DEPLOYMENT GUIDE

SAML 2.0 Single Sign-on (SSO) Deployment Guide with Ping Identity

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.

The purpose of this document is to provide a quick deployment guide that administrators can use to deploy the A10 Networks® Thunder® Series Security Assertion Markup Language (SAML) feature with SAML 2.0-compliant PingFederate Identity Provider (IdP) solutions from Ping Identity. The guide provides a step-by-step configuration explaining how to set up the Thunder Series with the Application Access Management (AAM) SAML solution and configuration parameters required within the SAML IdPs.

SAML Overview

SAML is an XML-based open-standard format for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP). SAML was developed by the Security Services Technical Committee of OASIS. With the introduction of SAML support in the A10 Networks Advanced Core Operating System 4.0 (ACOS® 4.0) platform, the ACOS solution acts as a service provider within the security topology and delegates authentication and authorization to identify providers. In multi-domain services using the same identity provider, SAML is the best fit, is easy to integrate, and provides seamless federation with an identity provider even when clients originate from different service domains.

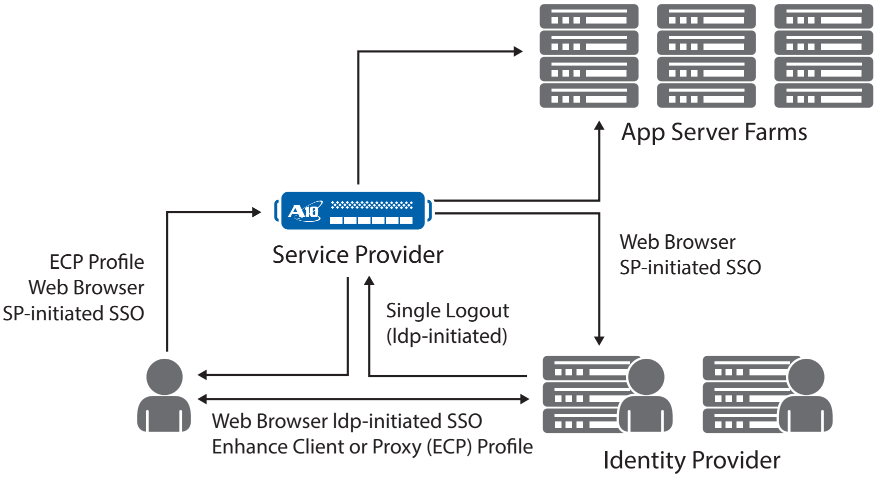


Figure 1. SAML deployment topology

With SAML in ACOS 4.0, the AAM feature plays an important role to protect resources and ensure that access requested are granted. Before access is granted to resources, clients need to pass authentication and meet AAM authorization policies. Also, the security administrator needs a configuration authentication template and authorization policy in order to perform authentication control.

This guide is designed to provide detailed instructions on how to integrate A10 Thunder Series with PingFederate IdPs. The integration has been tested specifically with A10 Thunder Series 4.0 Build 329 and PingFederate release 7.3.1.1.

Integration Topology

The following diagram provides an overview of how the Thunder Series solution integrates with a third-party PingFederate SAML device.

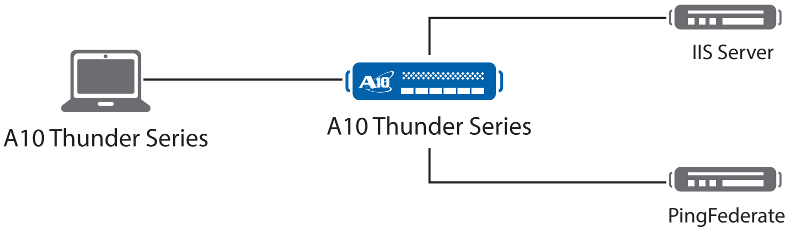


Figure 2. Thunder Series integration with third-party PingFederate SAML device

Note: Before deploying the SAML solution within Thunder Series devices, the IdP solution must be deployed. This guide does not cover the installation procedures of PingFederate. Hence, the user of this deployment guide must already have an understanding of all SAML requirements, the PingFederate management interface, as well as how to make configuration changes to the IdP.

