How-To Library

Informatica

Enabling SAML Authentication with Active Directory Federation Services in Informatica 10.4.0

Abstract

You can enable users to log into Informatica web applications using single sign-on. This article explains how to configure single sign-on in an Informatica 10.4.0 domain using Security Assertion Markup Language (SAML) and Microsoft Active Directory Federation Services (AD FS).

Supported Versions

- Informatica Data Engineering Integration 10.4.0
- Informatica Enterprise Data Catalog 10.4.0
- Informatica Enterprise Data Preparation 10.4.0
- Informatica PowerCenter® 10.2 x

Table of Contents

Overview

You can configure Security Assertion Markup Language (SAML) authentication in an Informatica version 10.4.0 domain using the Microsoft Active Directory Federation Services (AD FS) identity provider.

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

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

- Informatica Administrator
- Informatica Analyst
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation

You can configure an Informatica domain to use the following versions of AD FS:

- Microsoft Active Directory Federation Services 2.0
- Microsoft Active Directory Federation Services 4.0

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

SAML Authentication Process

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

The following steps describe the basic SAML authentication flow:

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

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

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

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

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

Enable SAML Authentication in a Domain

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

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

1. Create an LDAP configuration to connect to the LDAP identity store that contains Informatica web application user accounts. You also create an LDAP security domain, and then import the user accounts into the security domain.
2. Export the Identity Provider Assertion Signing Certificate from the identity provider.
3. Import the Identity Provider Assertion Signing certificate into a truststore file on each gateway node in the domain. You can import the certificate into the Informatica default truststore file, or into a custom truststore file.
4. Add one or more relying party trusts in the identity provider, and map LDAP attributes to the corresponding types used in security tokens issued by the identity provider.
5. Add the URL for each Informatica web application to the identity provider.
6. Enable SAML authentication in the domain.
7. Enable SAML authentication on every gateway node in the domain.

Before You Enable SAML Authentication

Ensure the Windows network and Informatica domain gateway nodes are configured to use SAML authentication.

To ensure that the Informatica domain can use SAML authentication, validate the following requirements:

Verify that the required services are deployed and configured on the Windows network.

SAML authentication requires the following services:

- Microsoft Active Directory
- Microsoft Active Directory Federation Services

Ensure the Informatica web application services use secure HTTPS connections.

By default, AD FS requires that web application URLs use the HTTPS protocol.

Ensure that the system clocks on the AD FS host and all gateway nodes in the domain are synchronized.

The lifetime of SAML tokens issued by AD FS is set according to the AD FS host system clock. Ensure that the system clocks on the AD FS host and all gateway nodes in the domain are synchronized.

To avoid authentication issues, the lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within 120 seconds of a gateway node's system time by default.

Step 1. Create a Security Domain for Web Application User Accounts

Create a security domain for web application user accounts that will use SAML authentication, and then import each user's LDAP account from Active Directory into the domain.

You must import the LDAP accounts for all users that use SAML authentication into the security domain. After importing the accounts into the domain, assign the appropriate Informatica domain roles, privileges and permissions to the accounts within the LDAP security domain.

1. In the Administrator tool, click the **Users** tab, and then select the **Security** view.
2. Click the **Actions** menu and select **LDAP Configuration**.

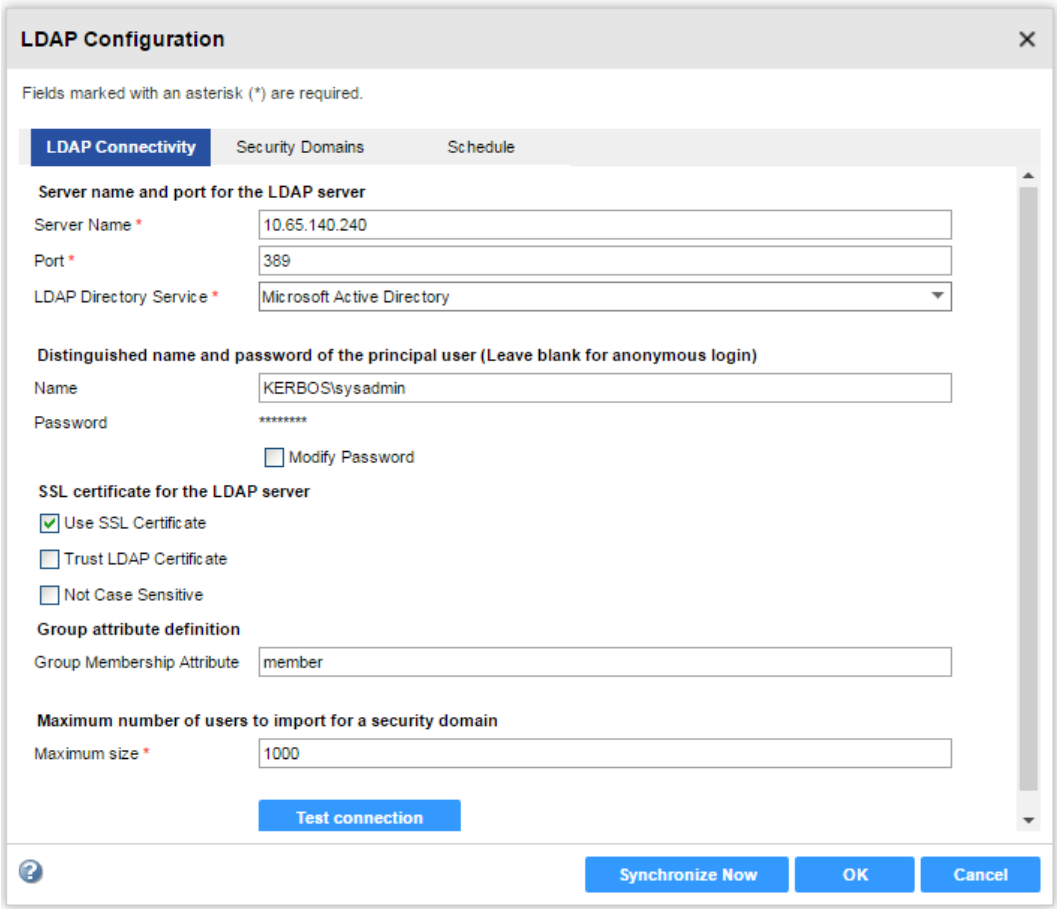
   The **LDAP Configuration** dialog box opens.
3. Click the **LDAP Connectivity** tab.
4. Configure the connection properties for the Active Directory server.

   The following table describes the server connection properties:

Property	Description
Server Name	Host name or IP address of the Active Directory server.
Port	Listening port for the Active Directory server. The default value is 389.
LDAP Directory Service	Select Microsoft Active Directory.
Name	Distinguished name (DN) for the principal LDAP 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 directory service.
Password	Password for the principal LDAP user.

Property	Description
Use SSL Certificate	Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol. If the LDAP server uses SSL, you must import the certificate into a truststore file on every gateway node within the Informatica domain. You must also set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables if you do not import the certificate into the default Informatica truststore.
Trust LDAP Certificate	Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.
Not Case Sensitive	Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups. Enable this option.
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 distinguished names (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. 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. The default value is 1000.

