parameters to generate the SPN format.

   The following table describes the parameters you must specify:

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

   If you set the service principal at node level, the utility displays the **+Node** button. If you set the service principal at process level, the utility displays the **+Node** and **+Service** buttons.

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

   You can enter multiple nodes for a domain.

8. To generate the SPN format for a service, click **+Service** and specify the service name in the **Service On Node** field.

   The **Service On Node** field displays only if you set the service principal at process level and you click **+Service**. You can enter multiple services for a node. The services appear immediately below the node that they run on.

9. To remove a node from the list, click **-Node**.

The Informatica SPN Format Generator deletes the node. If you have added services to the node, the services are deleted with the node.

10. To remove a service from a node, clear the service name field.
11. Click **Next**.

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

The SPN Format Generator generates a text file that contains the SPN and keytab file names in the format required for the Informatica domain.

Running the Informatica Kerberos SPN Format Generator on UNIX

You can run the Informatica Kerberos SPN Format Generator to generate a file that shows the correct format for the SPNs and keytab file names required in the Informatica domain.

1. On a machine that hosts the Informatica node, go to the following Informatica directory:
   `<InformaticaDirectory>/Tools/Kerberos`
2. On a shell command line, run the SPNFormatGenerator.sh file.
3. Press **Enter** to continue.
4. In the **Service Principal Level** section, select the level at which to set the Kerberos service principals for the domain.

   The following table describes the levels you can select:

Level	Description
1->Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
2->Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

5. Enter the domain and node parameters required to generate the SPN format.

The following table describes the parameters you must specify:

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

If you set the service principal at node level, the prompt **Add Node?** appears. If you set the service principal at process level, the prompt **Add Service?** appears.

6. At the **Add Node?** prompt, enter 1 to generate the SPN format for an additional node. Then enter the node name and node host name.

   To generate the SPN formats for multiple nodes, enter 1 at each **Add Node?** prompt and enter a node name and node host name.
7. At the **Add Service?** prompt, enter 1 to generate the SPN format for a service that will run on the preceding node. Then enter the service name.

   To generate the SPN formats for multiple services, enter 1 at each **Add Service?** prompt and enter a service name.
8. Enter 2 to end the **Add Service?** or **Add Node?** prompts.

   The SPN Format Generator displays the path and file name of the file that contains the list of service principal and keytab file names.
9. Press Enter to exit the SPN Format Generator.

The SPN Format Generator generates a text file that contains the SPN and keytab file names in the format required for the Informatica domain.

Step 5. Review the SPN and Keytab Format Text File

The Kerberos SPN Format Generator generates a text file named SPNKeytabFormat.txt that lists the format for the service principal and keytab file names required by the Informatica domain. The list includes the SPN and keytab file names based on the service principal level you select.

Review the text file and verify that there are no error messages.

The text file contains the following information:

Entity Name

Identifies the node or service associated with the process.

SPN

Format for the SPN in the Kerberos principal database. The SPN is case sensitive. Each type of SPN has a different format.

An SPN can have one of the following formats:

Keytab type	SPN Format
NODE_SPN	isp/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_AC_SPN	_AdminConsole/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_HTTP_SPN	HTTP/<*NodeHostName*>@<*REALMNAME*> **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	<*ServiceName*>/<*NodeName*>/<*DomainName*>@<*REALMNAME*>

Keytab File Name

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

The keytab file names use the following formats:

Keytab type	Keytab File Name
NODE_SPN	<*NodeName*>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<*ServiceName*>.keytab

Keytab Type

Type of the keytab. The keytab type can be one of the following types:

- NODE_SPN. Keytab file for a node process.
- NODE_AC_SPN. Keytab file for the Informatica Administrator service process.
- NODE_HTTP_SPN. Keytab file for HTTP processes in a node.
- SERVICE_PROCESS_SPN. Keytab file for a service process.

Service Principals at Node Level

The following example 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@MY.SVCREALM.COM               Node01.keytab
NODE_SPN
Node01        HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM      webapp_http.keytab
NODE_HTTP_SPN
Node02        isp/Node02/InfaDomain@MY.SVCREALM.COM               Node02.keytab
```

```
NODE_SPN
Node02        HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
Node03        isp/Node03/InfaDomain@MY.SVCREALM.COM              Node03.keytab
NODE_SPN
Node03        HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
```

Service Principals at Process Level

The following example 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@MY.SVCREALM.COM
Node01.keytab          NODE_SPN
Node01             _AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab   NODE_AC_SPN
Node01             HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab     NODE_HTTP_SPN
Node02             isp/Node02/InfaDomain@MY.SVCREALM.COM
Node02.keytab          NODE_SPN
Node02             _AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab   NODE_AC_SPN
Node02             HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab     NODE_HTTP_SPN
Service10:Node01   Service10/Node01/InfaDomain@MY.SVCREALM.COM
Service10.keytab       SERVICE_PROCESS_SPN
Service100:Node02  Service100/Node02/InfaDomain@MY.SVCREALM.COM
Service100.keytab      SERVICE_PROCESS_SPN
Service200:Node02  Service200/Node02/InfaDomain@MY.SVCREALM.COM
Service200.keytab      SERVICE_PROCESS_SPN
```

Step 6. Create the Service Principal Names and Keytab Files

After you generate the list of SPN and keytab file names in the format required by Informatica, send a request to the Kerberos administrator to add the SPNs to the Kerberos principal database and create the keytab files.

Use the following guidelines when you create the SPN and keytab files:

The user principal name (UPN) must be the same as the SPN.

When you create a user account for the service principal, you must set the UPN with the same name as the SPN. The application services in the Informatica domain can act as a service or a client depending on the operation. You must configure the service principal to be identifiable by the same UPN and SPN.

A user account must be associated with only one SPN. Do not set multiple SPNs for one user account.

Enable delegation in Microsoft Active Directory.

You must enable delegation for all user accounts with service principals used in the Informatica domain. In the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

Delegated authentication happens when a user is authenticated with one service and that service uses the credentials of the authenticated user to connect to another service. Because services in the Informatica domain need to connect to other services to complete an operation, the Informatica domain requires the delegation option to be enabled in Microsoft Active Directory.

For example, when a PowerCenter client connects to the PowerCenter Repository Service, the client user account is authenticated with the PowerCenter Repository Service principal. When the PowerCenter Repository Service connects to the PowerCenter Integration Service, the PowerCenter Repository Service principal can use the client user credential to authenticate with the PowerCenter Integration Service. There is no need for the client user account to also authenticate with the PowerCenter Integration Service.

Use the ktpass utility to create the service principal keytab files.

Microsoft Active Directory supplies the ktpass utility to create keytab files. Informatica supports Kerberos authentication only on Microsoft Active Directory and has certified only keytab files that are created with ktpass.

The keytab files for a node must be available on the machine that hosts the node. By default, the keytab files are stored in the following directory: `<INFA_HOME>/isp/config/keys`.

When you receive the keytab files from the Kerberos administrator, copy the keytab files to the directory specified for the keytab files used in the Informatica domain.

Troubleshooting the Service Principal Names and Keytab Files

You can use Kerberos utilities to verify that the service principal and keytab file names created by the Kerberos administrator match the service principal and keytab file names that you requested. You can also use the utilities to determine the status of the Kerberos key distribution center (KDC).

You can use Kerberos utilities such as *setspn*, *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.

Note: The following examples show ways to use the Kerberos utilities to verify that SPNs and keytab files are valid. The examples might be different than the way that the Kerberos administrator uses the utilities to create the SPNs and keytab files required for the Informatica domain. For more information about running the Kerberos utilities, see the Kerberos documentation.

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

klist

You can use *klist* 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>
```

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

```
Keytab name: FILE:int_srvc01.keytab
KVNO Timestamp         Principal
---- ----------------- --------------------------------------------------------
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
   3 12/31/69 19:00:00 int_srvc01/node01_vMPE/Domn96_vMPE@REALM
```

kinit

You can use *kinit* to request a ticket-granting ticket for a user account to verify that the KDC is running and can grant tickets. To request a ticket-granting ticket for a user account, run the following command:

```
kinit <user_account>
```

You can also use *kinit* to request a ticket-granting ticket and verify that the keytab file can be used to establish a Kerberos connection. To request a ticket-granting ticket for an SPN, run the following command:

```
kinit -V -k -t <keytab_file> <SPN>
```

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

```
Using default cache: /tmp/krb5cc_10000073
Using principal: int_srvc01/node01_vMPE/Domn96_vMPE@REALM
Using keytab: int_srvc01.keytab
Authenticated to Kerberos v5
```

setspn

You can use *setspn* to view, modify, or delete the SPN of an Active Directory service account. On the machine that hosts the Active Directory service, open a command line window and run the command.

To view the SPNs that are associated with a user account, run the following command:

```
setspn -L <user_account>
```

The following output example shows the SPN associated with the user account `is96svc`:

```
Registered ServicePrincipalNames for CN=is96svc,OU=AllSvcAccts,OU=People,
DC=ds,DC=intrac0rp,DC=zec0rp:
       int_srvc01/node02_vMPE/Domn96_vMPE
```

To view the user accounts associated with an SPN, run the following command:

```
setspn -Q <SPN>
```

The following output example shows the user account associated with the SPN `int_srvc01/node02_vMPE/Domn96_vMPE`:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
CN=is96svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        int_srvc01/node02_vMPE/Domn96_vMPE

Existing SPN found!
```

To search for duplicate SPNs, run the following command:

```
setspn -X
```

The following output example shows multiple user accounts associated with one SPN:

```
Checking domain DC=ds,DC=intrac0rp,DC=zec0rp
Processing entry 1125
HOST/mtb01.REALM is registered on these accounts:
        CN=Team1svc,OU=AllSvcAccts,OU=People,DC=ds,DC=intrac0rp,DC=zec0rp
        CN=MTB1svc,OU=IIS,OU=WPC960K3,OU=WINServers,DC=ds,DC=intrac0rp,DC=zec0rp
```

Note: Searching for duplicate SPNs can take a long time and a large amount of memory.

kdestroy

You can use *kdestroy* to delete the active Kerberos authorization tickets and the user credentials cache that contains them. If you run *kdestroy* without parameters, you delete the default credentials cache.

Step 7. Configure Kerberos Authentication for the Domain

Run infasetup to change the authentication for the Informatica domain to Kerberos network authentication.

Note: Verify that all repository objects are checked in before you configure the domain to use Kerberos authentication.

When you run the infasetup command to change the domain authentication, the command creates the following LDAP security domains:

- Internal security domain. The internal security domain is an LDAP security domain with the name *_infaInternalNamespace*. The _infaInternalNamespace security domain contains the default administrator user account created when you configure Kerberos authentication. After you configure Kerberos authentication, you cannot add users to the _infaInternalNamespace security domain or delete the security domain.
- User realm security domain. The user realm security domain is an empty LDAP security domain with the same name as the Kerberos user realm. After you configure Kerberos authentication, you can import users from the Kerberos principal database into the user realm security domain.

The infasetup command also creates an administrator user account. You specify the user name for the administrator user. After you configure Kerberos authentication, the _infaInternalNamespace security domain contains the administrator user account.

To configure the domain to use Kerberos authentication, run the following command:

```
infasetup switchToKerberosMode
```

1. On a gateway node, run the infasetup command to change the authentication for the domain.

   At the command prompt, go to the directory where the Informatica command line programs are located. By default, the command line programs are installed in the following directory: `<InformaticaInstallationDir>/isp/bin`
2. Run the infasetup command with the required options and arguments.

   Enter the following commands:
   - Windows: `infasetup switchToKerberosMode`
   - UNIX: `infasetup.sh switchToKerberosMode`

The following table describes the options for the switchToKerberosMode command:

Option	Argument	Description
-administratorName -ad	administrator_name	User name for the domain administrator account that is created when you configure Kerberos authentication. The user account must be in the Kerberos principal database. After you configure Kerberos authentication, this user is included in the *_infaInternalNamespace* security domain.
-ServiceRealmName -srn	realm _name_of_node_spn	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.
-UserRealmName -urn	realm _name_of_user_spn	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.
-SPNShareLevel -spnSL	PROCESS |NODE	Service principal level for the domain. Set the property to one of the following levels: - Process. The domain requires a unique service principal name (SPN) and keytab file for each node and each service on a node. The number of SPNs and keytab files required for each node depends on the number of service processes that run on the node. Use the process level option if the domain requires a high level of security, such as a production domain. - Node. The domain uses one SPN and keytab file for the node and all services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option if the domain does not require a high level of security, such as a test or development domain. Default is process.

The switchToKerberosMode command changes the authentication mode for the domain from native or LDAP user authentication to Kerberos network authentication.

Step 8. Update the Nodes in the Domain

Run the infasetup command to update all other nodes in the domain with the Kerberos authentication server information.

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

To update the gateway and worker nodes, use the following commands:

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. On a machine that hosts an Informatica node, run the infasetup command to update the node.

   At the command prompt, go to the directory where the Informatica command line programs are located. By default, the command line programs are installed in the following directory: `<InformaticaInstallationDir>/isp/bin`

2. 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`

   The following table describes the options to update the Kerberos authentication information for a node:

Option	Argument	Description
-EnableKerberos -krb	enable_kerberos	Configures the Informatica domain to use Kerberos authentication.
-ServiceRealmName -srn	realm _name_of_node_spn	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.
-UserRealmName -urn	realm _name_of_user_spn	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.

Step 9. Update the Client Machines

Copy the Kerberos configuration file and set the environment variable on the machines that host the Informatica clients. You must also configure the browser to access the Informatica web applications.

After you configure the Informatica domain to run with Kerberos authentication, perform the following tasks on the Informatica client tools:

Copy the Kerberos configuration file to the client machines.

Copy the configuration file to each machine that hosts an Informatica client. You must copy the `krb5.conf` file to the following directory: `<Informatica Client Directory>/shared/security`

Set the KRB5_CONFIG environment variables with the Kerberos configuration file.

Use the KRB5_CONFIG environment variable to store the path and file name of the Kerberos configuration file, `krb5.conf`. You must set the KRB5_CONFIG environment variable on each machine that hosts an Informatica client.

Configure the web browser.

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

On UNIX, create a credentials cache file for single sign-on

To run the Informatica command line programs on UNIX with single sign-on, you must generate a credentials cache file to authenticate the user account running the commands on the Kerberos network. Use the *kinit* utility from MIT Kerberos to generate the credentials cache file. The credentials cache file enables a user to run the commands without the user name and password options.

If you use a credentials cache file, you must set the default path and filename for the credentials cache in KRB5CCNAME environment variable.

For more information about running the Informatica command line programs on UNIX with single sign-on, see the *Informatica Command Reference*.

Step 10. Start the Informatica Domain

After you configure the Informatica domain to use Kerberos authentication, start the domain and the Administrator tool.

1. On Windows, you can start the Informatica service from the Control Panel or the Start menu.

   To start Informatica from the Windows Start menu, click **Programs** > **Informatica [Version]** > **Server** . Right-click **Start Informatica Services** and select **Run as Administrator**.

   On UNIX, run the following command to start the Informatica daemon:

   ```
   infaservice.sh startup
   ```

   By default, infaservice.sh is installed in the following directory: `<INFA_HOME>/tomcat/bin`

2. Start the Informatica Administrator.

   Use the following URL to start the Administrator tool: `http://<fully qualified hostname>:<http port>`. If you configured the Administrator tool to use a secure connection, use the HTTPS protocol: `https://<fully qualified hostname>:<http port>`

   When you start the Administrator tool, you must add the URL to the list of trusted sites for the browser.

3. Select the security domain for your user account.

   If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

After You Configure Kerberos Authentication

If the service principal level for the domain is at process level, the domain requires an SPN and keytab file for every service that you create in the domain. Before you enable a service, verify that an SPN and keytab file is available for the service. Kerberos cannot authenticate the application service if the service does not have a keytab file in the Informatica directory.

If SPNs and keytab files are not available for the application services you plan to create on the domain, you must create the SPN and keytab file before you enable the service. You can use the Informatica Kerberos SPN Format Generator to generate the format of the SPN and keytab file name for the service. To save time, decide on the names of the services you want to create and the nodes on which they will run. Then run the utility to generate the SPN and keytab file name format for all the services at one time.

For more information about running the Informatica Kerberos SPN Format Generator, see "Step 4. Generate the Principal Name and Keytab Format" on page 35

Send a request to the Kerberos administrator to add the SPNs to the principal database and to create the corresponding keytab file.

