How-To Library

Informatica

Configuring SAML-based Single Sign-on for Informatica 10.1.1 Web Applications

Abstract

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

Supported Versions

- Informatica Big Data Management™ 10.1.1
- Informatica Data Quality 10.1.1
- Informatica Data Services 10.1.1
- Informatica Data Transformation 10.1.1
- Informatica PowerCenter® 10.1.1

Table of Contents

SAML Authentication Overview

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

Security Assertion Markup Language is an XML-based data format for exchanging authentication information between a service provider and an identity provider. In an Informatica domain, the Informatica web application is the service provider. Microsoft Active Directory Federation Services (AD FS) 2.0 is the identity provider, which authenticates web application users with your organization's LDAP or Active Directory identity store.

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.

SAML-based Single Sign-on Setup

Configure Active Directory Federation Services (AD FS) and the Informatica domain to use SAML-based single sign-on.

To configure SAML-based single sign-on for supported Informatica web applications, perform the following tasks:

1. Create an LDAP security domain for Informatica web application user accounts, and then import the users into the domain from Active Directory.
2. Export the Identity Provider Assertion Signing Certificate from AD FS.
3. Import the Identity Provider Assertion Signing certificate into the Informatica default truststore file on each gateway node in the domain.
4. Add Informatica as a relying party trust in AD FS and map LDAP attributes to the corresponding types used in security tokens issued by AD FS.
5. Add the URL for each Informatica web application to AD FS.
6. Enable single-sign on for Informatica web applications within the Informatica 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 2.0

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-based single-sign on, 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-based single-sign on to access the Administrator tool, the Analyst tool, and the Monitoring tool 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**.

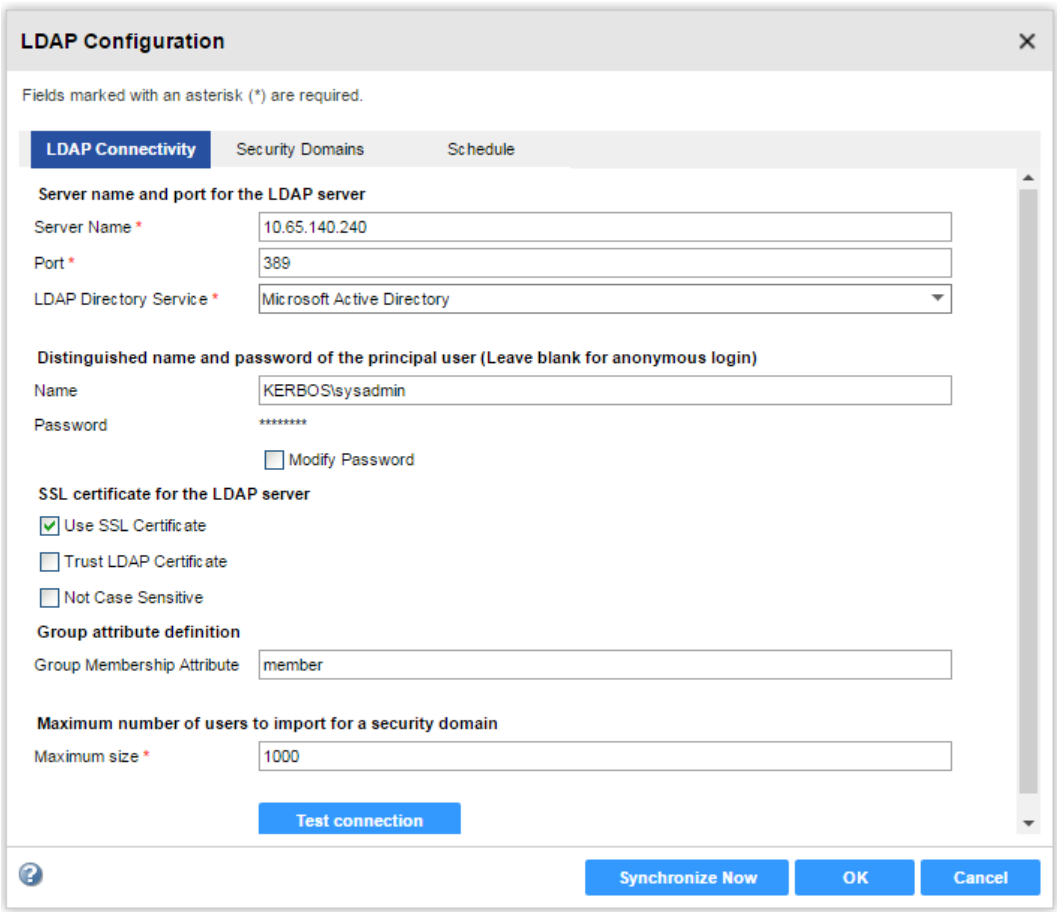
   The **LDAP Configuration** dialog box opens.
3. Click the **LDAP Connectivity** tab.
4. Configure the connection properties for the Active Directory server.

   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 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.
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.

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 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.