The following image shows the connection details for an LDAP server set in the LDAP Connectivity panel of the **LDAP Configuration** dialog box.

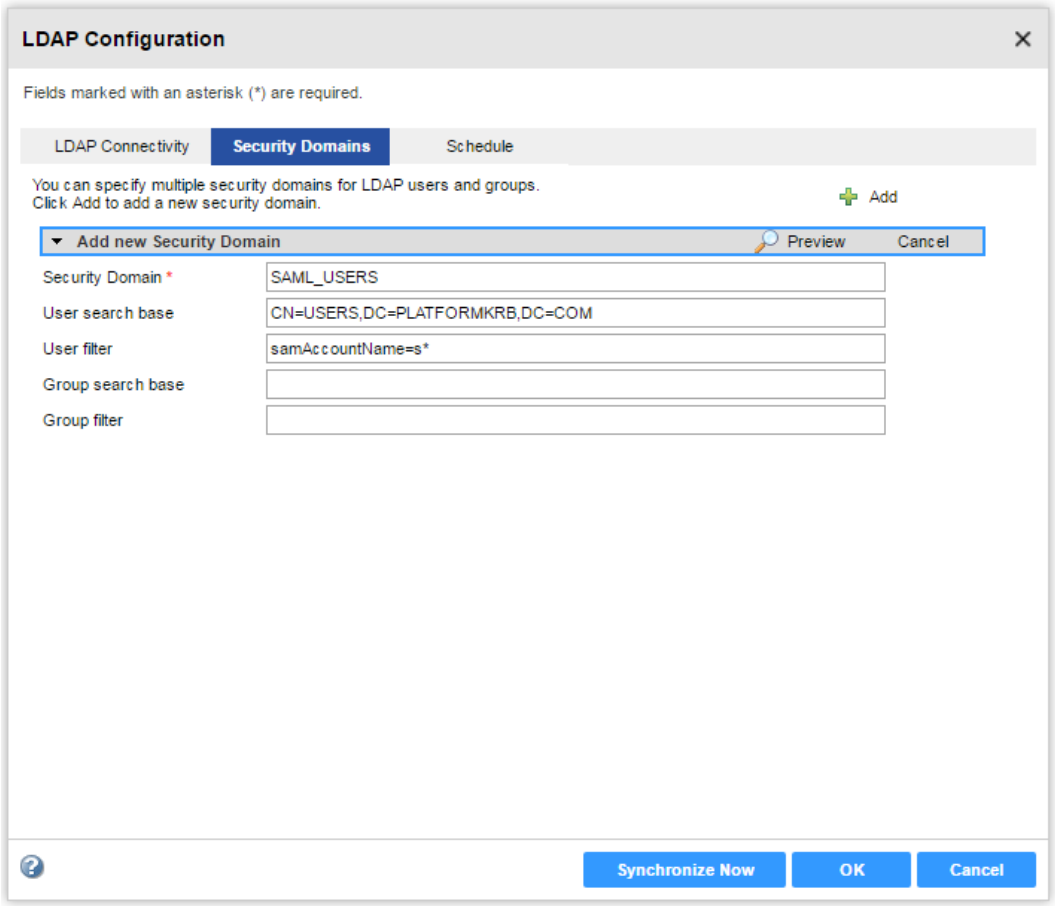


5. Click **Test Connection** to verify that the connection to the Active Directory server is valid.
6. Click the **Security Domains** tab.
7. Click **Add** to create a security domain.
8. Enter the security domain properties.

The following table describes the security domain properties:

Property	Description
Security Domain	Name of the LDAP security domain. The name is not case sensitive and must be unique within the domain. The name 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. In 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. For example, to search the Users container that contains user accounts in the example.com Windows domain, specify CN=USERS,DC=EXAMPLE,DC=COM.
User filter	An LDAP query string that specifies the criteria for searching for users in Active Directory. The filter can specify attribute types, assertion values, and matching criteria. For Active Directory, format the query sting as: `sAMAccountName=<account>`
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in Active Directory.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

The following image shows the properties for an LDAP security domain named SAML_USERS set in the Security Domains panel of the **LDAP Configuration** dialog box. The user filter is set to import all users beginning with the letter "s".



9. Click **Synchonize Now**.

   The security domain appears in the Users view.
10. Expand the domain in the Navigator to view the imported user accounts.
11. Set the appropriate roles, privileges, and permissions on the user accounts that will access each web application.

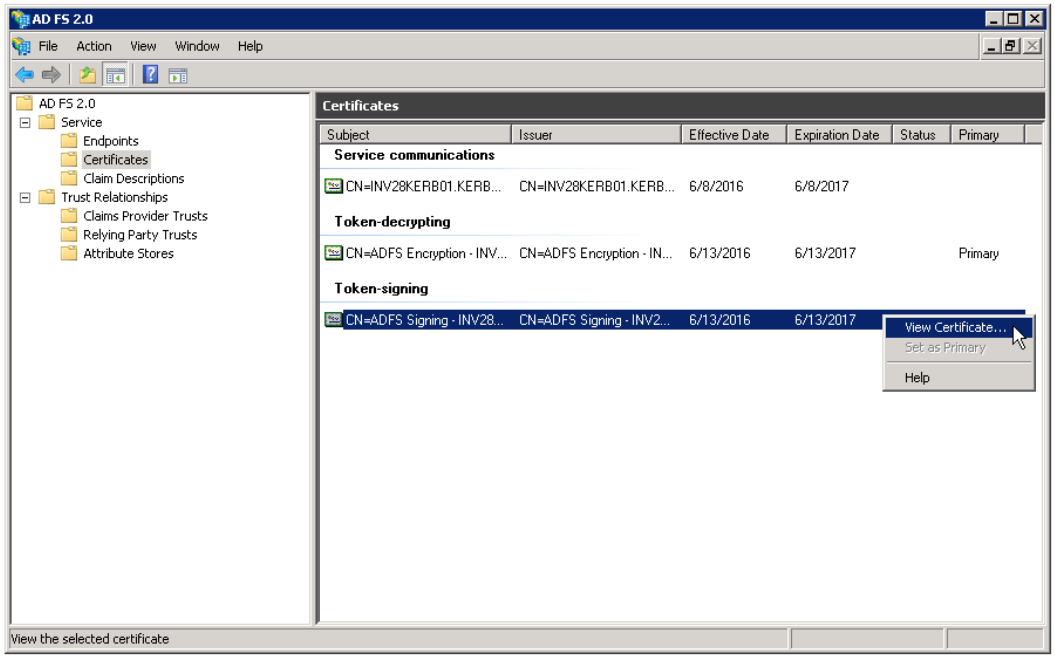
Step 2. Export the Certificate from AD FS

Export the Assertion Signing certificate from AD FS.

The certificate is a standard X.509 certificate used to sign the assertions within the SAML tokens that AD FS issues to Informatica web applications. You can generate a self-signed Secure Sockets Layer (SSL) certificate for AD FS, or you can get a certificate from a certificate authority and import it into AD FS.