When you receive the keytab files from the Kerberos administrator, copy the files to the directory specified for the keytab file. By default, keytab files are stored in the following directory: <INFA_HOME>/isp/config/keys

If the service principal for the domain is at node level, you can create and enable application services without creating additional SPNs and keytab files.

CHAPTER 5

Domain Security

This chapter includes the following topics:

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. For example, you can secure the communication between the services in the domain but not secure the connection between the Model Repository Service and the repository database.

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. You can provide the keyword that the installer uses to generate the encryption key. 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
- Between the PowerCenter Integration Service and DTM processes

Web application services

You can secure the connection between a web application service, such as the Analyst Service, and the browser

Sources and targets

You can enable secure communication between the Data Integration Service and PowerCenter Integration Service and the source and target databases.

Data storage

Informatica encrypts sensitive data, such as passwords, when it stores data in the domain. Informatica generates an encryption key based on a keyword that you provide 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.

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 Data Integration Service and the Model Repository Service
- The Data Integration Service and the workflow processes
- The PowerCenter Integration Service and the PowerCenter 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.

If you use RSA encryption, you must use 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`.

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_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

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.

For more information about how to create a custom keystore and truststore, see the Informatica How-To Library article How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain: https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

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 and truststore 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.

Option	Argument	Description
-NodeTruststore -nt	node_truststore_directory	Optional if you use the default SSL certificate from Informatica. Required if you use your SSL certificate. Directory that contains the truststore files. The Informatica domain requires the SSL certificate in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. 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. Required if you use your SSL certificate. 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 and truststore files for all nodes in the domain.
6. Restart the domain.

After you complete updating all nodes in the domain, you must update the machines that host the Informatica client tools. Set the location of the SSL certificates in the Informatica truststore environment variables.

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 and truststore 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. Required if you use your SSL certificate. Directory that contains the truststore files. The Informatica domain requires the SSL certificate in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. 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. Required if you use your SSL certificate. 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 and truststore files for all nodes in the domain.

9. Restart the domain.

After you complete updating all nodes in the domain, you must update the machines that host the Informatica client tools. Set the location of the SSL certificates in the Informatica truststore environment variables.

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, such as the Developer tool. Specify the location and password of the truststore files used to secure the domain with environment variables.

If you use the default Informatica SSL certificate, you do not need to set the INFA_TRUSTSTORE or INFA_TRUSTSTORE_PASSWORD environment variable. When you install the Informatica clients, the installer sets the environment variables and installs the default truststore files in the following directory: `<Informatica installation directory>\clients\shared\security`

If you provide the SSL certificates to use, copy the truststore files to the machine that hosts the client and set the INFA_TRUSTSTORE variable to the directory that contains the truststore files. You must have truststore files in JKS and PEM format named `infa_truststore.jks` and `infa_truststore.pem`. You must also set the INFA_TRUSTSTORE_PASSWORD variable with the password for the `infa_truststore.jks` file.

Set the following environment variables for the truststore information:

INFA_TRUSTSTORE

Set this variable to the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named `infa_truststore.jks` and `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

Set this variable to the password for the `infa_truststore.jks` file. The password must be encrypted. Use the command line program pmpasswd to encrypt the 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_l ocation	Required. Path and file name of the truststore file that contains the SSL certificate for the database.
-DatabaseTruststorePassword -dbtp	database_truststore_p assword	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 PowerCenter Repository Database

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

The PowerCenter Repository Service connects to the PowerCenter repository database through native connectivity.

When you create a PowerCenter 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 PowerCenter repository on a secure Oracle database, configure the Oracle database tnsnames.ora and sqlnet.ora client files with the secure connection information.

Secure Model Repository Database

When you create a Model Repository Service, you can create the associated Model repository in a database secured with the SSL protocol.

The Model Repository Service connects to the Model repository database through JDBC drivers.

1. Set up a database secured with the SSL protocol.
2. In the Administrator tool, create a Model Repository Service.
3. In the **New Model Repository Service** dialog box, enter the general properties for the Model Repository Service and click **Next**.
4. Enter the database properties and the JDBC connection string for the Model Repository Service.

   To connect to a secure database, enter the secure database parameters in the **Secure JDBC Parameters** field. Informatica treats the value of **Secure JDBC Parameters** field as sensitive data and stores the parameter string encrypted.

   The following list describes the secure database 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.

TrustStore

Required. Path and file name of the truststore file that contains the SSL certificate for the database. If you do not include the path for the truststore file, Informatica looks for the file in the following default directory: `<InformaticaInstallationDirectory>/tomcat/bin`

TrustStorePassword

Required. Password for the truststore file for the secure database.

Note: Informatica appends the secure JDBC parameters to the JDBC connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameter in the **Secure JDBC Parameters** field.

5. Test the connection to verify that the connection to the secure repository database is valid.
6. Complete the process to create a Model Repository Service.

Secure Communication for Workflows and Sessions

By default, when you enable secure communication option for the domain, Informatica secures the connection between the Data Integration Service and PowerCenter Integration Service and the DTM processes.

In addition, if you run PowerCenter sessions on a grid, you can enable an option to secure the data communication between the DTM processes.

To enable secure data communication between DTM processes in PowerCenter sessions, select the **Enable Data Encryption** option for the PowerCenter Integration Service.

Note: PowerCenter sessions require more CPU and memory when the DTM processes run in secure mode. Before you enable secure data communication between DTM processes for PowerCenter sessions, determine whether the domain resources are adequate for the additional load.

Enabling Secure Communication for PowerCenter DTM Processes

To secure the connection between the DTM processes in PowerCenter sessions running on a grid, configure the PowerCenter Integration Service to enable the data encryption for DTM processes.

1. In the Navigator of the Administrator tool, select the PowerCenter Integration Service.
2. In the contents panel, click the Properties view.
3. Go to the PowerCenter Integration Service Properties section and click Edit.
4. On the **Edit PowerCenter Integration Service Properties** window, select **Enable Data Encryption**.
5. Click **OK**.

When you run a PowerCenter session on a grid, the DTM processes send encrypted data when they communicate with other DTM processes.

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.

Connections to web application services

You can secure the connection between the following web application services and the browser:

- Analyst Service
- Web Services Hub Console Service
- Metadata Manager Service
- Data Analyzer Service

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.

If you use RSA encryption, you must use 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.

Informatica Web Application Services

Configure a secure connection for a web application service when you create or configure it. Each application service has specific properties for the secure HTTPS connection.

Security for the Analyst Tool

When you create the Analyst Service, you can configure the secure HTTPS properties for the Analyst tool.

To secure the connection between the browser and the Analyst Service, configure the following Analyst Service properties:

Property	Description
Enable Secure Communication	Select to enable a secure connection between the Analyst tool and the Analyst Service.
HTTPS Port	Port number that the Informatica Analyst web application runs on when you enable the Transport Layer Security (TLS) protocol. Use a different port number than the HTTP port number.
Keystore File	Directory where the keystore file that contains the digital certificates is stored.

Property	Description
Keystore Password	Plain-text password for the keystore file. If this property is not set, the Analyst Service uses the default password *changeit*.
SSL Protocol	Informatica recommends that you leave this field blank. The version of TLS enabled depends on the value. A blank field enables the highest version of TLS available. If you enter a value, earlier versions of TLS might be enabled. The behavior is based on the Java version for your environment. For more information, see the documentation for your Java version.

Security for the Web Services Hub Console

When you create the Web Services Hub Service, you can configure the secure HTTPS properties for the Web Services Hub console.

To secure the connection between the browser and the Web Services Hub Service, configure the following Web Services Hub Service properties:

Property	Description
URLScheme	Indicates the security protocol that you configure for the Web Services Hub: - HTTP. Run the Web Services Hub on HTTP only. - HTTPS. Run the Web Services Hub on HTTPS only. - HTTP and HTTPS. Run the Web Services Hub in HTTP and HTTPS modes.
HubPortNumber (https)	Port number for the Web Services Hub on HTTPS. Appears when the URL scheme selected includes HTTPS. Required if you choose to run the Web Services Hub on HTTPS. Default is 7343.
Keystore File	Path and file name of the keystore file that contains the keys and certificates that are required for an HTTPS connection.
Keystore Password	Password for the keystore file. If this property is not set, the Web Services Hub uses the default password *changeit*.

Security for Metadata Manager

When you create the Metadata Manager Service, you can configure the secure HTTPS properties for the Metadata Manager web application.

To secure the connection between the browser and the Metadata Manager Service, configure the following Metadata Manager Service properties:

Property	Description
Enable Secure Sockets Layer	Indicates that you want to configure a secure connection for the Metadata Manager web application. **Note:** This property is displayed when you create a Metadata Manager Service. To secure the connection for an existing Metadata Manager Service, set the **URL Scheme** configuration property to HTTPS.
Port Number	Port number that the Metadata Manager application runs on. Default is 10250.

Property	Description
Keystore File	Keystore file that contains the keys and certificates required if you configure a secure connection for the Metadata Manager web application. **Note:** The Metadata Manager Service uses RSA encryption. Therefore, Informatica recommends that you use a security certificate that was generated with the RSA algorithm.
Keystore Password	Password for the keystore file.

Security for Data Analyzer (Deprecated)

When you create the Reporting Service, you can configure the secure HTTPS properties for Data Analyzer.

To secure the connection between the browser and the Reporting Service, configure the following Reporting Service property:

Property	Description
Enable HTTPS on port	The SSL port that the Reporting Service uses for secure connections. You can edit the value if you have configured the HTTPS port for the node where you create the Reporting Service. Enter a value between 1 and 65535 and ensure that it is not the same as the HTTP port. If the node where you create the Reporting Service is not configured for the HTTPS port, you cannot configure HTTPS for the Reporting Service. Default is 16443.

Note: Effective in version 10.1, Informatica deprecated Data Analyzer and the Reporting Service. Informatica will drop support for Data Analyzer and the Reporting Service in a future release.

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 Appendix C, “Default List of Cipher Suites” on page 233

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.

For a higher level of security, install the Java Cryptography Extension (JCE) to enable support for cipher suites that use AES-256.

Create the Cipher Suite Lists

Before you can configure the Informatica domain to use specific cipher suites, create a whitelist to specify cipher suites to support in addition to the default list or a blacklist to specify 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 the command line utilities. 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. You must use the command line utilities to create the Informatica domain, gateway nodes, and worker nodes. For more information, see the entries for the following commands in the *Informatica Command Reference*: DefineDomain, DefineGatewayNode, and DefineWorkerNode.