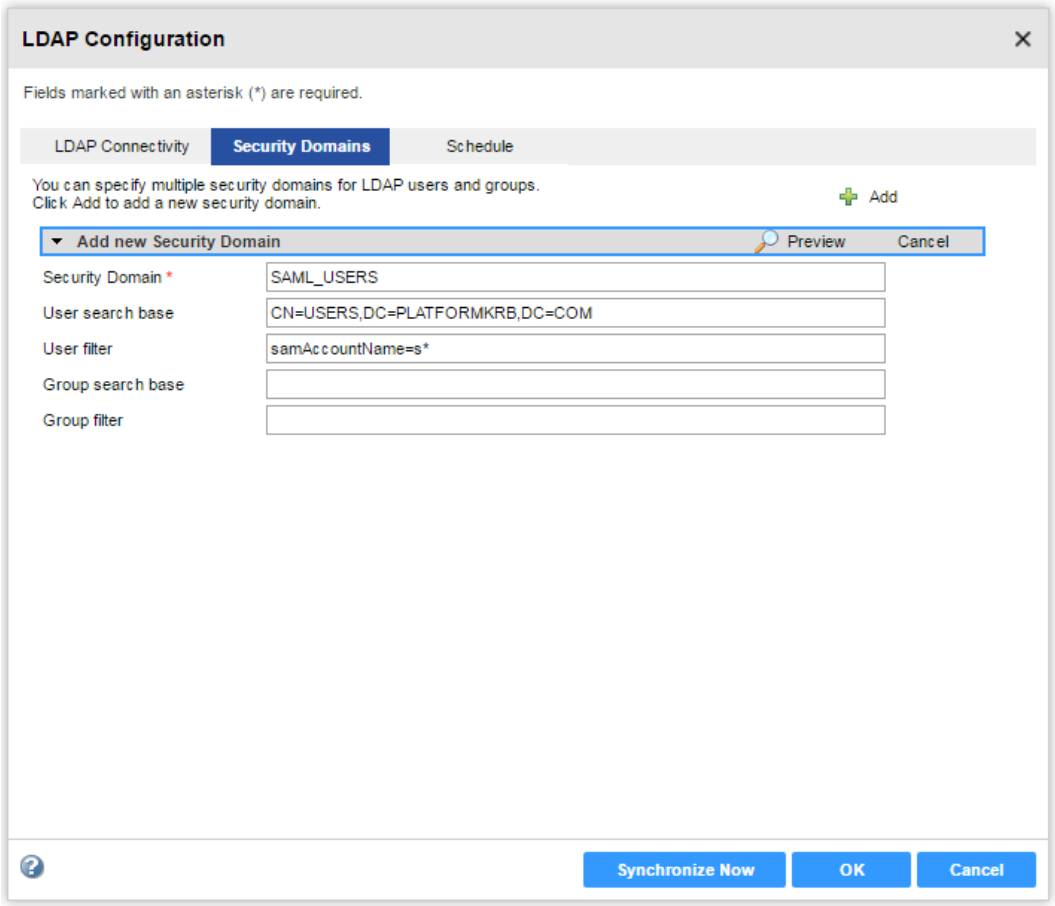


5. Click **Test Connection** to verify that the connection to the Active Directory server is valid.
6. Click the **Security Domains** tab.
7. Click **Add** to create a security domain.
8. Enter the security domain properties.

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.
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.

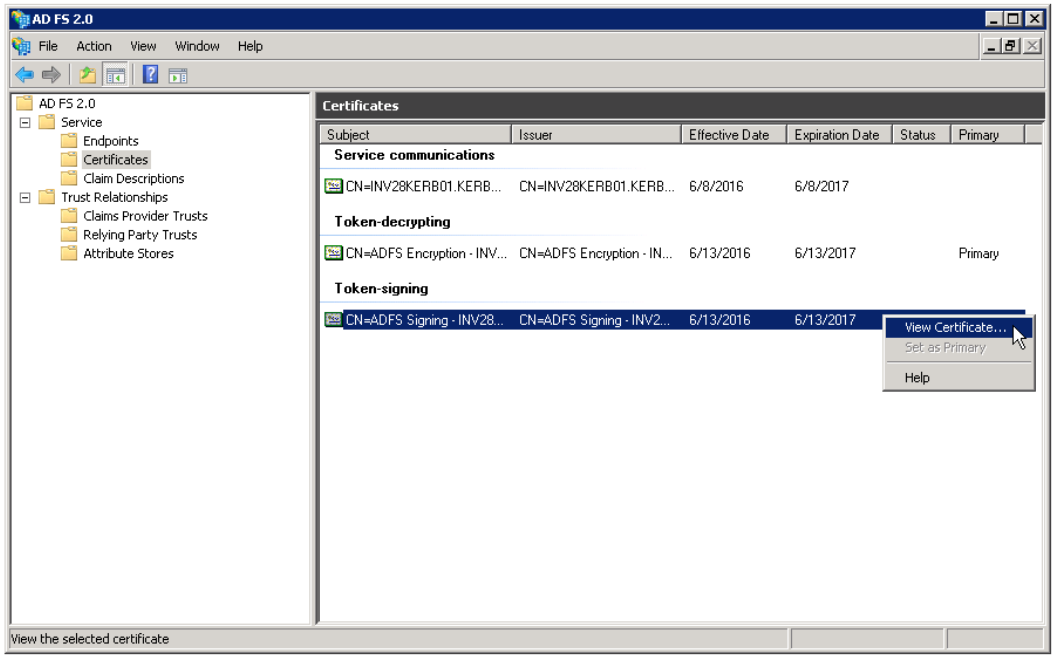
Step 2. Export the Certificate from AD FS

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.

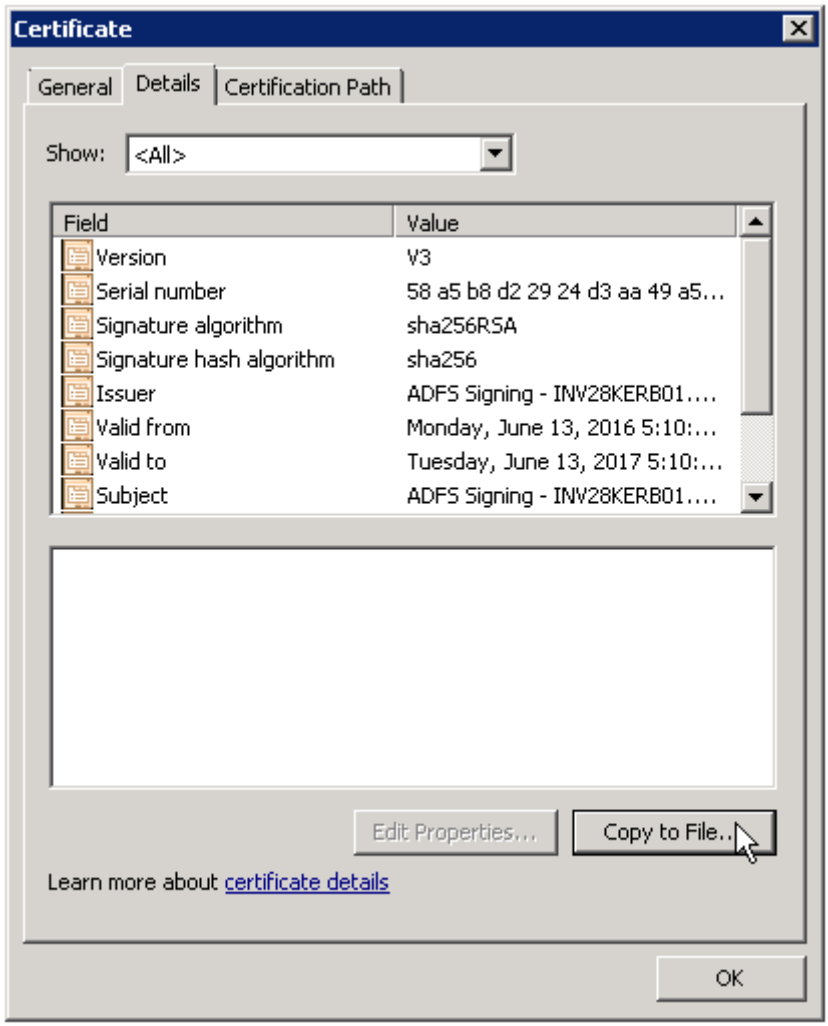
1. Log in to the AD FS Management Console.
2. Expand the **Service** > **Certificates** folder.