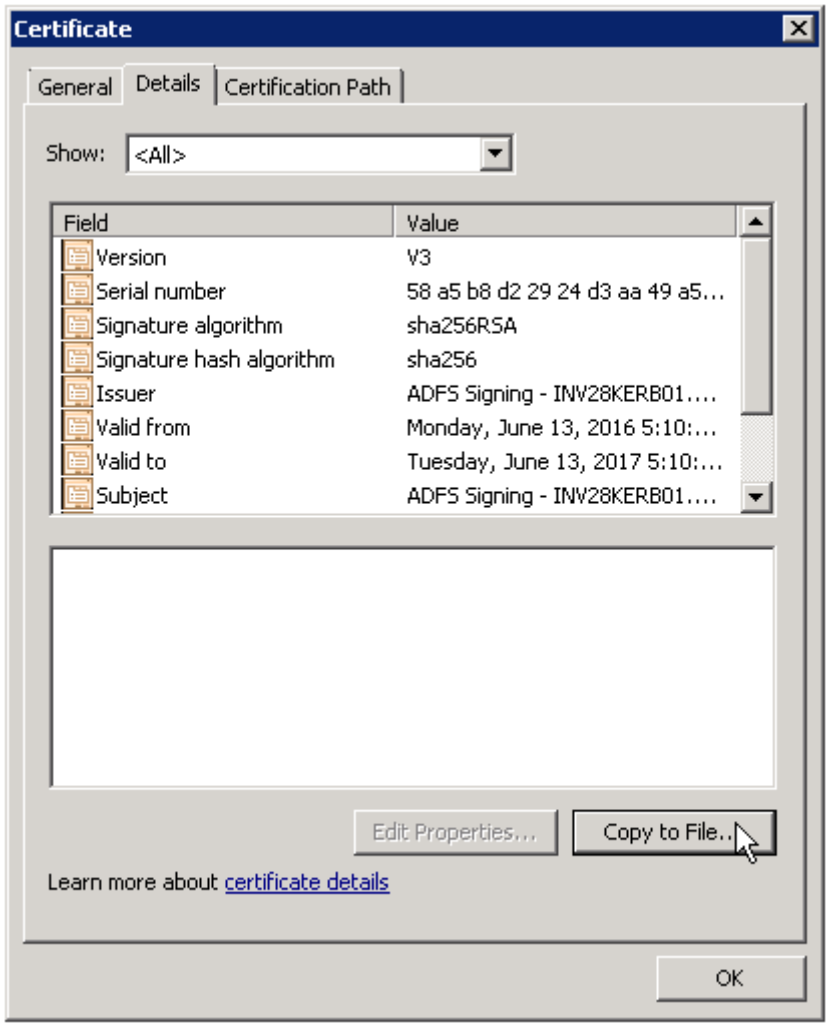
1. Log in to the AD FS Management Console.
2. Expand the **Service** > **Certificates** folder.

3. Right-click the certificate under Token-signing in the Certificates pane, and then select **View Certificate**, as shown in the following image:



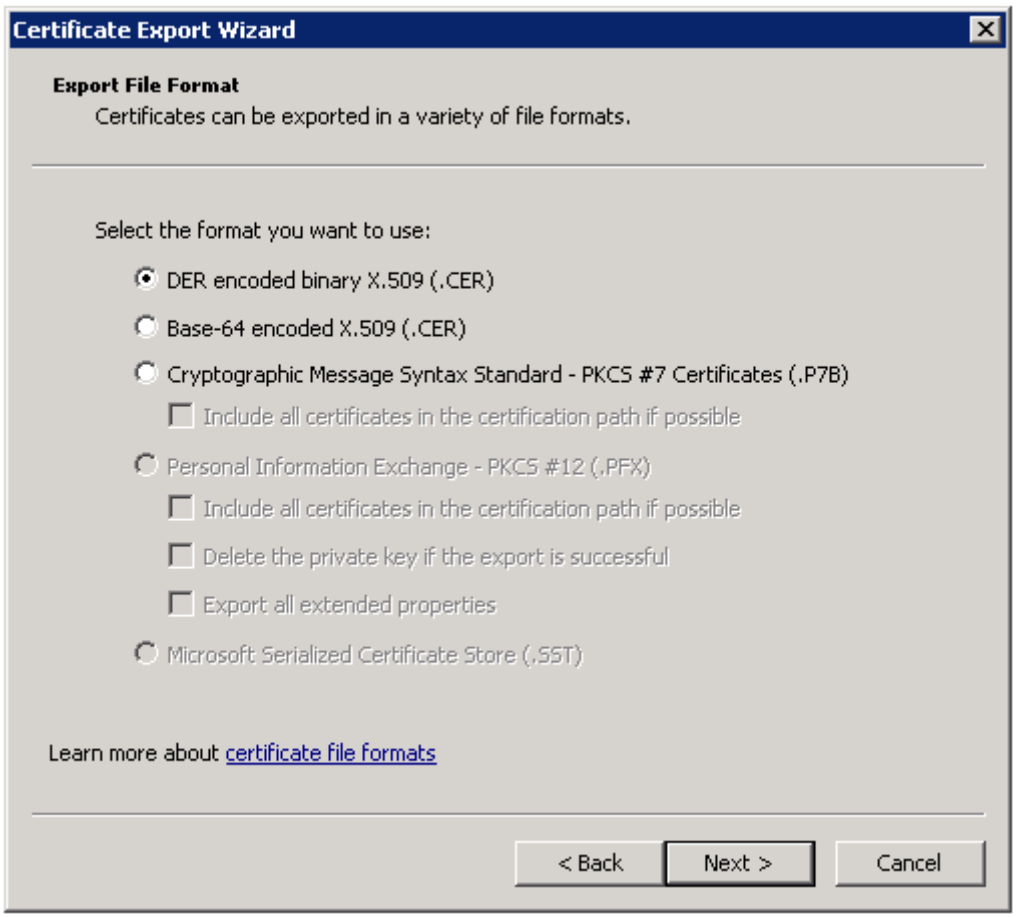
The **Certificate** dialog appears.

4. Click the **Details** tab, and then click **Copy to File**, as shown in the following image:



The **Certificate Export Wizard** appears.

5. Select **DER encoded binary X.509 (.CER)** as the format, as shown in the following image:



6. Click **Next**.
7. Enter the certificate file name and the location to export it to, and click **Next**.
8. Click **OK**, and then click **Finish** to complete the export.

Step 3. Import the Certificate into the Truststore Used for SAML Authentication

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

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

The file name of the default Informatica truststore file is `infa_truststore.jks`. The file is installed in the following location on each node:

```
<Informatica installation directory>\services\shared\security\infa_truststore.jks
```

Note: Do not replace the default `infa_truststore.jks` file with a custom truststore file.

If you import the certificate into a custom truststore file, you must save the truststore file in a different directory than the directory containing the default Informatica truststore file. The truststore file name must be `infa_truststore.jks`.

You can use the Java keytool key and certificate management utility to create an SSL certificate or a certificate signing request (CSR) as well as keystores and truststores in JKS format. The keytool is available in the following directory on domain nodes:

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

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

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

Step 4. Configure Active Directory Federation Services

Configure AD FS to issue SAML tokens to Informatica web applications.