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

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 listCiphers -l EFFECTIVE -dc true
   ```

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 PowerCenter connection objects in the Workflow Manager. You create Data Service , Data Quality, or Profiling connections in the Developer tool or in the Administrator tool.

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

- Oracle
- Microsoft SQL Server
- IBM DB2

Data Integration Service Sources and Targets

When you create a connection object for the Data Integration Service to process mappings, data profiles, scorecards, or SQL data services, you can define a connection to a database secured with the SSL protocol.

The Data Integration Service connects to the source or target database through JDBC drivers. When you configure the connection to a secure repository database, you must include the secure connection parameters in the JDBC connection string.

1. Set up a database secured with the SSL protocol to use as a source or target.
2. In the Administrator tool, create a connection.
3. In the **New Connection** dialog box, select the connection type. and click **OK**.

   You can create a connection to a secure DB2, Microsoft SQL Server, or Oracle database.
4. In the **New Connection - Step 1 of 3** dialog box, enter the properties for the connection and click **Next**.
5. In the **New Connection - Step 2 of 3** page, enter the connection string to the database.

   To connect to a secure database, enter the secure database parameters in the **Advanced JDBC Security Options** field. Informatica treats the value of the **Advanced JDBC Security Options** field as sensitive data and stores the parameter string encrypted.

   The following list describes the secure database 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.

   TrustStore

   Required. Path and file name of the truststore file that contains the SSL certificate for the database.

   TrustStorePassword

   Required. Password for the truststore file for the secure database.

   Note: Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the **Advanced JDBC Security Options** field.
6. Test the connection to verify that the connection to the secure database is valid.
7. Complete the process to create the relational connection.

PowerCenter Sources and Targets

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

You can connect to relational PowerCenter 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 PowerCenter 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 a keyword that you provide to create an encryption key with which to encrypt sensitive data.

During installation, you must provide a keyword for the installer to use to generate 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 name of the domain, the keyword for the encryption key, and the encryption key file in a secure location. The domain name, keyword, and encryption key are required when you change the encryption key for the domain or move a repository to another domain. If you lose the encryption key file, you need the keyword to generate the encryption key again. If you lose the keyword and encryption key, you cannot 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.

Note: If the domain contains a Reporting Service, do not change the encryption key. The migrateEncryptionKey command fails if the domain contains a Reporting Service.

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 following options required to generate an encryption key:

Option	Argument	Description
-keyword -kw	keyword	The text string used as the base word from which to generate an encryption key. The keyword must meet the following criteria: - From 8 to 20 characters long - Includes at least one uppercase letter - Includes at least one lowercase letter - Includes at least one number - Does not contain spaces
-domainName -dn	domain_name	Name of the Informatica domain.
-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.

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. **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.

7. Upgrade all Model Repository Services, PowerCenter Repository Services, and Metadata Manager Services.

   You can upgrade a Model Repository Service and a PowerCenter Repository Service in the Administrator tool or at the command prompt. You can upgrade a Metadata Manager Service in the Administrator tool.

   Note: The Metadata Manager Service must be disabled before you can upgrade it.

   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
Model Repository Service	`infacmd mrs UpgradeContents`
PowerCenter 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 lists the default port associated with the Informatica domain:

Type	Default Port
Domain configuration	Default is 6005. You can change the default port when during installation. You can modify the port after installation with the infasetup updateGatewayNode command.
Service Manager	6006
Service Manager Shutdown	6007
Informatica Administrator (HTTP)	6008
Informatica Administrator (HTTPS)	8443
Informatica Administrator shutdown	6009
Service Process (Minimum)	6013
Service Process (Maximum)	6113

Analyst Service

The following table lists the default port associated with the Analyst Service:

Type	Default Port
Analyst Service (HTTP)	8085
Analyst Service (HTTPS)	No default port. Enter the required port number when you create the service.
Analyst Service (Staging database)	No default port. Enter the database port number.

Content Management Service

The following table lists the default port associated with the Content Management Service:

Type	Default Port
Content Management Service (HTTP)	8105
Content Management Service (HTTPS)	No default port. Enter the required port number when you create the service.

Data Director Service

The following table lists the default port associated with the Data Director Service:

Type	Default Port
Data Director Service (HTTP)	No default port. Enter the required port number when you create the service.
Data Director Service (HTTPS)	No default port. Enter the required port number when you create the service.

Data Integration Service

The following table lists the default port associated with the Data Integration Service:

Type	Default Port
Data Integration Service (HTTP proxy)	8085
Data Integration Service (HTTP)	8095
Data Integration Service (HTTPS)	No default port. Enter the required port number when you create the service.
Profiling Warehouse database	No default port. Enter the database port number.
Human Task database	No default port. Enter the database port number.

Metadata Manager Service

The following table lists the default port associated with the Metadata Manager Service:

Type	Default Port
Metadata Manager Service (HTTP)	Default is 10250.
Metadata Manager Service (HTTPS)	No default port. Enter the required port number when you create the service.

PowerExchange Listener Service

Use the same port number that you specify in the SVCNODE statement of the DBMOVER file.

If you define more than one Listener Service to run on a node, you must define a unique SVCNODE port number for each service.

PowerExchange Logger Service

Use the same port number that you specify in the SVCNODE statement of the DBMOVER file.

If you define more than one Listener Service to run on a node, you must define a unique SVCNODE port number for each service.

Reporting Service (Deprecated)

The following table lists the default port associated with the Reporting Service:

Type	Default Port
Reporting Service (HTTP)	16080
Reporting Service (HTTPS)	16443

Reporting and Dashboards Service (Deprecated)

The following table lists the default port associated with the Reporting and Dashboards Service:

Type	Default Port
Reporting and Dashboards Service (HTTP)	No default port. Enter the required port number when you create the service.
Reporting and Dashboards Service (HTTPS)	No default port. Enter the required port number when you create the service.

Web Services Hub Service

The following table lists the default port associated with the Web Services Hub Service:

Type	Default Port
Web Services Hub Service (HTTP)	7333
Web Services Hub Service (HTTPS)	7343

CHAPTER 6

Security Management in Informatica Administrator

This chapter includes the following topics:

Using Informatica Administrator Overview

Informatica Administrator is the tool that you use to manage the Informatica domain and Informatica security.

Use the Administrator tool to complete the following types of tasks:

- Domain administrative tasks. Manage logs, domain objects, user permissions, and domain reports. Generate and upload node diagnostics. Monitor Data Integration Service jobs and applications. Domain objects include application services, nodes, grids, folders, database connections, operating system profiles, and licenses.
- Domain administrative tasks. Manage logs, domain objects, and user permissions. Monitor Data Integration Service jobs and applications.
- Domain administrative tasks. Manage logs, domain objects, and user permissions.
- Security administrative tasks. Manage users, groups, roles, and privileges.

Note: If you have PowerCenter Express Personal Edition, you do not have access to the security features.

The Administrator tool has the following tabs:

- **Manage**. View and edit the properties of the domain and objects within the domain.
- **Monitor**. View the status of profile jobs, scorecard jobs, preview jobs, mapping jobs, SQL data services, web services, and workflows for each Data Integration Service.
- **Monitor**. View the status of profile jobs, preview jobs, mapping jobs, SQL data services, and web services for each Data Integration Service.

- **Monitor**. View the status of profile jobs, preview jobs, mapping jobs, and workflows for the Data Integration Service.
- **Monitor**. View and monitor Ultra Messaging deployments.
- **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.
- **Security**. Manage users, groups, roles, and privileges. If you have PowerCenter Express Personal Edition, you do not have access to the Security tab.
- **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.
- **Help**. Access help for the current tab, determine the Informatica version, and configure the data usage policy.

User Security

The Service Manager and some application services control user security in application clients. Application clients include Data Analyzer, Informatica Administrator, Informatica Analyst, Informatica Developer, Metadata Manager, and PowerCenter Client. The Service Manager and some application services control user security in application clients. Application clients include Informatica Administrator and Informatica Developer. The Service Manager and some application services control user security in application clients. Application client includes Informatica Administrator.

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.

You can also use HTTPS for secure connection to the domain and the application services. The following application services provide HTTPS connection along with the Informatica domain:

- Data Integration Service
- Analyst Service
- Content Management Service
- Metadata Manager Service
- Reporting Service

- Reporting and Dashboards Service
- Web Service Hub Service

You can also use HTTPS for secure connection to the domain and the application services. The following application services support HTTPS connection along with the Informatica domain:

- Data Integration Service
- Analyst Service

You can also use HTTPS for secure connection to the domain and the application services.

Encryption

Informatica encrypts passwords sent from application clients to the Service Manager. Informatica uses AES encryption with multiple 128-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.

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.

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.

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. For example, if you open the Analyst tool from the Administrator tool, you must log out of the Analyst tool and the Administrator tool separately.

Note: To use single sign-on between the Administrator tool, the Analyst tool, and the Monitoring 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. For example, if you launch the Administrator tool from the Developer tool, you must log in to the Administrator 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:

- Data Integration Service
- Metadata Manager Service
- Model Repository Service
- PowerCenter Repository Service
- Reporting Service

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:

- Data Integration Service
- Model 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:

- Data Analyzer repository
- Model repository
- PowerCenter repository
- PowerCenter repository for Metadata Manager

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 Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting 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.

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 Model Repository Service.
- You add or remove native users or groups.

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. For example, if you try to edit a project in Informatica Developer, the Model Repository Service authorizes your request based on your privilege, role, and permission assignments.

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 and operating system profiles. You can also view users that have privileges for a service.

Note: If you have PowerCenter Express Personal Edition, you do not have access to the Security tab

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.

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, or roles. Select an object in the Navigator and click the Actions menu to create, delete, or move groups, users, or roles.
- Right-click an object. Right-click an object in the Navigator to display the create, delete, and move 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.

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.

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.

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. Right-click a group and select Navigate to Item to display the group details in the contents panel.

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.

Users

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator
- PowerCenter Client
- Metadata Manager
- Data Analyzer
- Informatica Developer
- Informatica Analyst
- Jaspersoft

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator
- Informatica Developer

A user with an account in the Informatica domain can log in to Informatica Administrator.

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.

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.

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.

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. Right-click a user and select Navigate to Item to display the user details in the contents panel.

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.

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. Right-click a role and select Navigate to Item to display the role details in the contents panel.

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.

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.

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 secure domain to a non-secure domain or from a non-secure domain to a secure domain, you must delete the domain configuration in the Developer tool and PowerCenter 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.

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, node, license, database connections, 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.

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.

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.

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.

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 7

Users and Groups

This chapter includes the following topics:

Users and Groups OverviewUsers and Groups

To access the application services and objects in the Informatica domain and to use the application clients, you must have a user account. The tasks you can perform depend on the type of user account you have and the type of PowerCenter Express license.

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.

Note: If you install PowerCenter Express Personal Edition you must use the default administrator account for all operations. You cannot create users or groups and manage permissions.

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.
- 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.

- 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.
- 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, like the Developer tool and Analyst tool. You can also unlock a user account.
- Account lockout. You can configure account lockout to lock a user account when the user specifies an incorrect login in the Administrator tool or the Developer tool. You can also unlock a user account.
- Account lockout. You can configure account lockout to lock a user account when the user specifies an incorrect login in the Administrator tool. 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

An Informatica domain can have the following types of accounts:

- Default administrator
- Domain administrator
- Application client administrator
- User

The Informatica domain has a default administrator account.

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.

The default administrator is a user account in the native security domain. You cannot create a default administrator. 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.

The domain administrator can log in to the Administrator tool 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:

Data Analyzer administrator

Has full permissions and privileges in Data Analyzer. The Data Analyzer administrator can log in to Data Analyzer to create and manage Data Analyzer objects and perform all tasks in the application client.

To create a Data Analyzer administrator, assign a user the Administrator role for a Reporting Service.

Informatica Analyst administrator

Has full permissions and privileges in Informatica Analyst. The Informatica Analyst administrator can log in to Informatica Analyst to create and manage projects and objects in projects and perform all tasks in the application client.

To create an Informatica Analyst administrator, assign a user the Administrator role for an Analyst Service and for the associated Model Repository Service.

Informatica Developer administrator

Has full permissions and privileges in Informatica Developer. The Informatica Developer administrator can log in to Informatica Developer to create and manage projects and objects in projects and perform all tasks in the application client.

To create an Informatica Developer administrator, assign a user the Administrator role for a Model Repository Service.

Metadata Manager administrator

Has full permissions and privileges in Metadata Manager. The Metadata Manager administrator can log in to Metadata Manager to create and manage Metadata Manager objects and perform all tasks in the application client.

To create a Metadata Manager administrator, assign a user the Administrator role for a Metadata Manager Service.

Jaspersoft administrator

Administrator privileges map to the ROLE_ADMINISTRATOR role in Jaspersoft.

Test Data administrator

Has full permissions and privileges in Test Data Manager. The Test Data Manager administrator can log in to Test Data Manager to create and manage Test Data Manager objects and perform all tasks in the application client.

To create a Test Data administrator, assign a user the Administrator role for a Test Data Manager Service.

PowerCenter Client administrator

Has full permissions and privileges on all objects in the PowerCenter Client. The PowerCenter Client administrator can log in to the PowerCenter Client to manage the PowerCenter repository objects and perform all tasks in the PowerCenter Client. The PowerCenter Client administrator can also perform all tasks in the pmrep and pmcmd command line programs.

To create a PowerCenter Client administrator, assign a user the Administrator role for a PowerCenter 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 create, edit, and delete users depending on the type of PowerCenter Express license. You can assign roles, permissions, and privileges to a user account. The roles, permissions, and privileges assigned to the user determines the tasks the user can perform within the Informatica domain. If you have the PowerCenter Express Personal Edition, you cannot create users or groups. You must use the default Administrator user to perform all tasks.

You can create, edit, and delete users depending on the type of license. You can assign roles, permissions, and privileges to a user account. The roles, permissions, and privileges assigned to the user determines the tasks the user can perform within the Informatica domain.

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 UsersCreating UsersCreating 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. **Note:** Data Analyzer uses the user account name and security domain in the format *UserName@SecurityDomain* to determine the length of the user login name. The combination of the user name, @ symbol, and security domain cannot exceed 128 characters.
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: < > “ **Note:** In Data Analyzer, the full name property is equivalent to three separate properties named first name, middle name, and last name.
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > “

Property	Description
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 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 click Add.
5. To remove an LDAP user from a group, select an LDAP user in the Assigned Users column and 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.

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. 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 PowerCenter

When you delete a user who owns objects in the PowerCenter 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."

Deleting Users of Data Analyzer

When you delete a user, Data Analyzer deletes the alerts, alert email accounts, and personal folders and dashboards associated with the user.

Data Analyzer deletes all reports that a user subscribes to based on the security profile of the report. Data Analyzer keeps a security profile for each user who subscribes to the report. A report that uses user-based security uses the security profile of the user who accesses the report. A report that uses provider-based security uses the security profile of the user who owns the report.

When you delete a user, Data Analyzer does not delete any report in the public folder owned by the user. Data Analyzer can run a report with user-based security even if the report owner does not exist. However, Data Analyzer cannot determine the security profile for a report with provider-based security if the report owner does not exist. Before you delete a user, verify that the reports with provider-based security have a new owner.

For example, you want to delete UserA who has a report in the public folder with provider-based security. Create or select a user with the same security profile as UserA. Identify all the reports with provider-based security in the public folder owned by UserA. Then, have the other user with the same security profile log in and save those reports to the public folder, with provider-based security and the same report name. This ensures that after you delete the user, the reports stay in the public folder with the same security.

Deleting Users of Metadata Manager

When you delete a user who owns shortcuts and folders, Metadata Manager moves the user's personal folder to a folder named Deleted Users owned by the default administrator. The deleted user's personal folder contains all shortcuts and folders created by the user. Any shared folders remain shared after you delete the user.

If the Deleted Users folder contains a folder with the same user name, Metadata Manager names the additional folder "Copy (n) of <username>."

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 oie 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

Number of Domain Users	Maximum Heap Size (1-5 Services)	Maximum Heap Size (6-10 Services)
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 infacmd isp getUserActivityLog command or the Logs tab of the Administrator tool to view user activity logs. View user activity log events to determine when a user created, updated, or removed services, nodes, users groups, or roles.

Run the following command to view the user activity log events for all users:

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

The command requires the Administrator role or membership in the Administrator group.

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 on the command line or write it 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.

For more information about user activity logs and the Logs tab of the Administrator tool, see the *Informatica Administrator Guide*.

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.

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.

You can assign roles, permissions, and privileges to a group. The roles, permissions, and privileges assigned to the group determines the tasks that users in the group can perform within the Informatica domain.

You can assign roles, permissions, and privileges to a group. 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.

A native group can contain 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.

A native group can contain 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 Data Integration Service is configured to use operating system profiles, it runs mappings, profiles, and workflows with the operating system profile. If the PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter Integration Service runs. The PowerCenter 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 PowerCenter 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 PowerCenter 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.

Operating System Profile Properties for the Data Integration Service

The following table describes the operating system profile properties for the Data 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 systems where the Data Integration Service runs. The Data Integration Service runs mappings, workflows, and profiling jobs using the system access of the operating system user.
$DISRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters: * ? < > " | , [ ]
$DISTempDir	Directory for temporary files created when jobs are run. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/disTemp.
$DISCacheDir	Directory for index and data cache files for transformations. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/cache.
$DISSourceDir	Directory for source flat files used in a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/source.
