Achieve Single Sign-on (SSO) for Microsoft ADFS

Leverage A10 Thunder ADC Application Access Manager (AAM)

Table of Contents

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

The purpose of this document is to provide administrators with a guide they can use to deploy A10 Networks® Thunder® ADC line of Application Delivery Controllers Security Assertion Markup Language (SAML), a feature specific to Microsoft Active Federation Services (ADFS) solutions with SAML 2.0 compliancy. This guide will provide detailed configuration steps for how to set up A10 Thunder ADC to authenticate using SAML 2.0 protocol with the SAML 2.0 HTTP POST binding.

SAML Overview

Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between an identity provider (IdP) and a service provider. SAML is a product of OASIS Security Services Technical Committee. With the introduction of SAML support in A10 Networks Advanced Core Operating System (ACOS®) version 4.0, Thunder ADC can act as a service provider in a security topology and delegate authentication and authorization to identify providers. In multi-domain services using the same identity provider, SAML offers easy integration and seamless federation with an identity provider even with clients that originate from different service domains.

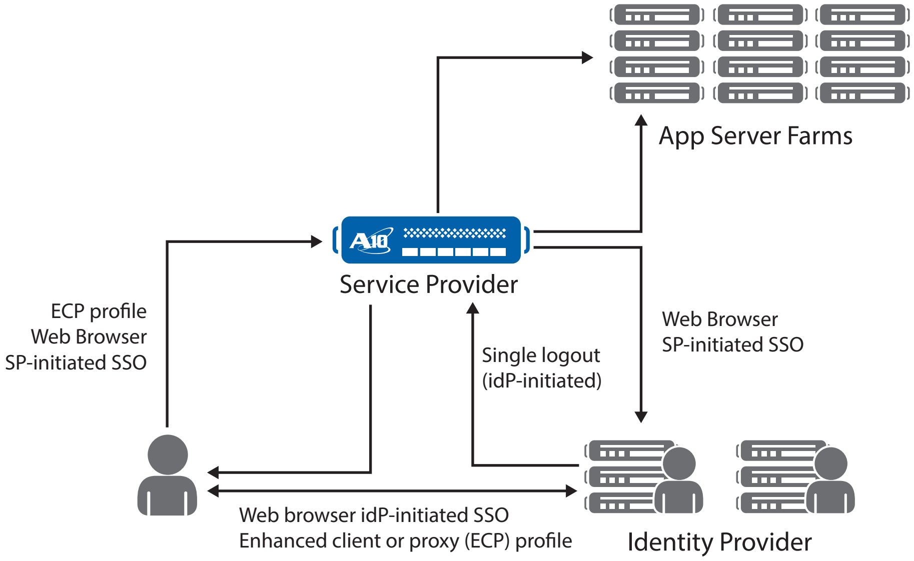


Figure 1: A10 Networks ACOS 4.0 SAML integration overview

With SAML in ACOS 4.0, the Application Access Management (AAM) feature plays an important role to protect resources and distribute access requests. Before access is granted, clients need to provide authentication credentials and meet AAM authorization policies. A security administrator configures an authentication template and an authorization policy in order to perform authentication control.

This guide is designed to provide detailed instructions on how to integrate with Microsoft ADFS IdP. The integration has been tested specifically with the A10 Thunder line of Application Delivery Controllers running ACOS 4.0 and Microsoft ADFS 2.0.

Integration Topology

The following diagram is an overview on how the A10 Networks solution integrates with a third-party Microsoft ADFS SAML device.

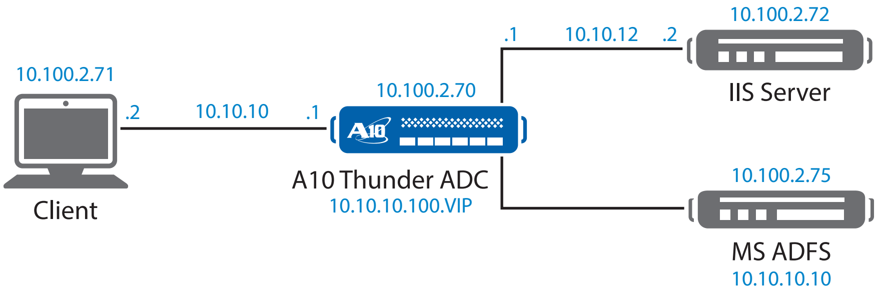


Figure 2: Topology overview

Deployment Prerequisites

To deploy SAML, security administrators must complete the following steps:

1. System Clocks – Synchronize the system clocks of A10 Thunder ADC and the IdP or use Network Time Protocol (NTP) configuration to ensure that time settings are synchronized. A few minutes time drift is acceptable. This is an important requirement to integrate the service provider and the identity provider.
2. Users List – The users list within the IdP has to be preconfigured before the integration starts. Each user will have unique account credentials to access the website, and the user has to be configured within the IdP application. Bulk provisioning may be available, so ask your IdP provider for more details.
3. Identity Provider – SAML 2.0 compliancy is required for the integration with Thunder ADC to work. In this guide, we will integrate with Microsoft ADFS. If you need additional support for another SAML IdP provider, please contact your regional sales team.
4. Service Provider – Thunder ADC acts as a service provider with the SAML topology. The request is front-ended by a service provider and the authentication is passed within the IdP. This configuration is typically called "service provider Initiated." In some cases, a topology where the IdP takes the first request also works and this topology is called "IdP initiated." A SP-initiated and IdP-initiated SSO can be deployed at the same time.
5. Configuration Steps

The Thunder ADC SAML configuration requires a list of steps to get the solution working. To make deployment easier, here are the configuration steps for an administrator to follow.

Step 1: AAM Authentication SAML Service Provider

This section allows the administrator to define the SAML Authentication configuration. This covers the IdP and service provider configuration for SAML, and it includes the configuration of the Thunder ADC and the IdP.

Step 2: Create AAM Authentication Template

The purpose of this configuration is to define the authentication settings; this is also a template that can be used for other configurations within A10 Thunder ADC.

Step 3: Create AAM AAA Policy

Create an AAM authentication, authorization and accounting (AAA) policy. This policy is required for SAML authentication to work. It enables administrators to allow and deny access to application resources. This policy must be configured and defined before you can deploy authentication.

Step 4: AAM Policy Binding to VIP

This section allows the administrator to bind the AAM Authentication template to the virtual IP address (VIP).

Note: Once the AAM policy has been bound to the VIP address, open up a browser and access the protected application. If the AAM policy allows access, the site should prompt the client on access assuming that the IdP credentials were correct. Likewise, if the AAM policy has deny privileges, the site should prevent users from accessing application resources.