Deployment Requirements

To deploy SAML, the following parts of the topology are required:

1. Thunder Series and the IdP server clock must be synchronized or use Network Time Protocol (NTP) configuration to match time. This is an important requirement to make sure that service provider and IdP integrate. A few minutes time drift is acceptable.
2. Users within the IdP have to be preconfigured before the integration starts. Each user will have a unique account credential to access the website. Each user has to be configured within the IdP application. Bulk provisioning may be possible so ask your IdP provider for more details.
3. Identity Provider-SAML 2.0 compliancy is required for the Thunder Series integration to work. In this guide, we will integrate with PingFederate. If you need additional support for other SAML IdP providers, please contact your A10 Networks regional sales team.
4. The Thunder Series acts as a service provider with the SAML topology. The request is made at the frontend 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."

Configuration Steps

The Thunder Series SAML configuration requires a list of steps to get the solution working. To make deployment easier, we have a set of configuration steps that the administrator can follow.

Step 1: Define AAM SAML Authentication for IdP and Service Provider

This section allows the administrator to define the SAML Authentication configuration; it covers the IdP and service provider configuration for SAML.

Step 2: Create AAM Authentication Template

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

Step 3: Create AAM AAA Policy

An AAM authentication, authorization and accounting (AAA) policy is required for SAML authentication to work. This policy provides "allow and deny" access to the resources available. This policy must be configured and defined before you can deploy AAM Authentication.

Step 4: Bind AAM Policy to VIP

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

Note: Once the VIP AAM policy has been bound to the VIP, open up a browser and access the website/application. If the AAM policy has "allow" privileges, the site should prompt the client for access assuming that the IdP credentials are correct. Likewise, if the AAM policy has "deny" privileges, the site should prompt the client with a no access prompt.

PingFederate Requirements

Minimum Hardware Requirements

- Intel Pentium 4, 1.8 GHz processor
- 1 GB of RAM
- 250 MB of available hard drive space

Minimum Hardware Recommendations

- Multi-core Intel Xeon processor or higher (Windows/Linux)
- 4 CPU/Cores recommended
- Multi-core SPARC processor (Solaris)
- 4 CPU/Cores recommended
- 4 GB of RAM
- 1.5 GB available to PingFederate
- 500 MB of available hard drive space

Supported Browsers

For the PingFederate administrative console:

- Chrome 31.x or higher
- Firefox 33.1 or higher
- Internet Explorer (version 8 or higher)

Authentication and Authorization Process

The process diagram below describes a detailed topology and sequential procedures on how ACOS and IdP integrate.

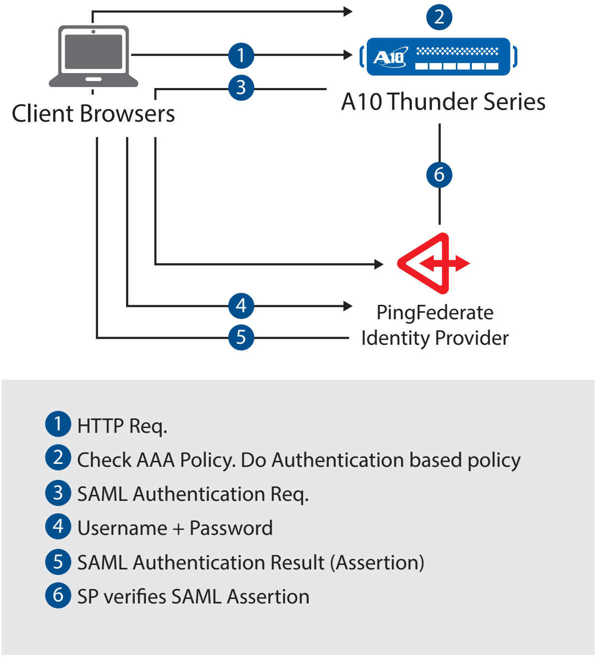
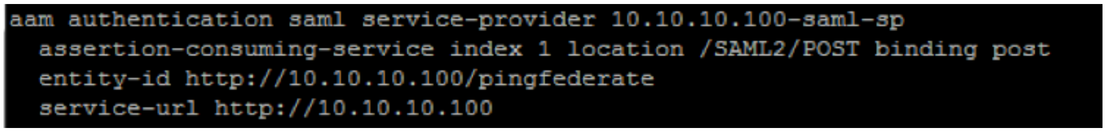

