



Outlook Web Access (OWA) WS-Federation SSO with A10 Thunder Series

Configure Microsoft Exchange 2010 SP3 OWA Service for SSO Capability with ADFS 2.0 and A10 Thunder Series

Table of Contents

Installing Microsoft Exchange Server 2010 SP3.....	3
Prepare Your System	3
1. Configure your basic system.	3
2. Prepare to Install Exchange Server 2010.....	4
Prepare the Active Directory and Domain	4
Install the Microsoft Filter Pack and Mandatory Packages.....	4
3. Install Exchange Server 2010	5
Configuration Guide for OWA with ADFS	5
Prerequisites	5
Generate a New Certificate for your Service.....	5
Run a Windows Update (optional).....	6
Create a New OWA Website for SSO	7
Creating a New Web Site.....	7
Create a Virtual Directory for a New OWA Web Site.....	9
Configure the OWA and ECP Service Authentication Types	9
Install WIF and C2TWS	11
Enable Federation for OWA and ECP	11
Generating the web.config file for SSO on the OWA website.....	11
Start the C2WTS Service	16
Configuring ADFS	18
Configuration Guide for A10 Thunder Series	21
Prerequisites.....	21
Configurations on A10 Thunder Series.....	22
Configuration Example	22
Configure ADFS Information	23
Act as a Service Provider.....	23
Information about OWA Servers	24
Authentication and Relay Tokens	24
Service Connectivity	25
Changes on ADFS	26
Modifying the Exchange Server.....	27
About A10 Networks.....	28

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

This guide describes how to achieve SAML-based claims authentication with OWA by configuring and deploying A10 Networks® A10 Thunder® Series with Active Directory Federation Services (ADFS) and consists of the following parts:

- An installed Microsoft Exchange Server 2010 SP3
- A configuration guide for OWA with ADFS
- A configuration guide for AD FS
- A configuration guide for A10 Thunder Series

Installing Microsoft Exchange Server 2010 SP3

Before you install Exchange Server 2010, see the following documents for the Exchange 2010 requirements:

- [Exchange 2010 System Requirements](#)
- [Planning Active Directory](#)

To use Exchange Server 2010 SP3, you must complete the following tasks:

1. Prepare your system.
2. Install Exchange Server 2010.
3. Upgrade from Exchange Server 2010 to Exchange Server SP3.

The following sections provide additional information about these tasks.

Prepare Your System

1. Configure your basic system.

- a. Install Windows Server 2008 R2 Standard / Enterprise.
- b. Join the server to the a10-tplab domain.

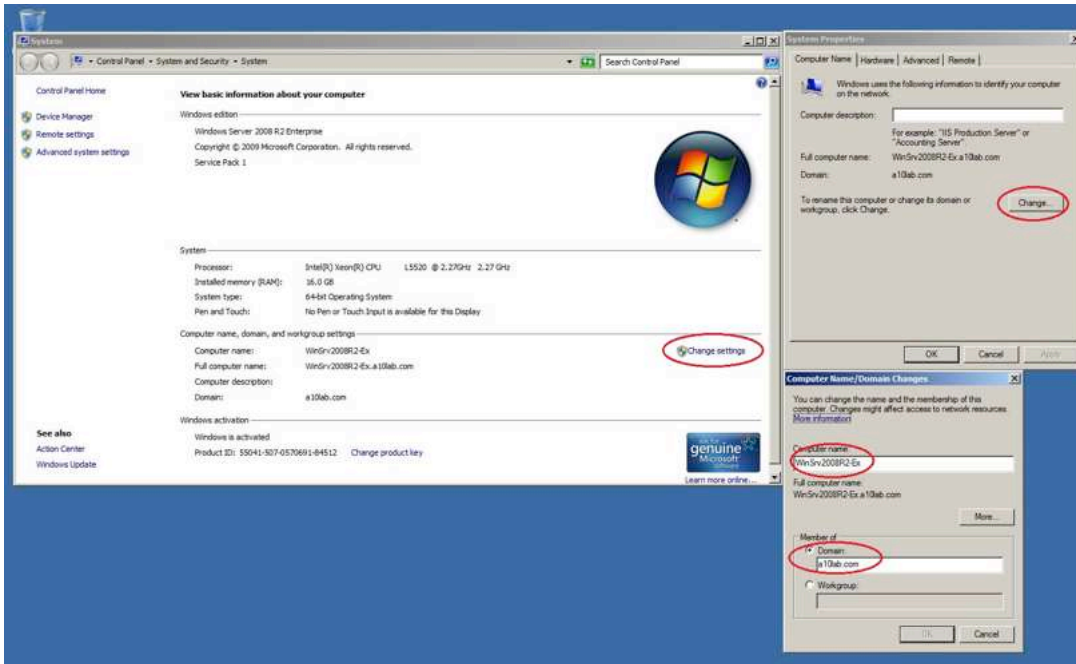


Figure 1: Configuring your system

2. Prepare to Install Exchange Server 2010

- a. Before you start, ensure that your login account has the privileges to configure the domain controller and the local system.
- b. Switch your user to account that is in domain admin group or Enterprise admin group.

Prepare the Active Directory and Domain

If you're deploying a new Exchange organization (There is no any exchange server installed in you domain). You must first install the Active Directory management tools and prepare your AD and domain for Exchange 2010.

To install the Active Directory management tools, run the following command in PowerShell:

```
ServerManagerCmd -i RSAT-ADDS
```

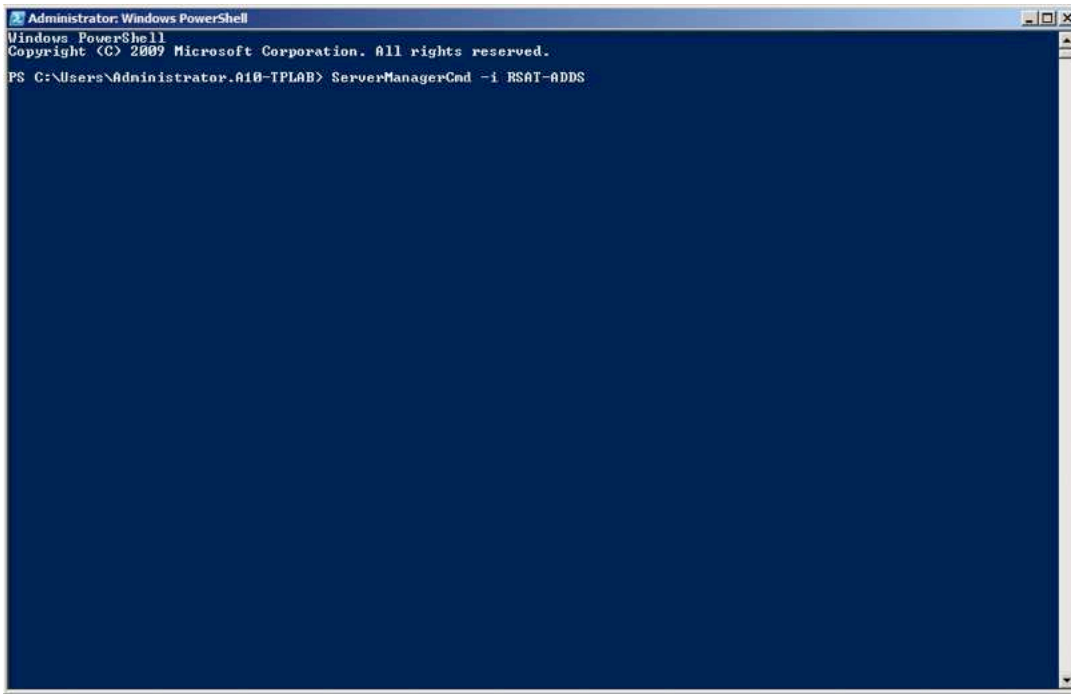


Figure 2: Installing the AD management tools

To prepare AD and Domain:

1. Insert the Exchange 2010 CD into your computer.
2. At the command prompt, go to directory in which the setup.com file is located.
3. Type following commands:
 - `setup /PrepareAD /OrganizationName:a10-tplab`
 - `setup /PrepareDomain`

Note: The user account should in the Enterprise Admins group and the schema Admins group.

Install the Microsoft Filter Pack and Mandatory Packages

To install the Microsoft Filter Pack, use the PowerShell console and enter the following commands to download and install the necessary Microsoft Office 2010 Filter Packs:

- `Import-Module ServerManager`
- `Add-WindowsFeature RSAT-ADDS`
- `Add-WindowsFeature Desktop-Experience, NET-Framework, NET-HTTP-Activation, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Web-Server, WAS-Process-Model, Web-Asp-Net, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-`

Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Igcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI -Restart

- Set-Service NetTcpPortSharing -StartupType Automatic

3. Install Exchange Server 2010

To install Exchange Server 2010, complete the following steps:

1. Insert the Exchange Server 2010 CD in your computer.
2. Run the **setup.exe** command.

Note: To upgrade to Exchange 2010 SP3, you must first download Exchange 2010 SP3 from the Microsoft Download Center and install it.

Configuration Guide for OWA with ADFS

Prerequisites

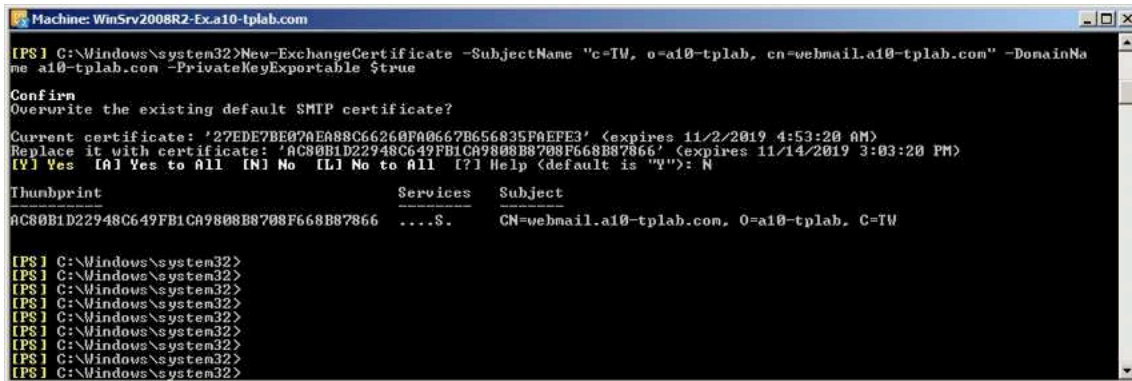
To configure OWA with ADFS, you must complete the following prerequisites.