A10 Networks Device Requirements

The SAML solution is supported on the following Thunder ADC and A10 Networks AX™ Series devices. ACOS 4.0 is supported on the following platforms:

A10 Networks Thunder ADC and Thunder CGN Hardware

- A10 Thunder 6630(S)
- A10 Thunder 6435
- A10 Thunder 6430(S)
- A10 Thunder 5630(S)
- A10 Thunder 5435(S) SPE
- A10 Thunder 5430(S)-11
- A10 Thunder 5430S
- A10 Thunder 4430(S)
- A10 Thunder 3030S (Non-FPGA)
- A10 Thunder 1030S (Non-FPGA)
- A10 Thunder 930 (Non-FPGA)

A10 Networks AX Series Hardware

- A10 AX 5630 ADC
- A10 AX 5200-11 ADC
- A10 AX 3530 CGN (non-FPGA)
- A10 AX 3400 CGN
- A10 AX 3200-12 ADC

A10 Networks vThunder line of virtual appliances

- vThunder ADC for Azure
- vThunder for VMware EXSi
- vThunder for KVM (with SR-IOV)
- vThunder for KVM
- vThunder for Hyper-V
- All A10 Networks Thunder HVA hybrid virtual appliances (Thunder 3030S HVA, Thunder 3530S HVA)

Microsoft ADFS Requirements

Minimum Hardware Recommendations

- Multi-core Intel Xeon processor or higher (Windows 2008 R2 64-bit or Windows 2012 (64-bit))
- 4 CPU/Cores recommended
- 4 GB of RAM
- 80 GB of available hard drive space
- Active Directory Domain Services (AD DS)
- Web Server Services (IIS)

Note: The following URL is the download site for ADFS 2.0 RTW (Release to Web):

http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=10909

Authentication and Authorization Process

The process diagram below describes a detailed topology and sequential procedures on how A10 Thunder ADC and Microsoft ADFS integrate.

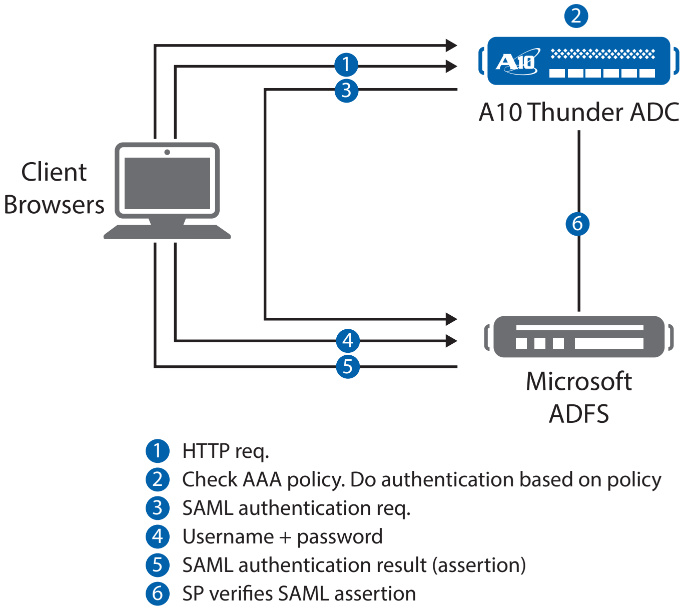
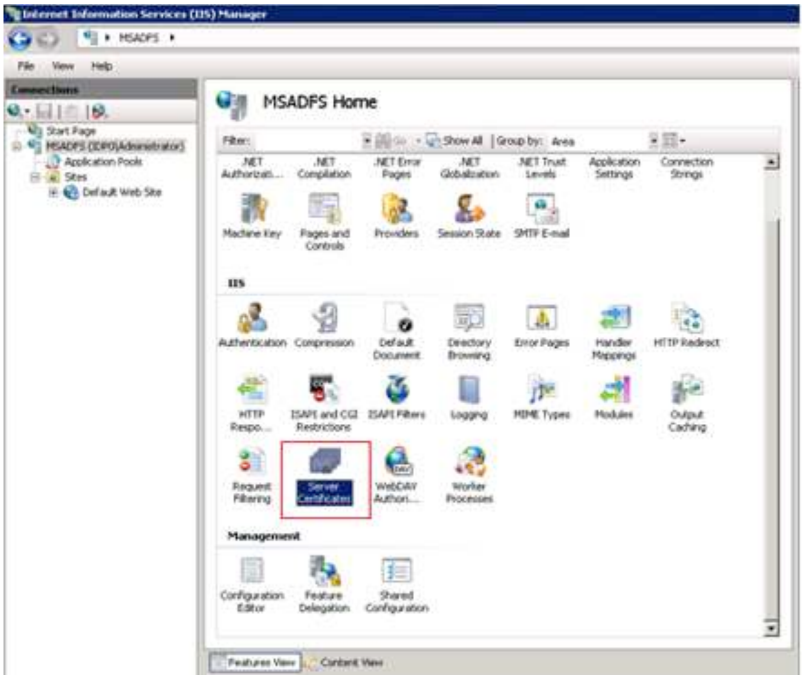

2
1
3
A10 Thunder ADC
Client Browsers
6
4
5
Microsoft ADFS
1 HTTP req.
2 Check AAA policy. Do authentication based on policy
3 SAML authentication req.
4 Username + password
5 SAML authentication result (assertion)
6 SP verifies SAML assertion

Figure 3: A10 Thunder ADC and Microsoft ADFS integration

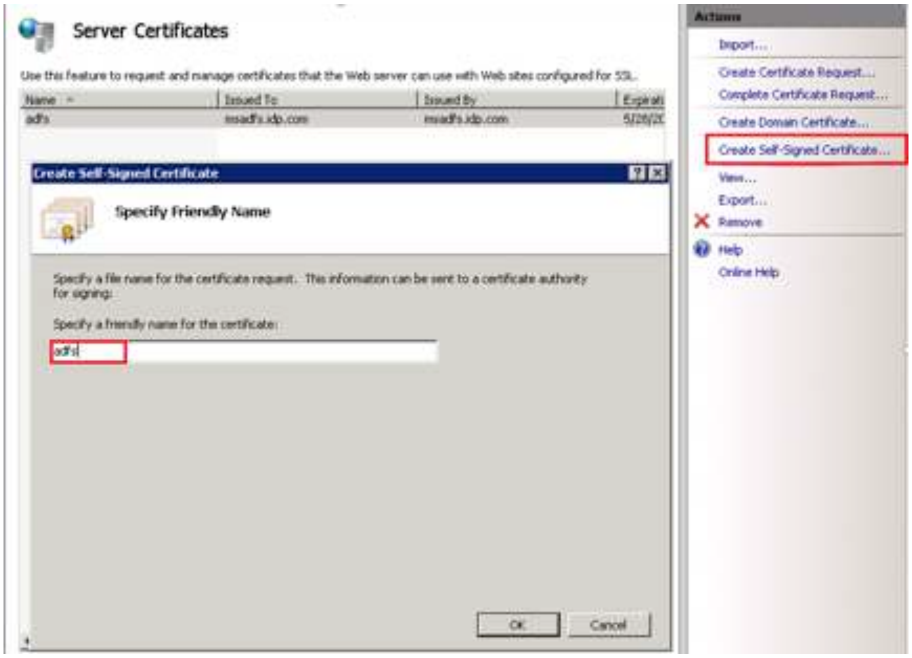
Web Server IIS Installation

This section provides detailed instructions on how to install a Secure Sockets Layer (SSL) self-signed certificate. As part of the requirement, you must have already installed IIS to move forward with the installation.