Client Browsers
A10 Thunder Series
PingFederate
Identity Provider
1
2
3
4
5
6
1 HTTP Req.
2 Check AAA Policy. Do Authentication based policy
3 SAML Authentication Req.
4 Username + Password
5 SAML Authentication Result (Assertion)
6 SP verifies SAML Assertion

Figure 3. ACOS and IdP integration

PingFederate Administration

This deployment guide is based on a specific version of the PingFederate application, namely PingFederate version 7.3.1.1.

Note: *In order to have a quick deployment of service provider initiated SAML, the AAM Authentication SAML service provider (refer to Figure 5) has to have a consistent configuration from both the service provider (ACOS) and the identity provider (PingFederate). The spaces and capitalizations within ACOS and the PingFederate configuration matter, so make sure that you verify those entries.*



```
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/pingfederate
  service-url http://10.10.10.100
```

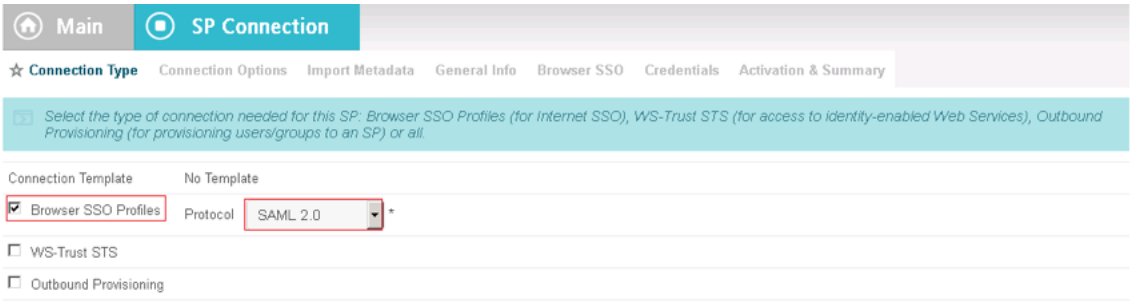
Figure 4: ACOS AAM Authentication SAML service provider configuration

To administer and configure PingFederate IdP, the administrator uses a web browser to configure the IdP management console, and security administrators must use administrator credentials to configure the service provider connections. Refer to the PingFederate requirements section for the approved management console browser.

Service Connection Configuration

To create a new service provider connection, navigate to the PingFederate main dashboard and within the SP Connection section, select "Create New."

Using the Connection Type tab, select Browser SS0 Profiles, and on the Protocol dropdown menu, select SAML 2.0, then click Next.



Select the type of connection needed for this SP: Browser SSO Profiles (for Internet SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

Connection Template No Template

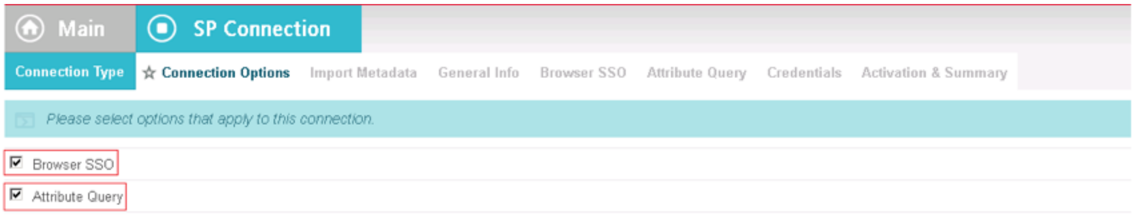
☑ Browser SSO Profiles Protocol SAML 2.0 *

□ WS-Trust STS

□ Outbound Provisioning

Figure 5. PingFederate SP connection

On the Connection Options tab, you must select both Browser SSO and Attribute Query and then click Next.