Use the AD FS Management Console to perform the following tasks:

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

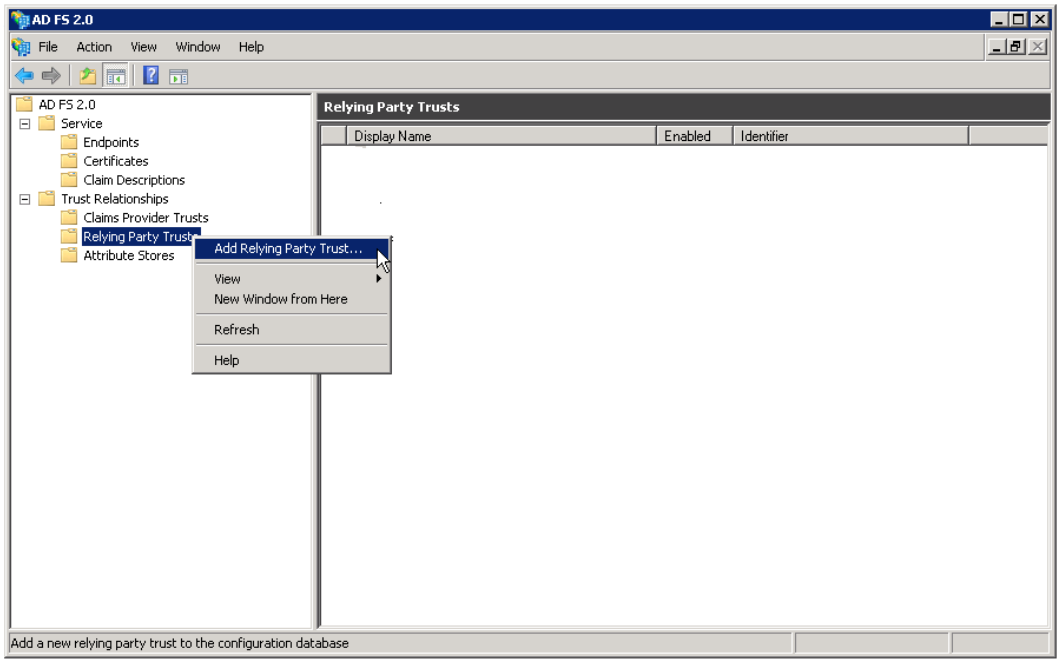
You provide the name of the relying party trust when you enable SAML authentication in a domain. Depending on your security requirements, you might create multiple relying party trusts in AD FS to enable domains used by different organizations within the enterprise to use SAML authentication.

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

Note: All strings are case sensitive in AD FS, including URLs.

1. Log in to the AD FS Management Console.
2. Expand the **Trust Relationships** > **Relying Party Trusts** folder.

3. Right-click the **Relying Party Trusts** folder, and then select **Add Relying Party Trust** as shown in the following image:

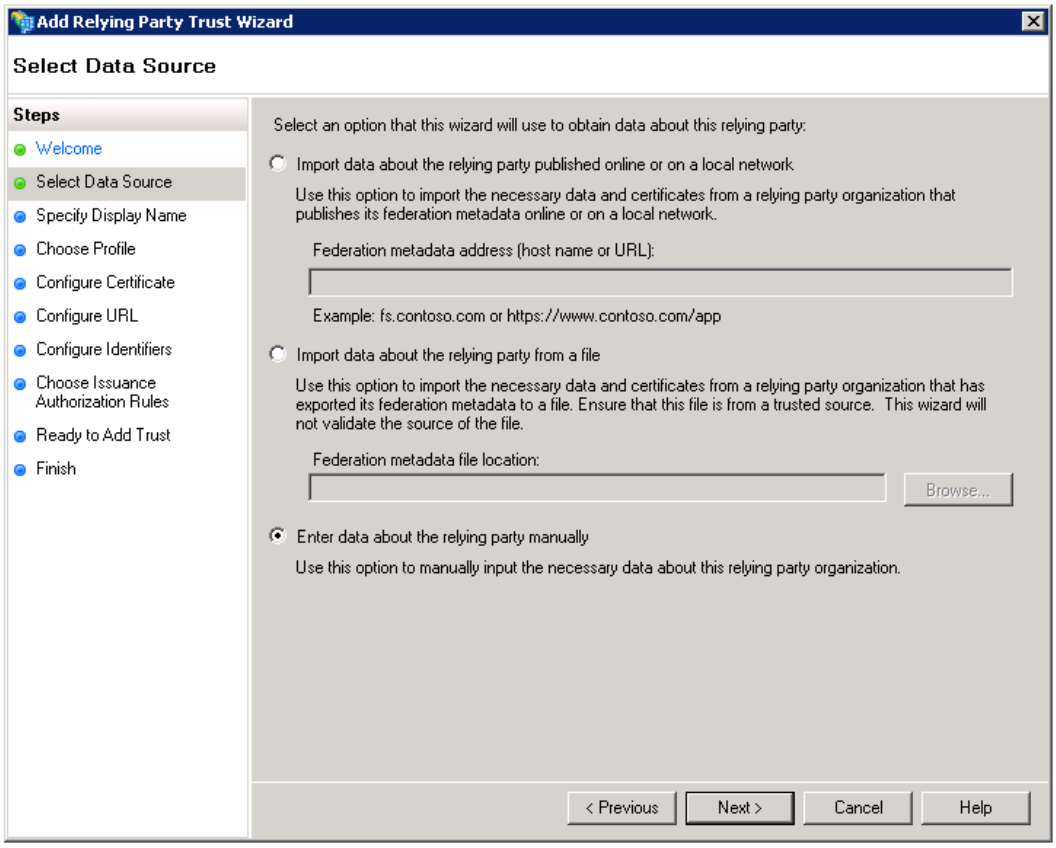


The **Add Relying Party Trust Wizard** appears.

4. Click **Start**.

The **Select Data Source** panel appears.

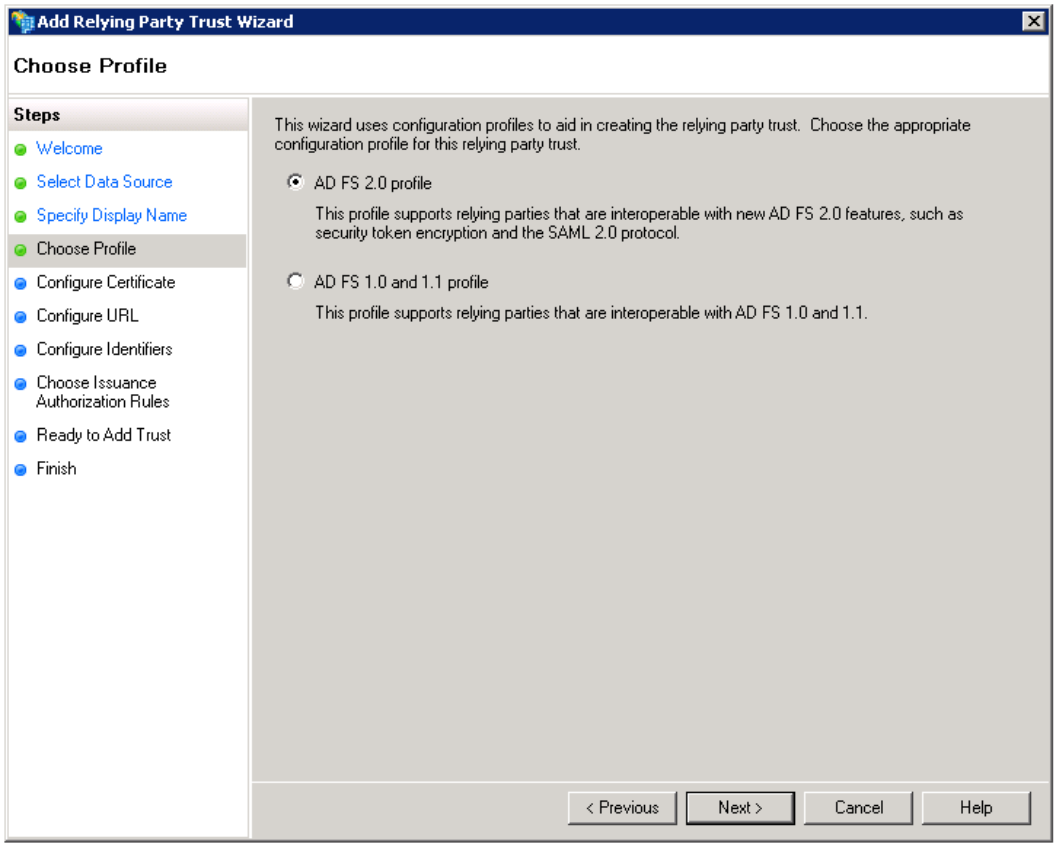
5. Click **Enter data about the relying party manually** as shown in the following image:



6. Click **Next**
7. Enter the relying party trust name, and then click **Next**.

   Note: Do not include the ? character in the relying party trust name.

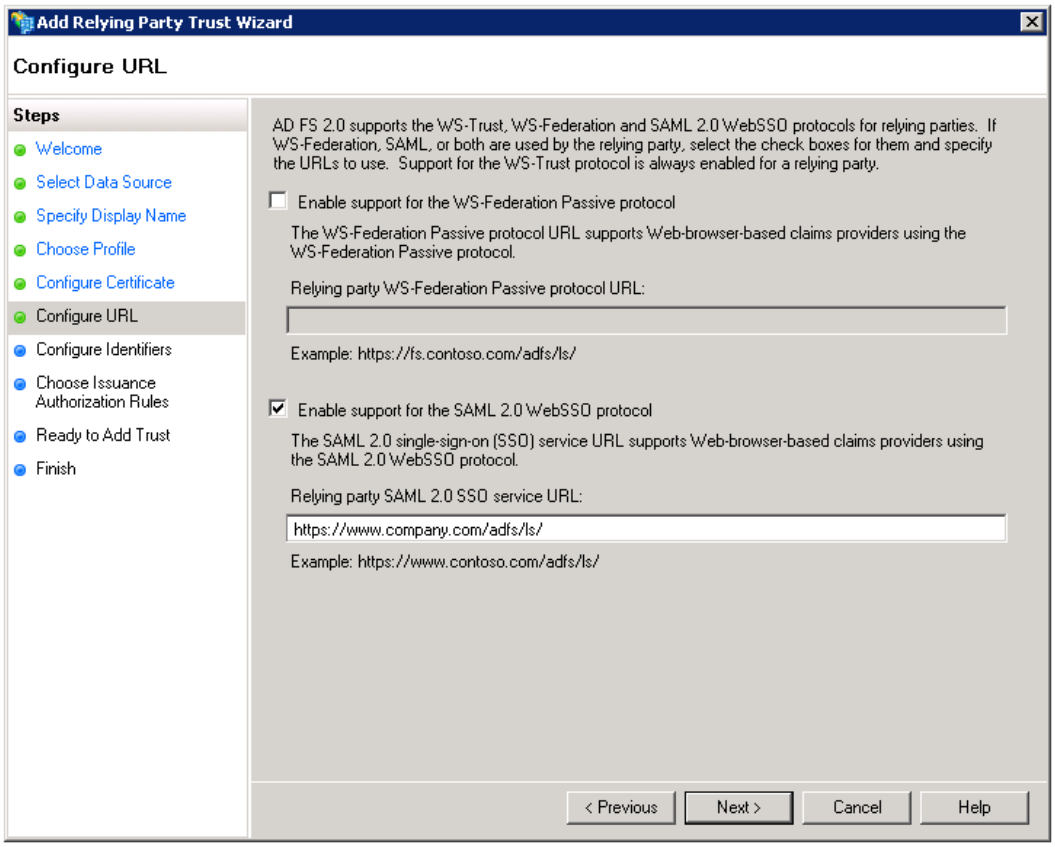
8. Click **AD FS 2.0 profile** as shown in the following image:



9. Click **Next**.

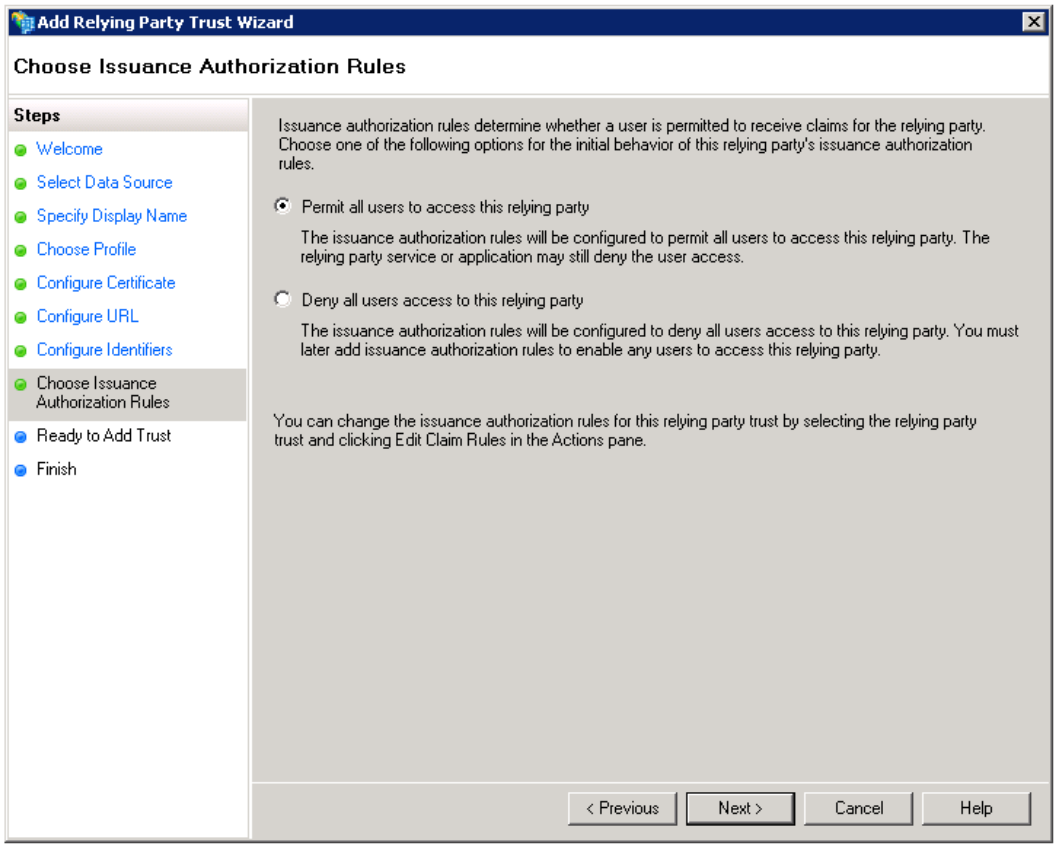
   Skip the certificate configuration panel in the wizard.