In the start menu, navigate to All Programs > Administrative Tools > Internet Information Services (IIS) manager. Within the console tree, double-click the icon named Server Certificates.



In the action pane, select **Create Self-signed Certificate**. On the "**Specify Friendly Name**" page, enter "**adfs**" and click **OK**.


Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expirati
adfs	msadfs.idp.com	msadfs.idp.com	5/26/2C

Create Self-Signed Certificate

Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

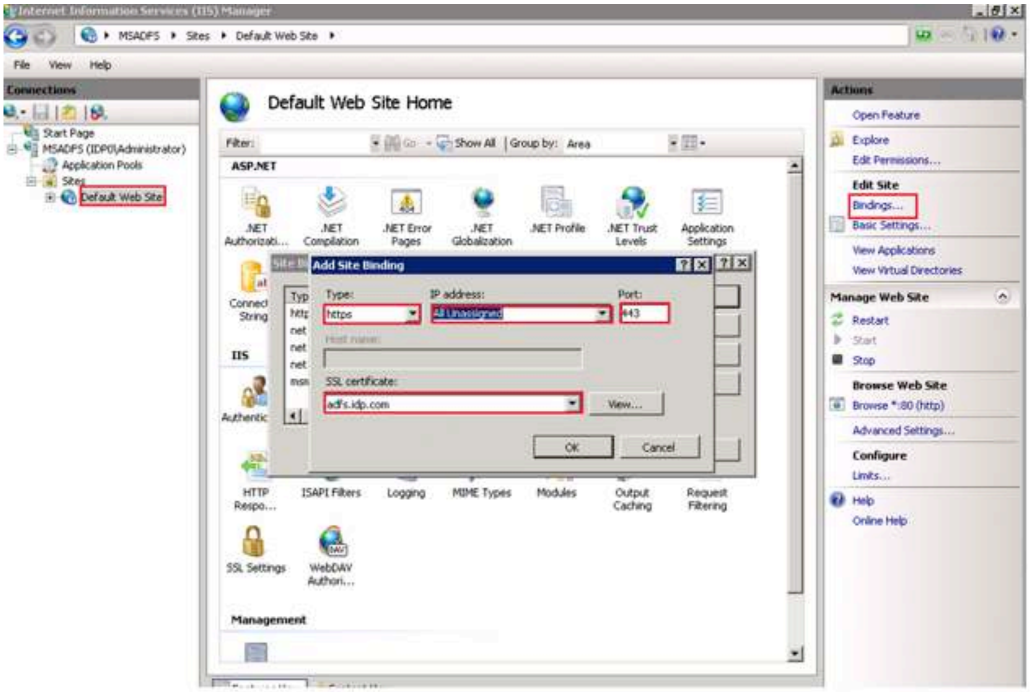
Specify a friendly name for the certificate:

adfs

Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
OK
Cancel

Now follow these steps:

1. In the console tree, select the **Default Web Site**.
2. In the **Actions** pane, click **Bindings**.
3. In the **Site Bindings** dialog box, click **Add**.
4. In the **Add Site Binding** dialog box, select **https**. In the **IP address** drop-down, select "**All Unassigned**" **and Port "443."** In the **Type** drop-down list, select the **adfs.idp.com** certificate. In the **SSL certificate** drop-down list, click **OK**, and then click **Close**.



Type: https

IP address: All Unassigned

Port: 443

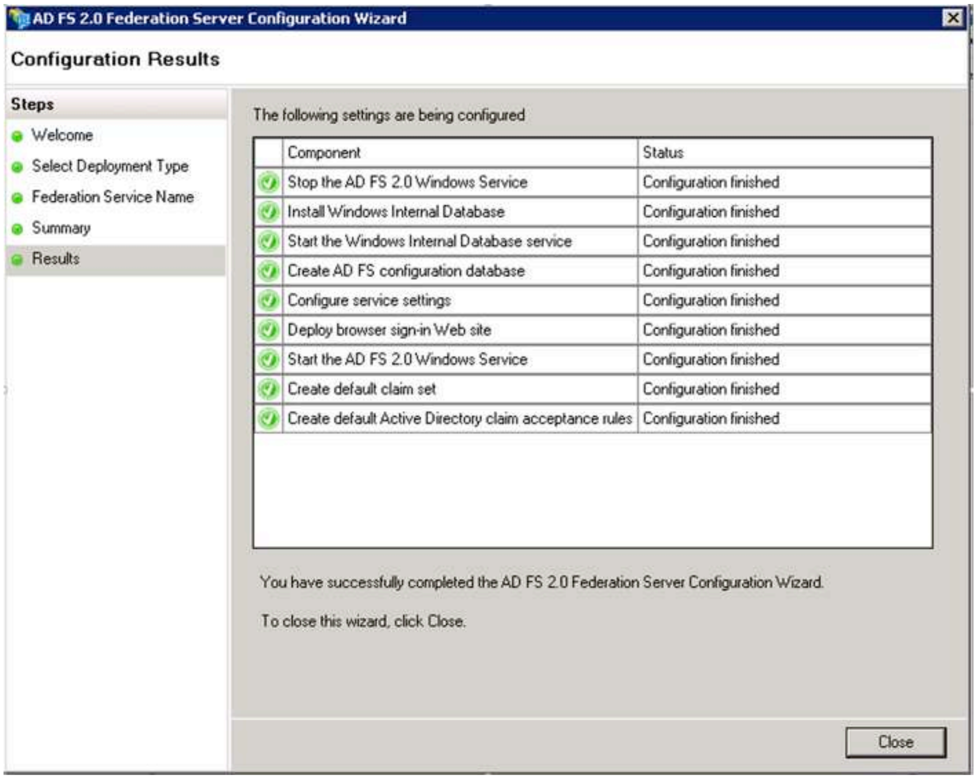
SSL certificate: adfs.idp.com

ADFS 2.0 Installation

1. After the download of the ADFS 2.0 image is complete, locate the **AdfsSetup.exe** installation package and then start the installation by double-clicking the executable file.
2. Follow the setup wizard page and accept the end user license agreement (EULA).
3. During the installation wizard process, you will be prompted with a Server Role window. In this segment of the installation, select "**Federation Server**" and then click **Next**.
4. You have now completed the installation of Microsoft ADFS 2.0 using the Setup Wizard.
5. You can use the Management console to administer the ADFS 2.0 system.

Configuring a Stand-alone Federation Server

1. In the **ADFS 2.0 Federation Server Configuration Wizard**, click to start the wizard.
2. On the installation options of **Select Stand-alone or Farm Deployment** page, click **Stand-alone federation server**, and then click **Next** to continue.
3. On the **Specify the Federation Service Name** page, verify that the **adfs.idp.com** certificate is selected, and then click **Next**.
4. On the **Ready to Apply Settings** page, review the settings, and then click **Next**.
5. On the **Configuration Results** page, click **Close**.