Generate a New Certificate for your Service

1. Enter the following command in the Exchange Manage PowerShell window to generate a self-signed certificate and use single-sign on (SSO) for your new web site:

```
New-ExchangeCertificate -SubjectName "c=TW, o=a10-tplab, cn=webmail.a10-tplab.com" -DomainName a10-tplab.com -PrivateKeyExportable $true
```

In this example, the service URL for OWA is *webmail.a10-tplab.com*.



```
Machine: WinSrv2008R2-Ex.a10-tplab.com
[PS] C:\Windows\system32>New-ExchangeCertificate -SubjectName "c=TW, o=a10-tplab, cn=webmail.a10-tplab.com" -DomainName a10-tplab.com -PrivateKeyExportable $true
Confirm
Overwrite the existing default SMTP certificate?
Current certificate: '27EDE7BE07AE88C66260FA0662B656835FAEFE3' (expires 11/2/2019 4:53:20 AM)
Replace it with certificate: 'AC80B1D22948C649FB1CA9808B8708F668B87866' (expires 11/14/2019 3:03:20 PM)
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): N

Thumbprint                               Services    Subject
-----
AC80B1D22948C649FB1CA9808B8708F668B87866  ....S.     CN=webmail.a10-tplab.com, O=a10-tplab, C=TW

[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>
```

Figure 3: Creating a new certificate for your service

2. Click Exchange Management Console > Server Configure.
3. On the Exchange Certificate tab, the certificate that you just created is displayed.
4. Right click on the certificate and select Assign Services to Certificate.

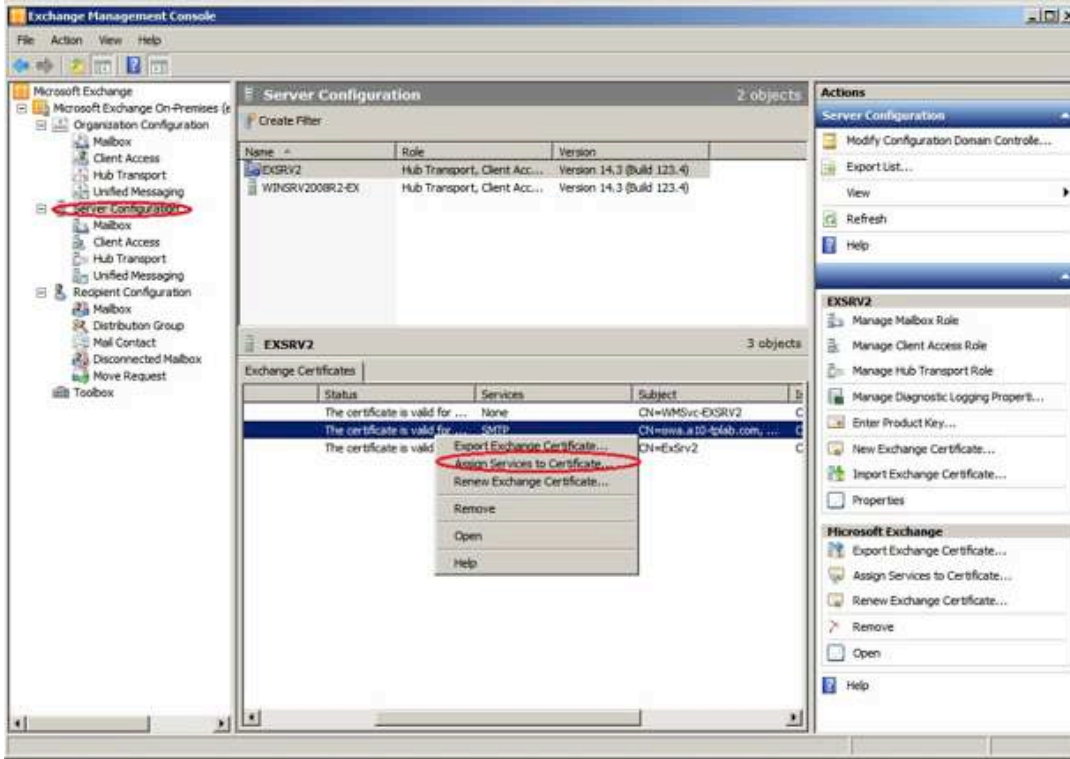


Figure 4: Assigning services to the certificate

5. Select the services that you want to use this new certificate and click **Assign**. In Figure 5, the **Internet Information Service (IIS)** option has been selected.

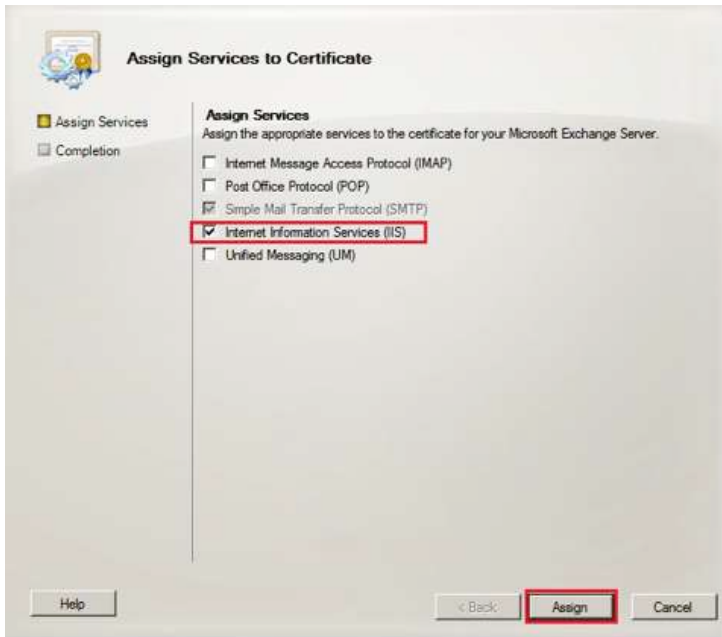


Figure 5: Assigning services to the certificate

Run a Windows Update (optional)

Before you can run a Windows update, ensure that all critical fixes for the Exchange Server are installed.

Create a New OWA Website for SSO

You can create a new OWA web site for SSO.

Creating a New Web Site

Using IIS mmc, create a new web site in IIS on the Client Access Server, and bind it to the new IP address and the SSL certificate.

To create a new web site:

1. Open IIS Manager, right click on **Sites** and select “Add Web Site.”

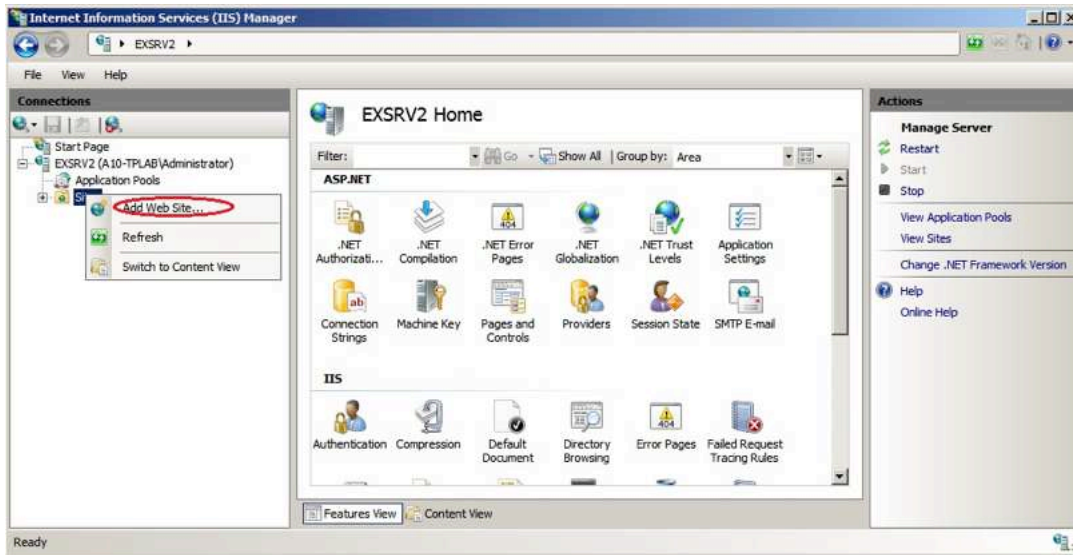


Figure 6: Creating a new web site

2. Configure your new web site by completing the following tasks:
 - a. In **Site name**, enter the site name.
 - b. In the **Content Directory** section, in **Physical path**, enter the physical path for your site.

Note: Click **Test Settings** to ensure that IIS can access the assigned path. Click **Connect as** to specify a user or credential to access the path.

- c. In **Type**, select **https** and enter an IP address and port number for your site.
- d. In **SSL Certificate**, assign the certificate that you created previously for this service binding.

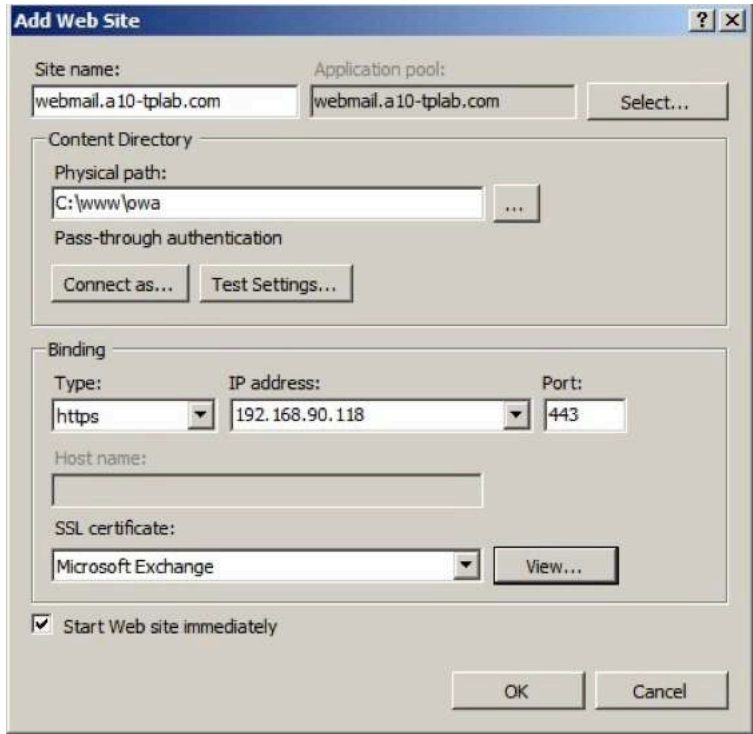


Figure 7: Configuring the web site

3. In **Application Pools**, right click your application and select **Advanced Settings**.
4. Change the Application Pool identity to **LocalSystem** and **Load User Profile** to **True**.
5. Click **OK**.

