Symantec™ Managed PKI®

Integrating Client Authentication Certificates for Web SSO through AD FS

Symantec

Symantec™ Managed PKI® Integrating Client Authentication Certificates for Web SSO through AD FS

Last updated January 1, 2015

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1

Integrating Managed PKI for Web SSO through AD FS

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile devices they use, whether you provide their devices or they bring their own.

Symantec's Managed PKI digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from several devices to thousands of devices, providing an in-the-cloud solution for quick deployment and easy management. It also incorporates features from Symantec's other leading security products.

Symantec's Managed PKI issues certificates that can be used to authenticate users for secure communications with company resources, such as VPNs and websites.

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. For example, consider a Service Provider (SP) who has a web application and ACME Corporation has an Identity Provider (IdP) Active Directory Federation Services (AD FS). ACME Corporation has a database of people who need to access the SP's web application. If John Smith from ACME Corporation wants to connect to the SP's web application, then the SP has to trust John Smith coming from ACME Corporation. The trust has to be established between AD FS and the SP.

The web application verifies if the user is already authenticated. If John Smith is authenticated, the browser allows to access the web application. If John Smith is not authenticated, the browser redirects to ACME's IdP to authenticate John Smith against ACME's database of users. The browser comes back to the SP's web application and provides the signed assertion from ACME's IdP which the SP can trust.

SAML enables web-based authentication and authorization scenarios including cross-domain Single Sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user. The user can use this signed assertion for other applications that use the SAML request.

This document describes how to obtain the Managed PKI Client Authentication certificate and allow third parties to use it through AD FS.

To achieve this, the enterprise must:

- Integrate Client Authentication certificate with the third-party web applications (as the Service Provider) through AD FS (as the Identity Provider).
- Configure AD FS.
- Configure the third-party web applications to use the MPKI certificate.

Note: This document uses Salesforce and Microsoft Office 365 as examples of these third-party web applications.

Partner Information

The following procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Salesforce.com/Force.com Microsoft
Product Name	Salesforce.com AD FS 2.0 and AD FS 3.0 Microsoft Office 365
Server	Windows 2008 R2 for AD FS 2.0 Windows 2012 R2 for AD FS 3.0

Prerequisities

- Set up Active Directory.
- Install and configure PKI Enterprise Gateway on a Windows 2008 R2 system. For more information, refer to *Symantec PKI Enterprise Gateway Deployment Guide*.
- Install and configure PKI Enterprise Gateway Autoenrollment Server. For more information, refer to *Symantec PKI Enterprise Gateway Autoenrollment Server Deployment Guide*.
- Install PKI Client. For more information, refer to *Symantec PKI Client Administrator's Guide*.

Note: Configuration of PKI Enterprise Gateway and PKI Enterprise Gateway Autoenrollment Server can vary depending on the deployment scenario within the enterprise environment and policies.

Integration Workflow

The following diagram describes the general steps required to set up the Symantec Managed PKI account and create the certificate profile:

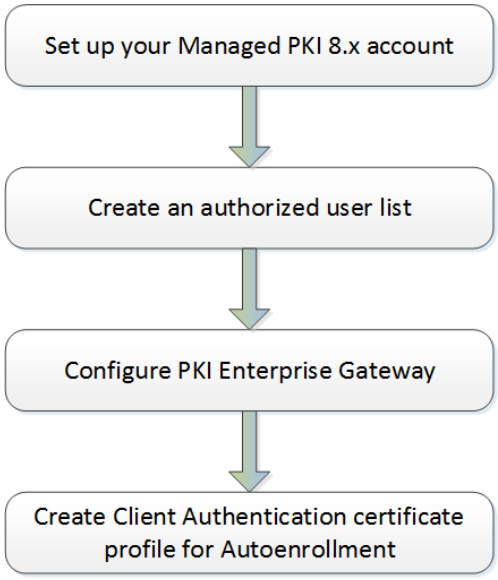

Figure 1-1 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.x account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.

- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create an authorized user list

1. Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.
2. On the PKI Manager dashboard, click **Manage authorized user lists** from the Tasks menu on the bottom navigation bar.
3. Click **Add authorized user lists** from the top of the resulting Manage authorized user lists page. The Add authorized user list page appears.
4. Enter the user list information, listed in Table 1-2.

Table 1-2 Information required for User Lists

Field	Description
User list friendly name and description	Enter a unique name and description to identify this user list.
User list directory type	Select whether your user store is an Active Directory or LDAP user store.
Set as default for new profiles	Identify if this user list will be used for all new certificate profiles by default.
Directory groups	Enter the directory group based on the directory type selected.

5 Click **Save**.

Task 3. Configure PKI Enterprise Gateway

1 On the PKI Manager dashboard, click **Manage PKI Enterprise Gateways** from the Tasks menu on the bottom navigation bar.

2 Click **Add PKI Enterprise Gateways** from the top of the resulting Manage PKI Enterprise Gateways. The PKI Enterprise Gateway settings page appears.

3 Enter the PKI Enterprise Gateway configuration information, listed in Table 1-3.

Table 1-3 Information required for PKI Enterprise Gateway

Field	Description
PKI Enterprise Gateway friendly name and description	Enter a unique name and description to identify this gateway.
PKI Enterprise Gateway directory type	Select whether your user store is an Active Directory or LDAP user store.
Set as default for new profiles	Identify if this PKI Enterprise Gateway will be used for all new certificate profiles by default.
How is your PKI Enterprise Gateway deployed	Identify whether you will install PKI Enterprise Gateway in single-server or multiple-server mode.
URL where PKI Enterprise Gateway is installed	Enter the URL as specified by your administrator.
Authentication Service port number	Enter the port number as 9101. Certificate enrollment will fail if the port number is incorrect.
RA Agent port number	Enter the port number as 9102. Certificate enrollment will fail if the port number is incorrect.
RA Service port number	Enter the port number as 9100. Certificate enrollment will fail if the port number is incorrect.
Enable autoenrollment	Select this option for autoenrollment.
Autoenrollment Service Host	Enter the name of the server where PKI Enterprise Gateway resides. For example, enter `http://symc-18.78` instead of `http://symc-18.78.adfs.com`

The values you enter here are captured in the **egwService_Summary** log file, which is created on successful installation and configuration of PKI Enterprise Gateway. This file is available in **\Users\Public** folder on a Windows 2008 R2 system.

4 Click **Submit**.

Task 4. Create Client Authentication certificate profile for Autoenrollment

Managed PKI uses a certificate profile to define issued certificates. Complete the following steps to create your Managed PKI Client Authentication certificate profile:

1 On the PKI Manager dashboard, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.

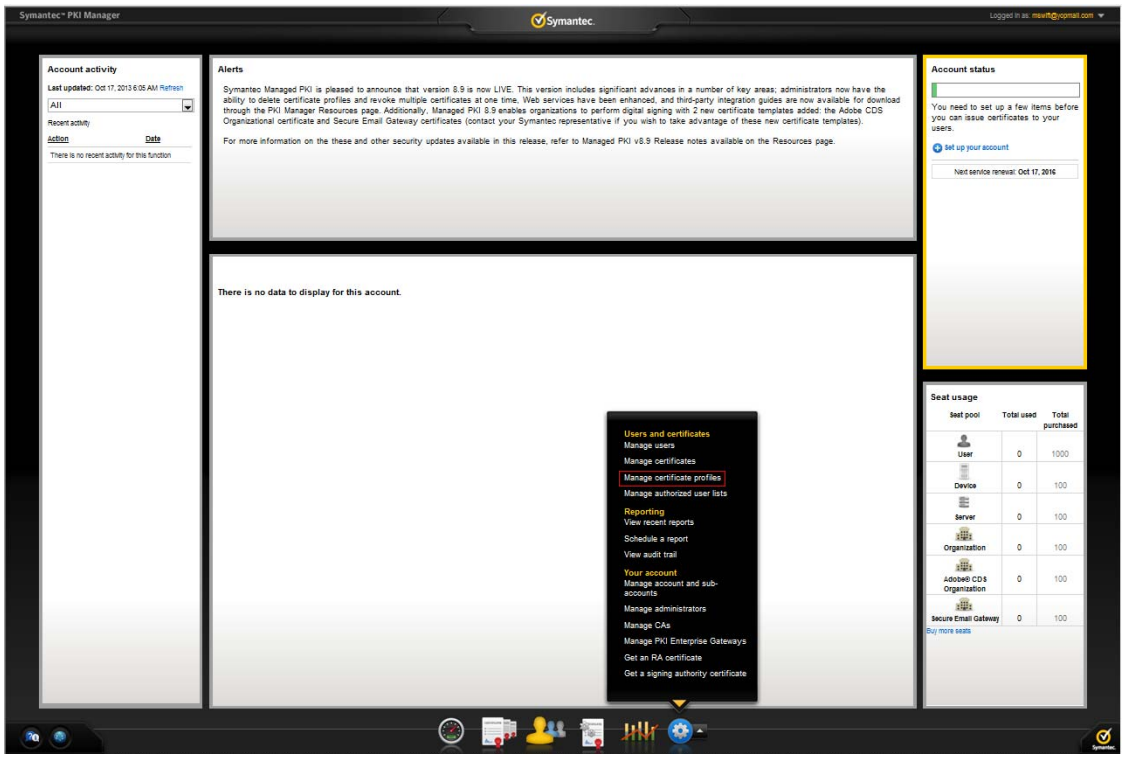

Figure 1-2 Manage Certificate Profile

2 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.

3 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.

4 Select **Client Authentication** as the certificate template and click **Continue**. The Customize certificate options page appears.

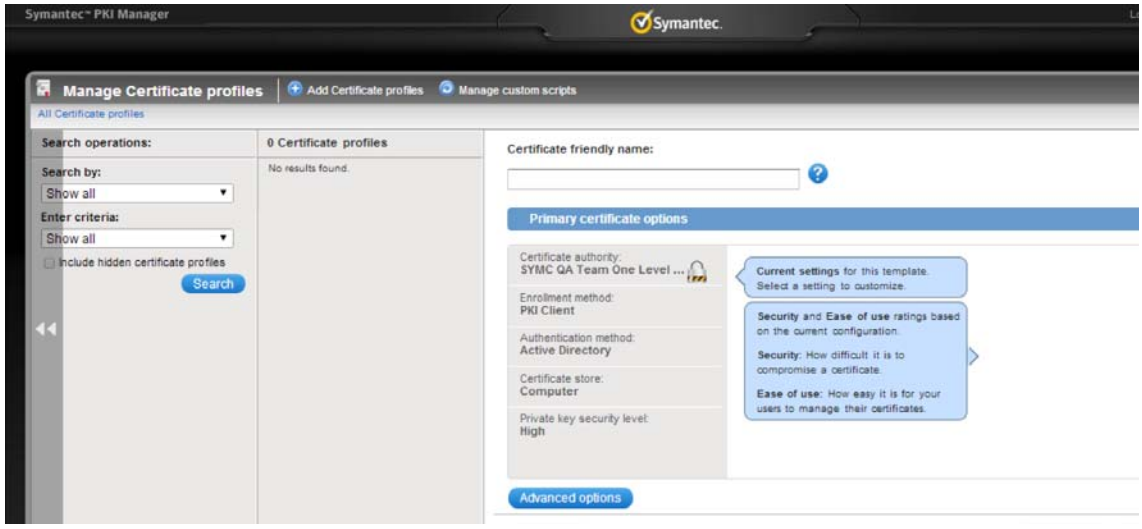

Figure 1-3 Client Authentication Certificate Options

5 Configure the certificate profile based on the way the users will enroll for the certificates.

- If the users will enroll for the certificates automatically, use the settings in Table 1-4.
- If the users will enroll for the certificates manually using the Managed PKI client, use the settings in Table 1-5.

Table 1-4 Certificate Profile configurations for Microsoft Autoenrollment

Options	Configuration
Certificate friendly name	Enter a certificate profile name.
Enrollment method	**Microsoft Autoenrollment**
Enrollment mode	**Silent**
Authentication method	Microsoft Autoenrollment
Certificate Store	Locked on **Computer**
Private key security level	**High**
Subject DN Common Name (CN)	Select **Active Directory attribute** for Source for the field's value. Select mail as **Attribute.**
Organization Unit (OU)	Locked to a fixed value
SubjectAltName Other Name (UPN)	Select **Active Directory attribute** for Source for the field's value. Select mail as **Attribute.**

Table 1-5 Certificate Profile configurations for PKI Client

Option	Configuration
Certificate friendly name	Enter a certificate profile name.
Enrollment method	**PKI Client**. Select the **Allow end users to download PKI Client** check box to allow end users to download PKI Client on their system.
Authentication method	Active Directory Select the appropriate Authorized user list and PKI Enterprise Gateway.
Certificate Store	Configurable
Private key security level	**High**
Subject DN Common Name	Select **Active Directory attribute** for Source for the field's value. Select mail as **Attribute**.
Organization Unit (OU)	Configurable
SubjectAltName Other Name (UPN)	Select **Active Directory attribute** for Source for the field's value. Select mail as **Attribute.**

6 Click **Save**.

7 If you selected the **Microsoft Autoenrollment** enrollment method, download the configuration file of the certificate profile to be imported in Autoenrollment configuration. For more information, refer to *Symantec PKI Enterprise Gateway Autoenrollment Server Deployment Guide*.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

Chapter 2

Configuring Salesforce to Use the Managed PKI Certificate

This chapter discusses how to configure Salesforce to integrate it with ADFS.

Prerequisities

- You must have administrative rights on Salesforce.com web site.
- You must have registered your domain on Salesforce.com web site.
- You must have created new users to your registered Salesforce domain. Later, these users will be mapped to Active Directory users.
- AD FS must be installed on a Windows 2008 R2 or Windows 2012 R2 server and an assertion signing certificate from AD FS must be available to be imported in Salesforce at a later point.

How the Salesforce Integration with AD FS Works

The following diagram describes how the administrator configures Salesforce, AD FS, and Managed PKI for Single sign-on:

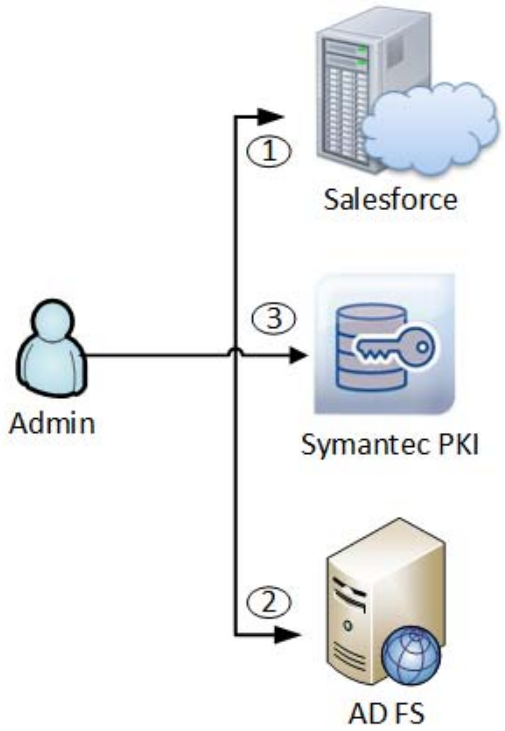

Figure 2-1 Administrator Configuration

1 Administrator logs into Salesforce and does the following:
   - Configures Single Sign On
   - Creates users with Federation ID mapping
   - Downloads Single Sign On configuration file from Salesforce

2 Administrator configures AD FS using the configuration file downloaded in step 1 and creates Federation ID mappings.

3 Administrator contacts Managed PKI and creates a Seat ID.

The following diagram describes the flow of events when an end user tries to log onto the Salesforce website:

.