Configuration Results

The following settings are being configured

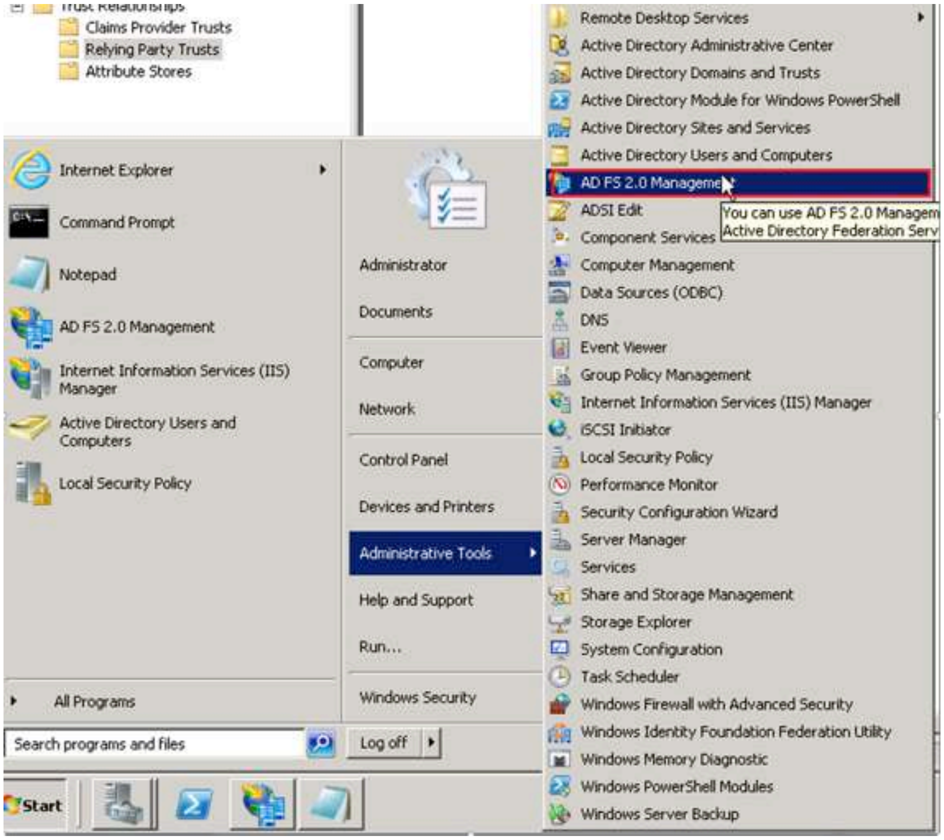
Component	Status
Stop the AD FS 2.0 Windows Service	Configuration finished
Install Windows Internal Database	Configuration finished
Start the Windows Internal Database service	Configuration finished
Create AD FS configuration database	Configuration finished
Configure service settings	Configuration finished
Deploy browser sign-in Web site	Configuration finished
Start the AD FS 2.0 Windows Service	Configuration finished
Create default claim set	Configuration finished
Create default Active Directory claim acceptance rules	Configuration finished

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Microsoft ADFS Administration

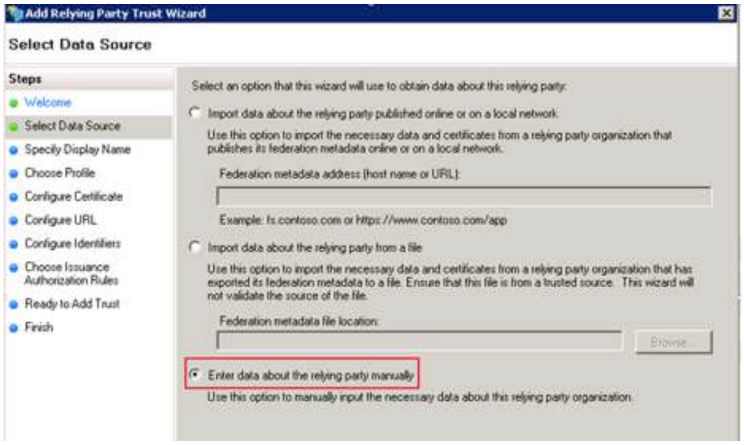
This deployment guide is designed for Microsoft ADFS 2.0 with an Active Directory 2008 R2 data store. ADFS 2.0 can also support Active Directory 2012. To administer ADFS, use ADFS 2.0 Management under Administrator Tools.



Relying Party Trusts

To enable the Relying Party Trusts function in ADFS, navigate to the ADFS Console > Trust Relationships > Relying Party Trusts > right-click and select "Relying Party Trust."

Select the option called "**Enter data about the relying party manually**" in the **Select Data Source** step.



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

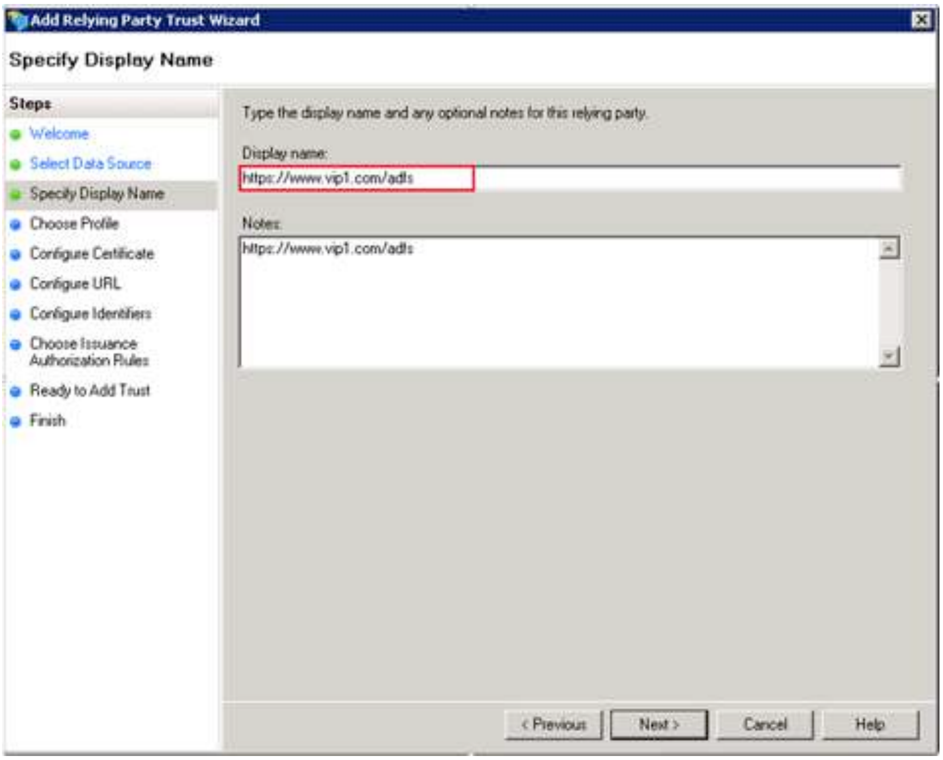
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Define the display name as https://www.vip1.com/adfs in the **Specify Display Name** step.