$DISTargetDir	Directory for target flat files used in a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/target.
$DISRejectedFilesDir	Directory for reject files. Reject files contain rows that were rejected when running a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/reject.
$DISLogDir	Directory for logs. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/disLogs.
Enable Hadoop Impersonation Properties	Indicates that the Data Integration Service uses the Hadoop impersonation user to run mappings, workflows, and profiling jobs in a Hadoop environment. Default Hadoop impersonation user is the logged in user. To specify a different Hadoop impersonation user, select **Use the Specified User as Hadoop Impersonation User** and enter a user name.

Property	Description
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. **Note:** On AIX, you must set the LD_LIBRARY_PATH environment variable to INFA_HOME/services/shared/bin for the Data Integration Service to successfully run mappings, profiles, and workflows with operating system profiles.
Flat File Cache Directory	Directory of the flat file cache where the Analyst tool stores uploaded flat files. If the Analyst Service connects to a Data Integration Service that uses operating system profiles, the operating system user specified in the operating system profile must have access to this flat file cache directory. When you import a reference table or flat file source, the Analyst tool uses the files from this directory to create a reference table or flat file data object. Restart the Analyst Service if you change the flat file location.

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 PowerCenter Integration Service uses the operating system profile to run workflows. The Data Integration Service uses the operating system profile to run mappings, profiles, and 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 one or both of the Integration Services that will use the operating system profile.

- PowerCenter Integration Service
- Data Integration Service
6. Configure the operating system profile properties for the Integration Services.
7. If the Data Integration Service runs mappings, profiles, and workflows in a Hadoop environment, configure the Hadoop impersonation properties as follows:
   a. Select **Enable Hadoop Impersonation Properties**.
   b. Choose to use the logged in user or specify a Hadoop impersonation user to run Hadoop jobs.
8. Optionally, configure the environment variables.
9. If the Analyst Service connects to a Data Integration Service that uses operating system profiles, configure the Analyst Service properties.
10. Click **Next**.

    The **Assign Groups and Users to Operating System Profile - Step 3 of 3** dialog box appears.
11. 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**.
12. 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.
13. 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**.
14. 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.
15. 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 **Data Integration Service** or the **PowerCenter Integration Service** that you want to configure.
6. Edit the Integration 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 PowerCenter 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** > **OS 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** > **OS 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. The Data Integration Service, Web Services Hub Service, and PowerCenter Integration Service are resilient application services that use a user name and password to authenticate with the Model Repository Service or PowerCenter Repository Service. If the Data Integration Service, Web Services Hub Service, or PowerCenter Integration Service continually try to restart after a failed login, the domain eventually locks the associated user account.

- 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 8

Privileges and Roles

This chapter includes the following topics:

Privileges and Roles Overview

You manage user security with privileges and roles.

You can modify privileges and roles depending on the type of PowerCenter Express license.

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.
- Domain privileges. Determine actions on the Informatica domain that users can perform using the Administrator tool.
- Analyst Service privilege. Determines actions that users can perform using Informatica Analyst.
- Content Management Service privilege. Determines actions that users can perform using reference tables in the Informatica Developer tool and the Informatica Analyst tool.
- Data Integration Service privilege. Determines actions on applications that users can perform using the Administrator tool and the infacmd command line program. This privilege also determines whether users can drill down and export profile results.
- Data Integration Service privilege. Determines actions on applications that users can perform using the Administrator tool. This privilege also determines whether users can drill down and export profile results.
- Metadata Manager Service privileges. Determine actions that users can perform using Metadata Manager.
- Model Repository Service privilege. Determines actions on projects that users can perform using Informatica Analyst and Informatica Developer.
- Model Repository Service privilege. Determines actions on projects that users can perform using Informatica Developer.
- PowerCenter Repository Service privileges. Determine PowerCenter repository actions that users can perform using the Repository Manager, Designer, Workflow Manager, Workflow Monitor, and the pmrep and pmcmd command line programs.
- PowerExchange application service privileges. Determine actions that users can perform on the PowerExchange Listener Service and PowerExchange Logger Service using the infacmd pwx commands.
- Reporting Service privileges. Determine reporting actions that users can perform using Data Analyzer.
- Reporting and Dashboards Service privileges. Determine actions that users can perform using Jaspersoft.
- Scheduler Service privileges. Determine actions that users can perform using the Scheduler Service.
- Test Data Manager Service privileges. Determine data discovery, data masking, data subset, and test data generation tasks that users can perform using the Test Data Manager.

Privileges determine the actions that users can perform in application clients. Informatica includes domain privileges that determine actions that users can perform using the Administrator tool.

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.
- Domain Administration. Includes privileges to manage the domain, folders, and application services.
- 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.
- Tools. Includes privileges to log in to the Administrator tool.
- Monitoring. Includes privileges to monitor Ultra Messaging deployments and view statistics.

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.

For example, the PowerCenter Developer role includes all the PowerCenter Repository Service privileges or actions that a developer performs.

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: https://kb.informatica.com/h2l/HowTo%20Library/1/0236-GroupsAndRolesToManageAccessControl.pdf.

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.

Domain Privileges

Domain privileges determine the actions that users can perform using the Administrator tool and the infacmd and pmrep command line programs.

Domain privileges determine the actions that users can perform using the Administrator tool.

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, and connections.

Privilege Group	Description
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.

Privilege Group	Description
Security Administration	Includes privileges to manage users, groups, roles, and privileges.
Domain Administration	Includes privileges to manage the domain, application services, and connections.
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.

Privilege Group	Description
Security Administration	Includes privileges to manage users, groups, roles, and privileges.
Domain Administration	Includes privileges to manage the domain, application services, and connections.
Monitoring	Includes privileges to monitor UM deployments and view statistics.
Tools	Includes privileges to log in to the Administrator tool.

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.

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.
- 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.
Web Services Hub	User can run the Web Services Report.

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. To enable and disable a Metadata Manager Service, users must also have permission on the associated PowerCenter Integration Service and PowerCenter Repository Service. - Receive application service alerts.

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.
Analyst Service	User is able to create and delete audit trail tables.
Metadata Manager Service	User is able to perform the following actions: - Back up Metadata Manager repository content. - Delete Metadata Manager repository content. - Upgrade the content of the Metadata Manager Service. **Note:** To create or restore Metadata Manager repository content, the user must belong to the default Administrator group.
Metadata Manager Service PowerCenter Repository Service	User is able to restore the PowerCenter repository for Metadata Manager.
Model Repository Service	User is able to perform the following actions: - Create and delete Model repository content. - Create, delete, and re-index the search index. - Upgrade the content of the Model Repository Service from the **Actions** menu or from the command line. The user must also have the Create, Edit and Delete Projects privilege on the Model Repository Service and write permission on the projects.
PowerCenter Integration Service	User is able to run the PowerCenter Integration Service in safe mode.

Permission On	Description
PowerCenter Repository Service	User is able to perform the following actions: - Back up, restore, and upgrade the PowerCenter repository. - Configure data lineage for the PowerCenter repository. - Copy content from another PowerCenter repository. - Close user connections and release PowerCenter repository locks. - Create and delete PowerCenter repository content. - Create, edit, and delete reusable metadata extensions in the PowerCenter Repository Manager. - Enable version control for the PowerCenter repository. - Manage a PowerCenter repository domain. - Perform an advanced purge of object versions at the repository level in the PowerCenter Repository Manager. - Register and unregister PowerCenter repository plug-ins. - Run the PowerCenter repository in exclusive mode. - Send PowerCenter repository notifications to users. - Update PowerCenter repository statistics. - Upgrade the content of the PowerCenter Repository Service.
Reporting Service	User is able to perform the following actions: - Back up, restore, and upgrade the content of the Data Analyzer repository. - Create and delete the content of the Data Analyzer repository.
Test Data Manager Service	User is able to perform the following actions: - Create and delete the Test Data Manager repository content. - Upgrade the content of the Test Data Manager 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.

Permission On	Description
Domain where application service runs, 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.
Model Repository Service	User is able to perform the following actions: - Create and delete Model repository content. - Create, delete, and re-index the search index.

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, Analyst tool, Developer tool, and infacmd command line program. Users can also copy connections in the Developer tool and can grant permissions on connections in the Administrator tool and infacmd command line program.

Users assigned the Manage Connections privilege can create, edit, and delete connections in the Administrator tool, Developer tool, and infacmd command line program. Users can also copy connections in the Developer tool and can grant permissions on connections in the Administrator tool and 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.
- Preview data or run a mapping 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.
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.

Monitoring Privilege Group

The privileges in the Monitoring privilege group determine which users can view and configure monitoring.

The following table lists the required permissions and the actions that users can perform with the privileges in the Manage Monitoring group:

Parent Privilege	Privilege	Permission On	Description
Manage Monitoring	Monitoring Configuration	Domain	User can configure monitoring settings.
Manage Monitoring	Report and Statistic Settings	Domain	User can configure monitoring statistics and reports.
View	View Jobs of All the Users in the Groups the User Belongs To	Domain	A user in a group can monitor the jobs run by other users in the group. If the user belongs to multiple groups, the user can see the jobs from all the groups.
View Jobs of All the Users in the Groups the User Belongs To	View Jobs of Other Users	Domain	User can view jobs of other users.
View	View Statistics	Domain	User can view the Summary Statistics view and statistics for domain objects. **Note:** In a domain that uses Kerberos authentication, users must also have the Administrator role for the Model Repository Service that is configured for monitoring.
View	View Reports	Domain	User can view reports for domain objects.
Access Monitoring	Access from Analyst Tool	Domain	User can access the Job Status workspace in the Analyst tool.

Parent Privilege	Privilege	Permission On	Description
Access Monitoring	Access from Developer Tool	Domain	User can access the Monitoring tool from the Developer tool.
Access Monitoring	Access from Administrator Tool	Domain	User can access the Monitor tab in the Administrator tool.
N/A	Perform Actions on Jobs	Domain	User can perform the following actions: - Abort jobs. - Reissue mapping jobs. - View job logs.

Users do not need the Access Informatica Administrator privilege to access the Monitoring tool.

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 or access the Monitoring tool.

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.

Analyst Service Privileges

The Analyst Service privilege determines actions that licensed users can perform on projects using the Analyst tool.

The following table lists the privileges and permissions required to manage projects and objects in projects:

Privilege	Permission	Description
Run Profiles and Scorecards	Read on projects. Execute on relational data source connection.	User is able to run profiles and scorecards for licensed users in the Analyst tool.
Access Mapping Specifications	Read on projects.	User is able to access mapping specifications for licensed users in the Analyst tool.
Load Mapping Specification Results	Write on projects.	User is able to load the results of a mapping specification for licensed users to a table or flat file. **Note:** Selecting this privilege also grants the **Access Mapping Specifications** privilege by default.
Manage Glossaries	-	User is able to manage the business glossary.
View Glossaries	-	User is able to view published Business Glossary assets in the Library workspace. This is equivalent to providing read permission for glossaries and Glossary assets in the Glossary Security workspace.
Workspace Access	-	User is able to access the following workspaces in the Analyst tool: - **Design** workspace. - **Discovery** workspace. - **Glossary** workspace. - **Scorecards** workspace. **Note:** Selecting this privilege also grants access to projects in the Analyst tool. If the user does not have this privilege, the user must have either the **Design Workspace**, **Discovery Workspace**, **Glossary Workspace**, or **Scorecards Workspace** privilege to access projects.
Design Workspace	-	User is able to access the **Design** workspace.
Discovery Workspace	-	User is able to access the **Discovery** workspace.
Glossary Workspace	-	User is able to access the **Glossary** workspace.
Scorecards Workspace	-	User is able to access the **Scorecards** workspace.

Content Management Service Privileges

The Content Management Service privileges determine actions that licensed users can perform on reference tables.

The following table lists the privileges and permissions required to manage reference tables:

Privilege	Permission	Description
Create Reference Tables	Write on project	- Create a reference table in the Analyst and Developer tool. - Create a reference table with infacmd rtm import. - Import a reference table object to the Model repository. - Copy a reference table in the Analyst and Developer tool. - Create a reference table from profile data. **Note:** The Create privilege also grants the Edit privilege by default.
Edit Reference Table Data and Metadata	Read on project	- Edit reference table data values in the Developer tool and Analyst tool. - Add profile data to a reference table. - Add or delete columns in a reference table. Change reference table metadata such as column names, descriptions, and default values.

Data Integration Service Privileges

The Data Integration Service privileges determine actions that users can perform on applications using the Administrator tool and the infacmd command line program. They also determine whether users can drill down and export profile results using the Analyst tool and the Developer tool.

The Data Integration Service privileges determine actions that users can perform on applications using the Administrator tool and the infacmd command line program. They also determine whether users can drill down and export profile results using the Developer tool.

The following table lists the actions that users can perform with the privilege in the Application Administration privilege group:

Privilege Name	Description
Manage Applications	User is able to perform the following actions: - Back up and restore an application to a file. - Deploy an application to a Data Integration Service and resolve name conflicts. - Start an application after deployment. - Find an application. - Start or stop objects in an application. - Configure application properties.

The following table lists the required permissions and the actions that users can perform with the privilege in the Profiling Administration privilege group:

Privilege Name	Permission On	Description
Drilldown and Export Results	Read on project Execute on relational data source connection is also required to drill down on live data	User is able to perform the following actions: - Drill down profiling results. - Export profiling results.

Metadata Manager Service Privileges

Metadata Manager Service privileges determine the Metadata Manager actions that users can perform using Metadata Manager.

The following table describes each Metadata Manager privilege group:

Privilege Group	Description
Catalog	Includes privileges to manage objects in the Browse page of the Metadata Manager interface.
Load	Includes privileges to manage objects in the Load page of the Metadata Manager interface.
Model	Includes privileges to manage objects in the Model page of the Metadata Manager interface.
Security	Includes privileges to manage objects in the Security page of the Metadata Manager interface.

Catalog Privilege Group

The privileges in the Catalog privilege group determine the tasks that users can perform on the **Browse** tab of the Metadata Manager application. A user with the privilege to perform a certain action also requires permissions to perform the action on a particular object. Configure permissions on the **Security** tab of the Metadata Manager application.

The following table lists the privileges in the Catalog privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
Share Shortcuts	n/a	Write	User is able to share a folder that contains a shortcut with other users and groups.
View Lineage	n/a	Read	User is able to perform the following actions: - Run data lineage analysis on metadata objects, categories, and business terms. - Run data lineage analysis from the PowerCenter Designer. Users must also have read permission on the PowerCenter repository folder.

Privilege	Includes Privileges	Permission	Description
View Related Catalogs	n/a	Read	User is able to view related catalogs.
View Reports	n/a	Read	User is able to view Metadata Manager reports in Data Analyzer.
View Profile Results	n/a	Read	User is able to view profiling information for metadata objects in the catalog from a relational source.
View Catalog	n/a	Read	User is able to perform the following actions: - View resources and metadata objects in the metadata catalog. - Search the metadata catalog.
View Relationships	n/a	Read	User is able to view relationships for metadata objects, categories, and business terms.
Manage Relationships	View Relationships	Write	User is able to create, edit, and delete relationships for custom metadata objects, categories, and business terms.
View Comments	n/a	Read	User is able to view comments for metadata objects, categories, and business terms.
Post Comments	View Comments	Write	User is able to add comments for metadata objects, categories, and business terms.
Delete Comments	- Post Comments - View Comments	Write	User is able to delete comments for metadata objects, categories, and business terms.
View Links	n/a	Read	User is able to view links for metadata objects, categories, and business terms.
Manage Links	View Links	Write	User is able to create, edit, and delete links for metadata objects, categories, and business terms.
View Glossary	n/a	Read	User is able to perform the following actions: - View business glossaries in the **Glossary** view. - Search business glossaries.
Manage Objects	n/a	Write	User is able to perform the following actions: - Edit metadata objects in the catalog. - Create, edit, and delete custom metadata objects. Users must also have the View Model privilege. - Create, edit, and delete custom metadata resources. Users must also have the Manage Resource privilege.

Load Privilege Group

The privileges in the Load privilege group determine the tasks that users can perform on the **Load** tab of the Metadata Manager application. A user with the privilege to perform a certain action also requires permissions to perform the action on a particular object. Configure permissions on the **Security** tab of the Metadata Manager application.

The following table lists the privileges and permissions required to manage an instance of a resource in the Metadata Manager warehouse:

Privilege	Includes Privileges	Permission	Description
View Resource	-	Read	User is able to perform the following actions: - View resources and resource properties in the Metadata Manager warehouse. - Export resource configurations. - Download the Metadata Manager Agent installer.
Load Resource	View Resource	Write	User is able to perform the following actions: - Load metadata for a resource into the Metadata Manager warehouse.* - Create links between objects in connected resources for data lineage. - Configure search indexing for resources. - Import resource configurations.
Manage Schedules	View Resource	Write	User is able to perform the following actions: - Create and edit schedules. - Add schedules to resources.
Purge Metadata	View Resource	Write	User is able to remove metadata for a resource from the Metadata Manager warehouse.
Manage Resource	- Purge Metadata - View Resource	Write	User is able to create, edit, and delete resources.
* To load metadata for Business Glossary resources, the Load Resource, Manage Resource, and View Model privileges are required.			

Model Privilege Group

The privileges in the Model privilege group determine the tasks that users can perform on the **Model** tab of the Metadata Manager application. You cannot configure permissions on a model.

The following table lists the privileges required to manage models:

Privilege	Includes Privileges	Permission	Description
View Model	-	-	User is able to open models and classes, and view model and class properties. View relationships and attributes for classes.
Manage Model	View Model	-	User is able to create, edit, and delete custom models. Add attributes to packaged and universal models.
Export/Import Models	View Model	-	User is able to import and export custom models. Import and export modified packaged and universal models.

Security Privilege Group

The privileges in the Security privilege group determines the tasks that users can perform on the **Security** tab of the Metadata Manager application.

By default, the Manage Catalog Permissions privilege in the Security privilege group is assigned to the Administrator, or a user with the Administrator role on the Metadata Manager Service. You can assign the Manage Catalog Permissions privilege to other users.

The following table lists the privilege and permission required to manage Metadata Manager security:

Privilege	Includes Privileges	Permission	Description
Manage Catalog Permissions	-	Full control	User is able to perform the following actions: - Assign users and groups permissions on resources, metadata objects, categories, and business terms. - Edit permissions on resources, metadata objects, categories, and business terms.

Model Repository Service Privileges

The Model Repository Service privileges determine actions that users can perform on projects using Informatica Analyst and Informatica Developer.

The Model Repository Service privileges determine actions that users can perform on projects using Informatica Developer.

The Model repository object permissions determine the tasks that users can complete on objects in projects.

The following table lists the required permissions and the actions that users can perform with the Model Repository Service privileges:

Privilege	Permission	Description
N/A	Read on project	User can view projects and objects in projects.
N/A	Write on project	User can create, edit, and delete objects in projects.
N/A	Grant on project	User can grant and revoke permissions on projects for users and groups.
Access Analyst	N/A	User can access the Model repository from the Analyst tool.
Access Developer	N/A	User can access the Model repository from the Developer tool.
Create, Edit, and Delete Projects	N/A	User can create projects.

Privilege	Permission	Description
Create, Edit, and Delete Projects	Write on projects	User can perform the following actions: - Edit projects. - Delete projects if the user created the projects. - Upgrade the content of the Model Repository Service. To upgrade the service from the **Actions** menu or from the command line, the user must also have the Manage Service privilege for the domain and permission on the Model Repository Service. To upgrade the service using the service upgrade wizard, the user must also have the Administrator role for the domain.
Manage Data Domains	N/A	User can create, edit, and delete data domains in the data domain glossary. This privilege is part of the **Data Domain Administration** privilege group.
