Secure Communication Requirements
Abstract
Informatica uses the SSL/TLS protocol to secure communication between components in the domain and between the domain and client components. The following article discusses the types of secure communication and their requirements.

Supported Versions
• Informatica 9.6.x

Table of Contents
Overview.................................................................................. 2
SSL/TLS Protocol................................................................. 3
Secure Communication Requirements........................................... 4
  Requirements for Secure Communication within the Domain......................... 4
  Requirements for Secure Connections to the Administrator Tool.......................... 5
  Requirements for Secure Connections to a Web Application Service.................. 6

Overview
In the Informatica domain, you can set up the following types of secure communication:
• Secure communication between services and between services and clients
• Secure connections to web application services

Informatica uses the SSL/TLS protocol to secure communication. The SSL/TLS protocol encrypts network traffic to protect it from potential threats such as man-in-the-middle attacks or packet sniffers. Since secure communication uses the SSL/TLS protocol, you must provide keystores and truststores. The requirements for a keystore or truststore depend on the type of security you set up.

Secure Communication within the Domain
When you enable secure communication within the domain, you secure the following connections:

Connections within the domain
  Secures the connection between services. Requires a keystore and truststore to provide and verify credentials because the components in the domain can act as server or client.

Connections between the domain and Informatica client applications
  Secures the connection between the domain and client applications, such as the Developer tool. The clients use a copy of the truststore that is used to secure connections within the domain to verify credentials.

To secure these connections when you install Informatica, select the Secure communication for the domain option.

To secure these connections after you install Informatica, use the command line programs.

Secure Connections to Web Application Services
You can secure the following connections:
Connections to the Administrator tool

Secures the connection between the Administrator tool and the browser. When you configure the Administrator tool, specify a keystore to provide credentials that the browser can accept.

To secure this connection, select Enable HTTPS for Informatica Administrator during installation or use the infasetup UpdateGatewayNode command after installation.

Connections to web application services

Secures the connection between a web application service, such as the Analyst Service, and the browser. When you configure a service, specify a keystore to provide credentials.

To secure these connections, select an HTTPS connection when you create or configure the service.

Secure Connections to Sources and Targets

You can secure the connection to the following relational sources or targets:

- Oracle
- Microsoft SQL Server
- IBM DB2

For more information about how to secure the connection to a relational database, see the documentation for that database and the Informatica Security Guide.

SSL/TLS Protocol

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 by a certificate authority (CA). 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 CA. Informatica recommends CA signed certificates for a higher level of security.

Note: Informatica requires that SSL certificates created with RSA encryption use more than 512 bits.

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

To secure connections, 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 Communication Requirements

The requirements for secure communication depend on the connection. You can secure the following connections:

- Connections within the domain and between the domain and Informatica client applications
- Connections to the Administrator tool
- Connections to the web application services

Requirements for Secure Communication within the Domain

You enable secure communication within the domain during installation when you select the **Enable secure communication for the domain** option. Alternatively, you can enable it after installation with the command line programs.

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

**Note:** Informatica provides default SSL certificates, keystores, and truststores for evaluating secure communication within the domain. These files are shared with all Informatica installations. Do not use them in a production environment.

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 the 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_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The keystores and truststores are in the correct directory.

- If you enable secure communication within the domain during installation, the keystores and truststores must be in a directory that is accessible to the installer.
- If you enable secure communication after installation, the directory must be accessible to the command line programs.

For information about how to create a custom keystore and truststore, see the Informatica How-To Library article 0700-How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain:

https://kb.informatica.com/h2I/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

For information about how to enable secure communication within the domain, see the *Informatica Installation and Configuration Guide* or the *Informatica Security Guide*.

Requirements for Secure Communication Between the Domain and Client Applications

When you enable secure communication within the domain, you also secure connections between the domain and Informatica client applications, such as the Developer tool. Secure connections between the domain and client
applications uses the same truststores as secure communication within the domain. Additionally, you must configure
the clients to work with a secure domain.

After you install the client applications, verify the following requirements are met:

**The truststore files exist on the machine where the clients run.**

- Use the truststores in PEM and JKS formats that you used to enable secure communication within the
domain.
- Copy them to a directory on the machine on which the client runs.

**You configured the environment variables.**

- You must configure the `INFA_TRUSTSTORE` and `INFA_TRUSTSTORE_PASSWORD` environment variables.
- Set `INFA_TRUSTSTORE` to the directory where the truststores are located on the machine where the clients run.
- Set `INFA_TRUSTSTORE_PASSWORD` to the encrypted password for the truststore in JKS format. Use the
`pmpasswd` command to encrypt the password.

**Note:** If you use the default SSL certificate, keystore, and truststore, you do not need to copy the truststore files to the
machine where the client runs or provide the truststore directory or password.

For more information about configuring the client to work with a secure domain, see the *Informatica Installation and
Configuration Guide* or the *Informatica Security Guide*.

**Requirements for Secure Connections to the Administrator Tool**

You can secure the connection to the Administrator tool during installation or after.

If you select **Enable HTTPS for Informatica Administrator** during installation, you can provide a SSL certificate and
keystore or the installer can generate a self-signed certificate and keystore. If you use the installer generated certificate
and keystore, no further action is required.

**Note:** Informatica recommends you use a certificate that is signed by a CA.

After you install Informatica, you can secure the connection to the Administrator tool with the `infasetup
UpdateGatewayNode` command.

Before you secure the connection to the Administrator tool, ensure 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.

**You imported the certificate into a keystore.**

- The certificate must be in a keystore in JKS format. Informatica requires that a keystore contain only one
certificate.
- If you use multiple gateway nodes, you can use the same certificate and keystore for all the gateway nodes
or a unique SSL certificate and keystore for each gateway node.

**The keystore is in the correct directory.**

- If you enable secure connections to the Administrator tool during installation, the keystore must be in a
directory that is accessible to the installer
- If you enable secure connections to the Administrator tool after installation, the keystore must be in a
directory that is accessible to the command line programs.
For information about how to secure the connection to the Administrator tool during installation, see the *Informatica Installation and Configuration Guide*.

For information about how to secure the connection to the Administrator tool after installation, see the *Informatica Security Guide*.

**Requirements for Secure Connections to a Web Application Service**

You can secure the connection to a web application service, such as the Analyst service.

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 RSAP 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.

Each web application service can use a unique certificate or a shared one.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. Web application services can share a keystore if they use the same certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate.

**The keystore is in a accessible directory.**

The keystore must be in a directory that is accessible to the Administrator tool.

For more information about enabling secure communication for web client services, see the *Informatica Installation and Configuration Guide* or the *Informatica Security Guide*.

**Authors**

Brian Le  
Technical Writer