Add Relying Party Trust Wizard

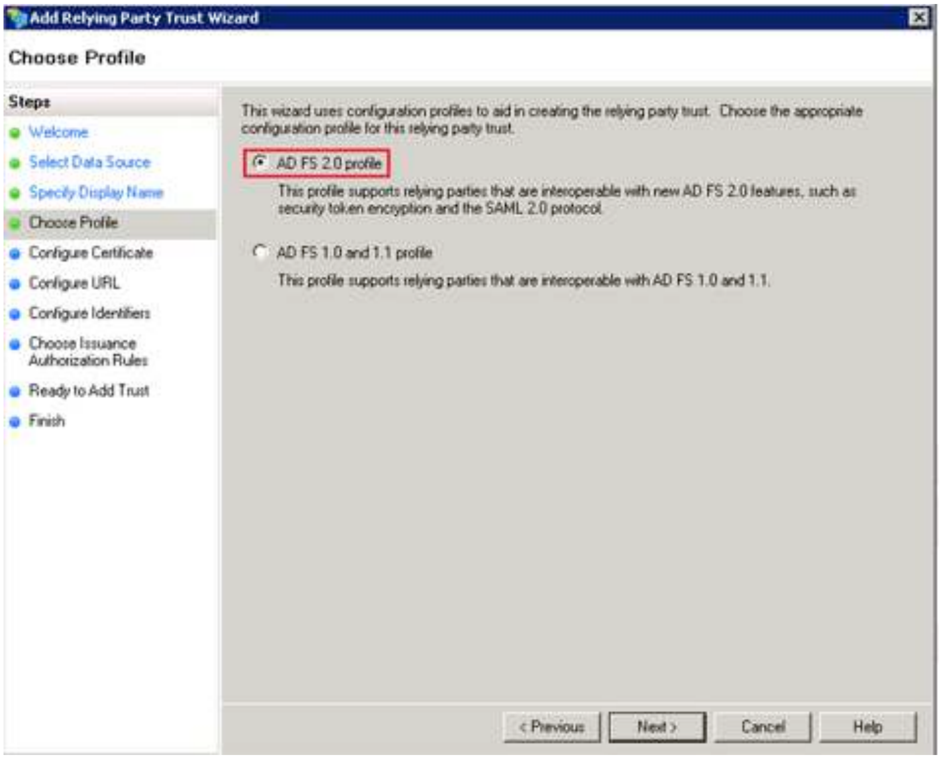
Specify Display Name

Type the display name and any optional notes for this relying party.

Display name: https://www.vip1.com/adfs

Notes: https://www.vip1.com/adfs

Select the ADFS 2.0 profile in the Choose Profile step.



This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

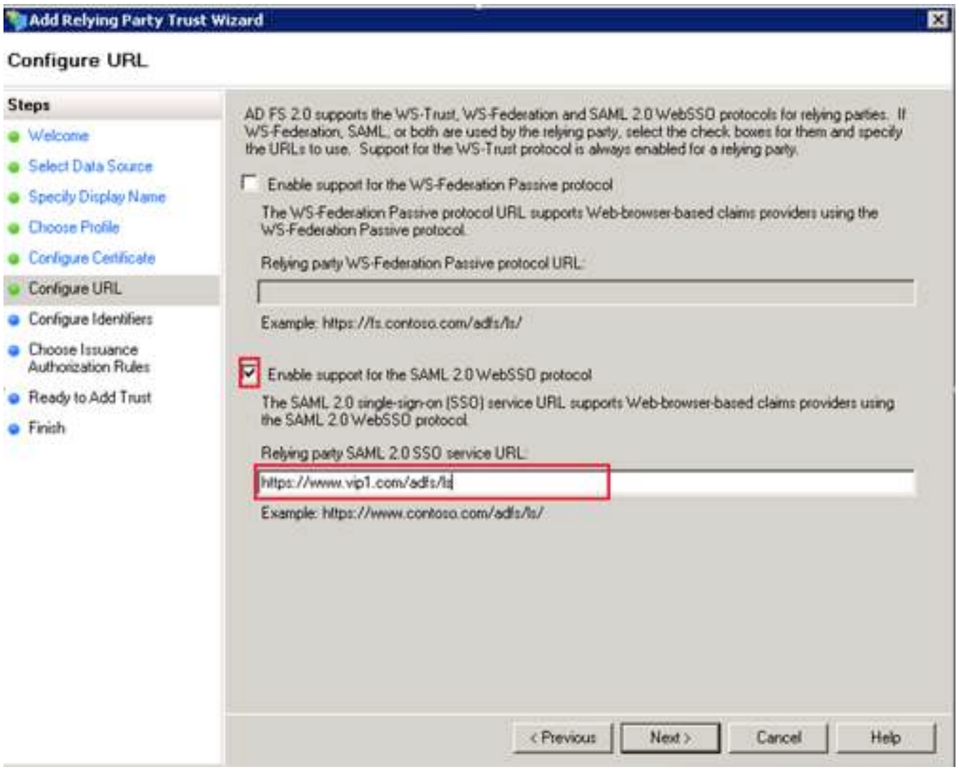
● AD FS 2.0 profile

This profile supports relying parties that are interoperable with new AD FS 2.0 features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

Select "Enable support for the SAML 2.0 WebSSO protocol" in the Configure URL step.



