SharePoint SAML-based Claims Authentication with A10 Thunder ADC

How to integrate SharePoint SAML-based claims authentication with Microsoft Active Directory Federation Services (AD FS) and A10 Thunder ADC
Table of Contents

Overview ........................................................................................................................................................................................................................................... 3
Install SharePoint Server 2010 R2 ........................................................................................................................................................................................................................................... 3
AD FS Configuration ........................................................................................................................................................................................................................................... 3
  Phase 1: Create an AD FS relying party for the SharePoint web application. .......................................................................................................................... 3
  Phase 2: Configure the Claim Rule .......................................................................................................................................................................................... 12
  Phase 3: Export the token signing certificate ........................................................................................................................................................................ 14
Configure the SharePoint Server .................................................................................................................................................................................................................... 19
  Phase 1: Configure SharePoint 2010 to trust AD FS as an identity provider ........................................................................................................... 19
  Phase 2: Configure the SharePoint web application to use claim-based authentication and AD FS as the trusted identity provider ........................................................................................................................................................................................................................................... 23
  Phase 3: Configure the IIS server .......................................................................................................................................................................................... 29
Configuration Guide for Thunder ADC ........................................................................................................................................................................................................... 30
Verify Configuration and Deployment ........................................................................................................................................................................................................... 31
Reference .................................................................................................................................................................................................................................................. 32
About A10 Networks ......................................................................................................................................................................................................................... 32

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.
Overview

This guide describes how to authenticate SAML-based claims with SharePoint by configuring and deploying A10 Networks® Thunder® Application Delivery Controllers (ADC) with Active Directory Federation Services (AD FS).

This guide consists of the following parts:

- Install SharePoint server 2010 R2
- Configuration guide for AD FS
- Configuration guide for SharePoint
- Configuration guide for A10 Thunder ADC

This configuration guide assumes that you already have one working Active Directory (AD) and SQL database server.

Install SharePoint Server 2010 R2

To install SharePoint 2010 R2:

1. Install Windows server 2008 R2.
2. Configure the Windows server to join the AD domain.
3. Install the SharePoint server 2010 R2 by completing the following tasks:
   a. Install the software prerequisites.
   b. Install the SharePoint Server.

For more detailed information about installing SharePoint 2010 R2, see the Microsoft SharePoint 2010 Install Guide.

AD FS Configuration

Phase 1: Create an AD FS relying party for the SharePoint web application.

1. Add a new relying part for Thunder ADC SAML Service Provider (SP).
2. Start the **Relying Party Trust Wizard**.

![Figure 2: The relying party trust wizard](image1)

3. Select **Enter data about the relying party manually** and click **Next**.

![Figure 3: Selecting the data source](image2)
4. Enter the relying party display name and click Next.

![Figure 4: Specifying the display name](image)

5. Select AD FS profile and click Next.

![Figure 5: Selecting a profile](image)
6. Click Next.

For this deployment, encryption is not enabled, so do not specify an encryption certificate. To enable SAML assertion encryption between Thunder ADC and AD FS, import Thunder ADC’s service provider certificate.

![Figure 6: Configuring the certificate](image)

7. Select the **Enable support for the WS-Federation Passive protocol** checkbox.

8. In **Relying party WS-Federation passive protocol URL**, enter the name of the web application URL and add `/_trust/` to the end of the URL.

9. Click Next.
In configuration example below, web application name is `https://sp2010-sp1.a10lab.com/`.

**Figure 7: Configuring the URL**

10. Enter the name of the relying party trust identifier and click **Add**.
11. Click **Next**.
This identifier should be identical to the entity-ID of SAML service provider that was configured on Thunder ADC.

12. Select I do not want to configure multi-factor authentication settings for this relaying party trust at this time.

13. Click Next.
14. Select Permit all users to access this relying party.
15. Click Next.
16. Review the information on the page and click Next.
17. Select the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** checkbox.

18. Click **Close**.

![Add Relying Party Trust Wizard](image)

*Figure 12: Completing the wizard*
Phase 2: Configure the Claim Rule


![Figure 13: Editing claim rules](image)
2. In **Claim rule template**, select **Send LDAP Attributes as Claims**.
3. Click **Next**.