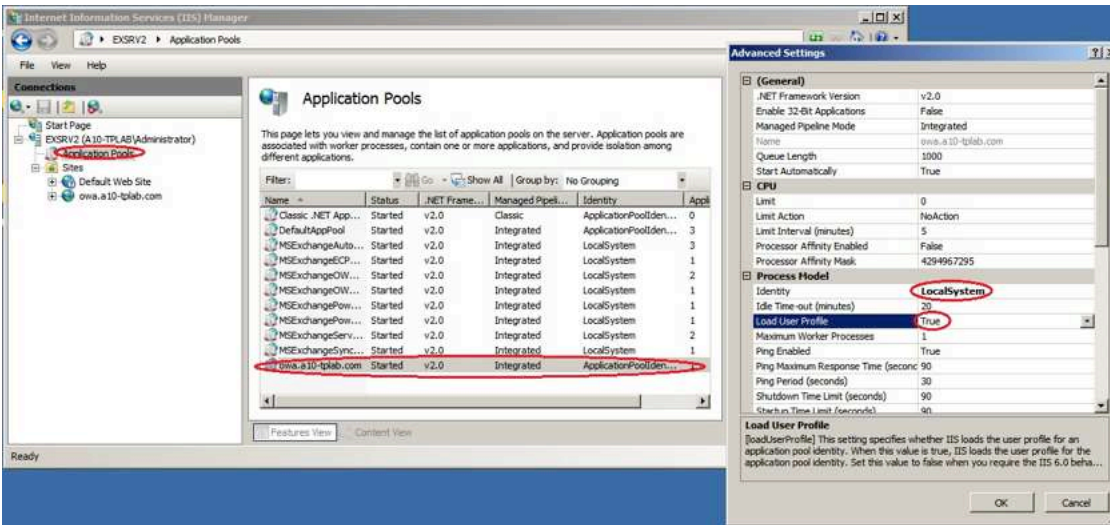


Figure 8: Configuring the application pools

Create a Virtual Directory for a New OWA Web Site

To create a virtual directory for a new OWA web site:

1. Launch an **Exchange Management** shell window and run the cmdlets to create a new OWA and ECP site.
2. For the `WebSiteName` parameter, enter the name of the web site that you created above:
 - a. `New-OWAVirtualDirectory -WebSiteName webmail.a10-tplab.com`
 - b. `New-ECPVirtualDirectory -WebSiteName webmail.a10-tplab.com`
3. Navigate to the OWA web site URL and enter your username and password.

Configure the OWA and ECP Service Authentication Types

To configure the OWA and ECP service authentication types:

1. Start the **Exchange Management Console** and under **Server Configuration**, select **Client Access**.
2. Display the properties of the newly created OWA.
3. On the **Authentication** tab of the **Properties** window, select the **Use one or more standard authentication methods** option.
4. Verify that no other options are selected.

Note: Ignore the Microsoft Exchange warning about missing authentication.

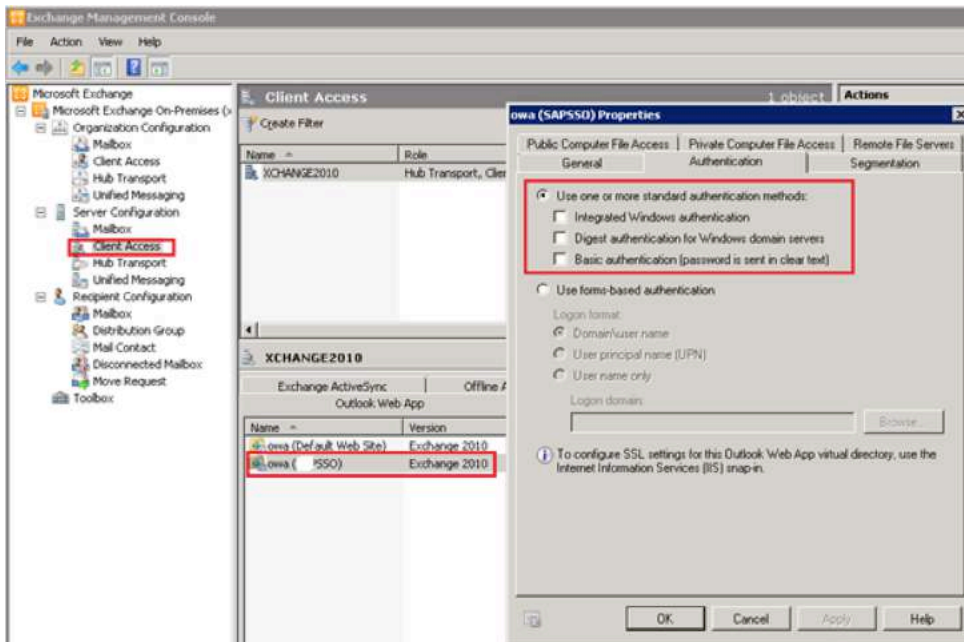


Figure 9: Configuring OWA service authentication types

5. Repeat steps 1-4 for the corresponding ECP.

Note: Ignore the Microsoft Exchange warning about missing authentication and reset IIS by using the `isreset /noforce` commands.

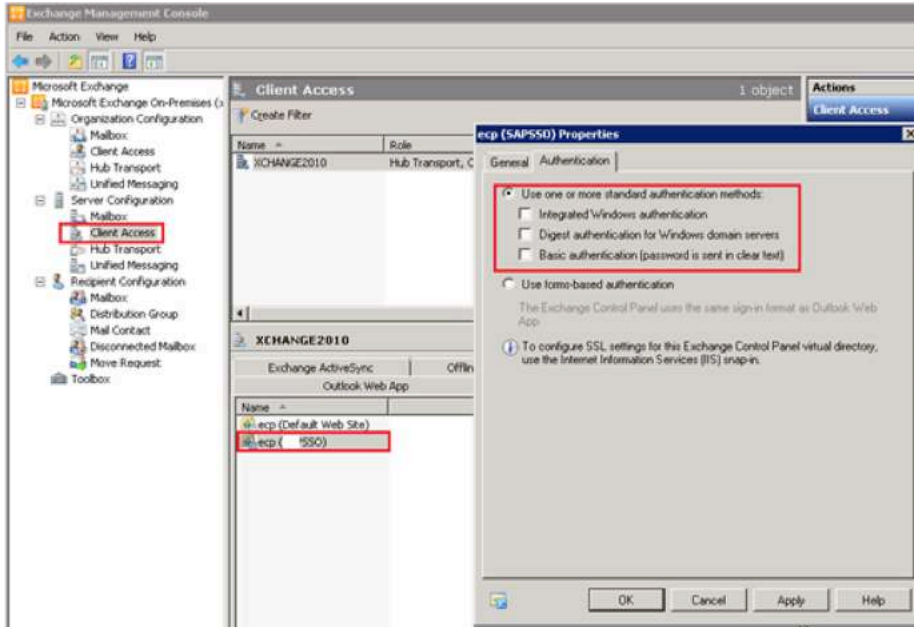


Figure 10: Configuring ECP service authentication types

- From IIS mmc, enable Anonymous authentication for OWA.

Note: Anonymous authentication should be already enabled for ECP, so you must reset IIS again.

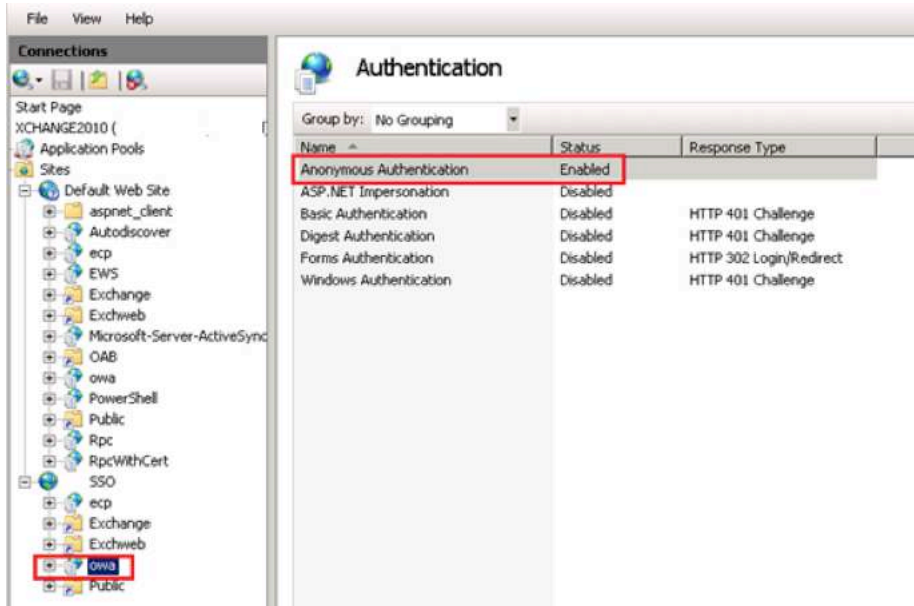


Figure 11: Enabling anonymous authentication for OWA

Install WIF and C2TWS

To install WIF and C2TWS:

1. Download the x86 or x64 WIF runtime package from <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17331>.
2. Select the appropriate file for your system:
 - a. For Windows Vista and Windows Server 2008, select the msu file with name that starts with Windows6.0.
 - b. For Windows 7 and Windows Server 2008 R2, select the msu file with name that starts with Windows6.1.
3. After the installation is complete, there should be a new service called Claims to **Windows Token Service** that is added to the CAS server.
4. Download and install the **WindowsIdentityFoundation-SDK-3.5.msi** file from <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=4451>.

Enable Federation for OWA and ECP

You can enable federation for OWA and ECP.

Generating the web.config file for SSO on the OWA website

You must create a web.config file in the folder that is mapped to the root of the web site that was created earlier. The contents of the web.config file can be the empty `<configuration>` tag.

Note: You must create a new web.config file in the folder that is mapped to the root of the web site.

Do not use the `<System Disk>:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\web.config` directory path.

In the example in Figure 7, the root directory for new OWA website is `C:\www\owa\`, so create a web.config in `c:\www\owa\` with the information in Figure 12.