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



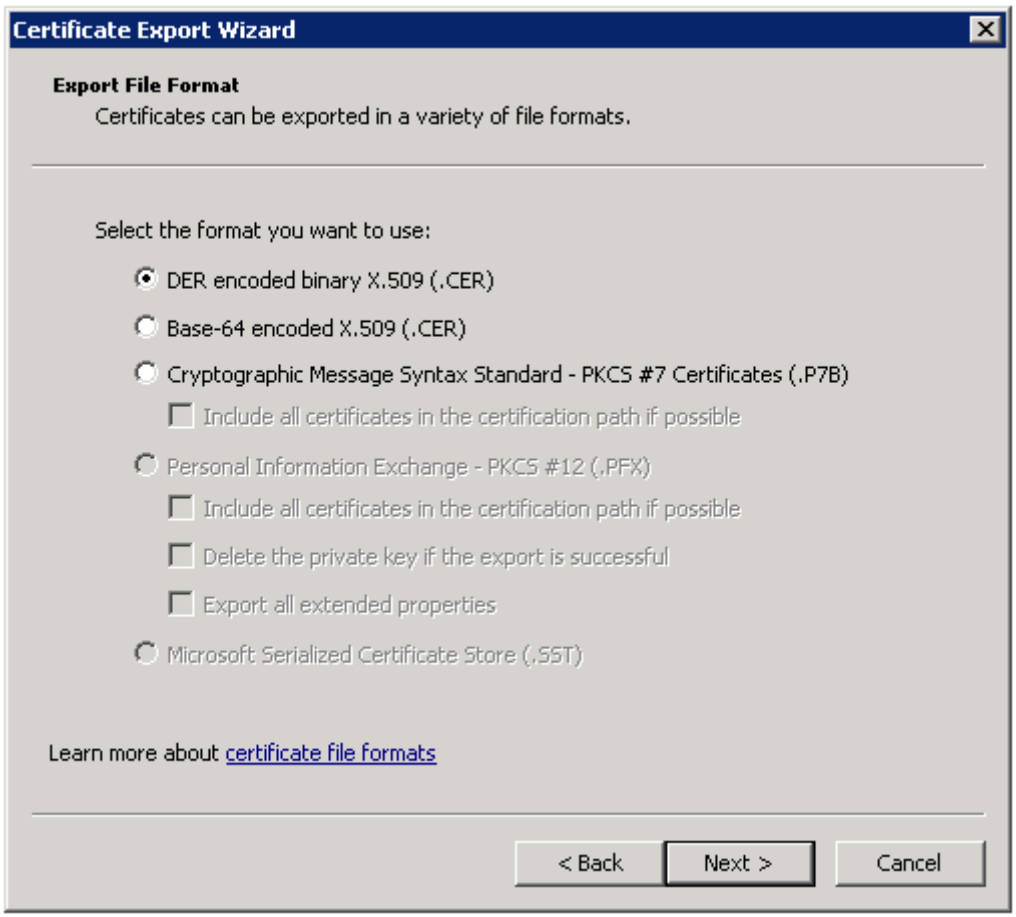
The **Certificate** dialog appears.

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 truststore file name must be `infa_truststore.jks`.

The default Informatica truststore file is installed in the following location on each node:

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

Use the Java keytool key and certificate management utility to import the certificate into the truststore file on each gateway node.

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:

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

3. From the command line, run the following command:

   ```
   keytool -import -alias <certificate alias name> -file <certificate path>\<certificate filename> -keystore <path to infa_truststore.jks> -storepass <password>
   ```

   Include the password for the truststore file.

4. Restart the node.

Step 4. Configure Active Directory Federation Services

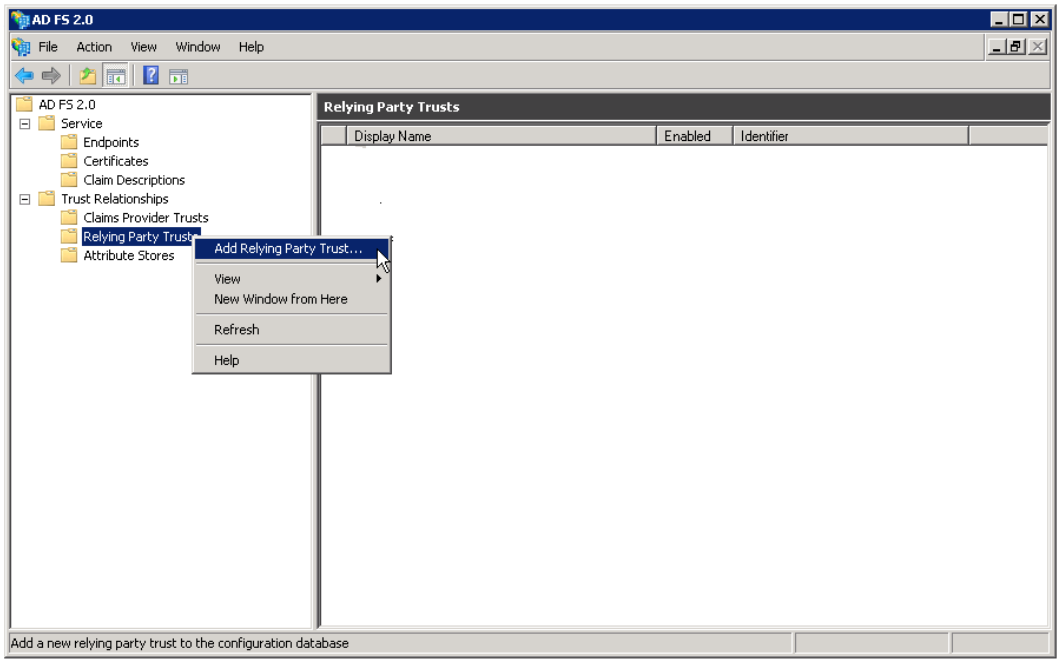
Configure AD FS to issue SAML tokens to Informatica web applications.