Manage Notifications	N/A	User can configure scorecard notifications. This privilege is part of the **Profiling Administration** privilege group.
Manage Team-based Development	N/A	User can manage the locked or unlocked states of Model repository objects. If the Model repository is integrated with a version control system, the user can manage the checked out or checked in states of objects. The user can also manage the ownership of checked-out objects.
Show Security Details	N/A	User can view the following details: - Names of projects for which users do not have read permission. - Error and warning message details.

Privilege	Permission	Description
N/A	Read on project	User can view projects and objects in projects.
N/A	Write on project	User can create, edit, and delete objects in projects.
N/A	Grant on project	User can grant and revoke permissions on projects for users and groups.
Access Developer	N/A	User can access the Model repository from the Developer tool.
Create, Edit, and Delete Projects	N/A	User can perform the following actions: - Create projects. - Upgrade the Model Repository Service.
Create, Edit, and Delete Projects	Write on project	User can perform the following actions: - Edit projects. - Delete projects if the user created the projects.
Show Security Details	N/A	User can view the following details: - Names of projects for which users do not have read permission. - Error and warning message details.

PowerCenter Repository Service Privileges

PowerCenter Repository Service privileges determine PowerCenter repository actions that users can perform using the PowerCenter Repository Manager, Designer, Workflow Manager, Workflow Monitor, and the pmrep and pmcmd command line programs.

The following table describes each privilege group for the PowerCenter Repository Service:

Privilege Group	Description
Tools	Includes privileges to access PowerCenter 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 PowerCenter Repository Service to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the PowerCenter repository level.
- Create, edit, and delete reusable metadata extensions.

Tools Privilege Group

The privileges in the PowerCenter Repository Service Tools privilege group determine the PowerCenter 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 PowerCenter repository using the Designer.
Access Repository Manager	-	User is able to perform the following actions: - Connect to the PowerCenter repository using the Repository Manager. - Run *pmrep* commands.
Access Workflow Manager	-	User is able to perform the following actions: - Connect to the PowerCenter repository using the Workflow Manager. - Remove a PowerCenter Integration Service from the Workflow Manager.
Access Workflow Monitor	-	User is able to perform the following actions: - Connect to the PowerCenter repository using the Workflow Monitor. - Connect to the PowerCenter Integration Service in the Workflow Monitor.

Note: When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service.

The appropriate privilege in the Tools privilege group is required for all users completing tasks in PowerCenter 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 PowerCenter 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, PowerCenter 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 PowerCenter Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the PowerCenter 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 PowerCenter 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 PowerCenter repository or to another PowerCenter 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 PowerCenter repository or to another PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter repository notification messages. - Run data lineage on design objects. Users must also have the View Lineage privilege for the Metadata Manager Service and read permission on the metadata objects in the Metadata Manager catalog. - 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 PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter repository notification messages. - Run data lineage on source and target objects. Users must also have the View Lineage privilege for the Metadata Manager Service and read permission on the metadata objects in the Metadata Manager catalog. - 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 PowerCenter 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 PowerCenter 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, PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter 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 PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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 PowerCenter Integration Service uses operating system profiles, users must also have permission on the operating system profile. When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service.

Global Objects Privilege Group

Privileges in the Global Objects privilege group and PowerCenter 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 PowerCenter 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 PowerCenter 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 PowerCenter 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.

PowerExchange Listener Service Privileges

The PowerExchange Listener Service privileges determine the infacmd pwx commands that users can run.

The following table describes the PowerExchange Listener Service privilege in the Informational Commands privilege group:

Privilege Name	Description
listtask	Run the infacmd pwx ListTaskListener command.

The following table describes each PowerExchange Listener Service privilege in the Management Commands privilege group:

Privilege Name	Description
close	Run the infacmd pwx CloseListener command.
closeforce	Run the infacmd pwx CloseForceListener command.
stoptask	Run the infacmd pwx StopTaskListener command.

PowerExchange Logger Service Privileges

The PowerExchange Logger Service privileges determine the infacmd pwx commands that users can run.

The following table describes each PowerExchange Logger Service privilege in the Informational Commands privilege group:

Privilege Name	Description
displayall	Run the infacmd pwx DisplayAllLogger command.
displaycpu	Run the infacmd pwx DisplayCPULogger command.
displaycheckpoints	Run the infacmd pwx DisplayCheckpointsLogger command.
displayevents	Run the infacmd pwx DisplayEventsLogger command.
displaymemory	Run the infacmd pwx DisplayMemoryLogger command.
displayrecords	Run the infacmd pwx DisplayRecordsLogger command.
displaystatus	Run the infacmd pwx DisplayStatusLogger command.

The following table describes each PowerExchange Logger Service privilege in the Management Commands privilege group:

Privilege Name	Description
condense	Run the infacmd pwx CondenseLogger command.
fileswitch	Run the infacmd pwx FileSwitchLogger command.
shutdown	Run the infacmd pwx ShutDownLogger command.

Reporting Service Privileges (Deprecated)

Reporting Service privileges determine the actions that users can perform using Data Analyzer.

The following table describes each privilege group for the Reporting Service:

Privilege Group	Description
Administration	Includes privileges to manage objects in the Administration tab of Data Analyzer.
Alerts	Includes privileges to manage objects in the Alerts tab of Data Analyzer.
Communication	Includes privileges to share dashboard or report information with other users.
Content Directory	Includes privileges to manage objects in the Find tab of Data Analyzer.

Privilege Group	Description
Dashboards	Includes privileges to manage dashboards in Data Analyzer.
Indicators	Includes privileges to manage indicators in Data Analyzer.
Manage Account	Includes privileges to manage objects in the Manage Account tab of Data Analyzer.
Reports	Includes privileges to manage reports in Data Analyzer.

Note: Effective in version 10.1, Informatica deprecated Data Analyzer, the Reporting Service, and all the Reporting Service privileges. Informatica will drop support for the Reporting Service in a future release.

Administration Privilege Group

Privileges in the Administration privilege group determine the tasks that users can perform in the Administration tab of Data Analyzer.

The following table lists the privileges and permissions in the Administration privilege group:

Privilege	Includes Privileges	Permission	Description
Maintain Schema	-	Read, Write, and Delete on: - Metric folder - Attribute folder - Template dimension folder - Metric - Attribute - Template dimension	User is able to create, edit, and delete schema tables.
Export/Import XML Files	-	-	User is able to export or import metadata as XML files.
Manage User Access	-	-	User is able to manage users, groups, and roles.
Set Up Schedules and Tasks	-	Read, Write, and Delete on time-based and event-based schedules	User is able to create and manage schedules and tasks.
Manage System Properties	-	-	User is able to manage system settings and properties.
Set Up Query Limits	- Manage System Properties	-	User is able to access query governing settings.
Configure Real-Time Message Streams	-	-	User is able to add, edit, and remove real-time message streams.

Alerts Privilege Group

Privileges in the Alerts privilege group determine the tasks users can perform in the Alerts tab of Data Analyzer.

The following table lists the privileges and permissions in the Alerts privilege group:

Privilege	Includes Privileges	Permission	Description
Receive Alerts	-	-	User is able to receive and view triggered alerts.
Create Real-time Alerts	- Receive Alerts	-	User is able to create an alert for a real-time report.
Set Up Delivery Options	- Receive Alerts	-	User is able to configure alert delivery options.

Communication Privilege Group

Privileges in the Communication privilege group determine the tasks users can perform to share dashboard or report information with other users.

The following table lists the privileges and permissions in the Communication privilege group:

Privilege	Includes Privileges	Permission	Description
Print	-	Read on report Read on dashboard	User is able to print reports and dashboards.
Email Object Links	-	Read on report Read on dashboard	User is able to send links to reports or dashboards in an email.
Email Object Contents	- Email Object Links	Read on report Read on dashboard	User is able to send the contents of a report or dashboard in an email.
Export	-	Read on report Read on dashboard	User is able to export reports and dashboards.
Export to Excel or CSV	- Export	Read on report Read on dashboard	User is able to export reports to Excel or comma-separated values files.
Export to Pivot Table	- Export - Export to Excel or CSV	Read on report Read on dashboard	User is able to export reports to Excel pivot tables.
View Discussions	-	Read on report Read on dashboard	User is able to read discussions.
Add Discussions	- View Discussions	Read on report Read on dashboard	User is able to add messages to discussions.

Privilege	Includes Privileges	Permission	Description
Manage Discussions	- View Discussions	Read on report Read on dashboard	User is able to delete messages and comments from discussions.
Give Feedback	-	Read on report Read on dashboard	User is able to create feedback messages.

Content Directory Privilege Group

Privileges in the Content Directory privilege group determine the tasks users can perform in the Find tab of Data Analyzer.

The following table lists the privileges and permissions in the Content Directory privilege group:

Privilege	Includes Privileges	Permission	Description
Access Content Directory	-	Read on folders	User is able to perform the following actions: - Access folders and content on the Find tab. - Access personal folders. - Search for items available to users with the Basic Consumer role. - Search for reports by name or search for reports you use frequently. - View reports from the PowerCenter Designer or Workflow Manager.
Access Advanced Search	- Access Content Directory	Read on folders	User is able to perform the following actions: - Search for advanced items. - Search for reports you create or reports used by a specific user.
Manage Content Directory	- Access Content Directory	Read and Write on folders	User is able to perform the following actions: - Create folders. - Copy folder. - Cut and paste folders. - Rename folders.
Manage Content Directory	- Access Content Directory	Delete on folders	User is able to delete folders.
Manage Shared Documents	- Access Content Directory - Manage Content Directory	Read on folders Write on folders	User is able to manage shared documents in the folders.

Dashboards Privilege Group

Privileges in the Dashboards privilege group determine the tasks users can perform on dashboards in Data Analyzer.

The following table lists the privileges and permissions in the Dashboards privilege group:

Privilege	Includes Privileges	Permission	Description
View Dashboards	-	Read on dashboards	User is able to view contents of personal dashboards and public dashboards.
Manage Personal Dashboard	- View Dashboards	Read and Write on dashboards	User is able to manage the personal dashboard.
Create, Edit, and Delete Dashboards	- View Dashboards	Read and Write on dashboards	User is able to perform the following actions: - Create dashboards. - Edit dashboards.
Create, Edit, and Delete Dashboards	- View Dashboards	Delete on dashboards	User is able to delete dashboards.
Access Basic Dashboard Creation	- View Dashboards - Create, Edit, and Delete Dashboards	Read and Write on dashboards	User is able to perform the following actions: - Use basic dashboard configuration options. - Broadcast dashboards as links.
Access Advanced Dashboard Creation	- View Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation	Read and Write on dashboards	User is able to use all dashboard configuration options.

Indicators Privilege Group

Privileges in the Indicators privilege group determine the tasks users can perform with indicators.

The following table lists the privileges and permissions in the Indicators privilege group:

Privilege	Includes Privileges	Permission	Description
Interact with Indicators	-	Read on report Write on dashboard	User is able to use and interact with indicators.
Create Real-time Indicator	-	Read and Write on report Write on dashboard	User is able to perform the following actions: - Create an indicator on a real-time report. - Create gauge indicator.
Get Continuous, Automatic Real-time Indicator Updates	-	Read on report	User is able to view continuous, automatic, and animated real-time updates to indicators.

Manage Account Privilege Group

The privilege in the Manage Account privilege group determines the task users can perform in the Manage Account tab of Data Analyzer.

The following table lists the privilege and permission in the Manage Account privilege group:

Privilege	Includes Privileges	Permission	Description
Manage Personal Settings	-	-	User is able to configure personal account preferences.

Reports Privilege Group

Privileges in the Reports privilege group determine the tasks users can perform with reports in Data Analyzer.

The following table lists the privileges and permissions in the Reports privilege group:

Privilege	Includes Privileges	Permission	Description
View Reports	-	Read on report	View reports and related metadata.
Analyze Reports	- View Reports	Read on report	User is able to perform the following actions: - Analyze reports. - View report data, metadata, and charts.
Interact with Data	- View Reports - Analyze Reports	Read and Write on report	User is able to perform the following actions: - Access the toolbar on the Analyze tab and perform data-level tasks on the report table and charts. - Right-click on items on the Analyze tab.
Drill Anywhere	- View Reports - Analyze Reports - Interact with Data	Read on report	User is able to choose any attribute to drill into reports.
Create Filtersets	- View Reports - Analyze Reports - Interact with Data	Read and Write on report	User is able to create and save filtersets in reports.
Promote Custom Metric	- View Reports - Analyze Reports - Interact with Data	Write on report	User is able to promote custom metrics from reports to schemas.
View Query	- View Reports - Analyze Reports - Interact with Data	Read on report	User is able to view report queries.
View Life Cycle Metadata	- View Reports - Analyze Reports - Interact with Data	Write on report	User is able to edit time keys on the Time tab.

Privilege	Includes Privileges	Permission	Description
Create and Delete Reports	- View Reports	Write and Delete on report	User is able to create or delete reports.
Access Basic Report Creation	- View Reports - Create and Delete Reports	Write on report	User is able to perform the following actions: - Create reports using basic report options. - Broadcast the link to a report in Data Analyzer and edit the SQL query for the report.
Access Advanced Report Creation	- View Reports - Create and Delete Reports - Access Basic Report Creation	Write on report	User is able to perform the following actions: - Create reports using all available report options. - Broadcast report content as an email attachment and link. - Archive reports. - Create and manage Excel templates. - Set provider-based security for a report.
Save Copy of Reports	- View Reports	Write on report	User is able to use the Save As function to save the with another name.
Edit Reports	- View Reports	Write on report	User is able to edit reports.

Reporting and Dashboards Service Privileges (Deprecated)

Reporting and Dashboards Service privileges map to roles in Jaspersoft.

The Access Privilege group contains all the Reporting and Dashboards Service privileges.

The following table describes each privilege for the Reporting and Dashboards Service:

Privilege Name	Description
Administrator	Users assigned to the administrator privilege can perform the following tasks in JasperReports Server: - Create sub-organizations. - Create, modify, and delete users. - Create, modify, and delete roles. - Log in as any user in the organization. - Create, modify, and delete folders and repository objects of all types. - Assign roles to users, including the ROLE_ADMINISTRATOR role that grants organization administrator privileges. - Set access permissions on repository folders and objects. This privilege maps to the ROLE_ADMINISTRATOR role in Jaspersoft.
Superuser	Users assigned to the superuser privilege can perform all the tasks that a user with the administrator privilege can perform. In addition, users with the superuser privilege can perform the following tasks in JasperReports Server: - Create top-level organizations. - Create users who can access all organizations. - Assign the ROLE_SUPERUSER role that grants system administrator privileges. - Set the system-wide configuration parameters. This privilege maps to the ROLE_SUPERUSER role in Jaspersoft.
Normal User	Users assigned to the normal user privilege can view reports in JasperReports Server. This privilege maps to the ROLE_USER role in Jaspersoft.

For more information about the privileges associated with these roles in Jaspersoft, see the Jaspersoft documentation.

Deprecated Behavior

Effective in version 10.1, Informatica deprecated the Reporting and Dashboards Service, JasperReports Server, and the Reporting and Dashboards Service privileges. Informatica will drop support for them in a future release. You should create additional reports using a third-party reporting tool.

Scheduler Service Privileges

Scheduler Service privileges determine the actions that users can perform on schedules and scheduled jobs.

The following table describes the Scheduler Service privileges and required permissions:

Privilege	Description	Requires Permission On
Create Schedule	User can create schedules. To create a schedule, the user must also have the Application Administration privilege on the Data Integration Service.	- Scheduler Service - Data Integration Service that runs the jobs that the user wants to schedule
Edit Schedule	User can edit, pause, and resume schedules. To edit a schedule, the user must also have the Application Administration privilege on the Data Integration Service.	- Scheduler Service - Data Integration Service that runs the jobs that the user wants to schedule

Privilege	Description	Requires Permission On
Delete Schedule	User can delete schedules.	Scheduler Service
View Schedules	User can view the **Schedules** view and schedules.	Scheduler Service

Test Data Manager Service Privileges

Test Data Manager Service privileges determine the actions that users can perform using the Test Data Manager. A user with the privilege to perform certain actions requires permissions to perform the action on a particular object. Configure permissions on the Security tab of the Administrator tool.

The following table describes each Test Data Manager privilege group.

Privilege Group	Description
Administration	Includes privileges to create and manage connections, roles and assign privileges to users and user groups from the Informatica Administrator, manage repositories, add licenses, and set up workflow and project attributes. **Note:** Before you can create users and groups, the default Informatica administrator user must assign Security Administration privileges to the Test Data Administrator user.
Data Domains	Includes privileges to view and manage data domains in the Test Data Manager.
Data Masking	Includes privileges to view and manage masking rules and policy assignments in the Test Data Manager.
Data Subset	Includes privileges to view and manage subset objects including entities, groups and templates in the Test Data Manager.
Policies	Includes privileges to view and manage policies in the Test Data Manager.
Projects	Includes privileges to view and manage projects, audit and import metadata, and execute plans and workflows in the Test Data Manager.
Rules	Includes privileges to view and manage masking and generation rules in the Test Data Manager.
Data Generation	Includes privileges to view and manage test data generation in the Test Data Manager.

Administration Privilege Group

The privileges in the Administration privilege group determine the administration tasks that Test Data Administrators can perform.

The following table lists the privileges in the Administration privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
Manage Preferences	-	Write	User can perform the following actions on the Informatica Administrator and Test Data Manager: - Create roles. - Edit roles. - Delete roles. - View roles. - Associate roles to users. - Associate privileges to users. - Associate roles to user groups. - Associate privileges to user groups. - Add licenses. - Set up the TDM repository. - Set up the PowerCenter repository. - Set up data domain sensitivity levels. - Configure a test data repository. - Configure a test data mart. - Set up project custom attributes. - Set up workflow generation attributes. - Enable data discovery. - Set up profiling services. - View administration objects. - Configure keyword search indexing options.
View Connections	-	Read	User can perform the following actions on the Connections page in the Test Data Manager: - View connections. - Test connections.
Manage Connections	View Connections	Write	User can perform the following actions on the Connections page in the Test Data Manager: - Create connections. - Edit connections. - Delete connections. - View connections. - Test connections. - Configure a test data repository. - Configure a test data mart.

Connections Privilege Group

The privileges in the Connections privilege group determine the tasks that users can perform on the Connections page of the TDM Workbench. The following table lists the privileges in the Connections privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Connections	-	Read	User can view connections and test connections in the TDM Workbench.
Manage Connections	View Connections	Write	User can perform the following actions on the Connections page in the TDM Workbench: - Create connections. - Edit connections. - Delete connections. - View connections. - Test connections.

Data Domains Privilege Group

The privileges in the Data Domains privilege group determine the tasks that users can perform on data domains on the Policies page of the Test Data Manager.

The following table lists the privileges in the Data Domains privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Data Domains	-	Read	User can view data domains in the Test Data Manager.
Manage Data Domains	View Data Domains	Write	User can perform the following actions on data domains in the Test Data Manager: - Create data domains. - Edit data domains. - Delete data domains. - View data domains.

Data Masking Privilege Group

The privileges in the Data Masking privilege group determine the tasks that users can perform on the Project | Define | Data Masking view of the Test Data Manager. You can assign rules and polices to table columns from this view.

The following table lists the privileges in the Data Masking privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Data Masking	-	Read	User can view data masking assignments in the Test Data Manager.
Manage Data Masking	View Data Masking	Write	User can perform the following data masking assignment actions in the Test Data Manager: - Add rule and policy assignments. - Delete rule and policy assignments. - Override rule properties. - View data masking assignments.

Data Subset Privilege Group

The privileges in the Data Subset privilege group determine the tasks that users can perform on data subset objects in the Test Data Manager.

The following table lists the privileges in the Data Subset privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Data Subset	-	Read	User can perform the following data subset actions in the Test Data Manager: - View groups. - View templates - View entities. - View recent project objects.
Manage Data Subset	View Data Subset	Write	User can perform the following data subset actions in the Test Data Manager: - Create groups. - Edit groups. - Delete groups. - Add group parameters. - Create templates. - Edit templates. - Delete templates. - Add template parameters. - Create entity. - Edit entity. - Delete entity. - Add entity criteria. - Enable relationships. - Disable relationships. - Edit relationships - Review and act on changes. - Mark change review as complete.

Policies Privilege Group

The privileges in the Policies privilege group determine the tasks that users can perform on Policies in the Test Data Manager.

The following table lists the privileges in the Policies privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Policies	-	Read	User can view policies in the Test Data Manager.
Manage Policies	View Policies	Write	User can perform the following policy actions policies in the Test Data Manager: - Create policies. - Edit policies. - Delete policies. - View policies.

Projects Privilege Group

The privileges in the Projects privilege group determine the tasks that users can perform on Projects in the Test Data Manager.