10. Check **Enable support for the SAML WebSSO protocol**, and then enter the complete relying party URL, as shown in the following image:



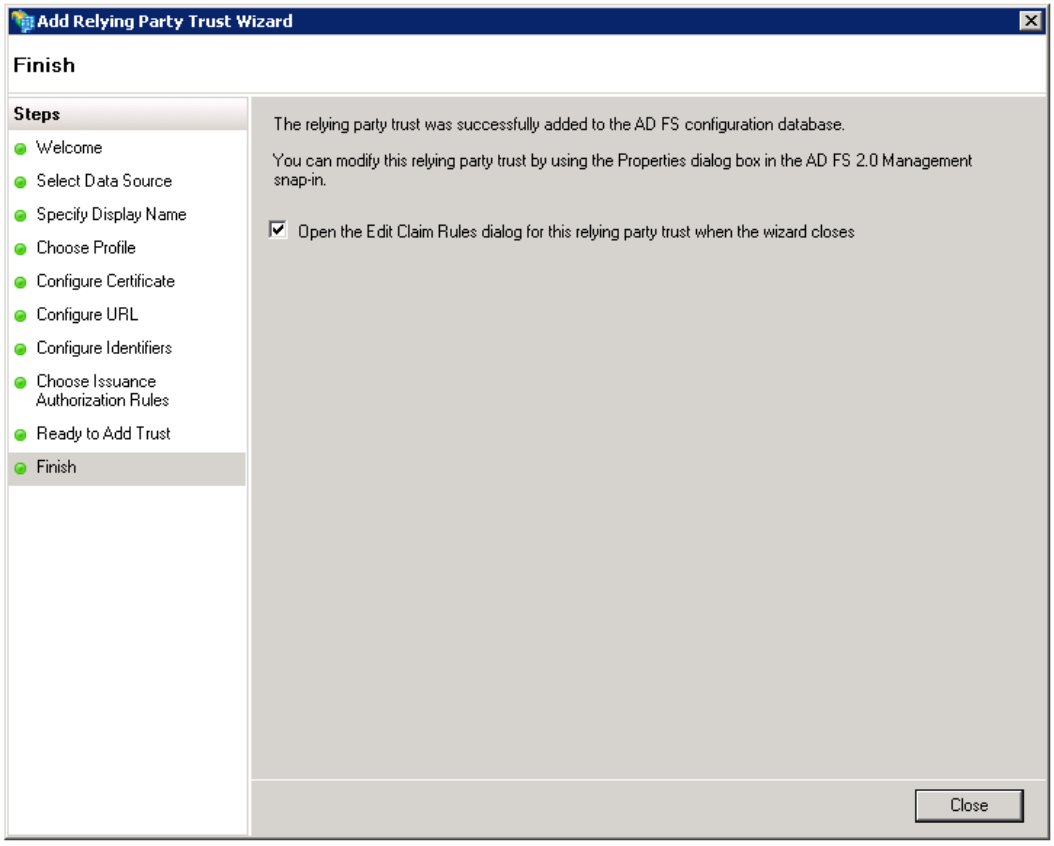
11. Click **Next**.
12. Enter the name of the relying party trust in the Relying party trust identifier field. Click **Add**, and then click **Next**.

13. Select **Permit all users to access the relying party** as shown in the following image:



14. Click **Next**.

15. Check **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** as shown in the following image:



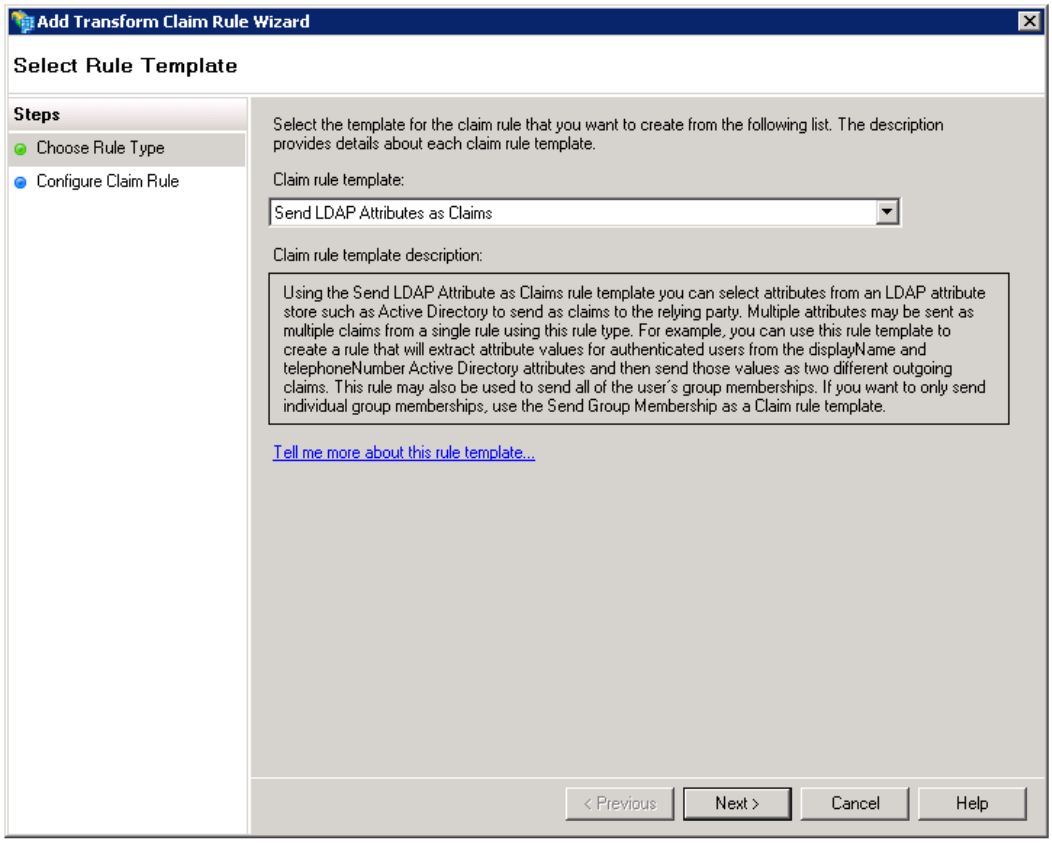
16. Click **Close**.

    The **Edit Claim Rules for Informatica** dialog box appears.