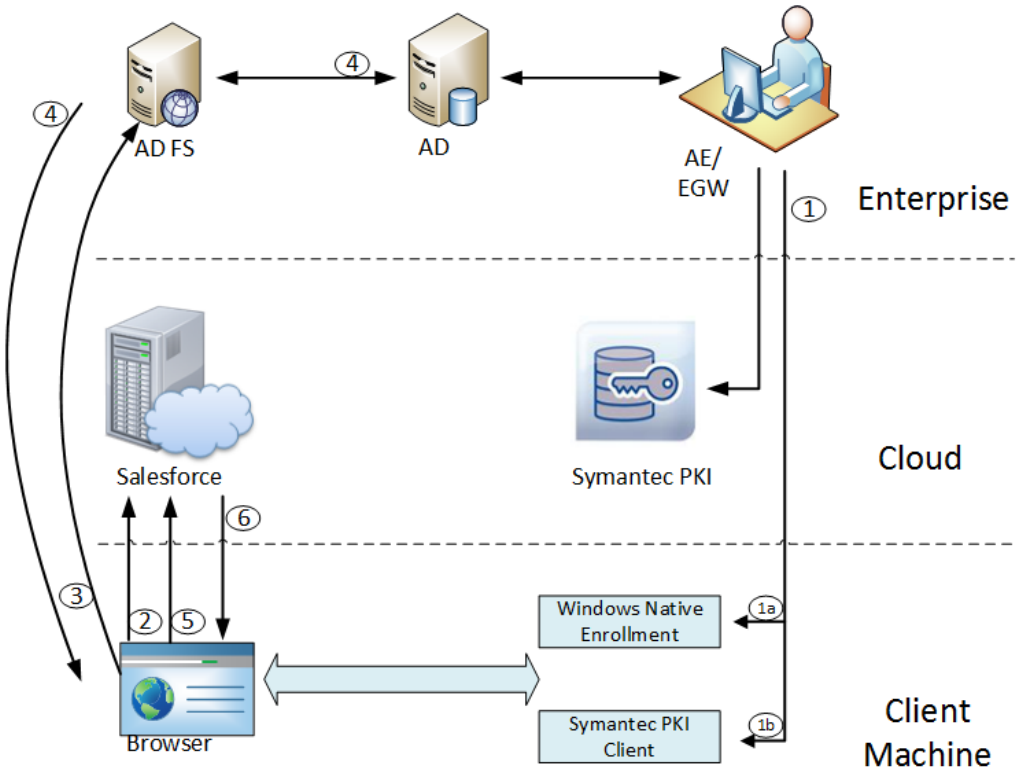

Figure 2-2 End User Configuration

1 When an end user logs into a machine or a certificate policy is pushed to an end-user machine through a Windows group policy, the autoenrollment client checks the Active Directory and the local certificate store to determine for which certificate template it can enroll the end user. The Autoenrollment server requests a certificate from Symantec Managed PKI. The certificate can be installed in one of the following ways:

   a Certificate installed on Windows Native enrollment only for Internet Explorer browser.

   b Certificate installed on Symantec PKI Client.

   For more information, refer to *Symantec PKI Enterprise Gateway Autoenrollment Server Deployment Guide*.

2 End user tries to reach the hosted web application on Salesforce from their browser.

3 Salesforce generates a SAML authentication request. The SAML request is encoded and embedded into a URL and sent to AD FS.

4 AD FS authenticates the user in AD. After authentication, user information is taken from AD and a SAML response is generated.

5 The browser submits the request to Salesforce, which logs the user in if the response is successfully verified.

6 The user is redirected to the destination URL.

Configuring Salesforce for SSO

To configure SAML settings for Single Sign-On with Salesforce.com:

1 Go to Salesforce.com web site and login as an administrator.

2 In the left navigation pane, click **Administer Security → Controls Single→ Sign-On Settings**. The Single Sign-On Settings page appears.

3 On the Single Sign-On Settings page, click **Edit**.

4 Under **Federated Single Sign-On Using SAML**, select **SAML Enabled** and click **Save**.

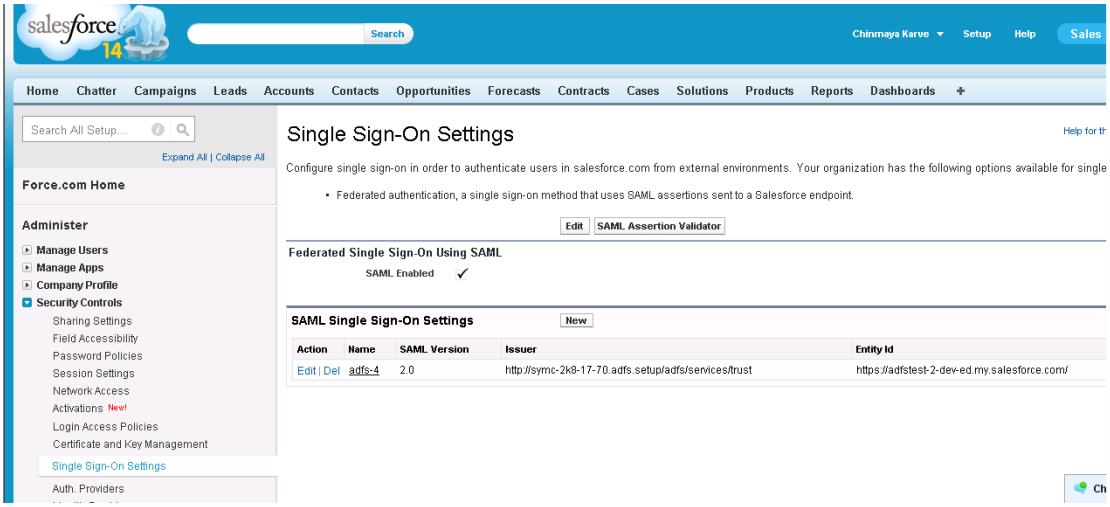

Figure 2-3 Single Sign-On Settings

5 Click **New** for SAML Single Sign-On Settings. The SAML Single Sign-On Settings page is displayed. Enter the field values as listed in Table 2-1 to add a SAML Single Sign-On.

Table 2-1 SAML Single Sign-On Settings

Field	Description
Name	Enter user friendly name for your configuration. For example, ADFS_SF_SSO
API Name	Automatically displays API name based on the name you entered in the Name field. You can modify the API name if required.
SAML Version	The version of SAML your identity provider uses. The SAML version for the current Salesforce version is 2.0.
User Provisioning Enabled	Select to enable just-in-time user provisioning for SAML.
Issuer	Your AD FS trust url. For example: `http://<your adfs system fqdn>/adfs/services/trust`
Entity Id	Your registered domain on Salesforce.com portal. For example: `https://<your registered domain>.salesforce.com`
Identity Provider Certificate	The authentication certificate issued by your identity provider. Refer to your vendor documentation for instructions on obtaining this certificate.