![Select Rule Template]

*Figure 14: Choosing the rule type*

4. In **Claim rule name**, enter the name of the claim rule.
5. In the **Attribute store** drop-down list, select **Active Directory**.
6. Configure the LDAP attribute mappings to the outgoing claim type as shown in Figure 15.
7. Click **Finish** and click **OK**.
Phase 3: Export the token signing certificate

Export the signing certificate for the AD FS server and copy the certificate to a location that SharePoint 2010 can access. This token signing certificate will be used by SharePoint to verify the claim token that is offered by AD FS.

1. On the AD FS 2.0 management console, expand the Service node, and click the Certificates folder.
2. Under Token-signing, right click the certificate, and click View Certificate.
3. On the Details tab, click **Copy to File**.

*Figure 17: Certificate details*
4. Select **DER encoded binary X.509 (.CER)** and click **Next**.

*Figure 18: Certificate Export Wizard*
5. Enter the exported certificate name and click **Next**.

*Figure 19: Selecting the file that will be exported*

![Completing the Certificate Export Wizard](image)

*Figure 20: Completing the Certificate Export*
Configure the SharePoint Server

Phase 1: Configure SharePoint 2010 to trust AD FS as an identity provider.

1. Import the AD FS token signing certificate by using PowerShell.
   a. Start the SharePoint 2010 Management Shell.

![Starting the SharePoint 2010 Management Shell]

*Figure 20: Starting the SharePoint 2010 Management Shell*
b. Import the token signing certificate that was copied from the AD FS server.

![Figure 21: Importing the token signing certificate](image)

Figure 21: Importing the token signing certificate

c. Replace the path in yellow with your AD FS token signing certificate path.

```
PS C:\Users\Administrator> New-SPTrustedRootAuthority -Name "SJ ADFS Token Signing Cert" -Certificate $cert
```

d. Define a unique identifier for claims mapping by using Windows PowerShell:

i. Create the email address claim mapping:

```
$emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
```

ii. Create UPN claim mapping:

```
(upnClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" -IncomingClaimTypeDisplayName "UPN" -SameAsIncoming
```

iii. Create the role claim mapping:

```
roleClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -IncomingClaimTypeDisplayName "Role" -SameAsIncoming
```

iv. Create the Primary SID claim mapping:

```
$primarySidClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid" -IncomingClaimTypeDisplayName "SID" -SameAsIncoming
```
2. Create a new authentication provider by using the following PowerShell commands:

The URL in yellow should be changed to **your ADFS server name**.

```powershell
$realm = "urn:sharepoint:<SharePointWebAppName>"
$signInURL = "https://adfs.a10lab.com/adfs/ls"
$ap = New-SPTrustedIdentityTokenIssuer -Name <ProviderName> -Description <ProviderDescription> -realm $realm -ImportTrustCertificate $cert
-ClaimsMappings $emailClaimMap,$upnClaimMap,$roleClaimMap,$sidClaimMap
-SignInUrl $signInURL -IdentifierClaim $emailClaimMap.InputClaimType
```

*Figure 22: Creating the primary SID claim mapping*

*Figure 23: Creating a new authentication provider*
3. Verify that an authentication provider has been successfully created.

![Figure 24: Verifying that an authentication provider has been created](image)
Phase 2: Configure the SharePoint web application to use claim-based authentication and AD FS as the trusted identity provider.

1. In SharePoint Central Administration, click Application Management.
2. In the Web Applications section, click Manage web applications.

3. Click the New icon in the top left to create a new web application.
4. In Authentication, select Claims Based Authentication.
5. In **Security Configuration**, under Use Secure Sockets Layer (SSL), select **Yes**.

![Figure 26: Using Secure Sockets Layer](image)

6. In **Claims Authentication Types**, select **Trusted Identity provider**, and select the name of your SAML identity provider. This is the name that was created by entering the `New-SPTtrustedIdentityTokenIssuer` command.

![Figure 27: Claims authentication types](image)
7. In **Enable Customer Experience Improvement Program**, select **No**, and click **OK**.

![Image of creating a new web application](image)

*Figure 28: Creating a new web application*

8. Click the **Create Site Collection** link to create a SharePoint site.

![Image of creating a new site collection](image)

*Figure 29: Creating a new site collection*
9. In **Title**, enter the site title and a **Description**.