Please select options that apply to this connection.

☑ Browser SSO

☑ Attribute Query

Figure 6. PingFederate connection type

Skip the "Import data" section, and continue on with the General Info section.

In the General Info tab, enter the following information:

Partner Entity ID (Connection ID): *http://10.10.10.100/pingfederate

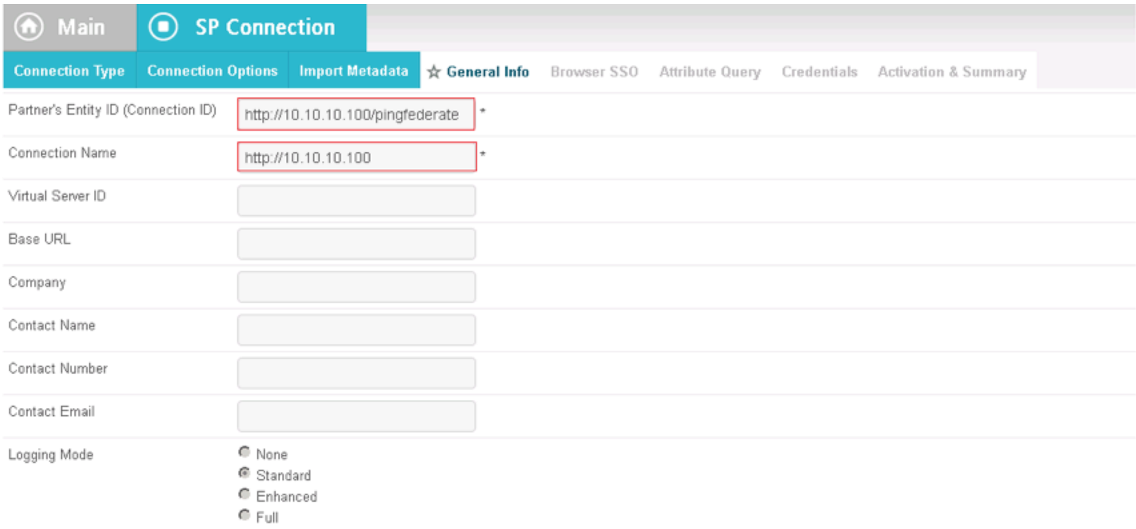
Sample AAM CLI Entity-ID configuration

```
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/pingfederate
  service-url http://10.10.10.100
```

Connection Name: *****http://10.10.10.100***

Sample AAM CLI Service URL configuration

```
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/pingfederate
  service-url **http://10.10.10.100
```



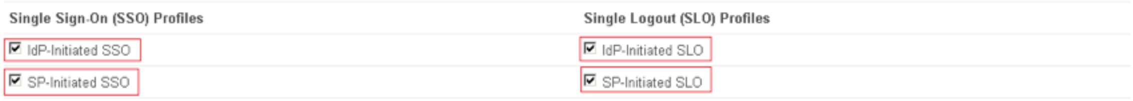
Partner's Entity ID (Connection ID)	http://10.10.10.100/pingfederate *
Connection Name	http://10.10.10.100 *
Virtual Server ID	
Base URL	
Company	
Contact Name	
Contact Number	
Contact Email	
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

Figure 7. PingFederate metadata

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain language identifier for this connection. Optionally, you can specify a Virtual Server ID for *your own server* to use when communicating with this partner. If set, the virtual ID will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints. The rest of the menu such as Company, Contact Name and others are all optional parameters.