The following table lists the privileges in the Projects privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Project	-	Read	User can perform the following actions on projects in the Test Data Manager: - View projects. - View plans. - View plan detail reports. - View plan audit reports. - View recent projects. - View data set versions.
Manage Project	View Project	Write	User can perform the following actions on projects in the Test Data Manager: - Create projects - Edit projects. - Delete projects - View projects. - Associate users to projects. - Associate user groups to projects. - Associate or remove rules to projects. - Associate or remove policies to projects - Create plans. - Edit plans. - Delete plans. - Generate plans. - Edit a data set version. - Delete a data set version.

Privilege	Includes Privileges	Permission	Description
Discover Project	-	Write	User can perform the following discover actions on projects in the Test Data Manager: - Classify tables. - Mark discovery as complete. - Associate data domains to columns. - Mark columns as restricted. - Mark columns as sensitive - Set similar value column - Remove similar value columns - Add primary keys - Remove primary Keys - Create logical constraints - View logical constraints - Edit logical Constraints - Delete Logical Constraints - View projects. - View profiled data domains. - Approve or reject profile data domains. - Mark data domain classification as complete. - View profiled primary keys. - Approve or reject profiled primary keys. - Mark primary key discovery as complete. - View profiled entities. - Approve or reject profiled entities. - Mark entity discovery as complete. - View project risk analysis. - View recent project sensitive data distribution.
Generate Project	-	Write	User can generate workflows in the Test Data Manager.
Execute Project	-	Write	User can perform the following execute actions on projects in the Test Data Manager: - Execute plans. - Execute workflows. - Stop workflows. - Abort workflows. - Recover workflows. - View plan execution. - Create a data set version. - Reset a data set version.
Monitor Project	-	Read	User can perform the following monitor actions on projects in the Test Data Manager: - Monitor project jobs. - View project job logs. - Monitor jobs across projects. - View job logs across projects.
Audit Project	-	Read	User can view recent activity on projects and plans in the Test Data Manager.
Import Metadata	-	Write	User can perform the following actions on projects in the Test Data Manager: - Import sources - Delete sources.

Note: A user with Manage Project privilege must have at least the following levels of privileges to be able to create a plan with each component.

- View connection from the Administration privilege group. To create a plan.
- View data subset from the Data Subset privilege group. To create a plan with subset components.
- View masking rules from the Rules privilege group. To create a plan with masking components.
- View generation rules from the Rules privilege group. To create a plan with generation components.

Rules Privilege Group

The privileges in the Rules privilege group determine the tasks that users can perform on data masking and data generation rules in the Test Data Manager.

The following table lists the privileges in the Data Masking privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Masking Rules	-	Read	User can view masking rules in the Test Data Manager.
Manage Masking Rules	View Masking Rules	Write	User can perform the following actions on data masking rules in the Test Data Manager: - Create masking rules. - Edit masking rules. - Delete masking rules. - View masking rules.
View Generation Rules	-	Read	User can view generation rules in the Test Data Manager.
Manage Generation Rules	View Generation Rules	Write	User can perform the following actions on data generation rules in the Test Data Manager: - Create generation rules. - Edit generation rules. - Delete generation rules. - View generation rules.

Data Generation Privilege Group

The privileges in the Data Generation privilege group determine the test data generation tasks that users can perform in the Test Data Manager.

The following table lists the privileges in the Data Generation privilege group and the permissions required to perform a task on an object:

Privilege	Includes Privileges	Permission	Description
View Data Generation	-	Read	User can view data generation rule assignments in the Test Data Manager.
Manage Data Generation	View Data Generation	Write	User can perform the following actions on data generation in the Test Data Manager: - View data generation rule assignments - Add data generation rule assignments. - Delete data generation rule assignments. - Override data generation rule assignments.

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 PowerCenter Repository Service. A domain can contain multiple PowerCenter Repository Services. You can assign the Developer role to a user for the Development PowerCenter Repository Service. You can assign a different role to that user for the Production PowerCenter Repository Service.

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.

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.

UMSM has the following types of roles:

- Administrator. This is a system-defined role that has privileges to administer the Administrator tool. With this role, you can create and manage user accounts, create the Ultra Messaging Service and configure it, configure UMSM components, and UM deployments.
- Operator. This is a custom role that has privileges to monitor UM deployments.

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, Analyst Service, Data Integration Service, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting 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.

When you assign the Administrator role to a user or group for the domain, Data Integration Service, or Model 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.

When you assign the Administrator role to a user or group for the domain or Ultra Messaging 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, Data Integration Service, or PowerCenter Repository Service, the user or group can complete some tasks that are determined by the Administrator role, not by privileges or permissions.

When you assign the Administrator role to a user or group for the domain or Data Integration Service, the user or group can complete some tasks that are determined by the Administrator role, not by privileges or permissions.

When you assign the Administrator role to a user or group for the domain or Ultra Messaging 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, Data Integration Service, or PowerCenter Repository Service and then grant the user or group full permissions on all domain or PowerCenter repository objects. However, this user or group cannot complete the tasks determined by the Administrator role.

You can assign a user or group all privileges for the domain or Data Integration Service and then grant the user or group full permissions on all domain objects. However, this user or group cannot complete the tasks determined by the Administrator role.

You can assign a user or group all privileges for the domain or Ultra Messaging Service and then grant the user or group full permissions on all domain 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, Data Integration Service, and PowerCenter Repository Service:

The following table lists the tasks determined by the Administrator role for the domain or Data Integration Service:

The following table lists the tasks determined by the Administrator role for the domain or Ultra Messaging Service:

Service	Tasks
Domain	- Configure domain properties. - 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.
Data Integration Service	- Upgrade the Data Integration Service using the Actions menu.
PowerCenter Repository Service	- Assign operating system profiles to repository folders if the PowerCenter Integration Service uses operating system profiles.* - Change the owner of folders and global objects.* - Configure folder and global object permissions.* - Connect to the PowerCenter Integration Service from the PowerCenter Client when running the PowerCenter Integration Service in safe mode. - Delete a PowerCenter 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 PowerCenter repository folder owner or global object owner can also complete these tasks.

Service	Tasks
Domain	- Configure domain properties. - Grant permission on the domain - Manage and purge log events. - Receive domain alerts. - View user activity log events.

Service	Tasks
Domain	- Configure domain properties. - Grant permission on the domain - Manage and purge log events. - Receive domain alerts. - View user activity log events.

Custom Roles

A custom role is a role that you can edit or delete.

By default, the Administrator tool includes the following custom roles:

- Analyst Service custom role
- Metadata Manager Service custom roles
- Operator custom role
- PowerCenter Repository Service custom roles
- Reporting Service custom roles
- Test Data Manager 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 Metadata Manager Service, PowerCenter Repository Service, or Reporting Service in the following situations:

  - The application service is disabled.
  - The PowerCenter 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 Metadata Manager Service, PowerCenter Repository Service, or Reporting Service.

You cannot assign privileges and roles to users and groups for an existing Metadata Manager Service, PowerCenter Repository Service, or Reporting Service in the following situations:

- The application service is disabled.
- The PowerCenter Repository Service is running in exclusive mode.

I cannot assign privileges to a user for an enabled Reporting Service.

Data Analyzer uses the user account name and security domain name in the format `UserName@SecurityDomain` to determine the length of the user login name. You cannot assign privileges or roles to a user for a Reporting Service when the combination of the user name, @ symbol, and security domain name exceeds 128 characters.

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 PowerCenter 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 PowerCenter Repository Service in the Administrator tool to perform the following actions in the Repository Manager:

- Perform an advanced purge of object versions at the PowerCenter 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 PowerCenter Repository Service running in exclusive mode.

The Service Manager might not have synchronized the list of users and groups in the PowerCenter repository with the list in the domain configuration database. To synchronize the list of users and groups, restart the PowerCenter Repository Service.

I am assigned all privileges in the Folders privilege group for the PowerCenter 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 PowerCenter Repository Service can complete the following folder management tasks:

- Assign operating system profiles to folders if the PowerCenter 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.

I am assigned the Administrator role for the Metadata Manager Service, but I cannot create or restore the Metadata Manager repository.

To create or restore the Metadata Manager repository, you must be in the default Administrator group. Users in the default Administrator group have more privileges than users that are assigned the Administrator role for an application service.

I am assigned the Load Resources privilege for the Metadata Manager Service, but I get an "insufficient privileges" error when I try to load Business Glossary resources.

To load Business Glossary resources, the Load Resource, Manage Resource, and View Model privileges are required. You also need write permission on any business glossary resource that you want to load.

CHAPTER 9

Permissions

This chapter includes the following topics:

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 PowerCenter Repository Service, but not on the Production PowerCenter Repository Service. The user can edit or remove the Development PowerCenter Repository Service, but not the Production PowerCenter 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:

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 Analyst tool Developer tool	You can assign permissions on connections defined in the Administrator tool, Analyst tool, or Developer tool. These tools share the connection permissions.

Object Type	Tool	Description
Data Analyzer objects	Data Analyzer	You can assign permissions on Data Analyzer folders, reports, dashboards, attributes, metrics, template dimensions, and schedules.
Domain objects	Administrator tool	You can assign permissions on the following domain objects: domain, folders, nodes, grids, licenses, application services, and operating system profiles.
Metadata Manager catalog objects	Metadata Manager	You can assign permissions on Metadata Manager folders and catalog objects.
Model repository projects	Analyst tool Developer tool	You can assign permissions on projects defined in the Analyst tool and Developer tool. These tools share project permissions.
PowerCenter repository objects	PowerCenter Client	You can assign permissions on PowerCenter folders, deployment groups, labels, queries, and connection objects.
SQL data service objects	Administrator tool	You can assign permissions on SQL data objects, such as SQL data services, virtual schemas, virtual tables, and virtual stored procedures.
Web service objects	Administrator tool	You can assign permissions on web services or web service operations.

Object Type	Tool	Description
Connection objects	Administrator tool Developer tool	You can assign permissions on connections defined in the Administrator tool or Developer tool. These tools share the connection permissions.
Domain objects	Administrator tool	You can assign permissions on the following domain objects: domain, folders, node, and application services.
Model repository projects	Developer tool	You can assign permissions on projects defined in the Developer tool.

You can use the Administrator tool to configure permissions on a domain object. You can assign permissions on the following domain objects:

- domain
- node
- application services

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.

Permissions that users inherit. When users have permission on a domain, they inherit permission on all objects in the domain. When groups have permission on a domain object, all subgroups and users belonging to the group inherit permission on the domain object.

Permissions that users inherit. When users have permission on a domain, they inherit permission on all objects in the domain. When groups have permission on a domain object, all subgroups and users belonging to the group inherit permission on the domain object.

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 Data Integration Service or PowerCenter 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 PowerCenter 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.

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.
Node	Enables Administrator tool users to view and edit the node properties.
Application Service	Enables Administrator tool users to view and edit the application service properties.
License	Enables Administrator tool users to view and edit the license properties.

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.
Node	Enables Administrator tool users to view and edit the node properties.

Domain Object Type	Description of Permission
Application Service	Enables Administrator tool users to view and edit the application service properties.
License	Enables Administrator tool users to view and edit the license properties.

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 header of Infomatica Administrator, click **Manage** > **Permissions**.

   The **Manage Permissions** dialog box appears.
2. Click the **Groups** or **Users** tab.
3. Enter a string to search for users and groups, and click the **Filter** button.
4. Select a user or group.
5. Select a domain object 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.
6. Click **Close**.

7. Or, click **Edit Permissions** to edit direct permissions.

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.

Note: If you revoke direct permission on an object, the user or group might still inherit permission from a parent group or object.

1. In the header of Infomatica Administrator, click **Manage** > **Permissions**.

   The **Manage Permissions** dialog box appears.
2. Click the **Groups** or **Users** tab.
3. Enter a string to search for users and groups and click the **Filter** button.
4. Select a user or group.
5. Select a domain object and click the **Edit Direct Permissions** button.

   The **Edit Direct Permissions** dialog box appears.
6. To assign permission on the object, select **Allow**.
7. To revoke permission on the object, select **Revoke**.

   You can view whether the permission is directly assigned or inherited by clicking **View Permission Details**.
8. Click **OK**.
9. Click **Close**.

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. PowerCenter users run workflows assigned to the operating system profile.

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, and click **Grant Permission**.

   The **Assign Users/Groups to Operating System Profile** dialog box displays all users or groups that do not have permission on the operating system profile.
4. Enter the filter conditions to search for users and groups, and click the **Filter** button.
5. Select a user or group, and click **Next**.
6. Select **Allow**, and click **Finish**.

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 Analyst tool, Developer tool, or Administrator tool.

You can configure permissions on a connection in the Developer tool or Administrator tool.

Any connection permission that is assigned to a user or group in one tool also applies in other tools. For example, you grant GroupA permission on ConnectionA in the Developer tool. GroupA has permission on ConnectionA in the Analyst tool and Administrator tool also.

Any connection permission that is assigned to a user or group in one tool also applies in other tools. For example, you grant GroupA permission on ConnectionA in the Developer tool. GroupA has permission on ConnectionA in the Administrator tool also.

The following Informatica components use the connection permissions:

- Administrator tool. Enforces read, write, and execute permissions on connections.
- Analyst tool. Enforces read, write, and execute permissions on connections.
- Informatica command line interface. Enforces read, write, and grant permissions on connections.
- Developer tool. Enforces read, write, and execute permissions on connections.
  For SQL data services, the Developer tool does not enforce connection permissions. Instead, it enforces column-level and pass-through security to restrict access to data.
- Data Integration Service. Enforces execute permissions when a user tries to preview data or run a mapping, scorecard, or profile.
- Data Integration Service. Enforces execute permissions when a user tries to preview data or run a mapping, or profile.

Note: You cannot assign permissions on the following connections: profiling warehouse, data object cache database, or Model repository.

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. 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, 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.
- Use the connection in mappings in the Developer tool.
- Create profiles in the Analyst tool on objects in the connection.

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. 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 **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.
7. Click **Close**.
8. 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.

SQL Data Service Permissions

End users can connect to an SQL data service through a JDBC or ODBC client tool. After connecting, users can run SQL queries against virtual tables in an SQL data service, or users can run a virtual stored procedure in an SQL data service. Permissions control the level of access that a user has to an SQL data service.

You can assign permissions to users and groups on the following SQL data service objects:

- SQL data service
- Virtual table
- Virtual stored procedure

When you assign permissions on an SQL data service object, the user or group inherits the same permissions on all objects that belong to the SQL data service object. For example, you assign a user select permission on an SQL data service. The user inherits select permission on all virtual tables in the SQL data service.

You can deny permissions to users and groups on some SQL data service objects. When you deny permissions, you configure exceptions to the permissions that users and groups might already have. For example, you cannot assign permissions to a column in a virtual table, but you can deny a user from running an SQL SELECT statement that includes the column.

Types of SQL Data Service Permissions

You can assign the following permissions to users and groups:

- Grant permission. Users can grant and revoke permissions on the SQL data service objects using the Administrator tool or using the *infacmd* command line program.
- Execute permission. Users can run virtual stored procedures in the SQL data service using a JDBC or ODBC client tool.
- Select permission. Users can run SQL SELECT statements on virtual tables in the SQL data service using a JDBC or ODBC client tool.

Some permissions are not applicable for all SQL data service objects.

The following table describes the permissions for each SQL data service object:

Object	Grant Permission	Execute Permission	Select Permission
SQL data service	Grant and revoke permission on the SQL data service and all objects within the SQL data service.	Run all virtual stored procedures in the SQL data service.	Run SQL SELECT statements on all virtual tables in the SQL data service.
Virtual table	Grant and revoke permission on the virtual table.	-	Run SQL SELECT statements on the virtual table.
Virtual stored procedure	Grant and revoke permission on the virtual stored procedure.	Run the virtual stored procedure.	-

Assigning Permissions on an SQL Data Service

When you assign permissions on an SQL data service object, you define the level of access a user or group has to the 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 SQL data service object.
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 SQL data service 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 SQL Data Service

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 SQL data service 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 **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 SQL Data Service

You can edit direct permissions on an SQL data service 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 SQL data service 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 SQL Data Service

You can explicitly deny permissions on some SQL data service objects. When you deny a permission on an object in an SQL data service, you are applying an exception to the effective permission.

To deny permissions use one of the following infacmd commands:

- infacmd sql SetStoredProcedurePermissions. Denies Execute or Grant permissions at the stored procedure level.
- infacmd sql SetTablePermissions. Denies Select and Grant permissions at the virtual table level.
- infacmd sql SetColumnPermissions. Denies Select permission at the column level.

Each command has options to apply permissions (-ap) and deny permissions (-dp). The SetColumnPermissions command does not include the apply permissions option.

Note: You cannot deny permissions from the Administrator tool.

The Data Integration Service verifies permissions before running SQL queries and stored procedures against the virtual database. The Data Integration Service validates the permissions for users or groups starting at the SQL data service level. When permissions apply to a parent object in an SQL data service, the child objects inherit the permission. The Data Integration Service checks for denied permissions at the column level.

Column Level Security

An administrator can deny access to columns in a virtual table of an SQL data object. The administrator can configure the Data Integration Service behavior for queries against a restricted column.

The following results might occur when the user queries a column that the user does not have permissions for:

- The query returns a substitute value instead of the data. The query returns a substitute value in each row that it returns. The substitute value replaces the column value through the query. If the query includes filters or joins, the results substitute appears in the results.
- The query fails with an insufficient permission error.

For more information about configuring security for SQL data services, see the Informatica How-To Library article "How to Configure Security for SQL Data Services": https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf.

Restricted Columns

When you configure column level security, set a column option that determines what happens when a user selects the restricted column in a query. You can substitute the restricted data with a default value. Or, you can fail the query if a user selects the restricted column.

For example, an Administrator denies a user access to the salary column in the Employee table. The Administrator configures a substitute value of 100,000 for the salary column. When the user selects the salary column in an SQL query, the Data Integration Service returns 100,000 for the salary in each row.

Run the infacmd sql UpdateColumnOptions command to configure the column options. You cannot set column options in the Administrator tool.

When you run infacmd sql UpdateColumnOptions, enter the following options:

ColumnOptions.DenyWith=*option*

Determines whether to substitute the restricted column value or to fail the query. If you substitute the column value, you can choose to substitute the value with NULL or with a constant value. Enter one of the following options:

- ERROR. Fails the query and returns an error when an SQL query selects a restricted column.
- NULL. Returns null values for a restricted column in each row.
- VALUE. Returns a constant value in place of the restricted column in each row. Configure the constant value in the ColumnOptions.InsufficientPermissionValue option.

ColumnOptions.InsufficientPermissionValue=*value*

Substitutes the restricted column value with a constant. The default is an empty string. If the Data Integration Service substitutes the column with an empty string, but the column is a number or a date, the query returns errors. If you do not configure a value for the DenyWith option, the Data Integration Service ignores the InsufficientPermissionValue option.

To configure a substitute value for a column, enter the command with the following syntax:

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees_SQL -t Employee -c Salary -o
ColumnOptions.DenyWith=VALUE ColumnOptions.InsufficientPermissionValue=100000
```