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

- Add Informatica as a relying party trust in AD FS. The relying party trust definition enables AD FS to accept authentication requests from Informatica web applications.
- 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.

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 select **Add Relying Party Trust** as shown in the following image:

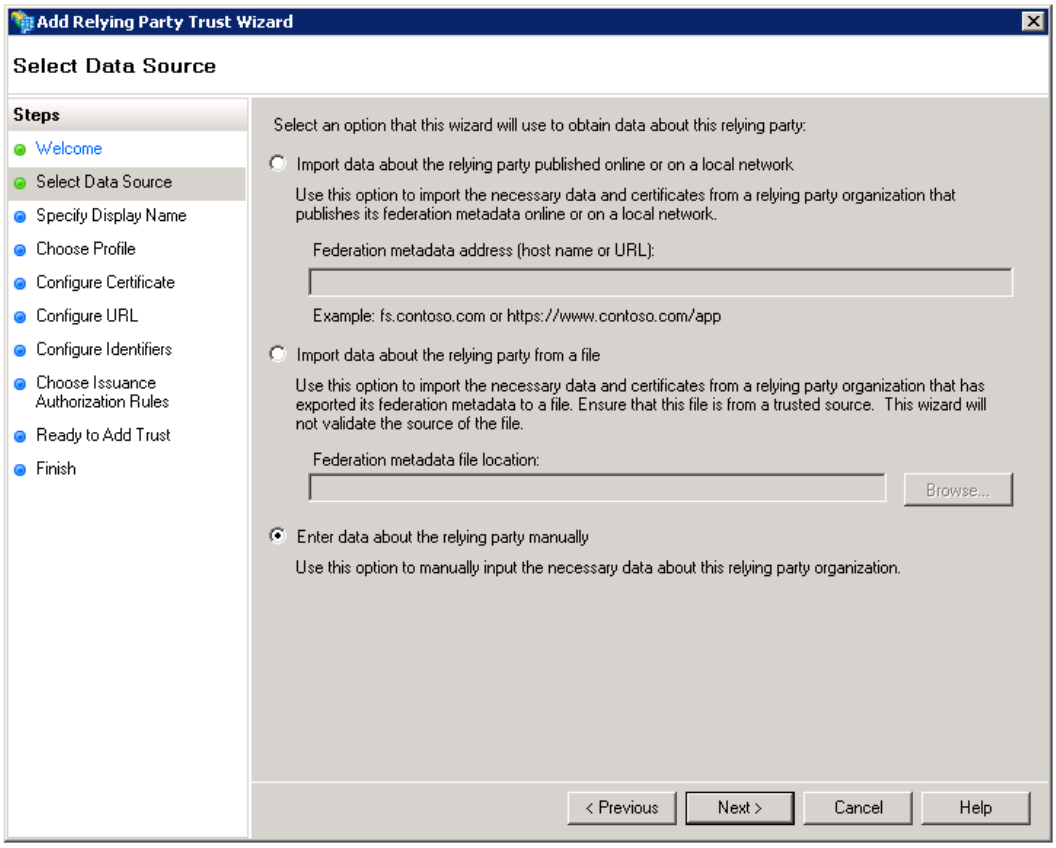


   The **Add Relying Party Trust Wizard** appears.

4. Click **Start**.

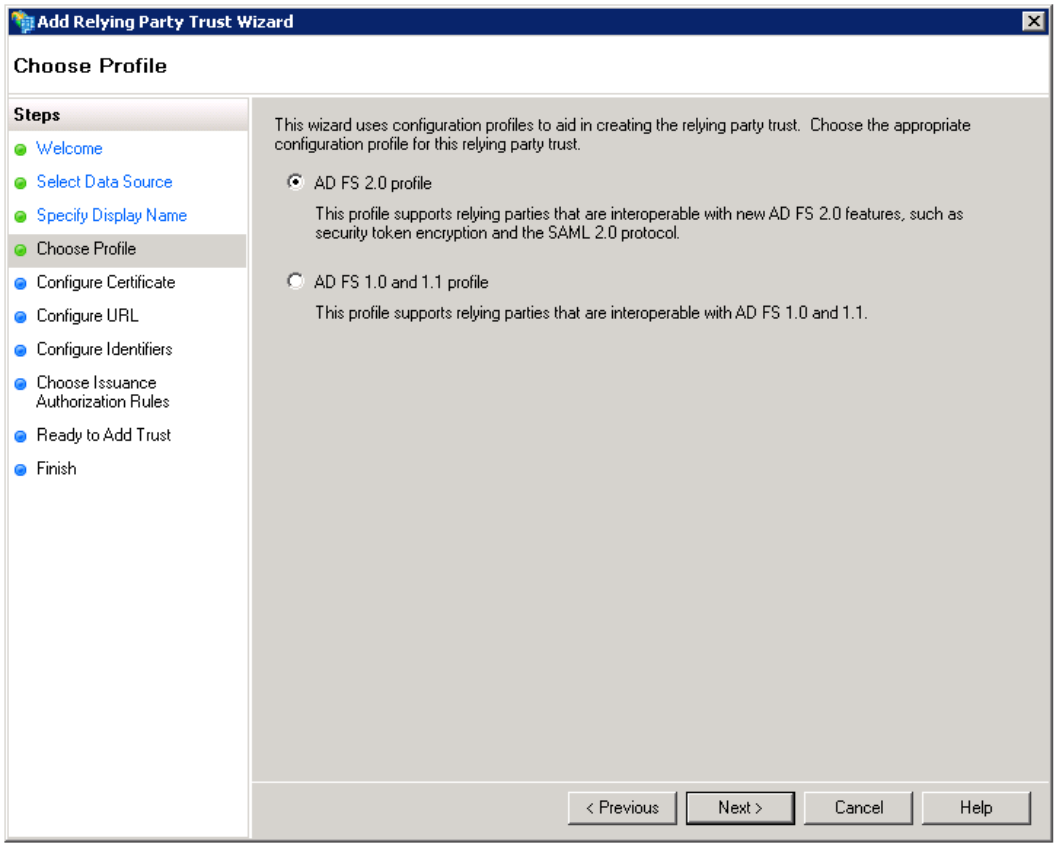
   The **Select Data Source** panel appears.