Click Next to configure the Browser SSO. Note that you have multiple options that cover Single Sign-On and Single Logout (SLO) profiles, with options of either IdP- or service provider initiated.

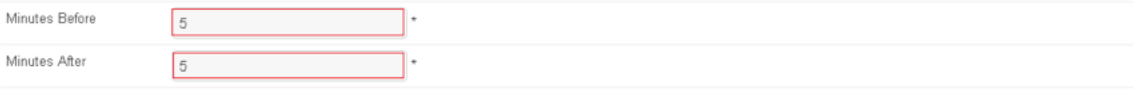
The ACOS AAM feature can support SSO and SLO profiles configured for IdP or service provider.



Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
☑ IdP-Initiated SSO	☑ IdP-Initiated SLO
☑ SP-Initiated SSO	☑ SP-Initiated SLO

***Note**: Service provider initiated SLO will be supported in a later 4.0 release.*

Click Next, then configure and select the default Assertion Lifetime settings of 5 minutes.



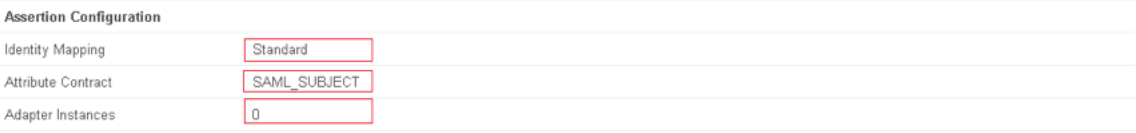
Minutes Before	5 *
Minutes After	5 *

Figure 8. SSO/SLO options

Assertion Creation

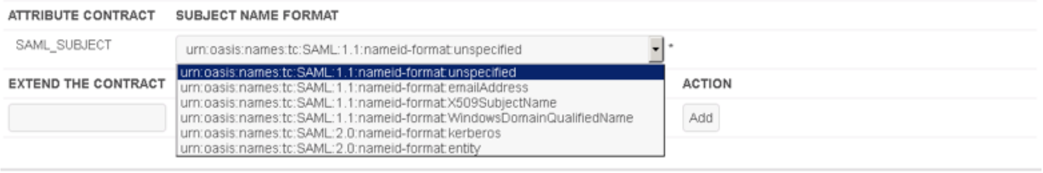
Identity mapping is the process by which users authenticated by the IdP are associated with user accounts local to the service provider. Select the type of name identifier that you will send to the service provider. Note that your selection may affect the way the service provider looks up and associates the user to a specific local account.

In this configuration, select Standard Identity Mapping, which sends the service provider a known attribute value as the name identifier. The service provider will often use account mapping to identify the user locally.



Assertion Configuration	
Identity Mapping	Standard
Attribute Contract	SAML_SUBJECT
Adapter Instances	0

Figure 9. Pingfederate Assertion Configuration



ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *

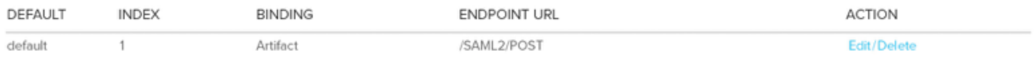
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
urn:oasis:names:tc:SAML:2.0:nameid-format:entity

Figure 10. Subject Name Format

For the Subject Name Format, select the nameid-format and set adapter instance settings to "0."

Assertion Consumer Service URL

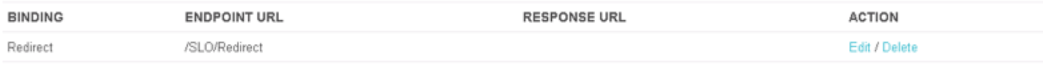
On the Assertion Consumer Service URL, you must add the following configuration. As the IdP, you send SAML assertions to the service provider's **Assertion Consumer Service**. The service provider may request that the SAML assertion be sent to one of several URLs via different bindings. Please provide the possible Assertion Consumer URLs below and select one to be the default.