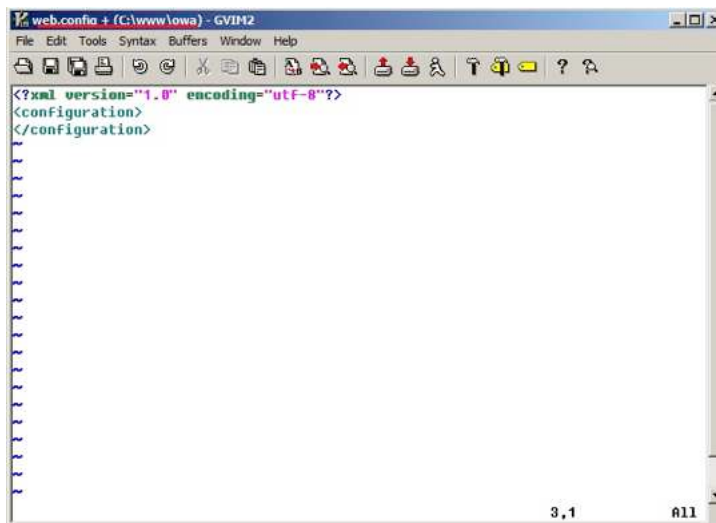


Figure 12: Sample web.config file for the new OWA web site

5. Start **FedUtil.exe** and on the first screen provide the location of the web.config file that was created earlier.
6. In **Application URI**, specify the complete URI for the new OWA application that was created earlier and click **Next**.

In the example in Figure 10, the **Application configuration location** is `c:\www\owa\web.config` and the **Application URI** is `https://webmail.a10-tplab.com/owa/`.

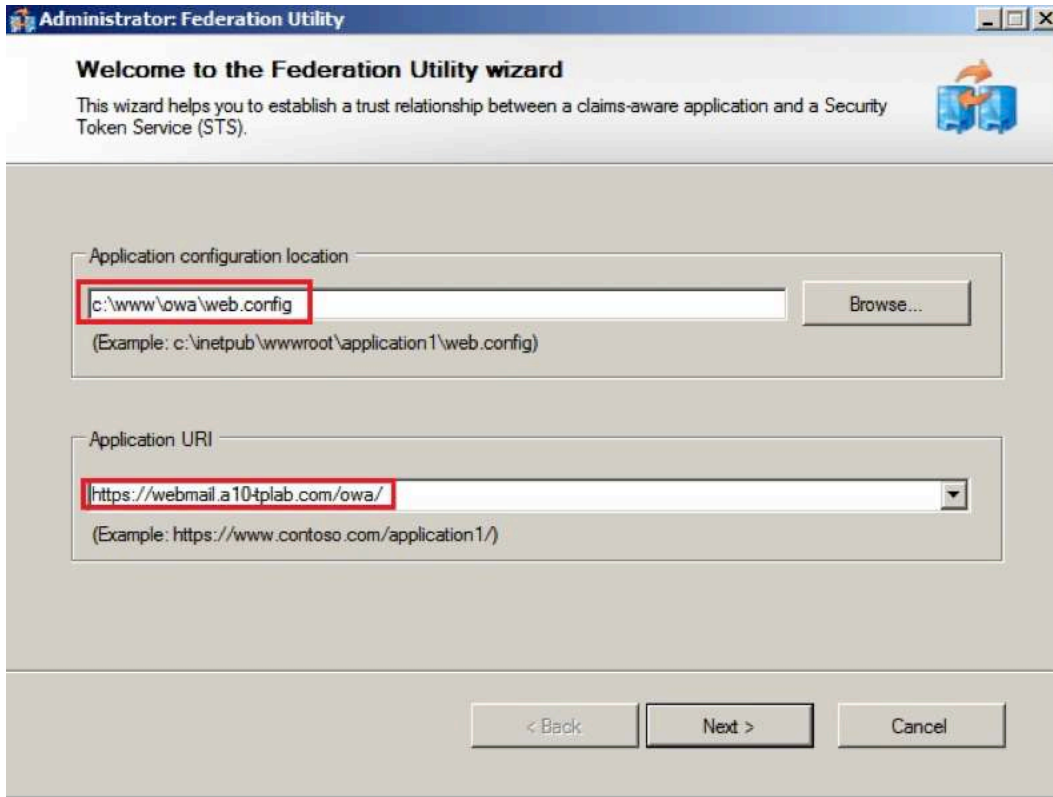


Figure 13: Using the Federation Utility Wizard

7. On the **Security Token Service** page, select **Use an existing STS** and enter the ADFS URL in the **STS WS-Federation meta document location**.
8. Skip the warning and click **Next**.

In the example in Figure 11, the document location is *https://idp.a10-tplab.com/FederationMetadata/2007-06/FederationMetadata.xml*, where idp.a10-tplab.com is the ADFS server. You should be able to check the metadata file by clicking the link.

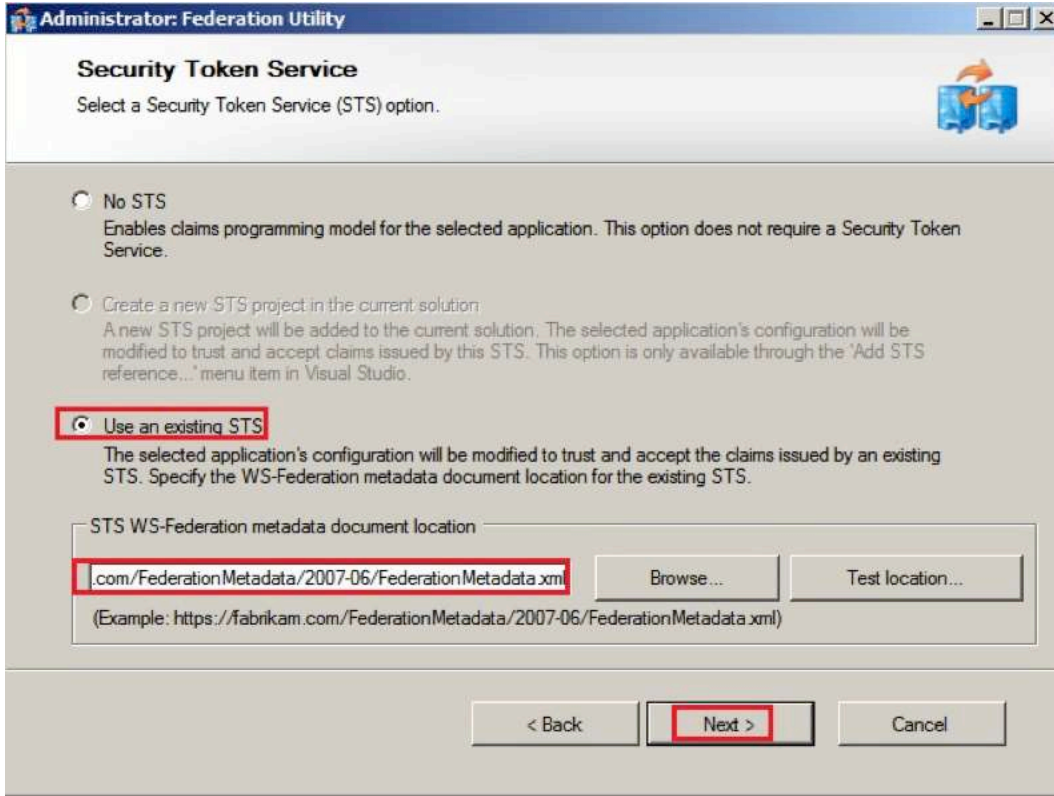


Figure 14: Configuring the Security Token Service

9. Accept the default values on the rest of the pages in the wizard.



Figure 15: Completing the Federation Utility Wizard

10. Open the web.config file for the new web site and complete the following tasks:

- Comment out the <httpmodules> section.
- Add the `runAllManagedModulesForAllRequests="true"` attribute to the <modules> tag.

The tag should now read <modules runAllManagedModulesForAllRequests="true">.

```

13 </authorization>
14 </system.web>
15 </location>
16 <system.web>
17 <authorization>
18 <deny users="*" />
19 </authorization>
20 <authentication mode="None" />
21 <compilation>
22 <assemblies>
23 <add assembly="Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
24 </assemblies>
25 </compilation>
26 </system.web>
27 <system.webServer>
28 <modules runAllManagedModulesForAllRequests="true">
29 <add name="WSFederationAuthenticationModule" type="Microsoft.IdentityModel.Web.WSFederationAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
30 <add name="SessionAuthenticationModule" type="Microsoft.IdentityModel.Web.SessionAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
31 </modules>
32 </system.webServer>
33 <microsoft.identitymodel>
34 <service>
35 <audienceUris>
36 <add value="https://webmail.a10-tplab.com/owa/" />
37 <add value="https://webmail-sp.a10-tplab.com/axowa" />
38 </audienceUris>
39 <securityTokenHandlers>
40 <add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
41 <samlSecurityTokenRequirement mapToWindows="true" useWindowsTokenService="true" />
42 </add>

```

Figure 16: Configuring the web.config file

11. Add the following tags after <audienceUris > in the following way:

```
<securityTokenHandlers>
```

```

<add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">

```

```

<samlSecurityTokenRequirement mapToWindows="true" useWindowsTokenService="true" />

```

```
</add>
```

```
</securityTokenHandlers>
```

```

21 <compilation>
22 <assemblies>
23 <add assembly="Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
24 </assemblies>
25 </compilation>
26 </system.web>
27 <system.webServer>
28 <modules runAllManagedModulesForAllRequests="true">
29 <add name="WSFederationAuthenticationModule" type="Microsoft.IdentityModel.Web.WSFederationAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
30 <add name="SessionAuthenticationModule" type="Microsoft.IdentityModel.Web.SessionAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
31 </modules>
32 </system.webServer>
33 <microsoft.identitymodel>
34 <service>
35 <audienceUris>
36 <add value="https://webmail.a10-tplab.com/owa/" />
37 <add value="https://webmail-sp.a10-tplab.com/axowa" />
38 </audienceUris>
39 <securityTokenHandlers>
40 <add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
41 <samlSecurityTokenRequirement mapToWindows="true" useWindowsTokenService="true" />
42 </add>
43 </securityTokenHandlers>
44 <applicationService>
45 <claimTypeRequired>
46 <!--Following are the claims offered by SIS 'http://ldp.a10-tplab.com/adfs/services/trust'. Add or uncomment claims that you require by your application and then update the federation metadata of this application.-->
47 <claimType type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" optional="true" />
48 <claimType type="http://schemas.microsoft.com/ws/2008/05/identity/claims/role" optional="true" />
49 <!--<claimType type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" optional="true" />-->