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



6. Click **Next**
7. Enter "Informatica" as the display name, and then click **Next**.

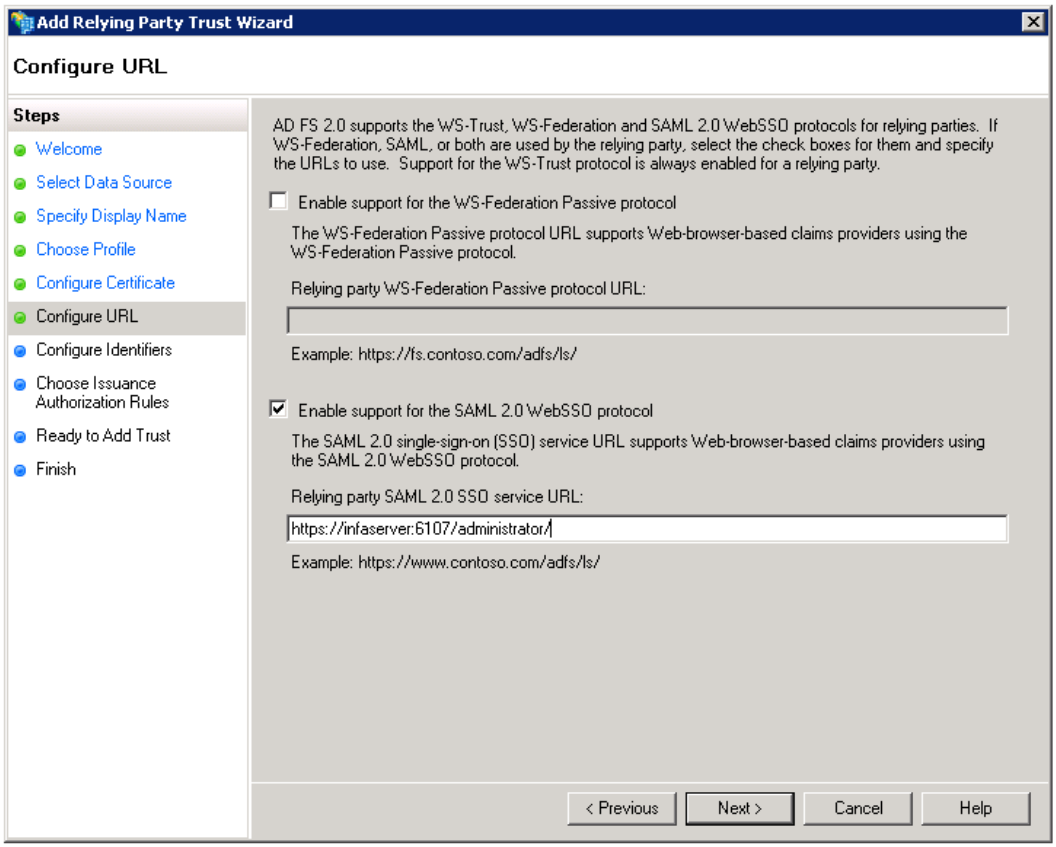
8. Click **AD FS 2.0 profile** as shown in the following image:



9. Click **Next**.

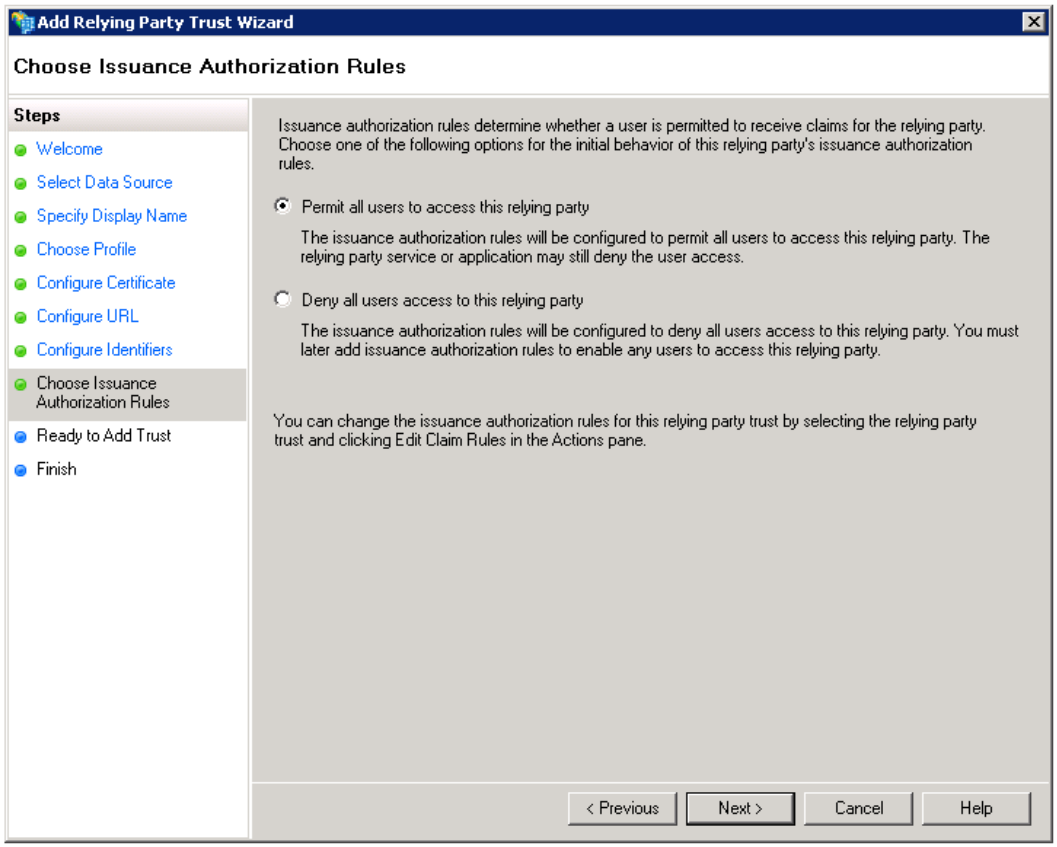
   Skip the certificate configuration panel in the wizard.