DEFAULT	INDEX	BINDING	ENDPOINT URL	ACTION
default	1	Artifact	/SAML2/POST	Edit/Delete

Figure 11. PingFederate Service URL

SLO Service URL



BINDING	ENDPOINT URL	RESPONSE URL	ACTION
Redirect	/SLO/Redirect		Edit / Delete

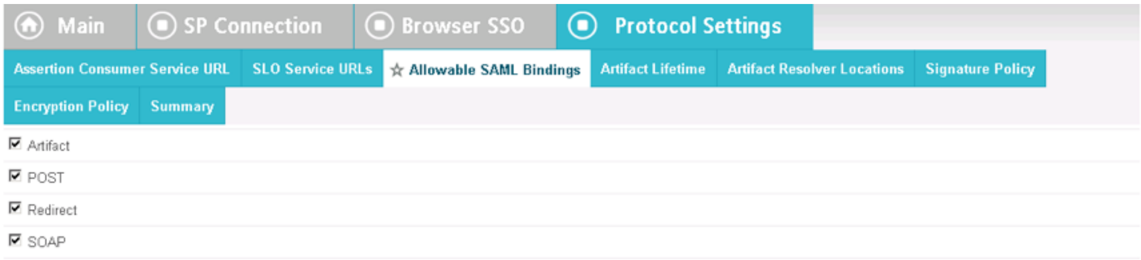
Figure 12. PingFederate Service URL configuration

For the SLO Service URL, you must enter the following information. You may send SAML logout messages to the service provider's **Single Logout Service**. Depending on the situation, the service provider may request that messages be sent to one of several URLs via different bindings. Please provide the endpoints that you would like to use.

Single logout (SLO) profile is used to disassociate a session with the principal. Normally once a principal has authenticated to an identity provider, it will create one established session with that principal. At some time later, the principal may want to terminate the session with session authority or session participant. This is what single logout messages are used for.

Allowable SAML Bindings

The ACOS system can support Artifacts, Post, Redirect and SOAP. For example, the service provider might send the message, "Which SAML bindings do you want to allow?" Depending on the type of application you have, you can select the different sets of SAML bindings that ACOS and PingFederate can integrate.



☑ Artifact

☑ POST

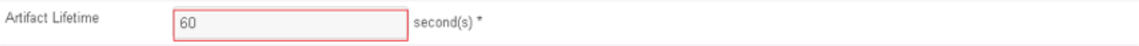
☑ Redirect

☑ SOAP

Figure 13. SAML binding options

Artifact Lifetime

Set the Artifact Lifetime setting to 60 seconds. This time setting represents short-lived tokens, and this is how long the recipient of the artifact should take to retrieve the corresponding message.

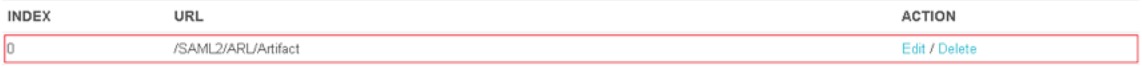


Artifact Lifetime 60 second(s) *

Figure 14. Artifact Lifetime configuration

Artifact Resolver Location

This section allows you to provide the remote party URLs that you will use to resolve/translate the artifact and get the actual protocol message.