AD FS 2.0 supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

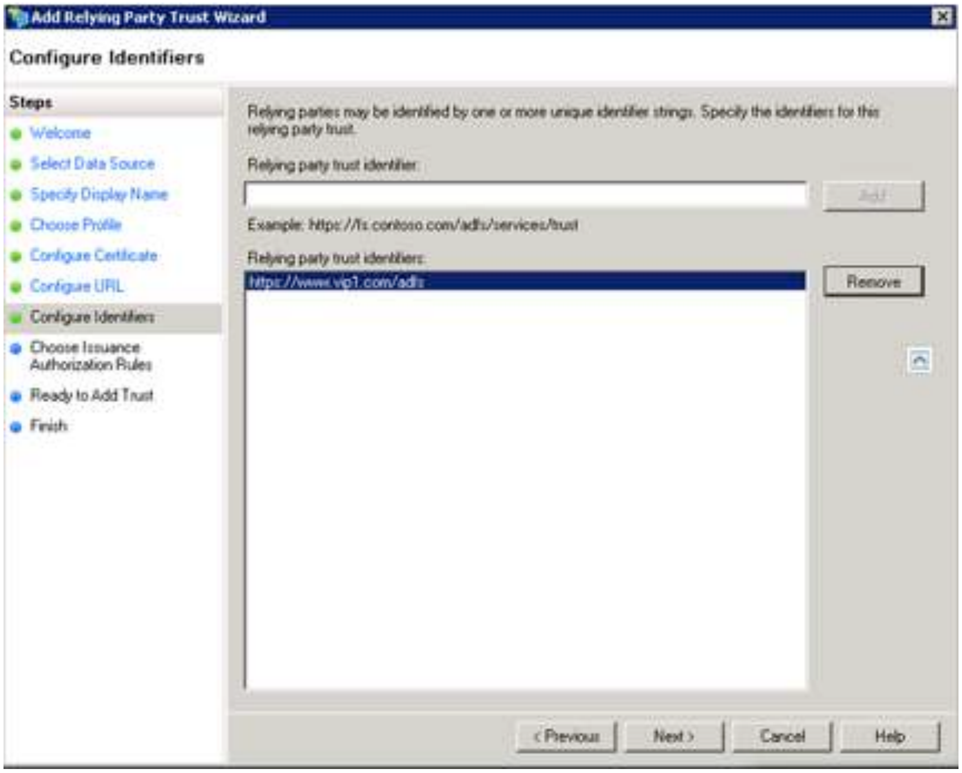
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://www.vip1.com/adfs/ls

Example: https://www.contoso.com/adfs/ls/

Add the trust identifiers as "https://www.vip1.com/adfs" in the **Configure Identifiers** step.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

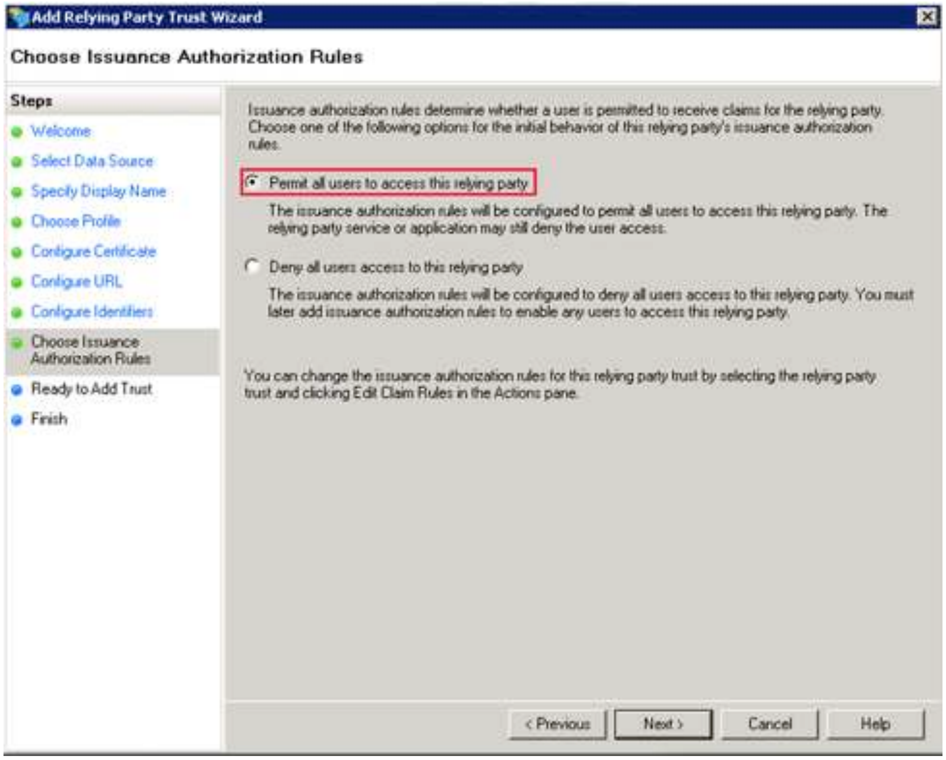
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

https://www.vip1.com/adfs

Select "**Permit all users to access this relying party**" in the **Issuance Authorization Rules** step.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

Once selected, click **Next**. At this point, ADFS Trust installation will be complete.

Deployment Topology Options

Thunder ADC's AAM solution supports two types of deployment with IdP providers. The solution can be deployed with the following options:

Front End, Service Provider-initiated Configuration

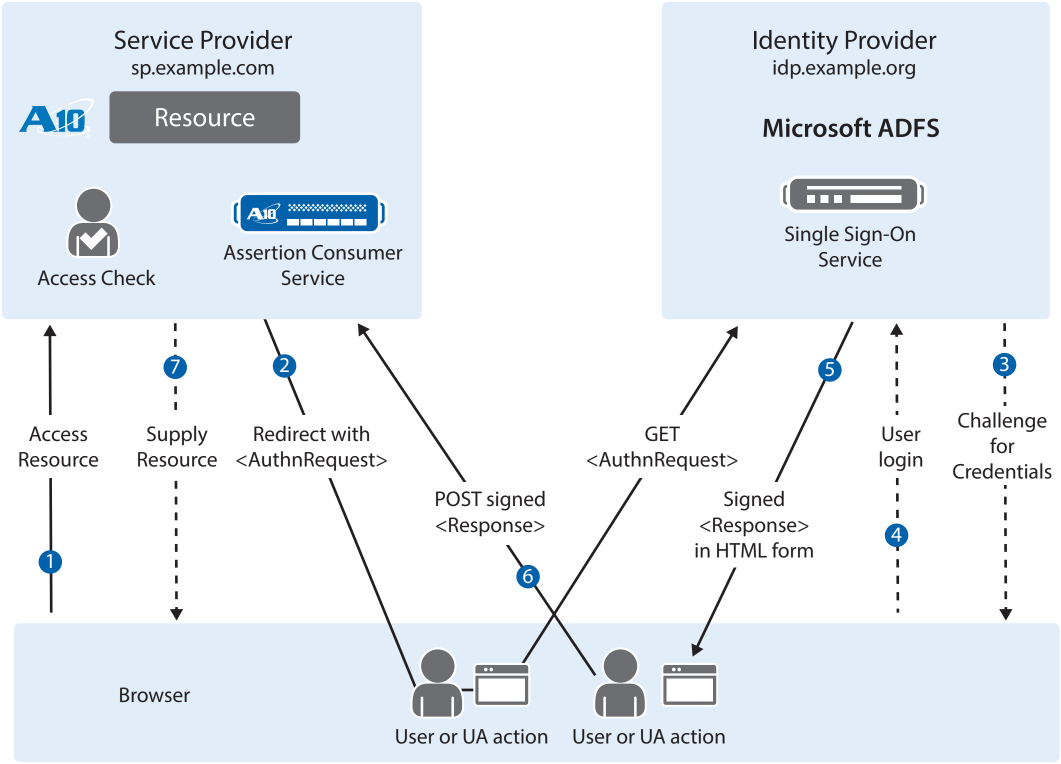


Figure 4: Front end service provider-initiated configuration

Back End, IdP-initiated Configuration

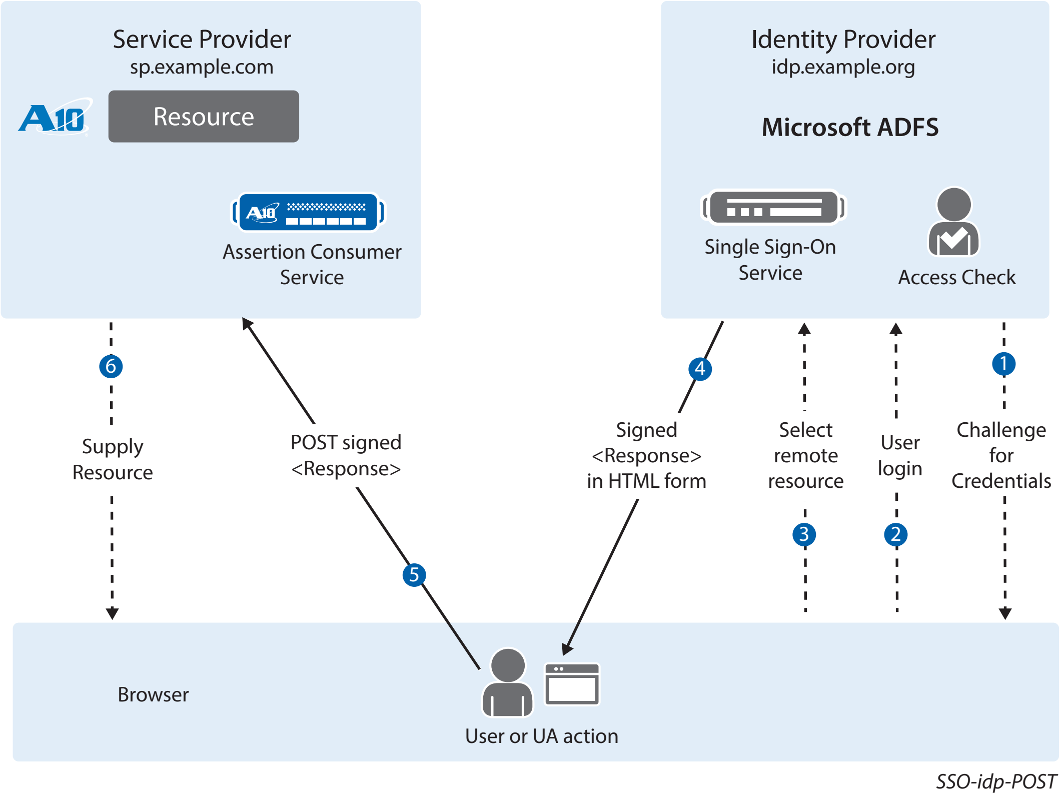


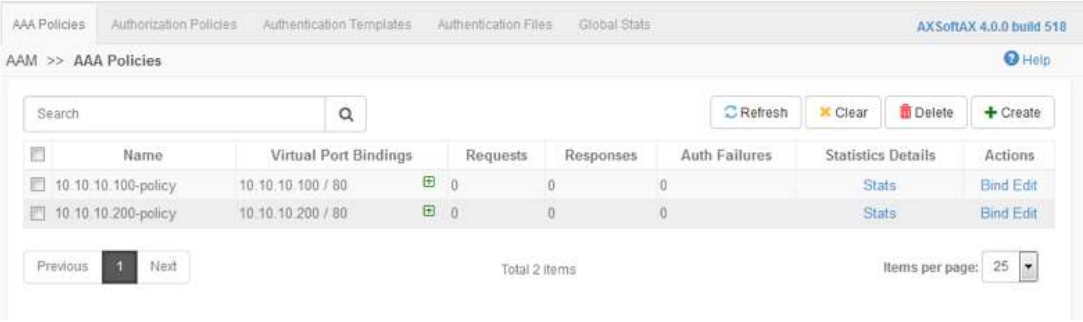
Figure 5: Back end IdP-initiated configuration

Thunder ADC Configuration

This section of the guide provides detailed steps on how to integrate A10 Thunder ADC and Microsoft ADFS. In the Thunder ADC configuration, the ADFS server has to be defined as an SAML authentication server.

SAML Service Provider Configuration

This section of the guide explains how to configure the AAM SAML portion. On the menu of the section of the GUI, navigate to **AAM Policies**.



☐	Name	Virtual Port Bindings		Requests	Responses	Auth Failures	Statistics Details	Actions
☐	10.10.10.100-policy	10.10.10.100 / 80	⊞	0	0	0	Stats	Bind Edit
☐	10.10.10.200-policy	10.10.10.200 / 80	⊞	0	0	0	Stats	Bind Edit

Sample GUI from the AAA Policies

[CLI configuration]

```
aam authentication saml service-provider adfs
  artifact-resolution-service index 0 location /adfs/services/trust/
  artifactresolution binding soap
  assertion-consuming-service index 0 location /SAML2/POST binding post
  single-logout-service location /lgo binding post
  certificate server
  entity-id https://www.vip.com/adfs
  service-url https://www.vip.com
```

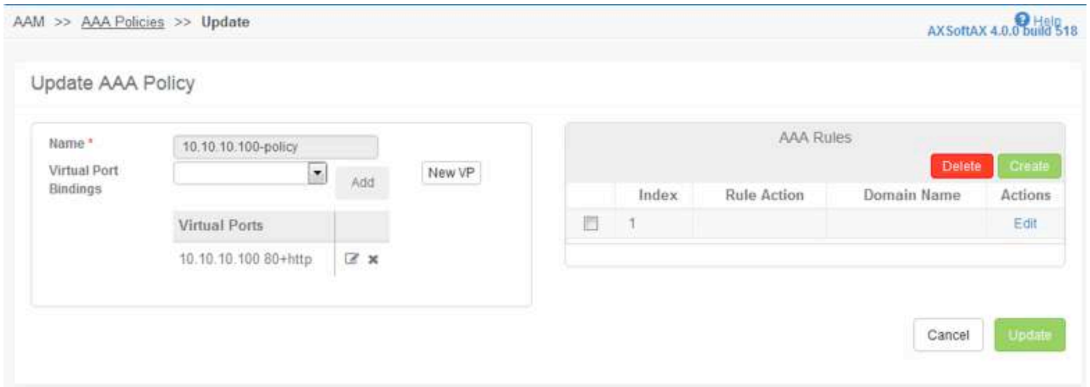
Note: The directories above must match the Thunder ADC and ADFS configurations.