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



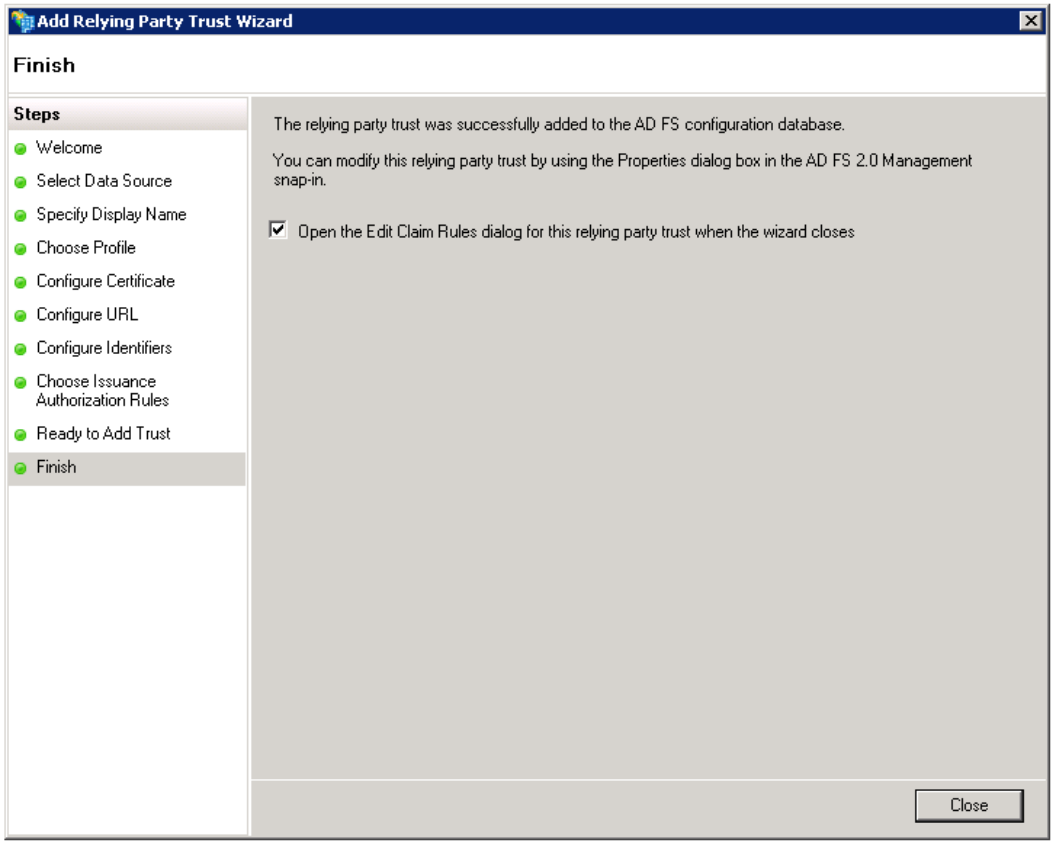
11. Click **Next**.
12. Enter "Informatica" in the Relying party trust identifier field. Click **Add**, and then click **Next**.

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:



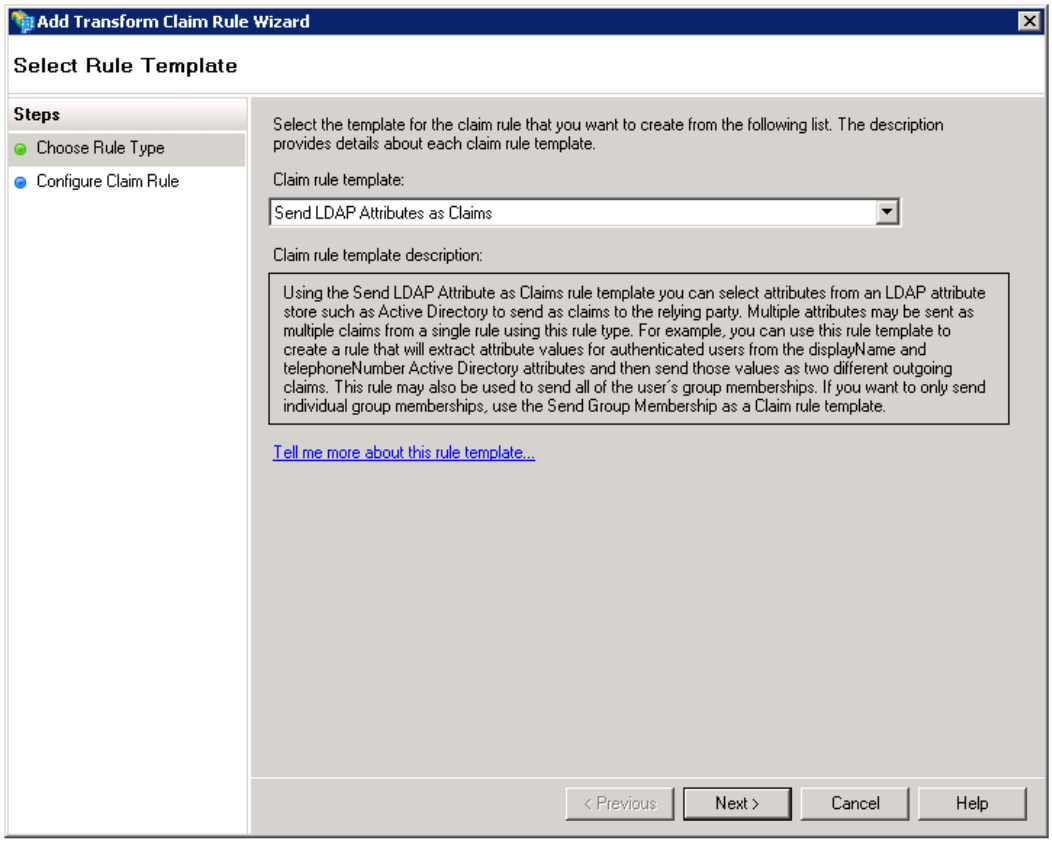
16. Click **Close**.