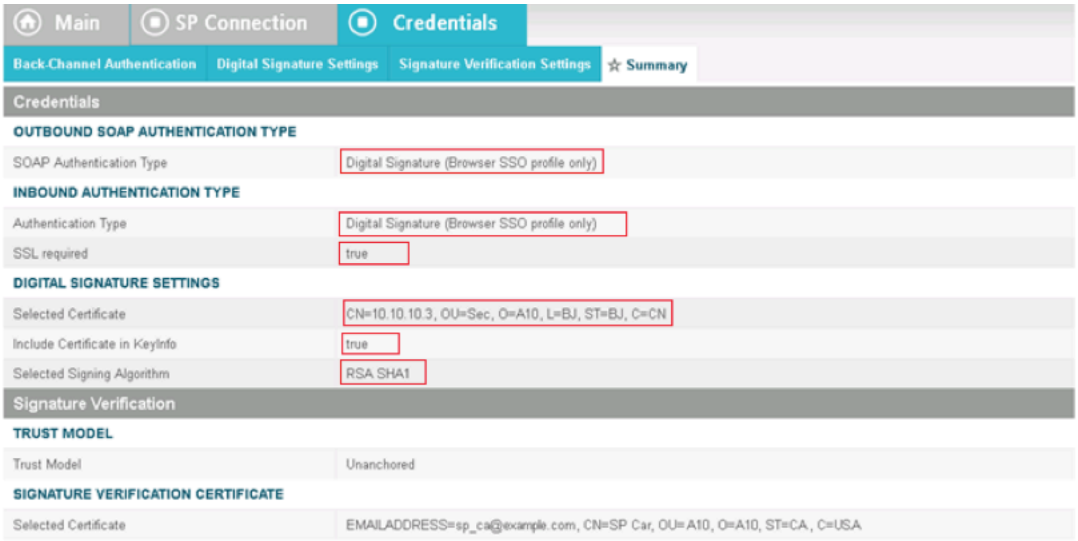
INDEX	URL	ACTION
0	/SAML2/ARL/Artifact	Edit / Delete

Figure 15. Artifact resolver URL

Set the signature policy to "false" and do not select any encryption policy which makes the parameter inactive. Save the configuration.

Credential Configuration

For credential settings, configure the following parameters.


Main
SP Connection
Credentials
Back-Channel Authentication
Digital Signature Settings
Signature Verification Settings
☆ Summary

Credentials	
OUTBOUND SOAP AUTHENTICATION TYPE	
SOAP Authentication Type	Digital Signature (Browser SSO profile only)
INBOUND AUTHENTICATION TYPE	
Authentication Type	Digital Signature (Browser SSO profile only)
SSL required	true
DIGITAL SIGNATURE SETTINGS	
Selected Certificate	CN=10.10.10.3, OU=Sec, O=A10, L=BJ, ST=BJ, C=CN
Include Certificate in KeyInfo	true
Selected Signing Algorithm	RSA SHA1
Signature Verification	
TRUST MODEL	
Trust Model	Unanchored
SIGNATURE VERIFICATION CERTIFICATE	
Selected Certificate	EMAILADDRESS=sp_ca@example.com, CN=SP Car, OU= A10, O=A10, ST=CA, C=USA

Figure 16. PingFederate credential options

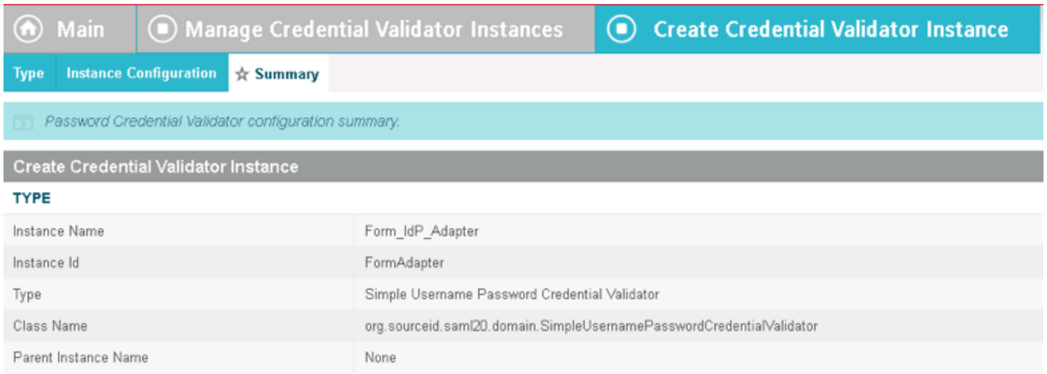
User Creation

This section of the guide explains how to create users within PingFederate. Within the PingFederate Console page, navigate to Authentication and click Password Credential Validators.