```

Figure 17: Configuring the web.config file

12. Uncomment following line and change the optional attribute to **true**:

```
<claimtype optional="true" type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn">
```

```

39 <securityTokenHandlers>
40 <add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
41 <claimTypeRequirements mapToWindows="true" useWindowsTokenService="true" />
42 </add>
43 </securityTokenHandlers>
44 <applicationService>
45 <claimTypeRequired>
46 <!--Following are the claims offered by STS 'http://idp.a10-tplab.com/adfs/services/trust'. Add or uncomment claims that you require by your application and then update the federation metadata of this application.-->
47 <claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" optional="true" />
48 <claimtype type="http://schemas.xmlsoap.org/ws/2008/06/identity/claims/role" optional="true" />
49 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" optional="true" />-->
50 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" optional="true" />-->
51 <claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" optional="true" />
52 <!--claimtype type="http://schemas.xmlsoap.org/claims/CommonName" optional="true" />-->
53 <!--claimtype type="http://schemas.xmlsoap.org/claims/EmailAddress" optional="true" />-->
54 <!--claimtype type="http://schemas.xmlsoap.org/claims/Group" optional="true" />-->
55 <!--claimtype type="http://schemas.xmlsoap.org/claims/UPN" optional="true" />-->
56 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname" optional="true" />-->
57 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier" optional="true" />-->
58 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier" optional="true" />-->
59 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant" optional="true" />-->
60 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod" optional="true" />-->
61 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid" optional="true" />-->
62 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarsid" optional="true" />-->
63 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/denyonlyprimarygroupsid" optional="true" />-->
64 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid" optional="true" />-->
65 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid" optional="true" />-->
66 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarsid" optional="true" />-->
67 <!--claimtype type="http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname" optional="true" />-->
68 <!--claimtype type="http://schemas.microsoft.com/2012/01/devicecontext/claims/isregistereduser" optional="true" />-->
69 <!--claimtype type="http://schemas.microsoft.com/2012/01/devicecontext/claims/identifier" optional="true" />-->

```

Figure 18: Configuring the web.config file

13. Add a path attribute to `<cookiehandler requireSsl="true"/>`.

The revised node should read `<cookieHandler requireSsl="true" path="/" />`.

Note: This step allows ECP to use the SSO cookie that was generated for OWA.

```

100 <!--claimtype type="http://schemas.microsoft.com/2012/12/certificatecontext/extension/certificateinformation" optional="true" />-->
101 <!--claimtype type="http://schemas.microsoft.com/2012/12/certificatecontext/extension/certificateinformation" optional="true" />-->
102 <!--claimtype type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprint" optional="true" />-->
103 <!--claimtype type="http://schemas.microsoft.com/2012/12/certificatecontext/field/x509version" optional="true" />-->
104 <!--claimtype type="http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork" optional="true" />-->
105 <!--claimtype type="http://schemas.microsoft.com/ws/2012/01/passwordexpirationline" optional="true" />-->
106 <!--claimtype type="http://schemas.microsoft.com/ws/2012/01/passwordexpirationdays" optional="true" />-->
107 <!--claimtype type="http://schemas.microsoft.com/ws/2012/01/passwordchangeurl" optional="true" />-->
108 <!--claimtype type="http://schemas.microsoft.com/claims/authmethodsreferences" optional="true" />-->
109 <!--claimtype type="http://schemas.microsoft.com/2012/01/requestcontext/claims/client-request-id" optional="true" />-->
110 </claimTypeRequired>
111 </applicationService>
112 <certificateValidation certificateValidationMode="None" />
113 <federatedAuthentication>
114 <wsfederation passiveRedirectEnabled="true" issuer="https://idp.a10-tplab.com/adfs/ls/" realm="https://webmail.a10-tplab.com/owa/" requireHttps="true">
115 <cookieHandler requireSsl="true" path="/" />
116 </wsfederation>
117 <issuerNameRegistry type="Microsoft.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
118 <trustedIssuers>
119 <add thumbprint="F25D32083C87C7000083AF009A545A42C801E1D17" name="http://idp.a10-tplab.com/adfs/services/trust" />
120 </trustedIssuers>
121 </issuerNameRegistry>
122 </service>
123 </microsoft.IdentityModel>
124 </configuration>

```

Figure 19: Configuring the web.config file

a. Run the FedUtil again on the web.config file.

This step updates the Federation metadata of new SSO-enabled web site with the additional UPN claim information.

b. Browse the federation meta data at `https://SSO OWA FQDN/FederationMetadata/2007-06/FederationMetadata.xml` and ensure that UPN appears as a mandatory claim type, where SSO OWA FQDN in the URL above is the domain name of the new OWA.

After you run the FedUtil again, the utility creates a metadata for the OWA service. The metadata is located in the `FederationMetadata\2007-06\FederationMetadata.xml` file in your website root directory. ADFS or another service or user can access the metadata by using the web service.

In the example, the URL for my service metadata should be:

`https://webmail.a10-tplab.com/FederationMetadata/2007-06/FederationMetadata.xml`

You can use your browser to test the link, and this link can also be used to configure your ADFS server.

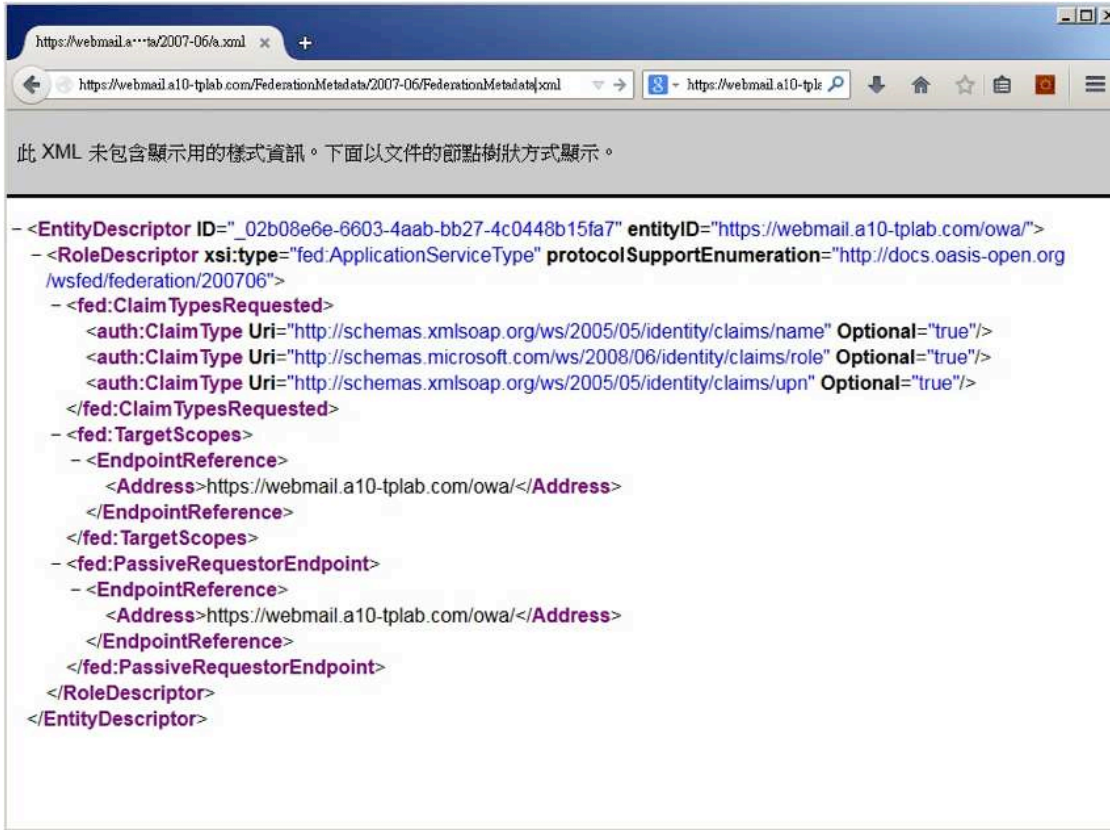


Figure 20: Testing the Link to the service metadata

Start the C2WTS Service

To start the C2WTS service:

1. Un-commenting following line in the C2TWS configuration file:

```
<add value="NT AUTHORITY\SYSTEM" />
```

This step allows you to configure the **Claim To Windows Token Service**, which allows Exchange to use it. The file is located in the <System Disk>\Program Files\Windows Identity Foundation\v3.5\c2wts\host.exe.config directory.

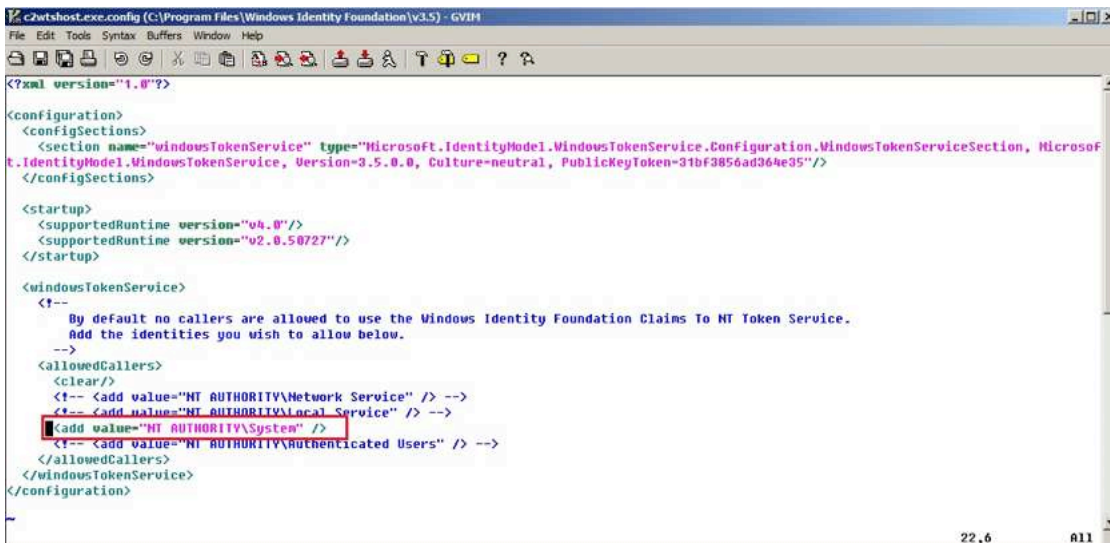


Figure 21: Starting the C2WTS service

2. In **Startup type**, select **Automatic** and verify that **Cryptographic Services** is already started.

If the service has not been started, start it now.

You can also make the C2WTS service dependent on the CryptSrv service. For more information, see <http://support.microsoft.com/kb/2512597>.