If you do not configure either option for a restricted column, default is not to fail the query. The query runs and the Data Integration Service substitutes the column value with NULL.

Adding Column Level Security

Configure column level security with the infacmd sql SetColumnPermissions command. You cannot set column level security from the Administrator tool.

An Employee table contains FirstName, LastName, Dept, and Salary columns. You enable a user to access the Employee table but restrict the user from accessing the salary column.

To restrict the user from the salary column, disable the Data Integration Service and enter an infacmd similar to the following command:

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd
Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

The following SQL statements return NULL in the salary column:

```
Select * from Employee
Select LastName, Salary from Employee
```

The default behavior is to return null values.

Web Service Permissions

End users can send web service requests and receive web service responses through a web service client. Permissions control the level of access that a user has to a web service.

You can assign permissions to users and groups on the following web service objects:

- Web service
- Web service operation

When you assign permissions on a web service object, the user or group inherits the same permissions on all objects that belong to the web service object. For example, you assign a user execute permission on a web service. The user inherits execute permission on web service operations in the web service.

You can deny permissions to users and groups on a web service operation. When you deny permissions, you configure exceptions to the permissions that users and groups might already have. For example, a user has execute permissions on a web service which has three operations. You can deny a user from running one web service operation that belongs to the web service.

Types of Web Service Permissions

You can assign the following permissions to users and groups:

- Grant permission. Users can manage permissions on the web service objects using the Administrator tool or using the *infacmd* command line program.
- Execute permission. Users can send web service requests and receive web service responses.

The following table describes the permissions for each web service object:

Object	Grant Permission	Execute Permission
Web service	Grant and revoke permission on the web service and all web service operations within the web service.	Send web service requests and receive web service responses from all web service operations within the web service.
Web service operation	Grant, revoke, and deny permission on the web service operation.	Send web service requests and receive web service responses from the web service operation.

Assigning Permissions on a Web Service

When you assign permissions on a web service object, you define the level of access a user or group has to the 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 web service object.
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 SQL data service 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 a Web Service

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 web service 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 **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 a Web Service

You can edit direct permissions on a web service for a user or group. When you edit permissions on a web service object, you can deny permissions on the object. 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 web service 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.
   - Select **Deny** to deny a permission on a web service object.
   - 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**.

CHAPTER 10

Audit Reports

This chapter includes the following topics:

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 as Commands

To run *infacmd as* commands, users must have one of the listed sets of domain privileges, Analyst Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd as* commands:

infacmd as Command	Privilege Group	Privilege Name	Permission On...
CreateAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
CreateService	Domain Administration	Manage Service	Domain or node where Analyst Service runs
DeleteAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
ListServiceOptions	-	-	Analyst Service
ListServiceProcessOptions	-	-	Analyst Service
UpdateServiceOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs
UpdateServiceProcessOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs

infacmd dis Commands

To run *infacmd dis* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd dis* commands:

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
BackupApplication	Application Administration	Manage Applications	Application
CancelDataObjectCacheRefresh	-	-	-
CreateService	Domain Administration	Manage Services	Domain or node where Data Integration Service runs
DeployApplication	Application Administration	Manage Applications	Application
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListComputeOptions	Domain Administration	Manage Services	Data Integration Service
ListDataObjectOptions	-	-	-
ListServiceOptions	Domain Administration	Manage Services	Data Integration Service

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
ListServiceProcessOptions	Domain Administration	Manage Services	Data Integration Service
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Application Administration	Manage Applications	Application
RestoreApplication	Application Administration	Manage Applications	Application
StartApplication	Application Administration	Manage Applications	Application
StopApplication	Application Administration	Manage Applications	Application
stopBlazeService	Application Administration	Manage Applications	Application
UndeployApplication	Application Administration	Manage Applications	Application
UpdateApplication	Application Administration	Manage Applications	Application
UpdateApplicationOptions	Application Administration	Manage Applications	Application
UpdateDataObjectOptions	Application Administration	Manage Applications	-
UpdateComputeOptions	Domain Administration	Manage Services	Data Integration Service
UpdateServiceOptions	Domain Administration	Manage Services	Data Integration Service
UpdateServiceProcessOptions	Domain Administration	Manage Services	Data Integration Service

infacmd es commands

Users must be assigned the Administrator role for the domain to run the following infacmd es commands:

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd ipc Commands

To run *infacmd ipc* commands, users must have one of the listed Model repository object permissions.

The following table lists the required privileges and permissions for *infacmd ipc* commands:

infacmd ipc Command	Privilege Group	Privilege Name	Permission On...
ExportToPC	-	-	Read on the folder that creates reference tables to be exported
genReuseReportFromPC	Tools	Access Repository Manager	-

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.

Users must be assigned the Administrator role for the domain to run the following commands:

- AddDomainLink
- AssignGroupPermission (on domain)
- AssignGroupPermission (on operating system profiles)
- AddServiceLevel
- AssignUserPermission (on domain)
- AssignUserPermission (on operating system profiles)
- CreateConnection
- CreateOSProfile
- PurgeLog
- RemoveDomainLink
- RemoveOSProfile
- RemoveServiceLevel
- SwitchToGatewayNode
- SwitchToWorkerNode
- UpdateDomainOptions
- UpdateGatewayInfo
- UpdateServiceLevel
- UpdateSMTPOptions

Users must be assigned the Administrator role for the domain to run the UpdateGatewayInfo command.

The following table lists the required privileges and permissions for *infacmd isp* commands:

infacmd isp Command	Privilege Group	Privilege Name	Permission On
GetNodeName	-	-	Node
UpdateGatewayInfo	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
AddAlertUser (for your user account)	-	-	-
AddAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-
AddConnectionPermissions	-	-	Grant on connection
AddDomainLink	-	-	-
AddDomainNode	Domain Administration	Manage Nodes and Grids	Domain and node
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)	-	-	-
AddGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting 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	-	-	-
AssignUserPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object

infacmd isp Command	Privilege Group	Privilege Name	Permission On
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, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignUserToGroup	Security Administration	Manage Users, Groups, and Roles	-
AssignedToLicense	Domain Administration	Manage Services	License object and application service
AssignISTOMMService	Domain Administration	Manage Services	Metadata Manager Service
AssignLicense	Domain Administration	Manage Services	License object and application service
AssignRoleToGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRoleToUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRSToWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
ConvertLogFile	-	-	Domain or application service

infacmd isp Command	Privilege Group	Privilege Name	Permission On
CreateFolder	Domain Administration	Manage Domain Folders	Domain or parent folder
CreateConnection	-	-	-
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 PowerCenter Integration Service runs, license object, and associated PowerCenter Repository Service
CreateMMService	Domain Administration	Manage Services	Domain or parent folder, node where Metadata Manager Service runs, license object, and associated PowerCenter Integration Service and PowerCenter Repository Service
CreateOSProfile	-	-	-
CreateReportingService	Domain Administration	Manage Services	Domain or parent folder, node where Reporting Service runs, license object, and the application service selected for reporting
CreateRepositoryService	Domain Administration	Manage Services	Domain or parent folder, node where PowerCenter Repository Service runs, and license object
CreateRole	Security Administration	Manage Users, Groups, and Roles	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
CreateSAPBWService	Domain Administration	Manage Services	Domain or parent folder, node or grid where SAP BW Service runs, license object, and associated PowerCenter Integration Service
CreateUser	Security Administration	Manage Users, Groups, and Roles	-
CreateWSHubService	Domain Administration	Manage Services	Domain or parent folder, node or grid where Web Services Hub runs, license object, and associated PowerCenter Repository Service
DisableNodeResource	Domain Administration	Manage Nodes and Grids	Node
DisableService (for Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service and associated PowerCenter Integration Service and PowerCenter Repository Service
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 Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service, and associated PowerCenter Integration Service and PowerCenter Repository Service
EnableService (for all other application services)	Domain Administration	Manage Service Execution	Application service

infacmd isp Command	Privilege Group	Privilege Name	Permission On
EnableServiceProcess	Domain Administration	Manage Service Execution	Application service
EnableUser	Security Administration	Manage Users, Groups, and Roles	-
ExportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ExportDomainObjects (for connections)	Domain Administration	Manage Connections	Read on connections
ExportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
generateHadoopConnectionFromHiveConection	-	-	-
GetFolderInfo	-	-	Folder
GetLastError	-	-	Application service
GetLog	-	-	Domain or application service
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 users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ImportDomainObjects (for connections)	Domain Administration	Manage Connections	Write on connections
ImportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
ListAlertUsers	-	-	Domain
ListAllGroups	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Read on connection
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
ListConnectionPermissions by Group	-	-	-
ListConnectionPermissions by User	-	-	-
ListDomainLinks	-	-	Domain
ListDomainOptions	-	-	Domain
ListFolders	-	-	Folders
ListGridNodes	-	-	-
ListGroupsForUser	-	-	Domain
ListGroupPermissions	-	-	-
ListGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
ListLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	-
ListLicenses	-	-	License objects
listMonitoringOptions	Monitoring	Monitoring Configuration	Domain
ListNodeOptions	-	-	Node
ListNodes	-	-	-
ListNodeResources	-	-	Node
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domain
ListRolePrivileges	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
ListSecurityDomains	Security Administration	Manage Users, Groups, and Roles	-
ListServiceLevels	-	-	Domain
ListServiceNodes	-	-	Application service
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	Domain
ListUserPermissions	-	-	-
ListUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting 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	-	-	-
purgeMonitoringData	Monitoring	Monitoring Configuration	Domain
RemoveAlertUser (for your user account)	-	-	-
RemoveAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-
RemoveConnection	-	-	Write on connection
RemoveConnectionPermissions	-	-	Grant on connection
RemoveDomainLink	-	-	-
RemoveFolder	Domain Administration	Manage Domain Folders	Domain or parent folder and folder being removed

infacmd isp Command	Privilege Group	Privilege Name	Permission On
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, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting 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	-
RemoveUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
RenameConnection	-	-	Write on connection
ResetPassword (for your user account)	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On
ResetPassword (for other users)	Security Administration	Manage Users, Groups, and Roles	-
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	PowerCenter Integration Service and Metadata Manager Service
UnassignLicense	Domain Administration	Manage Services	License object and application service
UnAssignRoleFromGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
UnAssignRoleFromUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
UnassignRSWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
UnassociateDomainNode	Domain Administration	Manage Nodes and Grids	Node
UpdateConnection	-	-	Write on connection

infacmd isp Command	Privilege Group	Privilege Name	Permission On
UpdateDomainOptions	-	-	-
UpdateFolder	Domain Administration	Manage Domain Folders	Folder
UpdateGatewayInfo	-	-	-
UpdateGrid	Domain Administration	Manage Nodes and Grids	Grid and nodes
UpdateIntegrationService	Domain Administration	Manage Services	PowerCenter Integration Service
UpdateLicense	Domain Administration	Manage Services	License object
UpdateMMService	Domain Administration	Manage Services	Metadata Manager Service
updateMonitoringOptions	Monitoring	Monitoring Configuration	Domain
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
UpdateReportingService	Domain Administration	Manage Services	Reporting Service
UpdateRepositoryService	Domain Administration	Manage Services	PowerCenter Repository Service
UpdateSAPBWService	Domain Administration	Manage Services	SAP BW Service
UpdateServiceLevel	-	-	-
UpdateServiceProcess	Domain Administration	Manage Services	PowerCenter Integration Service Each node added to the PowerCenter Integration Service
UpdateSMTPOptions	-	-	-
UpdateWSHubService	Domain Administration	Manage Services	Web Services Hub

infacmd mrs Commands

To run *infacmd mrs* commands, users must have one of the listed sets of domain privileges, Model Repository Service privileges, and Model repository object permissions.