10. Set the primary administrator and click **OK**.

![Figure 30: Creating the site collection](image)

After the web application and site have been created, edit the User Policy to add the users who can access this web application.

11. In **Application Management**, click **Manage Web Applications**.

12. Select the appropriate web application and click **User Policy**.

![Figure 30: Editing the user policy](image)
13. In Policy for Web Application, click **Add Users**.

![Add Users](image1)

**Figure 31: Adding users**

14. In **Zones**, select **All zones**, and click **Next**.

![Add Users](image2)

**Figure 32: Adding users**

15. In **Choose Users** section, add the permitted user account that is allowed to access this web application.

16. In **Choose Permissions**, select the permissions that you grant to users.

17. Click **Finish**.
To allow all AD FS authenticated users to access SharePoint, click the bottom right address icon.

18. In **Select People and Groups**, click the Search icon, and select **All Authenticated Users**.

---

**Figure 33: Adding users and permissions**

**Figure 34: Searching for all authenticated users**
19. Review the list of recently added users and click **OK**.

![List of recently added users](image1.png)

*Figure 35: List of recently added users*

### Phase 3: Configure the IIS server

1. Log in to the **Internet Information Services (IIS) Manager** console.
2. Expand the **Sites** node.
3. Right click on web application that you created for claim-based authentication and click **Bindings**.

![Modifying a SharePoint site](image2.png)

*Figure 36: Modifying a SharePoint site*
4. Select the https row and click Edit.

![Editing type HTTPS](image1.png)

Figure 37: Editing type HTTPS

5. Select a certificate for this HTTPS web application and click OK.

![Selecting the certificate](image2.png)

Figure 38: Selecting the certificate

**Configuration Guide for Thunder ADC**

1. Create a SAML service provider by entering the following commands:

   ```bash
   aam authentication saml service-provider sharepoint_sp
   adfs-ws-federation enable
   assertion-consuming-service index 0 location /_trust/ binding post
   entity-id https://sp2010-sp1.a10lab.com
   service-url https://sp2010-sp1.a10lab.com
   
   Note: The entity-id must be identical to the entity that was configured in AD FS Phase 1 Step 8. The assertion-consuming-service location must be the same as the location that was configured in ADFS Phase 1 Step 7.
   
   2. Create identity provider by downloading the ADFS metadata by using the

      and importing it to Thunder ADC.

      ![Downloading the ADFS metadata](image3.png)

      Figure 39: Downloading the ADFS metadata
3. Create a WS-Federation relay by entering the following commands:
   ```bash
   aam authentication relay ws-federation sharepoint_relay
   authentication-uri /_trust/
   ```

4. Create an AAM authentication template by entering the following commands:
   ```bash
   aam authentication template sharepoint_template
   type saml
   saml-sp sharepoint_sp
   saml-idp adfs
   relay sharepoint_relay
   ```

5. Create an AAA policy by entering the following commands:
   ```bash
   aam aaa-policy sharepoint_policy
   aaa-rule 1
   authentication-template sharepoint_template
   ```

6. Create an SLB service group, a client-SSL template, and a server-SSL template based on the testing environment.

7. Create a VIP by entering the following commands:
   ```bash
   slb virtual-server SJ_VIP 1.1.1.1
   port 443 https
   source-nat auto
   service-group sharepoint-group
   template server-ssl sp_server_ssl
   template client-ssl sp_client_ssl
   aaa-policy sharepoint_policy
   ```

**Verify Configuration and Deployment**

1. Access the SharePoint web application.
   The client is redirected to the AD FS login page.

   ![AD FS login page](image)

   *Figure 40: The AD FS login page*
2. Log in to SharePoint.

SharePoint identifies the logged in user account and displays a custom portal for this user.

![Welcome message after a successful login](image)

**Figure 40: Welcome message after a successful login**

*Note: Ensure that the date and time for Thunder ADC and ADFS are synchronized.*

**Reference**

For more information, see the following documentation:

- Configure SAML-based claims authentication with AD FS in SharePoint 2013
- Implement SAML-based authentication in SharePoint Server 2013
- Windows Server 2012 R2 AD FS Deployment Guide

**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](http://www.a10networks.com)