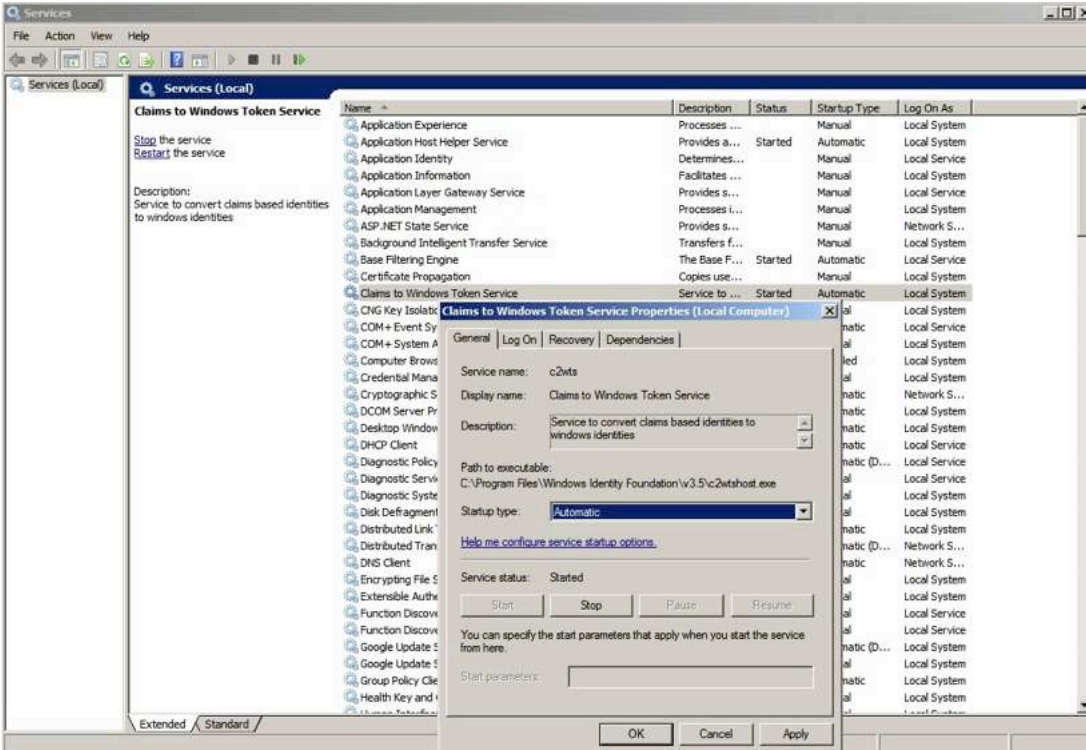


Figure 22: Configuring the Windows Token Service Properties

Configuring ADFS

To configure ADFS:

1. Add the Relying Party Trust in ADFS by using the **Add Relying Party Trust Wizard** and using OWA's Federation Metadata file.
2. In the **Select Data Source** step, enter the Federation metadata address, and click **Next**.

In Figure 23, the URL is `https://webmail.a10-tplab.com/FederationMetadata/2007-06/FederationMetadata.xml`.

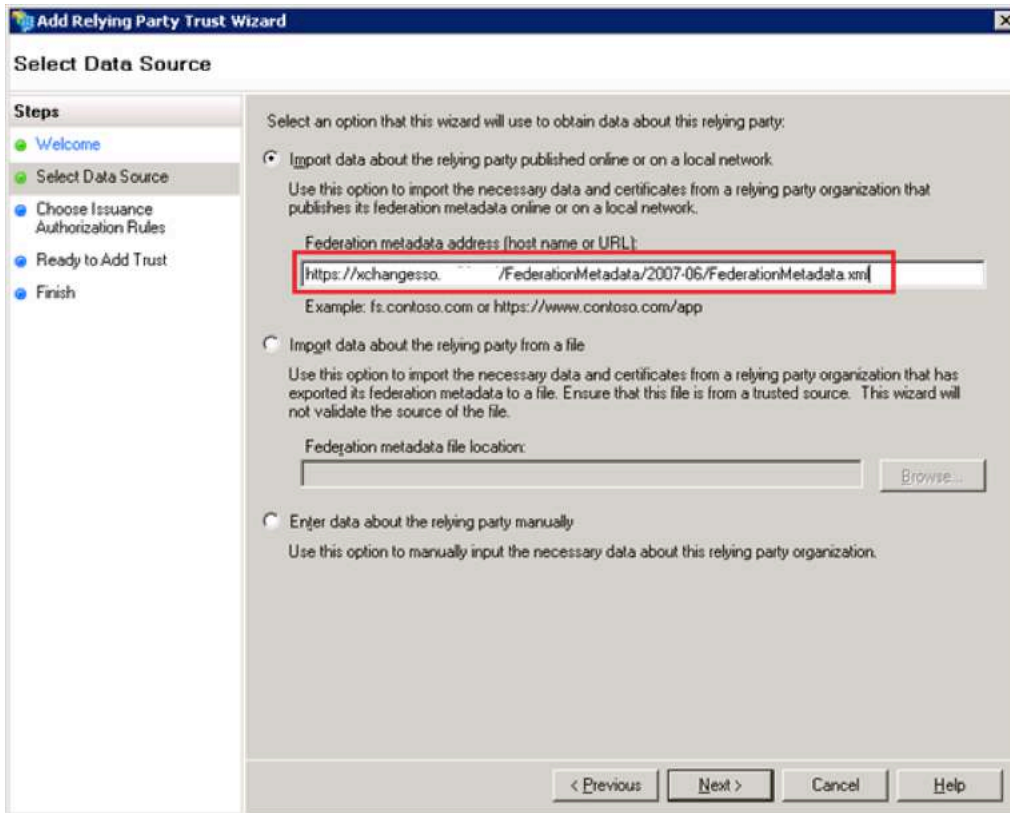


Figure 23: Adding the Relying Party Trust Wizard

3. In the **Specify Display Name** window, enter the display name, and click **Next**.

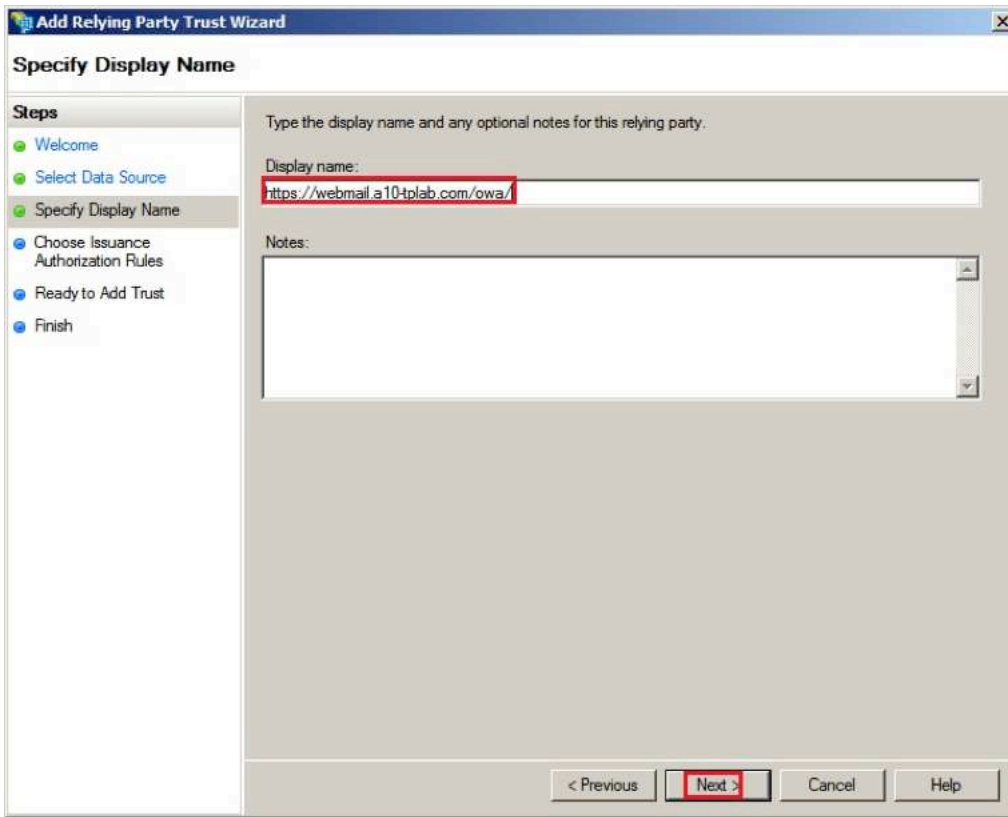


Figure 24: Configuring the Display Name

4. Since ADFS can get OWA configurations from the metadata, accept the default values on rest of the windows in the wizard.
5. Click **Close**.

6. In the **Edit Claim Rules** window, select **Send LDAP Attributes as Claims**, and click **Next**.

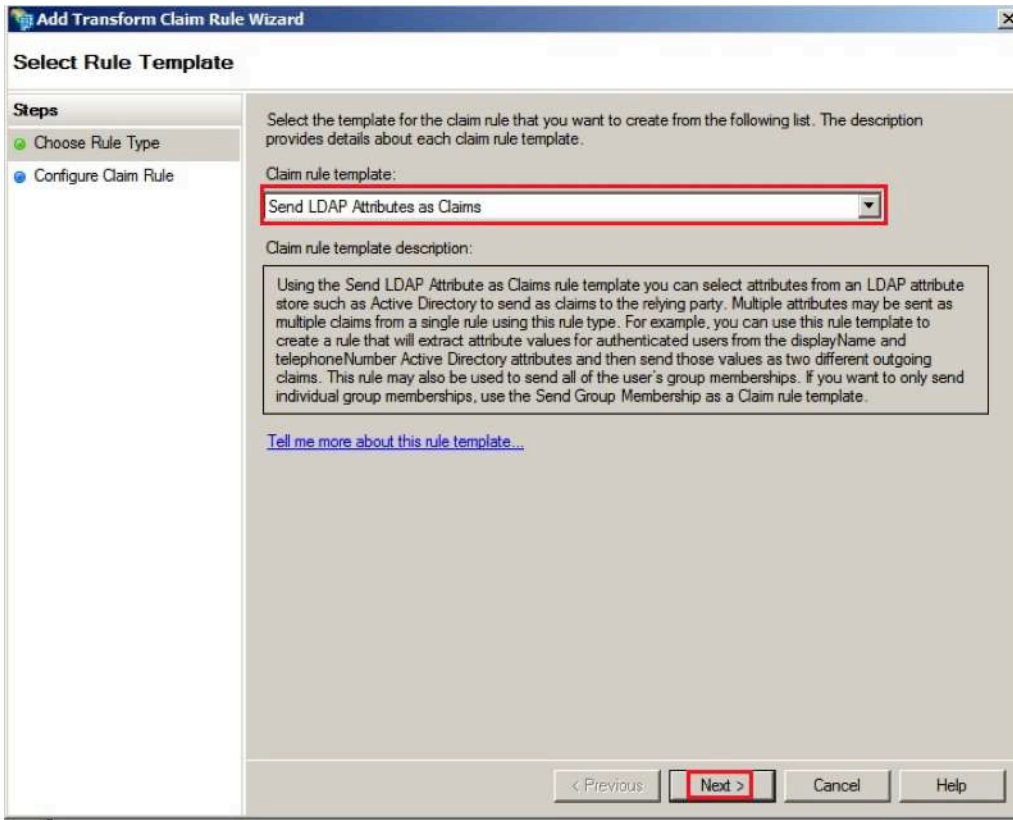


Figure 25: Editing the Claims Rule

7. In the **Edit Rule** window, complete the following steps:
- In **Claim rule name**, specify the name for this claim rules.
 - In **Attribute store**, select **Active Directory**.
 - Add the following mappings:
 - LDAP Attribute **User-Principal-Name** map to Outgoing Claim **UPN (mandatory)**
 - LDAP Attribute **SAM-Account-Name** map to Outgoing Claim **Name**
 - LDAP Attribute **SAM-Account-Name** map to Outgoing Claim **Role**
 - LDAP Attribute **User-Principal-Name** map to Outgoing Claim **Name ID** (recommend)

This step maps the Active Directory attributes to the outgoing token claims/attributes and passes to your service for authentication.