17. Click **Add Rule**.

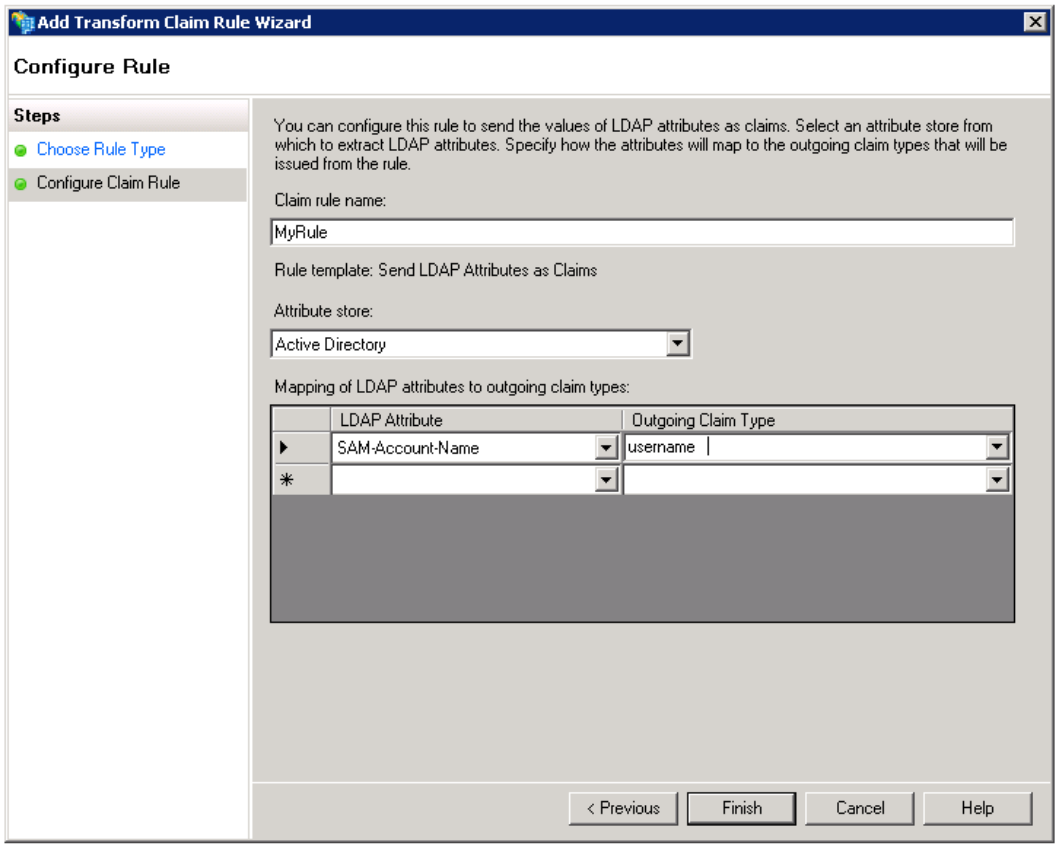
    The **Add Transform Claim Rule Wizard** opens.

18. Select **Send LDAP Attributes as Claims** from the menu, as shown in the following image:



19. Click **Next**.

20. Enter any string as the claim rule name, as shown in the following image:



21. Select Active Directory from the **Attribute store** menu.
22. Select SAM-Account-Name from the **LDAP Mapping** menu.
23. Enter "username" in the **Outgoing Claim Type** field.
24. Click **Finish**, then click **OK** to close the wizard.

Step 5. Add Informatica Web Application URLs to AD FS

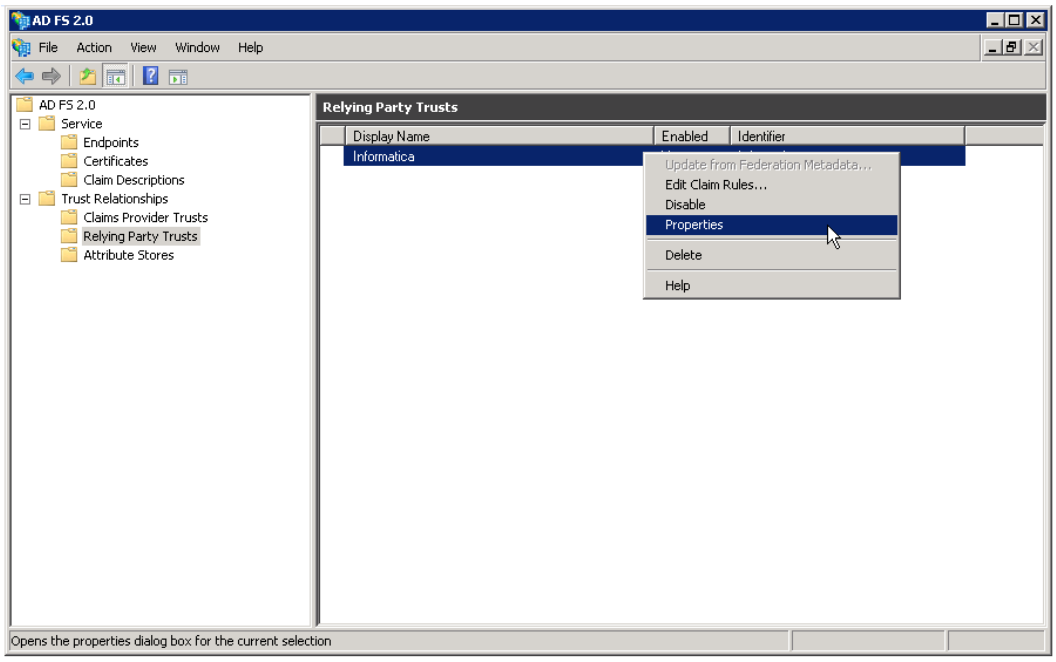
Add the URL for each Informatica web application using SAML authentication to AD FS.

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

You do not need to add the URL for the Administrator tool, because you already entered it as part of configuring AD FS.