AAA Policy

The AAA Policy section of the GUI is the section where the site administrator configures client permissions. Client policies can be configured based on domain or access list to control access within an application or site. They include:

1. Index-unique
2. Domain Name
3. Access-list
4. Action
5. Authentication template

Sample GUI Configuration



Update AAA Policy

Name *: 10.10.10.100-policy

Virtual Port Bindings:

Virtual Ports
10.10.10.100 80+http

AAA Rules

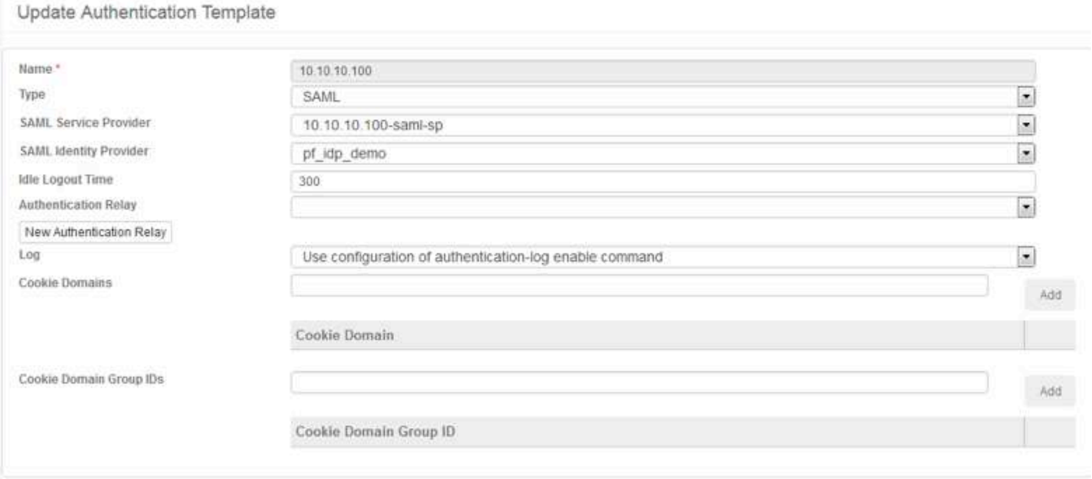
	Index	Rule Action	Domain Name	Actions
□	1			Edit

[CLI configuration]

```
aam aaa-policy 10.10.10.100-policy
  aaa-rule 1
    action allow
    authentication-template 10.10.10.100
```

Authentication Template Configuration

This section enables an administrator to configure the AAM Authentication template:



Update Authentication Template

Name *	10.10.10.100
Type	SAML
SAML Service Provider	10.10.10.100-saml-sp
SAML Identity Provider	pf_idp_demo
Idle Logout Time	300
Authentication Relay	
Log	Use configuration of authentication-log enable command
Cookie Domains	
Cookie Domain Group IDs	

[CLI configuration]

```
aam authentication template 10.10.10.100
  type saml
  saml-sp sp
  saml-idp adfs_idp_demo
  logout-idle-timeout 300
```

Export Metadata Information

Once the connection settings have been completed within A10 Thunder ADC and ADFS, you must export the metadata information. The metadata information has to match the ADFS host address, which includes the public key certificate and signing algorithm (for example: RSA SHA 1). Once completed, use the following command to import the metadata information to Thunder ADC.

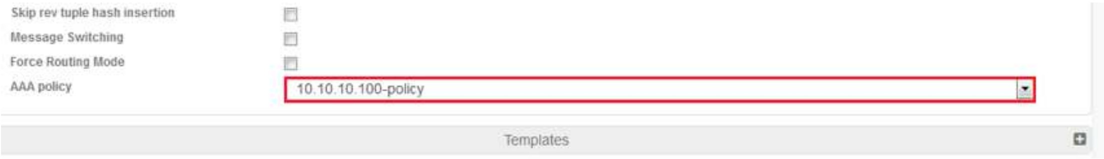
vThunder#import auth-saml-idp **adfs** tftp://**example.com/metadata**

Binding the AAA Policy to the VIP

Once the AAA policy has been configured, you must bind the policy to the respective VIP. The binding can be done from the CLI or from the GUI.

To bind the AAA policy to the VIP, navigate to the VIP Port under **ADC** > **Virtual Services** > **Virtual Port**

Select the **VIP Port** and edit. Within the **General Fields** tab, select the policy within the drop-down menu.



Skip rev tuple hash insertion	□
Message Switching	□
Force Routing Mode	□
AAA policy	10.10.10.100-policy

Summary

In summary, the configuration steps described in this deployment guide show how to set up Thunder ADC AAM integration with the ADFS application. With the introduction of SAML support in A10 Networks Advanced Core Operating System (ACOS) version 4.0, Thunder ADC can act as a service provider in a security topology and delegate authentication and authorization to identify providers. In multi-domain services using the same identity provider, SAML offers easy integration and seamless federation with an identity provider even with clients that originate from different service domains.

This integrated solution provides the following benefits:

- Minimizes the overwhelming nature of user interactions with traditional AAA servers
- Simplifies network authentication by using the A10 device as an authentication proxy
- Offloads web and authentication servers
- Enables A10 Thunder ADC to handle the sending and initial processing of authentication challenges, forwarding credentials to SAML IdP and granting access.

By using Thunder ADC, significant benefits are achieved for all authentication deployments. For more information about A10 Thunder ADC products, please refer to the following URLs:

https://www.a10networks.com/products/thunder-series/thunder-adc

www.a10networks.com/products/application_delivery_controllers.php

Appendix

Sample Configuration

```
hostname SAML
timezone UTC nodst
ntp server ntp
  prefer
interface management
  ip address 10.100.2.70 255.255.255.0
  ip default-gateway 10.100.2.1
interface ethernet 1
  enable
  ip address 10.10.10.1 255.255.255.0
interface ethernet 2
  enable
  ip address 10.10.12.1 255.255.255.0
ip nat pool saml-ipv4 10.10.10.17 10.10.10.19 netmask /24
aam authentication log enable
aam authentication saml service-provider 10.10.10.100-saml-sp
  assertion-consuming-service index 1 location /SAML2/POST binding post
  entity-id http://10.10.10.100/adfs
  service-url http://10.10.10.100
aam authentication saml service-provider adfs
aam authentication saml identity-provider adfs_idp_demo
  metadata adfs_idp
aam authentication saml identity-provider idp
aam authorization policy test
  attribute-rule 1
slb resource-usage virtual-port-count 1024
slb resource-usage virtual-server-count 512
slb server apache2 10.10.12.200
  port 80 tcp
aam authentication template 10.10.10.100
  type saml
  saml-sp 10.10.10.100-saml-sp
  saml-idp adfs_idp_demo
slb service-group http-sg tcp
  member apache2 80
!
slb service-group https-sg tcp
slb template client-ssl client-ssl-amm
slb virtual-server AAM-HTTPS 10.10.10.100
  port 80 http
    source-nat auto
    service-group http-sg
    aaa-policy 10.10.10.100-policy
end
```

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-16148-EN-01
May 2015

Worldwide Offices

North America sales@a10networks.com	**Taiwan** taiwan@a10networks.com
Europe emea_sales@a10networks.com	**Korea** korea@a10networks.com
South America latam_sales@a10networks.com	**Hong Kong** HongKong@a10networks.com
Japan jinfo@a10networks.com	**South Asia** SouthAsia@a10networks.com
China china_sales@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.