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

17. Click **Add Rule**.

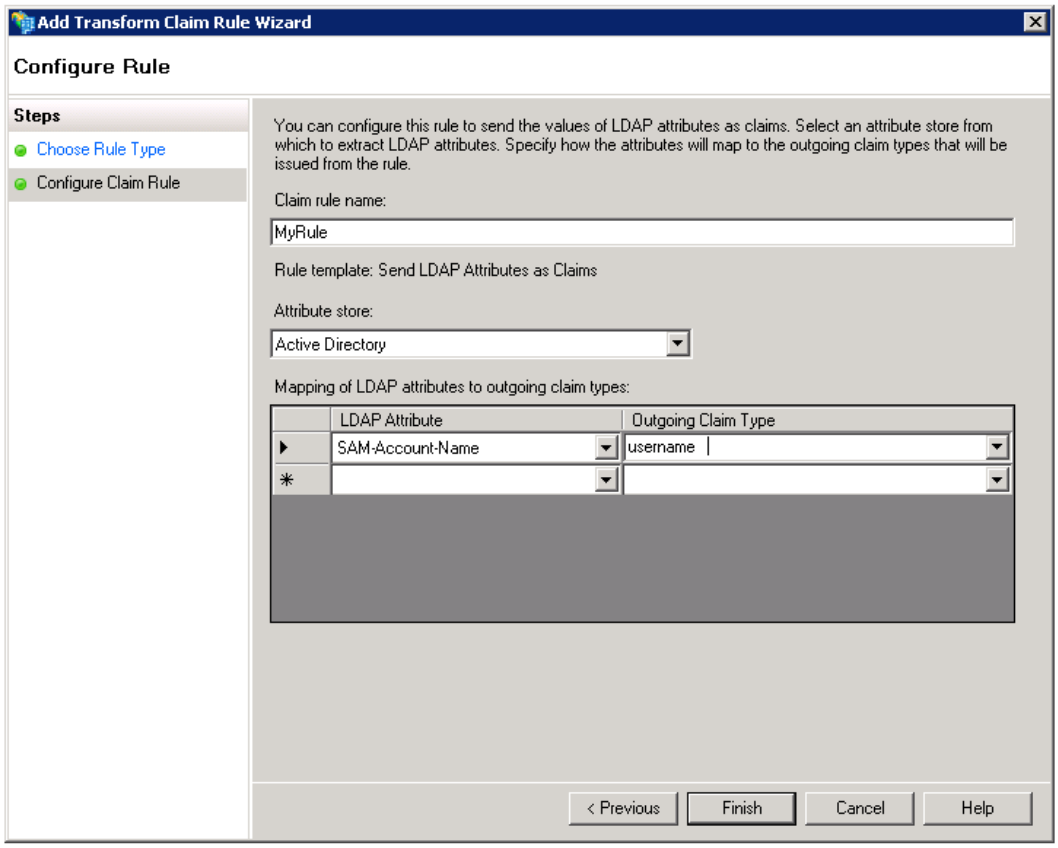
    The **Add Transform Claim Rule Wizard** opens.

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 image below:



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

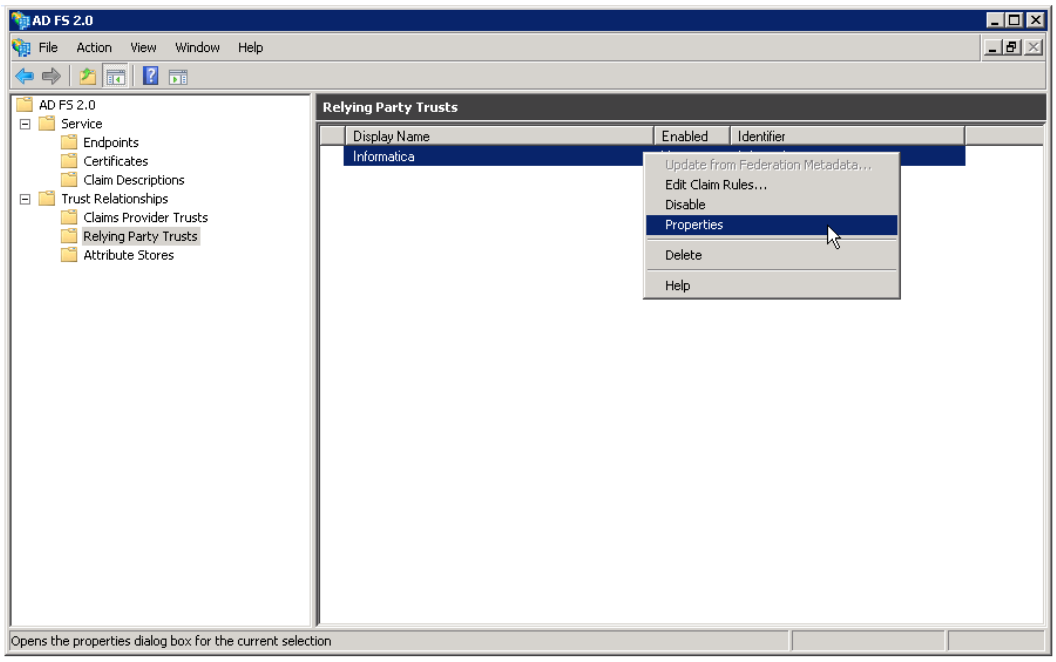
Add the URL for each Informatica web application using single sign-on to AD FS.