Table 2-1 SAML Single Sign-On Settings

Field	Description
Signing Certificate	The certificate used to generate the signature on a SAML request. Refer to your vendor documentation for instructions on obtaining this certificate.
SAML Identity Type	Select **Assertion contains the Federation ID from the User object**.
SAML Identity Location	Select **Identity is in the NameIdentifier element of the Subject statement**.
Identity Provider Login URL	The URL of your AD FS SAML endpoint, to which Salesforce.com will send SAML requests for SP-initiated login.
Identity Provider Logout URL	You can configure a URL to which the user will be sent after they log out.
Custom Error URL	Any custom URL that you want to display to the end users in case of login errors.
Service Provider Initiated Request Binding	Select HTTP Post as the binding mechanism.

6 Click **Save**. The **Salesforce Login URL** and **OAuth 2.0 Token Endpoint** is automatically generated.

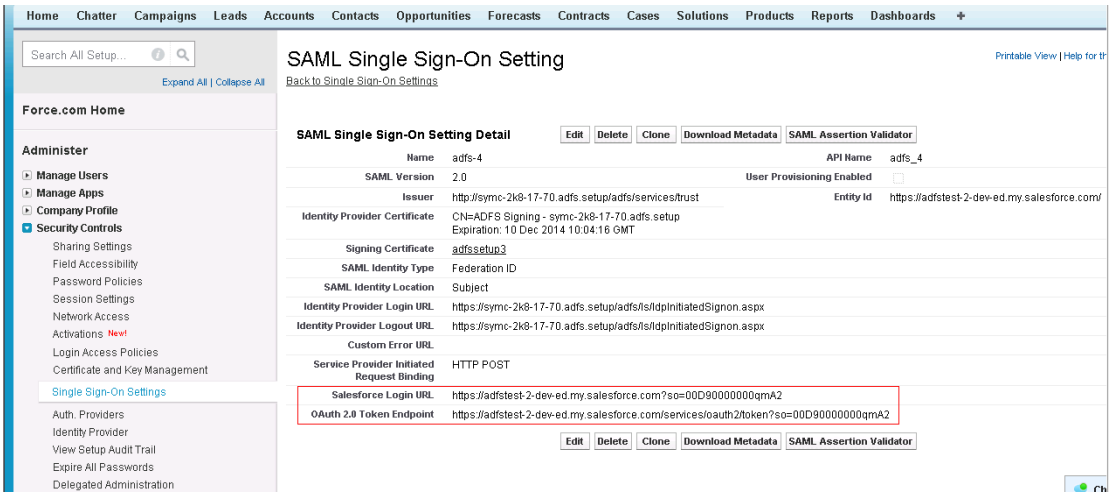

Figure 2-4 SAML Single Sign-On Setting

7 Click **Download Metadata** and save the XML file.

Configuring Salesforce

1 Click Salesforce.com web site.

2 Click **Administer → Manage Users → Users**.

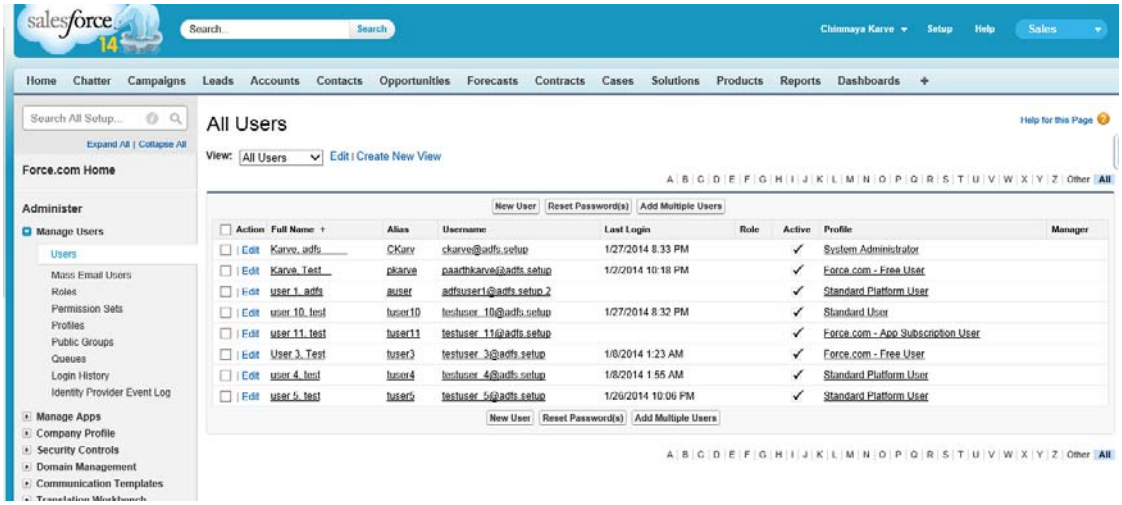

Figure 2-5 All Users

3 Select a user and click **Edit**. The User Edit page is displayed.

4 In Single Sign-On Information, enter the value for **Federation ID** that matches the **Name ID** element of Subject statement of SAML assertion generated by AD FS.

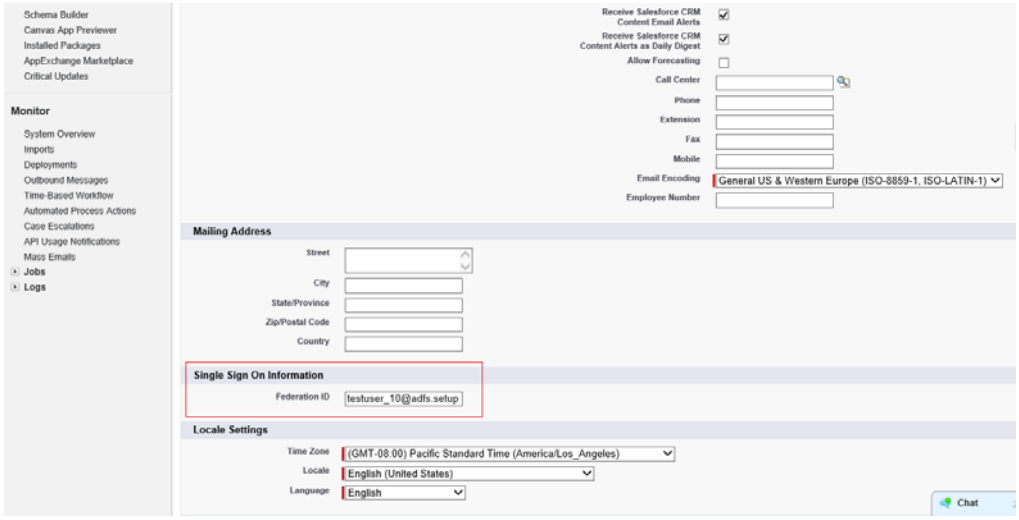

Figure 2-6 SSO Federation ID

5 Click **Save**.

6 Repeat this for the each user in Salesforce.com portal. Once Name ID and Federation ID values are matched, the user will be allowed the access the Salesforce.com web site.

Testing the configuration

1. Create a new user in AD with email ID as testuser@domainname.com where, domain name is the name of your enterprise setup.
2. Add the user to groups that are authorized for receiving Client Authentication certificates from Symantec's Managed PKI.
3. Create a new user in Salesforce.com with the `federationID=email ID` of the user.
4. Log into the Salesforce with the newly created user. A pop-up window appears on the user screen which prompts the user to install a new certificate.