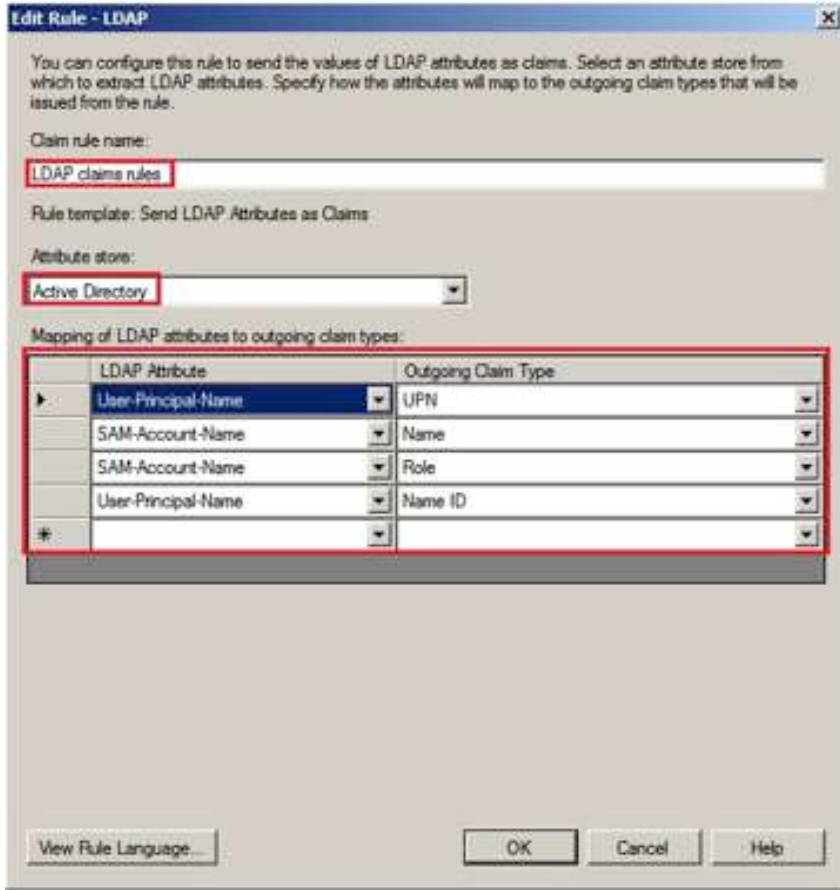


Figure 26: Editing the rules

This step completes the configuration. When you navigate to the new OWA URL it should redirect you to ADFS, and after you have been successfully authenticated, your email box is displayed.

Note: The default OWA should still support the original authentication setting.

Configuration Guide for A10 Thunder Series

Prerequisites

Before you deploy A10 Thunder in your environment, complete the following tasks:

- Verify that you can successfully authenticate to and access the OWA service.
- Ensure that all of the set up and configuration for OWA and ADFS is correct.

The topology might change after you deploy A10 Thunder in Figure 27:

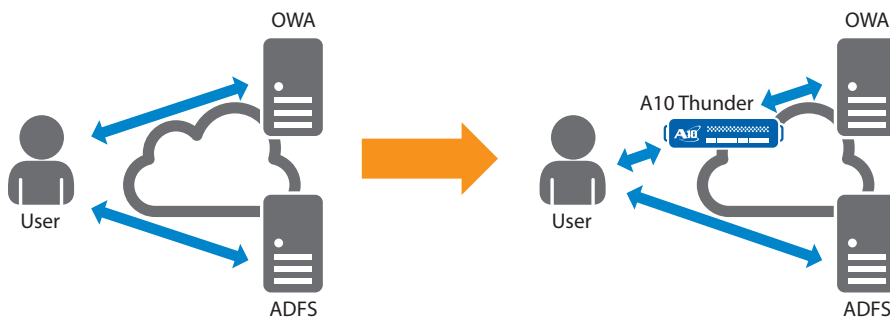


Figure 27: Sample A10 Thunder Series topology

After you deploy A10 Thunder in your topology, OWA no longer needs to redirect the user to ADFS for authentication. Instead, A10 Thunder becomes the service provider and completes the following process:

1. When users access A10 Thunder's service URL, A10 Thunder redirects the users and browser to ADFS for the WS-Federation token.
2. After users enter their credentials, and are successfully authenticated, ADFS redirects the users back to A10 Thunder with the tokens.
3. A10 Thunder relays the users' request and token to the OWA server.

Before this procedure can be successfully completed, complete the following prerequisites:

1. Configure A10 Thunder, which involves the following tasks:
 - a. Configure the ADFS information
 - b. Act as a service provider
 - c. Provide information about OWA servers
 - d. Authentication
 - e. Service connectivity
2. Configure ADFS to work with A10 Thunder instead of OWA.
3. Configure the OWA server to access the tokens that are issued by ADFS for A10 Thunder.

Configurations on A10 Thunder Series

In this chapter, the complete configuration for our example is described. If you have any issues with the configuration, you can go complete the steps below:

Configuration Example

1. Import ADFS metadata to the A10 Thunder Series.

For example, you can enter the following command:

```
import auth-saml-idp tp-idp use-mgmt-port ftp://ben@192.168.x.x/owa/
FederationMetadata/2007-06/FederationMetatdata.xml
```

2. Configure SSO by entering the following commands:

```
aam authentication saml service-provider axowa-sp
  adfs-ws-federation enable
  assertion-consuming-service index 0 location /axowa binding post
  entity-id https://webmail-sp.a10-tplab.com/axowa
  service-url https://webmail-sp.a10-tplab.com
!
aam authentication saml identity-provider tp-adfs
  metadata tp-idp
!
slb template server-ssl s1
!
slb server owa1 192.168.90.119
  port 443 tcp
!
aam authentication relay ws-federation ws_relay
  application-server exchange-owa
  authentication-uri /owa
!
aam authentication template a1
  type saml
  saml-sp axowa-sp
  saml-idp tp-adfs
```

```

    relay ws_relay
!
aam aaa-policy p1
    aaa-rule 1
        action allow
        authentication-template a1
!
slb service-group app-sg tcp
    member owa1 443
!
slb template client-ssl c1
    cert webmail-sp.a10-tplab.com.pem
    key webmail-sp.a10-tplab.com.pem
!
slb virtual-server vip1 192.168.91.56
    port 443 https
    source-nat auto
    service-group app-sg
    template server-ssl s1
    template client-ssl c1
    aaa-policy p1

```

Configure ADFS Information

We can configure ADFS by using the metadata that is provided by ADFS. You need to download the metadata and import the data to A10 Thunder.

To download the metadata:

1. Enter the following command:

```
import auth-saml-idp tp-idp use-mgmt-port ftp://ben@192.168.x.x/owa/
FederationMetadata/2007-06/FederationMetadata.xml
```

2. Create a **saml identity-provider** and assign the metadata to the identity provider by entering the following command:

```
aam authentication saml identity-provider tp-adfs
    metadata tp-idp
```

Act as a Service Provider

To configure A10 Thunder as a service provider, enter the following commands:

```
aam authentication saml service-provider axowa-sp
    adfs-ws-federation enable
    assertion-consuming-service index 0 location /axowa binding post
    entity-id https://webmail-sp.a10-tplab.com/axowa
    service-url https://webmail-sp.a10-tplab.com
```

The following list provides additional information about the commands:

- **adfs-ws-federation enable**: specify the service provider use WS-federation instead of SAML protocol.
- **assertion-consuming-server** is the endpoint provided by service provider.
- After ADFS or other identify provider complete the authentication they can forward or redirect the tokens to this endpoint. In this example, the SSO service URL is https://webmail-sp.a10-tplab.com. Therefore, **location** is configured to **/axowa** and another **service-url** option to https://webmail-sp.a10-tplab.com. The **index** and **binding** options follow the ADFS's configuration as **0** and **post**. (The configuration should map to ADFS's relying party trusts configuration, which will be configured later in Changes on ADFS.)

- **entity-id** is the unique name for this service provider.
- **service-url**, is the service URL for this service provider.

In this example, the URL is *https://webmail-sp.a10-tplab.com*.

Information about OWA Servers

In the example topology, only one OWA server is deployed in 192.168.90.119. You can deploy multiple OWA servers for load balancing.

To configure the back-end OWA server, enter the following commands:

```
slb server owa1 192.168.90.119
  port 443 tcp
!
slb service-group app-sg tcp
  member owa1 443
```

Authentication and Relay Tokens

To configure a ws-federation relay so that A10 Thunder can relay tokens to the backend OWA servers, enter the following commands:

```
aam authentication relay ws-federation ws_relay
  application-server exchange-owa
  authentication-uri /owa
```

These commands create a ws-federation relay called `ws_relay`, with the following options:

- **application-server** specifies the backend application server type. In the example, it is OWA server, so, you can configure it as **exchange-owa**.
- **authentication-url** is the URL path for the backend server to receive ws-federation tokens. The authentication path for OWA is **/owa**.

For the authentication information, enter the following commands:

```
aam authentication template a1
  type saml
  saml-sp axowa-sp
  saml-idp tp-adfs
  relay ws_relay
!
```

The **aam authentication template** specifies a template with the following options for authenticate methods:

- **type**, specifies the authentication type. In the example, it is **saml**.
- **saml-sp** specifies the service provider configuration. You must assign the previously configured **axowa-sp** to it.
- **saml-idp** specifies the identify provider configuration. You must assign the previously configured **p-adfs** to it.
- **relay** specifies the configuration for how we relay the token to the backend. You must assign the previously configured **ws_relay** to it.