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, since 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 image below:

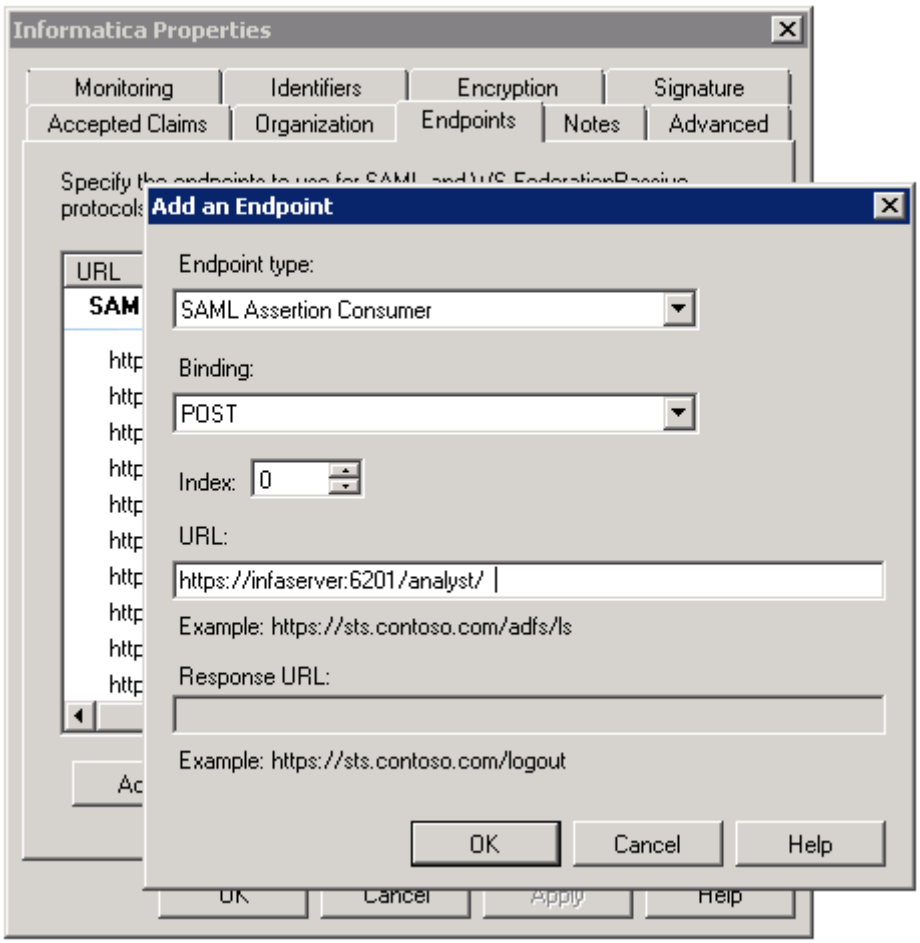


The **Informatica Properties** dialog box appears.

4. Click the **Endpoints** tab.

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

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



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

   Repeat this procedure for each web application.

Step 6. Enable SAML-based Single Sign-on

You can enable SAML-based single sign-on in an existing Informatica domain, or you can enable it when you install or create a domain.

Select one of the following options:

Enable single-sign on when you install the Informatica services.

You can enable SAML-based single sign-on and specify the identity provider URL when you configure the domain as part of the installation process.

Enable single sign-on in an existing domain.

Use the infasetup updateSamlConfig command to enable single sign-on in an existing Informatica domain. You can run the command on any gateway node within the 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:

```
infasetup updateSamlConfig -saml true -iu https://server.company.com/adfs/ls/
```

Enable single sign-on when you create a domain.

Use the infasetup defineDomain command to enable single sign-on when you create a domain.

The following example shows the SAML options as the final two options on the command line:

```
infasetup defineDomain -dn TestDomain -nn TestNode1 -na host1.company.com -cs
"jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp test_user -dt oracle -rf
$HOME/ISP/BIN/nodeoptions.xml -ld $HOME/ISP/1011/source/logs -mi 10000 -ma 10200 -ad
test_admin -pd test_admin -saml true -iu https://server.company.com/adfs/ls/
```

infasetup Command Options

Set the SAML options in the infasetup updateSamlConfig command to enable single sign-on in a domain or in the infasetup defineDomain command when you create a domain.

The following table describes the options and arguments:

Option	Argument	Description
-EnableSaml -saml	true|false	Required. Set this value to true to enable SAML-based single sign-on for supported Informatica web applications within the Informatica domain. Set this value to false to disable SAML-based SSO 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.

See the *Informatica Command Reference* for instructions on using the infasetup updateSamlConfig and infasetup defineDomain commands.

Getting the Identity Provider URL

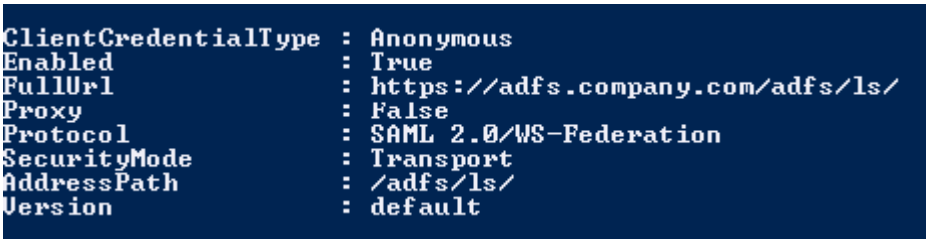
You must provide the SAML 2.0/WS-Federation URL for the AD FS server to enable single sign-on.

You set this URL as the value for the -iu option when you run the infasetup updateSamlConfig command or the infasetup defineDomain command. Use Windows PowerShell on the AD FS server to get the URL.

1. Open the Windows PowerShell command prompt window on the AD FS server. Select the Run as administrator option when you open the command prompt.
2. Type the following command at the Windows PowerShell command prompt:

```
Get-ADFSEndpoint
```

3. Find the FullUrl value returned for the SAML 2.0/WS-Federation protocol, as shown in the image below:



Author

Dan Hynes