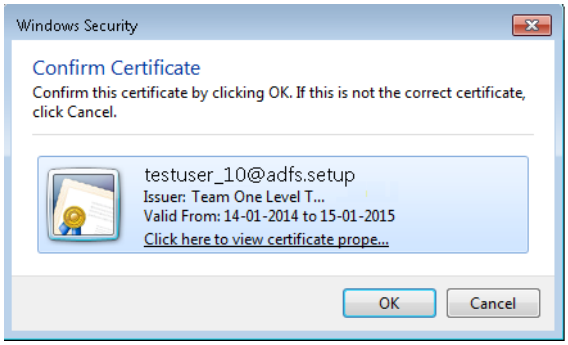

Figure 2-7 Certificate Installation

5. Install the certificate.
6. Open a new browser instance.
7. To log in to Salesforce.com select the following URL based on your set up.
   - For AD FS 2.0, https://<your adfs setup name>/adfs/ls/idpinitiatedsignon.aspx?loginToRp=https://<your Salesforce domain name>
   - For AD FS 3.0, https://<your adfs setup name>/adfs/ls/idpinitiatedsignon.htm?loginToRp=https://<your Salesforce domain name>
8. Select a certificate from the certificates listed in the pop-up window. The Salesforce.com page is displayed with the user's profile.

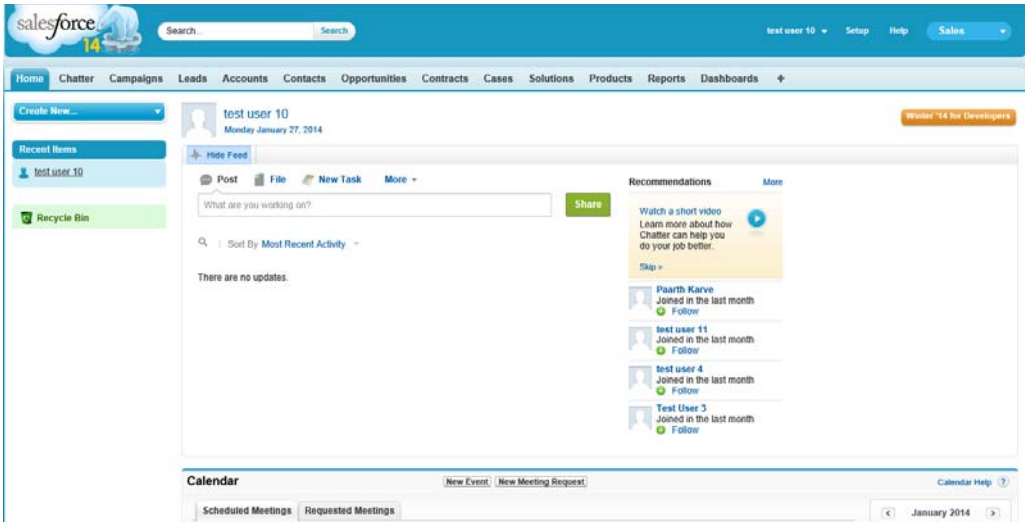

Figure 2-8 Salesforce User

Note: If the client authentication certificates are not displayed for end users on a Windows 2012 R2 system, refer to "Configuring the trusted issuers list in Windows 2012 R2" on page 23 for possible reasons and solutions.

Chapter 3

Configuring AD FS

This chapter discusses how to configure Microsoft Active Directory Federation Services (AD FS) to integrate with its partners.

The instructions in this chapter use Salesforce and Microsoft Office 365 as examples.

Prerequisites

- You must have installed Active Directory Federation Services 2.0 (AD FS) on a Windows 2008 R2 server.
- You must have enabled the Active Directory Federation Services role on the Windows 2012 R2 server.

Configuring AD FS to Deploy a Federation Server

You can use the AD FS console to configure services and policies for the deployment of a federation server.

Note: The interface for AD FS 2.0 and AD FS 3.0 are similar. The graphic images used in this document refer to AD FS 2.0 interface.

---

1. Log into the computer where AD FS is installed, as an administrator.
2. Click **Administrative Tools → AD FS Management**. The AD FS console is displayed.
3. In the left navigation pane, click **AD FS → Service → Certificates**. The certificates are grouped in the console by the type of certificate and its intended purpose.

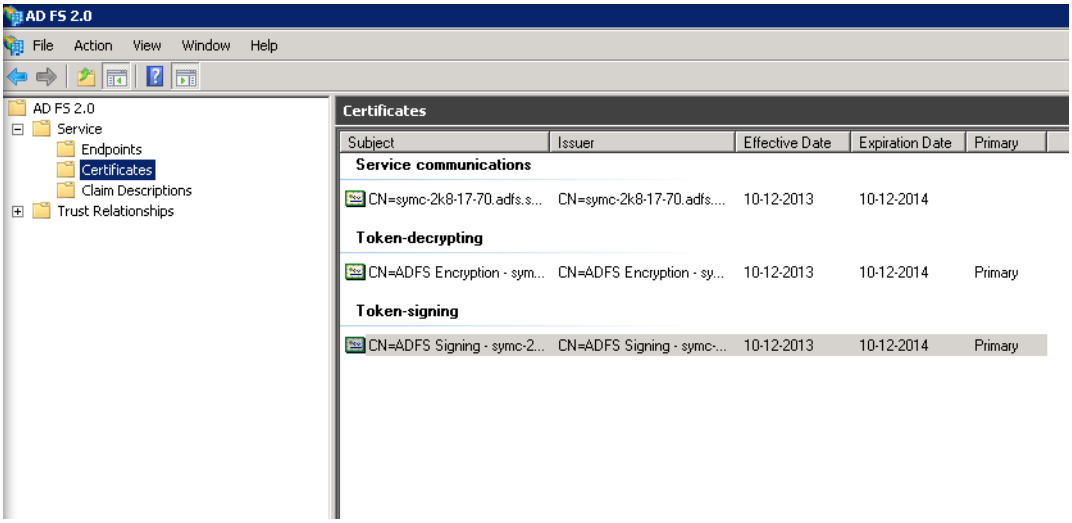

Figure 3-1 AD FS Certificates - Token Signing

4 Right-click the certificate under **Token-signing** and click **View Certificate**.

5 Go to the **Details** tab and click **Copy to File** to export the certificate. The Certificate Export Wizard is displayed.