Users can run the following commands, which are related to locking and versioning operations, on objects they own. Running the commands on objects that other users own requires the Manage Team-based Development privilege:

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

The following table lists the required privileges and permissions for *infacmd mrs* commands:

infacmd mrs Command	Privilege Group	Privilege Name	Permission On...
BackupContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CheckInObject	Domain Administration	Manage Team-based Development	The Model Repository Service
CreateContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CreateFolder	Domain Administration	For Developer tool: - Access Developer For Analyst tool: - Access Analyst - Discovery workspace access	The Model Repository Service
CreateProject	Domain Administration	Create, Edit and Delete Projects	The Model Repository Service
CreateService	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
DeleteContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
DeleteFolder	Domain Administration	For Developer tool: - Access Developer For Analyst tool: - Access Analyst - Discovery workspace access	The Model Repository Service

infacmd mrs Command	Privilege Group	Privilege Name	Permission On...
DeleteProject	Domain Administration	Create, Edit and Delete Projects	The Model Repository Service
ListBackupFiles	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListCheckedOutObjects	Domain Administration	Manage Team-based Development	The Model Repository Service
ListFolders	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListLockedObjects	Domain Administration	Manage Team-based Development	The Model Repository Service
ListProjects	Domain Administration	For Developer tool: - Access Developer For Analyst tool: - Access Analyst - Discovery workspace access	Domain or node where the Model Repository Service runs
ListServiceOptions	-	-	The Model Repository Service
ListServiceProcessOptions	-	-	The Model Repository Service
PopulateVCS	Domain Administration	Manage Team-based Development	The Model Repository Service
ReassignCheckedOutObject	Domain Administration	Manage Team-based Development	The Model Repository Service
RebuildDependencyGraph	-	-	The Model Repository Service
RenameFolder	Domain Administration	For Developer tool: - Access Developer For Analyst tool: - Access Analyst - Discovery workspace access	The Model Repository Service
RestoreContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
UndoCheckout	Domain Administration	Manage Team-based Development	The Model Repository Service
UnlockObject	Domain Administration	Manage Team-based Development	The Model Repository Service

infacmd mrs Command	Privilege Group	Privilege Name	Permission On...
UpdateServiceOptions	Domain Administration	Manage Service	The Model Repository Service
UpdateServiceProcessOptions	Domain Administration	Manage Service	The Model Repository Service
UpgradeContents	Model Repository Service Administration	Manage Service	The Model Repository Service

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...
GetRequestLog	-	-	-
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	Execute on connection objects used by the mapping

infacmd oie Commands

To run *infacmd oie* commands, users must have one of the listed Model repository object permissions.

The following table lists the required permissions for *infacmd oie* commands:

infacmd oie Command	Privilege Group	Privilege Name	Permission On...
ExportObjects	-	-	Read on project
ImportObjects	-	-	Write on project

infacmd ps Commands

To run *infacmd ps* commands, users must have one of the listed sets of profiling privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd ps* commands:

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
CreateWH	-	-	-
DropWH	-	-	-
Execute	-	-	Read on project Execute on the source connection object
List	-	-	Read on project
Purge	-	-	Read and write on project

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
CreateWH	-	-	-
DropWH	-	-	-

infacmd pwx Commands

To run *infacmd pwx* commands, users must have one of the listed sets of PowerExchange application service permissions and privileges.

The following table lists the required privileges and permissions for *infacmd pwx* commands:

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
CloseForceListener	Management Commands	closeforce	-
CloseListener	Management Commands	close	-
CondenseLogger	Management Commands	condense	-
CreateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
CreateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
DisplayAllLogger	Informational Commands	displayall	-
DisplayCPULogger	Informational Commands	displaycpu	-
DisplayEventsLogger	Informational Commands	displayevents	-
DisplayMemoryLogger	Informational Commands	displaymemory	-
DisplayRecordsLogger	Informational Commands	displayrecords	-
DisplayStatusLogger	Informational Commands	displaystatus	-
FileSwitchLogger	Management Commands	fileswitch	-
ListTaskListener	Informational Commands	listtask	-
ShutDownLogger	Management Commands	shutdown	-
StopTaskListener	Management Commands	stoptask	-
UpdateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
UpdateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs

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 rtm Commands

To run *infacmd rtm* commands, users must have one of the listed sets of Model Repository Service privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd rtm* commands:

infacmd rtm Command	Privilege Group	Privilege Name	Permission On...
Deployimport	-	-	-
Export	-	-	Read on the project that contains reference tables to be exported
Import	-	-	Read and Write on the project where reference tables are imported

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

infacmd sch Command	Privilege Group	Privilege Name	Permission On
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 sql Commands

To run *infacmd sql* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd sql* commands:

infacmd sql Command	Privilege Group	Privilege Name	Permission On...
ExecuteSQL	-	-	Based on objects that you want to access in your SQL statement
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-

infacmd sql Command	Privilege Group	Privilege Name	Permission On...
RenameSQLDataService	Application Administration	Manage Applications	-
SetColumnPermissions	-	-	Grant on the object
SetSQLDataServicePermissions	-	-	Grant on the object
SetStoredProcedurePermissions	-	-	Grant on the object
SetTablePermissions	-	-	Grant on the object
StartSQLDataService	Application Administration	Manage Applications	-
StopSQLDataService	Application Administration	Manage Applications	-
UpdateColumnOptions	Application Administration	Manage Applications	-
UpdateSQLDataServiceOptions	Application Administration	Manage Applications	-
UpdateTableOptions	Application Administration	Manage Applications	-

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 PowerCenter Repository Service privileges and PowerCenter repository object permissions.

When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter 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	-	-	-
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, PowerCenter Repository Service privileges, domain object permissions, and PowerCenter repository object permissions.

Users must be the object owner or have the Administrator role for the PowerCenter Repository Service to run the following commands:

- AssignPermission
- ChangeOwner
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- 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
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

pmrep Command	Privilege Group	Privilege Name	Permission
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 PowerCenter Repository Service
CreateConnection	Global Objects	Create Connections	-
CreateDeploymentGroup	Global Objects	Manage Deployment Groups	-
CreateFolder	Folders	Create	-
CreateLabel	Global Objects	Create Labels	-
Delete	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
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

pmrep Command	Privilege Group	Privilege Name	Permission
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
Notify	Domain Administration	Manage Services	Permission on PowerCenter 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

pmrep Command	Privilege Group	Privilege Name	Permission
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 PowerCenter Repository Service
Register	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
RegisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Restore	Domain Administration	Manage Services	Permission on PowerCenter 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
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

pmrep Command	Privilege Group	Privilege Name	Permission
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 PowerCenter Repository Service
UnregisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter 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 PowerCenter Repository Service
UpdateTargPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Upgrade	Domain Administration	Manage Services	Permission on PowerCenter 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 topics:

Analyst Service Custom Role

The Analyst Service Business Glossary Consumer is a custom Analyst Service role.

The following table lists the default privilege assigned to the Analyst Service Business Glossary Consumer custom role:

Privilege Group	Privilege Name
Workspace Access	Glossary Workspace

Metadata Manager Service Custom Roles

Metadata Manager Service custom roles include the Metadata Manager Advanced User, Metadata Manager Basic User, and Metadata Manager Intermediate User roles.

Metadata Manager Advanced User

The following table lists the default privileges assigned to the Metadata Manager Advanced User custom role:

Privilege Group	Privilege Name
Catalog	- Share Shortcuts - View Lineage - View Related Catalogs - View Reports - View Profile Results - View Catalog - View Relationships - Manage Relationships - View Comments - Post Comments - Delete Comments - View Links - Manage Links - View Glossary - Manage Objects
Load	- View Resource - Load Resource - Manage Schedules - Purge Metadata - Manage Resource
Model	- View Model - Manage Model - Export/Import Models
Security	Manage Catalog Permissions

Metadata Manager Basic User

The following table lists the default privileges assigned to the Metadata Manager Basic User custom role:

Privilege Group	Privilege Name
Catalog	- View Lineage - View Related Catalogs - View Catalog - View Relationships - View Comments - View Links
Model	View Model

Metadata Manager Intermediate User

The following table lists the default privileges assigned to the Metadata Manager Intermediate User custom role:

Privilege Group	Privilege Name
Catalog	- View Lineage - View Related Catalogs - View Reports - View Profile Results - View Catalog - View Relationships - View Comments - Post Comments - Delete Comments - View Links - Manage Links - View Glossary
Load	- View Resource - Load Resource
Model	View Model

Operator Custom Role

The Operator custom role includes privileges for managing, scheduling, and monitoring application services.

The following table lists the default privileges assigned to the Operator custom role:

Privilege Group	Privilege Name
Application Administration	Manage Applications
Domain Administration	Manage Service Execution
Model Repository Service Administration	Manage Team-based Development
Monitoring	The Monitoring privilege group includes the following privileges: - View: View Jobs of Other Users - View: View Statistics - View: View Reports - Access Monitoring: Access from Analyst Tool - Access Monitoring: Access from Developer Tool - Access Monitoring: Access from Administrator Tool - Perform Actions on Jobs **Note:** In a domain that uses Kerberos authentication, users must also have the Administrator role for the Model Repository Service that is configured for monitoring.

Privilege Group	Privilege Name
Scheduler	The Scheduler privilege group includes the following privileges: - Manage Scheduled Jobs: Create Schedule - Manage Scheduled Jobs: Delete Schedule - Manage Scheduled Jobs: Edit Schedule - Manage Scheduled Jobs: View Schedules
Tools	Access Informatica Administrator

PowerCenter Repository Service Custom Roles

The PowerCenter Repository Service custom roles include the PowerCenter Connection Administrator, PowerCenter Developer, PowerCenter Operator, and PowerCenter Repository Folder Administrator.

PowerCenter Connection Administrator

The following table lists the default privileges assigned to the PowerCenter Connection Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Manager
Global Objects	Create Connections

PowerCenter Developer

The following table lists the default privileges assigned to the PowerCenter Developer custom role:

Privilege Group	Privilege Name
Tools	- Access Designer - Access Workflow Manager - Access Workflow Monitor
Design Objects	- Create, Edit, and Delete - Manage Versions
Sources and Targets	- Create, Edit, and Delete - Manage Versions
Run-time Objects	- Create, Edit, and Delete - Execute - Manage Versions - Monitor

PowerCenter Operator

The following table lists the default privileges assigned to the PowerCenter Operator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Monitor
Run-time Objects	- Execute - Manage Execution - Monitor

PowerCenter Repository Folder Administrator

The following table lists the default privileges assigned to the PowerCenter 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

Reporting Service Custom Roles (Deprecated)

The Reporting Service custom roles include the Reporting Service Advanced Consumer, Reporting Service Advanced Provider, Reporting Service Basic Consumer, Reporting Service Basic Provider, Reporting Service Intermediate Consumer, Reporting Service Read Only Consumer, and Reporting Service Schema Designer.

Effective in version 10.1, Informatica deprecated the Reporting Service and the reporting service custom roles. Informatica will drop support for the Reporting Service in a future release.

Reporting Service Advanced Consumer (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Advanced Consumer custom role:

Privilege Group	Privilege Name
Administration	- Maintain Schema - Export/Import XML Files - Manage User Access - Set Up Schedules and Tasks - Manage System Properties - Set Up Query Limits - Configure Real-time Message Streams
Alerts	- Receive Alerts - Create Real-time Alerts - Set up Delivery Options
Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
Dashboard	- View Dashboards - Manage Personal Dashboards
Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

Reporting Service Advanced Provider (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Advanced Provider custom role:

Privilege Group	Privilege Name
Administration	Maintain Schema
Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search

Privilege Group	Privilege Name
Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation - Access Advanced Dashboard Creation
Indicators	- Interact With Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
Manage Accounts	Manage Personal Settings
Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

Reporting Service Basic Consumer (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Basic Consumer custom role:

Privilege Group	Privilege Name
Alerts	- Receive Alerts - Set Up Delivery Options
Communication	- Print - Email Object Links - Export - View Discussions - Add Discussions - Give Feedback
Content Directory	Access Content Directory
Dashboards	View Dashboards

Privilege Group	Privilege Name
Manage Account	Manage Personal Settings
Reports	- View Reports - Analyze Reports

Reporting Service Basic Provider (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Basic Provider custom role:

Privilege Group	Privilege Name
Administration	Maintain Schema
Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	- Print - Email Object Links - Email Object Contents - Export - Export To Excel or CSV - Export To Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation
Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

Reporting Service Intermediate Consumer (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Intermediate Consumer custom role:

Privilege Group	Privilege Name
Alerts	- Receive Alerts - Set Up Delivery Options
Communication	- Print - Email Object Links - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	Access Content Directory
Dashboards	- View Dashboards - Manage Personal Dashboards
Indicators	- Interact with Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	- View Reports - Analyze Reports - Interact with Data - View Life Cycle Metadata - Save Copy of Reports

Reporting Service Read Only Consumer (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Read Only Consumer custom role:

Privilege Group	Privilege Name
Reports	View Reports

Reporting Service Schema Designer (Deprecated)

The following table lists the default privileges assigned to the Reporting Service Schema Designer custom role:

Privilege Group	Privilege Name
Administration	- Maintain Schema - Set Up Schedules and Tasks - Configure Real-time Message Streams
Alerts	- Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	- Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	- Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search

Privilege Group	Privilege Name
Dashboards	- View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards
Indicators	- Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
Manage Accounts	Manage Personal Settings
Reports	- View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

Test Data Manager Service Custom Roles

The Test Data Manager Service custom roles include the Test Data Administrator, Test Data Developer, Test Data Project DBA, Test Data Project Developer, Test Data Project Owner, Test Data Risk Manager, and Test Data Specialist.

Test Data Administrator

The following table lists the default privileges assigned to the Test Data Administrator custom role:

Privilege Group	Privilege Name
Projects	Audit Project
Administration	- View Connections - Manage Connections

Test Data Developer

The following table lists the default privileges assigned to the Test Data Developer custom role:

Privilege Group	Privilege Name
Policies	- View Policies - Manage Policies
Rules	- View Masking Rules - Manage Masking Rules - View Generation Rules
Data Domains	- View Data Domains - Manage Data Domains
Projects	Audit project

Test Data Project DBA

The following table lists the default privileges assigned to the Test Data Project DBA custom role:

Privilege Group	Privilege Name
Projects	- View Project - Execute Project - Monitor Project - Audit Project
Administration	- View Connections - Manage Connections

Test Data Project Developer

The following table lists the default privileges assigned to the Test Data Project Developer custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	- View Masking Rules - View Generation Rules
Data Domains	View Data Domains
Projects	- View Project - Discover Project - Execute Project - Monitor Project - Audit Project - Import Metadata
Data Masking	- View Data Masking - Manage Data Masking

Privilege Group	Privilege Name
Data Subset	- View Data Subset - Manage Data Subset
Data Generation	- View Data Generation - Manage Data Generation
Administration	- View Connections - Manage Connections

Test Data Project Owner

The following table lists the default privileges assigned to the Test Data Project Owner custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	- View Masking Rules - View Generation Rules
Data Domains	View Data Domains
Projects	- View Project - Manage Project - Discover Project - Execute Project - Monitor Project - Audit Project - Import Metadata
Data Masking	- View Data Masking - Manage Data Masking
Data Subset	- View Data Subset - Manage Data Subset
Data Generation	- View Data Generation - Manage Data Generation
Administration	- View Connections - Manage Connections

Test Data Risk Manager

The following table lists the default privileges assigned to the Test Data Risk Manager custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	- View Masking Rules - View Generation Rules

Privilege Group	Privilege Name
Data Domains	View Data Domains
Projects	Audit project

Test Data Specialist

The following table lists the default privileges assigned to the Test Data Specialist custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	- View Masking Rules - Manage Masking Rules - View Generation Rules - Manage Generation Rules
Data Domains	- View Data Domains - Manage Data Domains
Projects	- Manage Project - View Project - Discover Project - Execute Project - Monitor Project - Audit Project - Import Metadata
Data Masking	- View Data Masking - Manage Data Masking
Data Subset	- View Data Subset - Manage Data Subset
Data Generation	- View Data Generation - Manage Data Generation
Administration	- View Connections - Manage Connections

Note: If you have upgraded to Informatica service 9.6.1 HotFix 2 from Informatica service 9.6.1, a user with the Test Data Specialist role cannot create or delete data generation rules. The role does not include the Manage Data Generation privilege. To enable users with this role to create and delete data generation rules, you must manually edit the role. Log in to the Administrator tool and edit the Test Data Manager service custom role to include the Manage Generation Rules privilege from the Rules privilege group.

APPENDIX C

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

INDEX

E

F

G

I

K

L

R

S

T

U

V

W