1. Log in to the AD FS Management Console.
2. Expand the **Trust Relationships** > **Relying Party Trusts** folder.

3. Right-click the **Informatica** entry and select **Properties**, as shown in the following image:

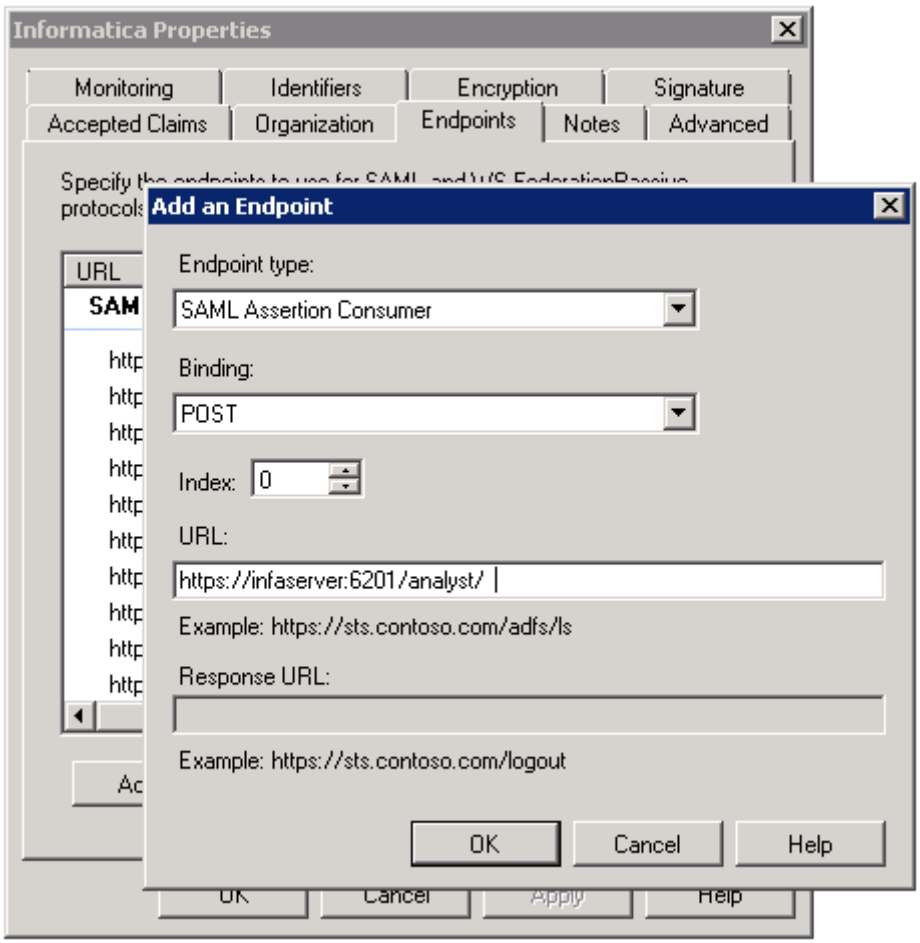


The **Informatica Properties** dialog box appears.

4. Click the **Endpoints** tab.

The **Add an Endpoint** dialog box appears.

5. Select **SAML Assertion Consumer** from the **Endpoint** type menu, and then select **POST** from the **Binding** menu, as shown in the following image:



6. Enter the complete URL for a supported Informatica web application, and then click **OK**.

   Repeat this procedure for each web application.

Step 6. Enable SAML Authentication in the Domain

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

Select one of the following options:

Enable SAML authentication when you install the Informatica services.

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

Enable SAML authentication in an existing domain.

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

Enable SAML authentication when you create a domain.

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

infasetup updateDomainSamlConfig Command Options

Set the SAML options in the infasetup updateDomainSamlConfig command to enable SAML authentication in a domain. Shut down the domain before you run the command.

Specify the identity provider URL as the value for the `-iu` option. The following example shows the command usage to configure a domain to use AD FS as the identity provider:

```
infasetup updateDomainSamlConfig -saml true -iu https://server.company.com/adfs/ls/ -spid
Prod_Domain -cst 240
```

The following table describes the options and arguments:

Option	Argument	Description
-EnableSaml -saml	true|false	Required. Set this value to true to enable SAML authentication for supported Informatica web applications within the Informatica domain. Set this value to false to disable SAML authentication for supported Informatica web applications within the Informatica domain.
-idpUrl -iu	identity_provider_url	Required if the -saml option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	service_provider_id	Optional. The relying party trust name or the service provider identifier for the domain as defined in Active Directory Federation Services (AD FS). If you specified "Informatica" as the relying party trust name in AD FS, you do not need to specify a value.
-ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	Optional. The allowed time difference between the AD FS host system clock and the master gateway node's system clock. The lifetime of SAML tokens issued by AD FS by is set according to the AD FS host system clock. The lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within the specified number seconds of the master gateway node's system clock. Values must be from 0 to 600 seconds. Default is 120 seconds.

See the *Informatica Command Reference* for instructions on using the infasetup updateDomainSamlConfig command.

infasetup DefineDomain Command Options

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

The following example shows the options to configure a domain to use AD FS as the identity provider in the final six options at the command prompt:

```
infasetup defineDomain -cs "jdbc:informatica:oracle://host:1521;sid=DB2" -dt oracle -dn TestDomain -
ad test_admin -pd test_admin -ld $HOME/ISP/1011/source/logs -nn TestNode1 -na host1.company.com -
saml true -iu https://server.company.com/adfs/ls/ -spid Prod_Domain -cst 240 -asca adfscert -std
\custom\security\ -stp password -mi 10000 -ma 10200 -rf $HOME/ISP/BIN/nodeoptions.xml
```

The following table describes the SAML options and arguments:

Option	Argument	Description
-EnableSaml -saml	true|false	Required. Set this value to true to enable SAML authentication for supported Informatica web applications within the Informatica domain. Set this value to false to disable SAML authentication for supported Informatica web applications within the Informatica domain.
-idpUrl -iu	identity_provider_url	Required if the -saml option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	service_provider_id	Optional. The relying party trust name or the service provider identifier for the domain as defined in Active Directory Federation Services (AD FS). If you specified "Informatica" as the relying party trust name in AD FS, you do not need to specify a value.
-ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	Optional. The allowed time difference between the AD FS host system clock and the master gateway node's system clock. The lifetime of SAML tokens issued by AD FS by is set according to the AD FS host system clock. The lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within the specified number seconds of the master gateway node's system clock. Values must be from 0 to 600 seconds. Default is 120 seconds.
-AssertionSigningCertificateAlias -asca	idp_assertion_signing_certificate_aliaseAlias	Required if the -saml option is true. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.
-SamlTrustStoreDir -std	saml_truststore_directory	Optional. The directory containing the custom truststore file required to use SAML authentication on gateway nodes within the domain. Specify the directory only, not the full path to the file. SAML authentication uses the default Informatica truststore if no truststore is specified.
-SamlTrustStorePassword -stp	saml_truststore_password	Required if you use a custom truststore. The password for the custom truststore file.

See the *Informatica Command Reference* for instructions on using the infasetup defineDomain command.

Step 7: Enable SAML Authentication on the Gateway Nodes

You must configure SAML authentication on every gateway node in the Informatica domain. Configure every gateway node in the domain to use SAML to ensure the SAML configuration on each node matches the domain level SAML configuration.

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

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

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

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

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

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

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

Gateway Node Command Options

Use the infasetup DefineGatewayNode command to enable SAML authentication when you create a gateway node. Use infasetup UpdateGatewayNode or infacmd isp SwitchToGatewayNode to enable SAML authentication on an existing node.

The SAML options are identical for all of these commands. The following example shows the SAML options as the final four options on the infasetup DefineGatewayNode command line:

```
infasetup defineGatewayNode -cs "jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp
test_user -dt oracle -dn TestDomain -nn TestNode1 -na host2.company.com:1234 -ld $HOME/ISP/1011/
source/logs -rf $HOME/ISP/BIN/nodeoptions.xml -mi 10000 -ma 10200 -ad test_admin -pd test_admin -
saml true -asca adfscert -std \custom\security\ -stp password
```

The following table describes the options and arguments:

Option	Argument	Description
-EnableSaml -saml	true|false	Required. Enables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the domain. Set this value to false to disable SAML authentication in the domain.
-AssertionSigningCertificateAlias -asca	idp_assertion_signing_certificate_aliaseAlias	Required if SAML authentication is enabled for the domain. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.
-SamlTrustStoreDir -std	saml_truststore_directory	Optional. The directory containing the custom truststore file required to use SAML authentication on gateway nodes within the domain. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.
-SamlTrustStorePassword -stp	saml_truststore_password	Required if you use a custom truststore. The password for the custom truststore file.

See the *Informatica Command Reference* for instructions on using the infasetup DefineGatewayNode, the infasetup UpdateGatewayNode, and the infacmd isp SwitchToGatewayNode commands.

Author

Dan Hynes