6 Select **DER encoded binary X.509 (.CER)** format and click **Next**.

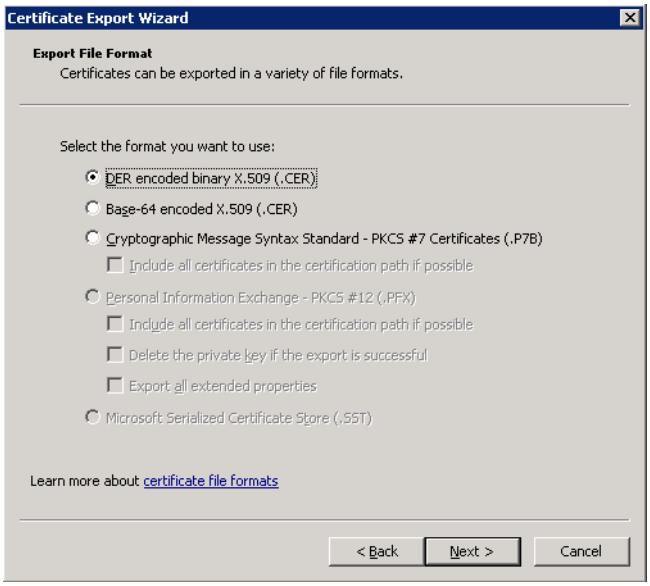

Figure 3-2 Certificate Export Wizard - DER Encoded Binary

7 Enter a file name to export the certificate and click **Finish**.

Add Relying Party Trust on AD FS

1 Log into the AD FS system, as an administrator.

2 Click **Administrative Tools → AD FS Management**. The AD FS console is displayed.

3 Click **Add Relying Party Trust**. The Add Relying Party Trust Wizard is displayed.

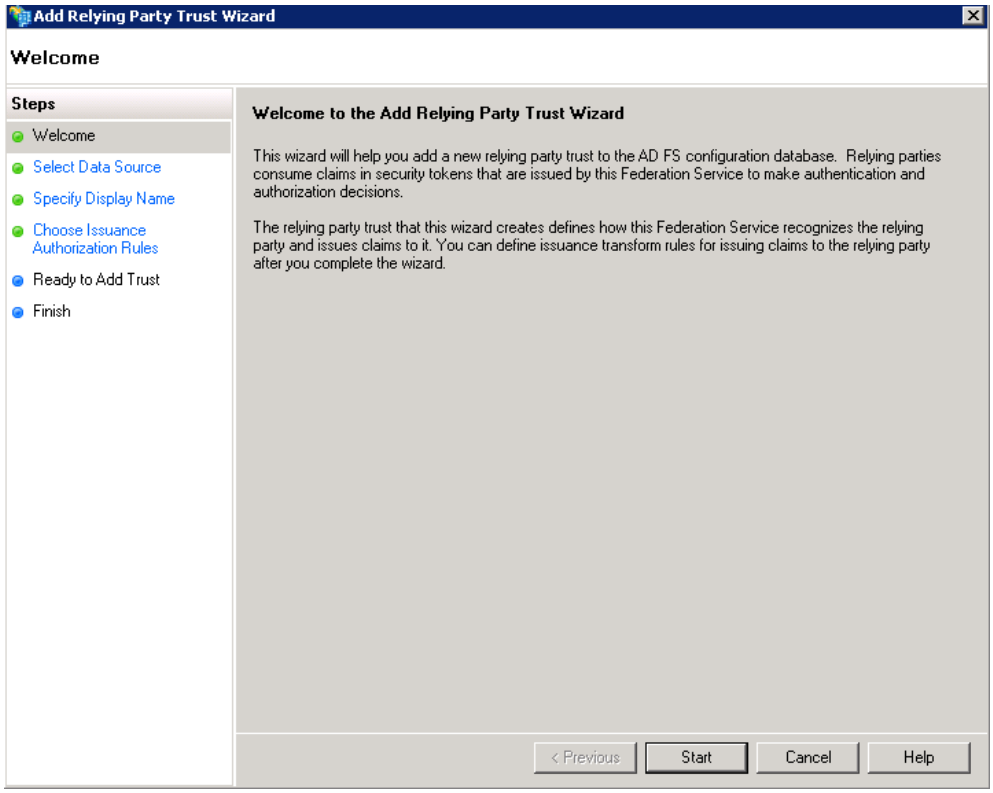

Figure 3-3 Add Relying Party Trust Wizard

4 Complete the steps in Table 3-1 to add a new relying party trust in AD FS configuration database.

Table 3-1 Add Relying Party Trust Wizard

Steps	Action
Welcome	Click **Start**.
Select Data Source	Click **Import data about relying party from a file**. Select and import the Metadata file saved as XML in "Configuring Salesforce for SSO" on page 12.
Specify Display Name	Enter a display name.
Choose Issuance Authorization Rules	Enter a display name for this relying party. **Note:** These instructions use Salesforce.com Select **Permit all user to access this relying party**.
Ready to Add Trust	Verify the **Ready to Add Trust** option.
Finish	Click **Finish** to add the relying party trust to the AD FS Configuration database.

5 Select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** and click **Close**. The Edit Claim Rules for Salesforce.com window is displayed.

Edit Claim rules in AD FS

1 In the **Issuance Transform Rules** tab, click **Add Rule**.

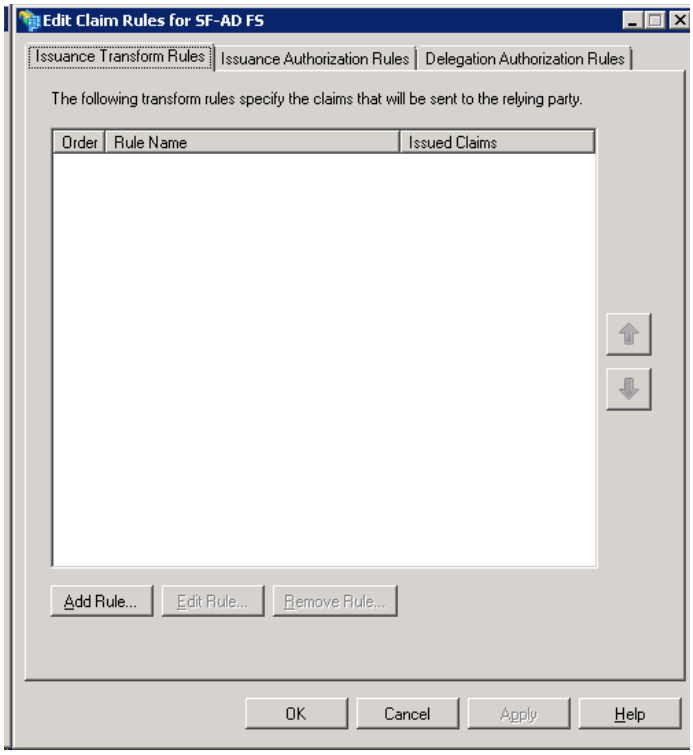

Figure 3-4 Edit Claim Rule

2 In Choose Rule Type, select **Send LDAP Attribute as Claims** and click **Next**.

- **a** Enter a Claim rule name. For example, UPN-NameID.
- **b** Select **Active Directory** as Attribute store.
- **c** For LDAP Attribute, select **User-Principal-Name (UPN)** and for Outgoing Claim Type select **Name ID**.
- **d** Click **Finish**.