Service Connectivity

- To configure SSL information to connect to the client, the back-end server, and the server address to receive requests from user, enter the following commands:

```
slb template server-ssl s1
!
aam aaa-policy p1
  aaa-rule 1
    action allow
    authentication-template a1
!
slb template client-ssl c1
  cert webmail-sp.a10-tplab.com.pem
  key webmail-sp.a10-tplab.com.pem
!
slb virtual-server vip1 192.168.91.56
  port 443 https
  source-nat auto
  service-group app-sg
  template server-ssl s1
  template client-ssl c1
  aaa-policy p1
```

- To configure SSL between A10 Thunder and the back-end server, enter the following command to create a blank server-ssl template:

```
slb template server-ssl s1
```

- To configure SSL between A10 Thunder and user, enter the following commands to create a client-ssl template and specify the certificate and the private key that you want to use for your service server:

```
slb template client-ssl c1
  cert webmail-sp.a10-tplab.com.pem
  key webmail-sp.a10-tplab.com.pem
```

Note: You can import the certificate and the private key by entering the **import cert** and **import cert-key** commands.

- To configure a policy for the service provider, enter the following commands:

```
aam aaa-policy p1
  aaa-rule 1
    action allow
    authentication-template a1
```

In this example, we do not need a policy. We added one rule to allow all requests and also assigned the authentication template.

- To specify the **IP address** and **port** for our service provider and assign the recently configured **back-end server(s)**, **SSL configurations** and **policy** to the service provider, enter the following commands:

```
slb virtual-server vip1 192.168.91.56
  port 443 https
  source-nat auto
  service-group app-sg
  template server-ssl s1
  template client-ssl c1
  aaa-policy p1
```

Changes on ADFS

Since the Identifiers/Entity-ID and service URL of A10 Thunder is different from OWA server, you should change the **Identifier** and Endpoints values in the ADFS **Relying Party Trusts**.

To change the identifier and endpoint values:

1. On the ADFS server, open **ADFS 2.0 Management**.
2. Select **Relying Party Trusts** and right click on the relying party for the OWA server.
3. Select **Properties**.

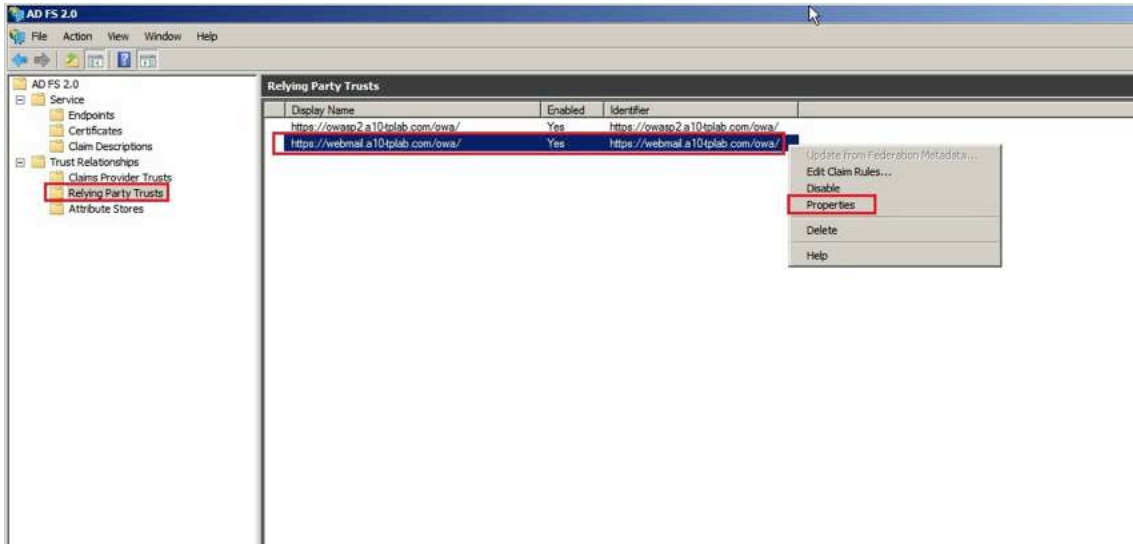


Figure 28: Making Changes in ADFS

4. On the **Identifiers** tab, in **Relying Party Identifier**, enter `https://webmail-sp.a10-tplab.com/axowa`, which is the A10 Thunder entity ID.
5. Click **OK**.

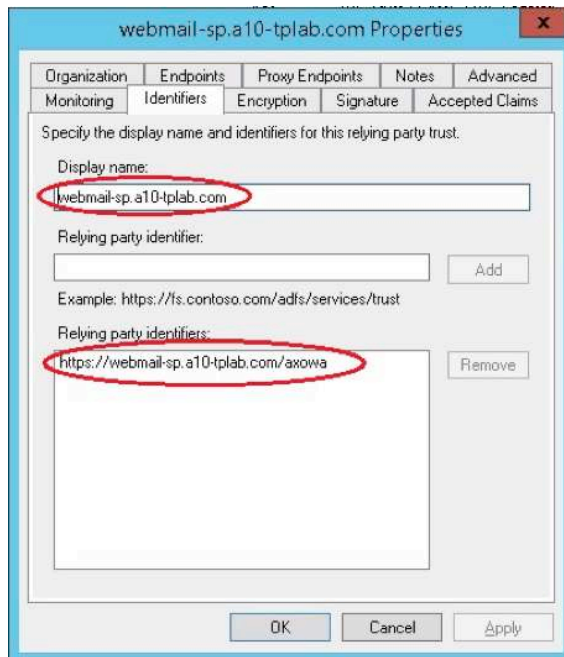


Figure 29: Updating the relying party identifier

6. On the **Endpoints** tab, select the POST Binding URL, and click **Edit**.
7. Change the **Trusted URL** of endpoint to `https://webmail-sp.a10-tplab.com/axowa`, which is A10 Thunder's Assertion Consuming Service location.

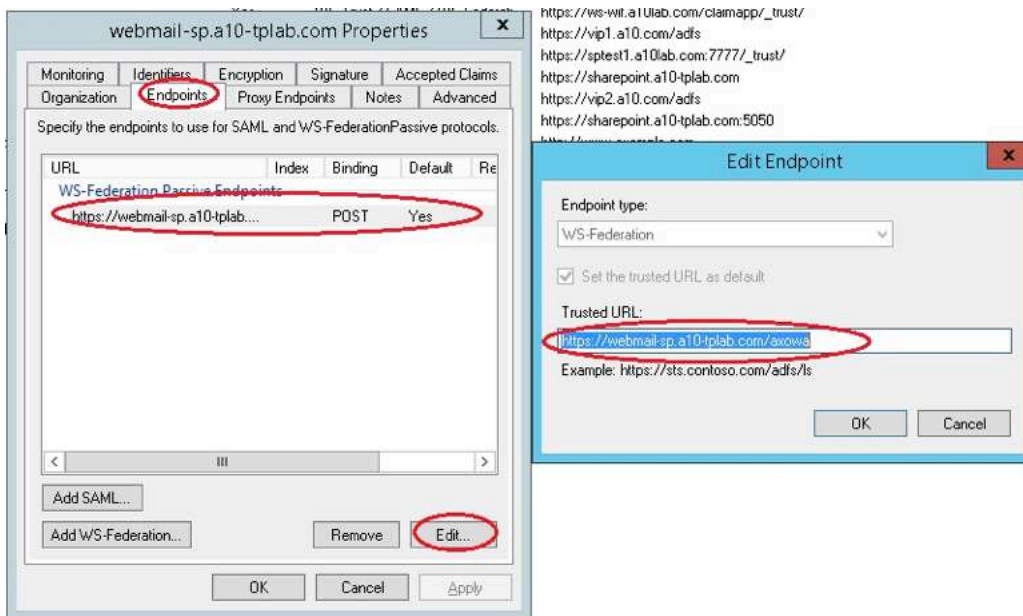


Figure 30: Modifying the endpoints value

Note: To allow the user to work with the OWA server directly with A10 Thunder, you can add the relying party again by following the steps in "Configuring ADFS".

Modifying the Exchange Server

To make changes on the Exchange server:

1. In OWA server, open the web.config file for the OWA service.
2. Add the Entity ID of A10 Thunder to the <audienceUris> tag.

For example, if the identifier of OWA is `https://webmail.a10-tplab.com/owa` and the Entity ID of A10 Thunder is `https://webmail-sp.a10-tplab.com/axowa`, change the web.config file from:

```
<audienceUris>
  <add value="https://webmail.a10-tplab.com/owa" />
</audienceUris>
```

to the following:

```
<audienceUris>
  <add value="https://webmail.a10-tplab.com/owa" />
  <add value="https://webmail-sp.a10-tplab.com/axowa" />
</audienceUris>
```

This will allow OWA to accept WS-Federation tokens that were issued for OWA and A10 Thunder.

```

20 <authentication mode="None" />
21 <compilation>
22 <assemblies>
23 <add assembly="Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
24 </assemblies>
25 </compilation>
26 </system.web>
27 <system.webServer>
28 <modules runAllManagedModulesForAllRequests="true">
29 <add name="WSFederationAuthenticationModule" type="Microsoft.IdentityModel.Web.WSFederationAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
30 <add name="SessionAuthenticationModule" type="Microsoft.IdentityModel.Web.SessionAuthenticationModule, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" preCondition="managedHandler" />
31 </modules>
32 </system.webServer>
33 <microsoft.identityModel>
34 <service>
35 <audienceUris>
36 <add value="https://webmail.a10-tplab.com/owa/" />
37 <add value="https://webmail-sp.a10-tplab.com/axowa/" />
38 </audienceUris>
39 <securityTokenHandlers>
40 <add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
41 <add type="Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" />
42 </add>
43 </securityTokenHandlers>
44 <applicationService>
45 <claimTypeRequired>
46 <!--Following are the claims offered by STS 'http://idp.a10-tplab.com/adfs/services/trust'. Add or uncomment claims that you require by your application and then update the federation metadata of this application.-->
47 <claimType type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" optional="true" />
48 <claimType type="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" optional="true" />

```

Figure 31: Modifying the web.config file

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16144-EN-02
June 2015

Worldwide Offices

North America
sales@a10networks.com

Europe
emea_sales@a10networks.com

South America
latam_sales@a10networks.com

Japan
jinfo@a10networks.com

China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com

Korea
korea@a10networks.com

Hong Kong
HongKong@a10networks.com

South Asia
SouthAsia@a10networks.com

Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: www.a10networks.com/contact or call to talk to an A10 sales representative.