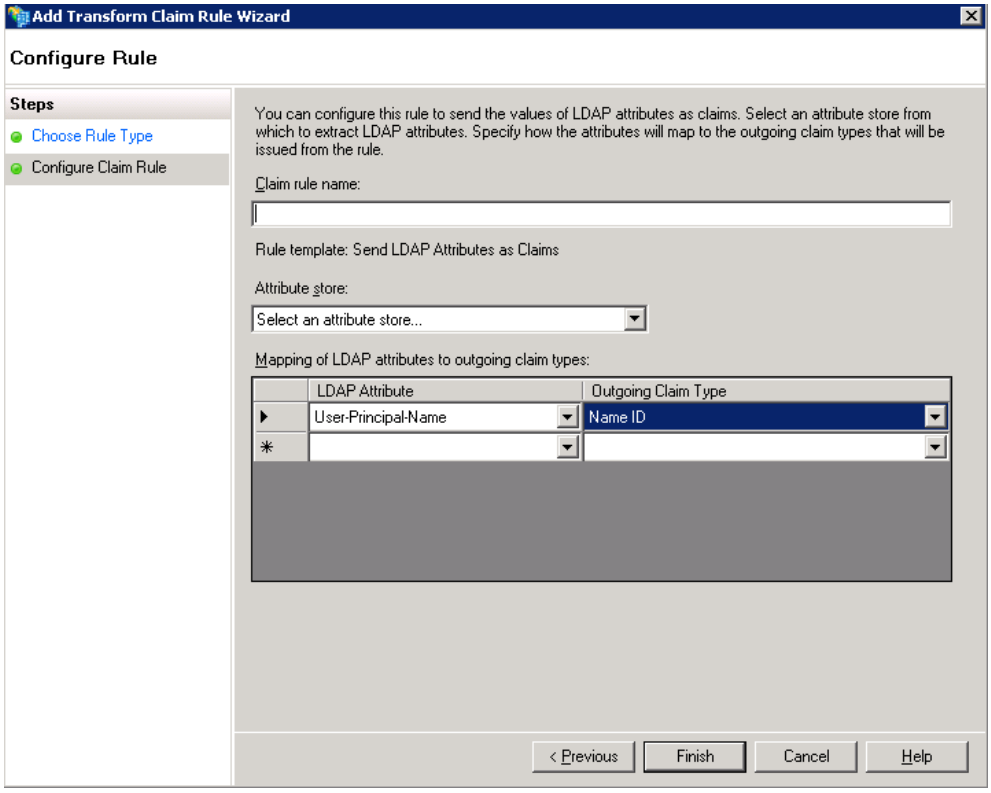

Figure 3-5 Configure Claim Rule

3 Click **OK**.

Add the Relying Party Trust for AD FS

1 In the left navigation pane, click **AD FS → Trust Relationships → Relying Party Trusts**. The Relying Party Trusts page appears.

2 Right-click the rule that you created and click **Properties**.

3 Click the **Advanced** tab and select **-1** as the secure hash algorithm. Microsoft recommends using SHA-1 algorithm.

4 Click **Apply** and click **OK**.

Enable the Endpoints for AD FS 2.0

The following instructions are applicable only for AD FS 2.0.

1 In the left navigation pane, click **AD FS 2.0→ Service → Endpoints**. The Endpoints page list the available endpoints.

2 Right-click `/adfs/services/trust/2005/certificate` from the list and choose **Enable**.

3 Restart the AD FS 2.0 services for the changes to take effect.

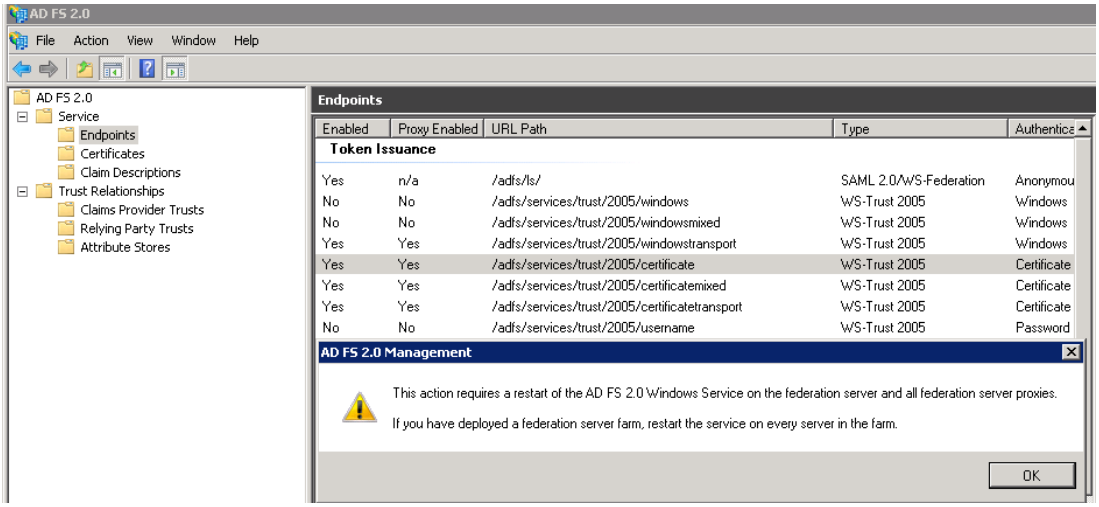

Figure 3-6 Endpoints

4 Navigate to `C:\inetpub\adfs\ls`.

5 Edit the **web.config** file settings. Under `<microsoft.identityServer.web>`, enable `TlsClient` method and disable other methods by commenting out the xml tags.

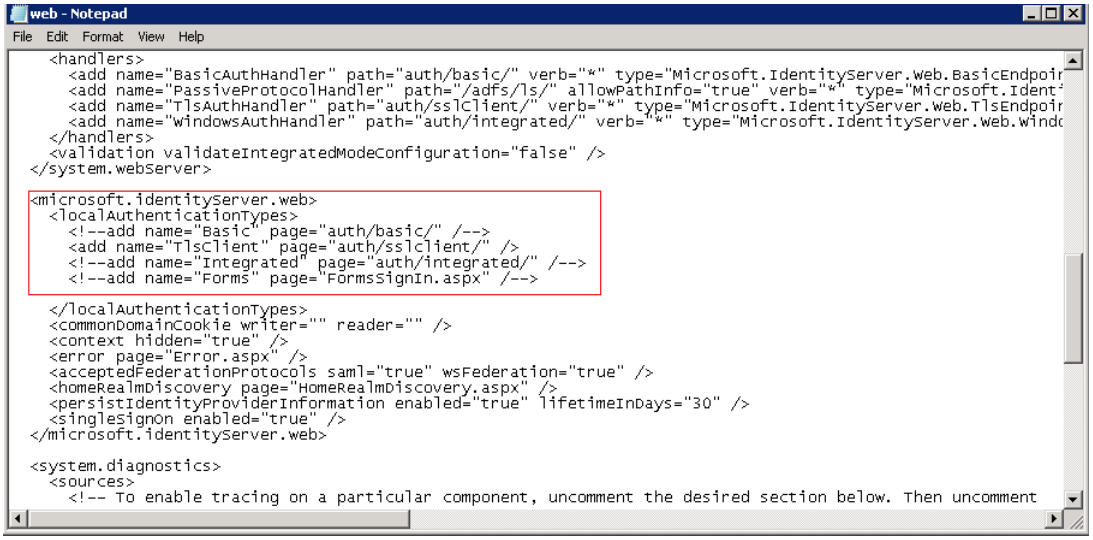

Figure 3-7 Web Configuration File Settings

Authentication Policies AD FS 3.0

The following instructions are applicable only for AD FS 3.0. Certificates can be configured for single factor and multi-factor authentication.

Primary Authentication Configuration

1. In the left navigation pane, click **AD FS 3.0 → Authentication Policies**. The Authentication Policies Overview page is displayed.
2. In Primary Authentication, click **Edit** in **Global Settings** option. The Edit Global Authentication Policy page is displayed.
3. Select the **Certificate Authentication** check box from Intranet and Extranet section and click **Apply**.

Multi-Factor Authentication Configuration

1. In the left navigation pane, click **AD FS 3.0 → Authentication Policies**. The Authentication Policies Overview page is displayed.
2. In Primary Authentication, click **Edit** in **Global Settings** option. The Edit Global Authentication Policy page is displayed.
3. Select **Forms Authentication** check box (make sure Certificate Authentication check box should not be selected here) from Intranet and Extranet section and click **Apply**.
4. In Multi-Factor Authentication, click **Edit** in **Global Setting** option. The Edit Global Authentication Policy page with Multi-Factor tab is displayed.
5. Select the **Certificate Authentication** check box from Additional Authentication Methods section and click **Apply**.

Configuring the trusted issuers list in Windows 2012 R2

Note: The following procedure is applicable only for AD FS 3.0 configured on a Windows 2012 R2 server.

Beginning with Windows Server 2012, the use of the Certificate Trust List (CTL) has been replaced with a certificate store-based implementation.

Although the maximum size of the trusted certification authorities list that the Schannel SSP supports (16 KB) remains the same as in Windows Server 2008 R2, in Windows Server 2012 there is a new dedicated certificate store for client authentication issuers so that unrelated certificates are not included in the message.

1. Enter **Start → Run → Regedit** to open the registry editor in Windows.
2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`
3. Check the value of **SendTrustedIssuerList** key and set the value to 0.
4. Create a new DWord (32-bit) Value registry entry with the name **ClientAuthTrustMode** and set the value as 2.
5. Restart the AD FS 3.0 server for the registry changes to take effect.

For information on the registry entries and its requirement in this integration, refer to http://technet.microsoft.com/en-us/library/hh831771.aspx#BKMK_TrustedIssuers

Chapter 4

Configuring Microsoft Office 365

This chapter discusses how to configure Microsoft Office 365 to integrate it with ADFS.

Prerequisities

- You must have administrative rights on the Office 365 portal.
- You must have a registered public domain.
- You must have created users in your enterprise Active Directory. These users will be mapped to the Office 365 users.
- AD FS 2.0 must be installed and configured on a Windows 2008 R2 server while AD FS 3.0 must be installed and configured on a Windows 2012 R2 server. See "Configuring AD FS" on page 17.

How the Office 365 Integration with AD FS Works

The following diagram describes how the administrator configures Office 365, AD FS, and Managed PKI for Single sign-on:

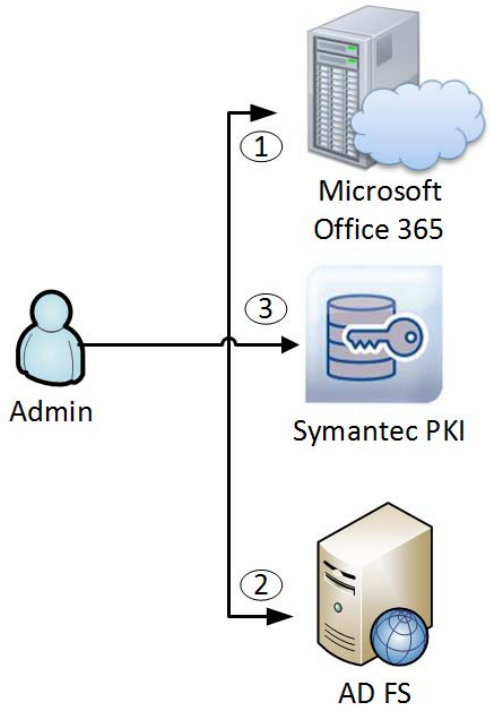

Figure 4-1 Administrator Configuration

1. Administrator logs into and configures Office 365 for Single Sign On.
2. Administrator prepares and configures the enterprise AD for identity federation.
3. Administrator contacts Managed PKI and creates a Seat ID.

The following diagram describes the flow of events when an end user tries to log onto the Office 365 portal:

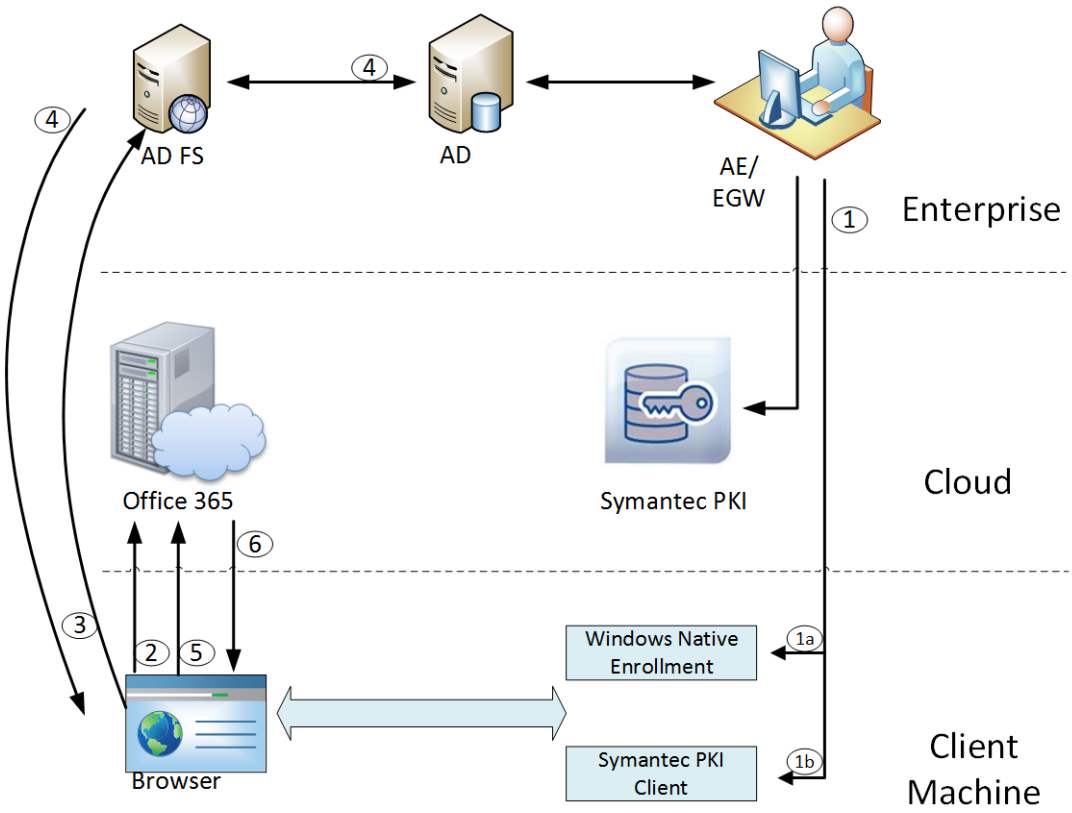

Figure 4-2 End User Configuration

1. When an end user logs into a machine or a certificate policy is pushed to an end-user machine through a Windows group policy, the autoenrollment client checks the Active Directory and the local certificate store to determine for which certificate template it can enroll the end user. The Autoenrollment server requests a certificate from Symantec Managed PKI. The certificate can be installed in one of the following ways:
   a. Certificate installed on Windows Native enrollment only for Internet Explorer browser.
   b. Certificate installed on Symantec PKI Client.

   For more information, refer to *Symantec PKI Enterprise Gateway Autoenrollment Server Deployment Guide*.
2. End user tries to reach the hosted Office 365 application from their browser and enters the account user name, for example, test_user@testdomain.com.
3. Office 365 generates a SAML authentication request. The SAML request is encoded and embedded into a URL and sent to AD FS.
4. AD FS authenticates the user in AD. After authentication, user information is taken from AD and the SAML response is generated.
5. The browser submits the request to Office 365, which logs the user in if the response is successfully verified.
6. The user is directed to the home page of the Office 365 services.

Configuring Microsoft Office 365 for SSO

To configure Office 365 for SSO, follow the steps listed in the document at http://www.microsoft.com/en-ie/download/details.aspx?id=28971

Note: The instructions in this document describe the configuration for AD FS 2.0. Follow the same procedure to configure Office 365 for SSO on AD FS 3.0.

Testing the configuration

1. Log into the Microsoft Office 365 portal with your test-user credentials.
2. From the list of certificates, select the appropriate certificate. You are directed to the Office 365 home page for the subscribed Office 365 services.