Create two sets of Credential Validator Instance and name them as "Form_IdP_Adapter" and "HTTP_Basic_IdP_Adapter."

Configure the following instance with the following parameters:

For Form_IdP_Adapter Instance:

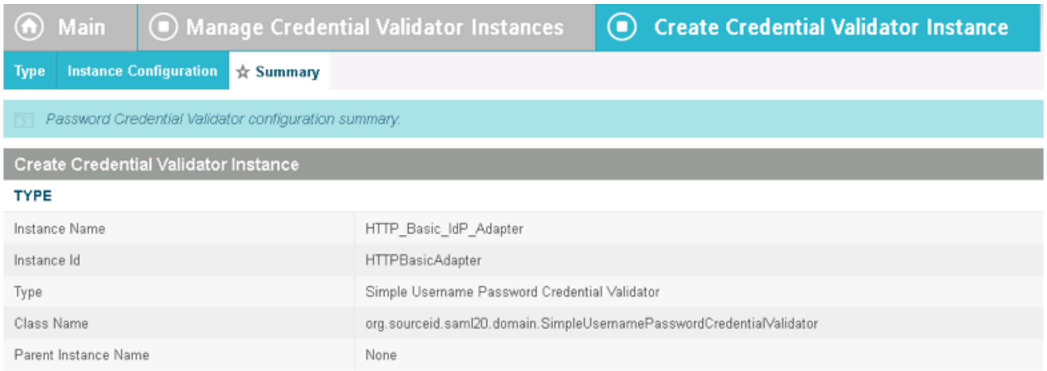

Main
Manage Credential Validator Instances
Create Credential Validator Instance
Type
Instance Configuration
☆ Summary

Password Credential Validator configuration summary.

Create Credential Validator Instance	
TYPE	
Instance Name	Form_IdP_Adapter
Instance Id	FormAdapter
Type	Simple Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.SimpleUsernamePasswordCredentialValidator
Parent Instance Name	None

Figure 17. Validator instance for Form Adapter

For HTTP_Basic_IdP_Adapter Instance:


Main
Manage Credential Validator Instances
Create Credential Validator Instance
Type
Instance Configuration
☆ Summary

Password Credential Validator configuration summary.

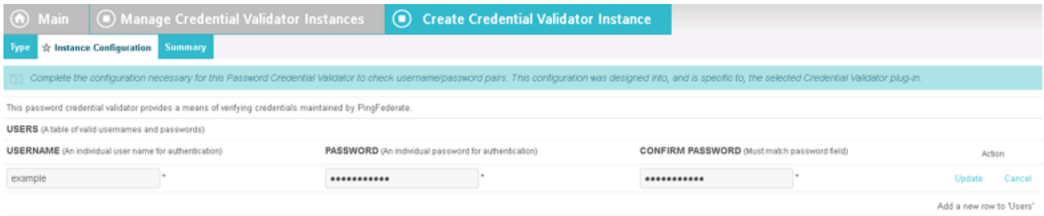
Create Credential Validator Instance

TYPE

Instance Name	HTTP_Basic_IdP_Adapter
Instance Id	HTTPBasicAdapter
Type	Simple Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.SimpleUsernamePasswordCredentialValidator
Parent Instance Name	None

Figure 18. PingFederate HTTP adapter

Once both credential validator instances have been created, navigate to the Instance Configuration and add a new row of users.


Main
Manage Credential Validator Instances
Create Credential Validator Instance
Type
☆ Instance Configuration
Summary

Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.

This password credential validator provides a means of verifying credentials maintained by PingFederate.

USERS (A table of valid usernames and passwords)

USERNAME (An individual user name for authentication)	**PASSWORD** (An individual password for authentication)	**CONFIRM PASSWORD** (Must match password field)	Action
example *	•••••••••••• *	•••••••••••• *	Update Cancel

Add a new row to 'Users'

Figure 19. User/password configuration

Deployment Topology Options

The Thunder Series AAM solution offers two options to deploy with IdP providers as follows:

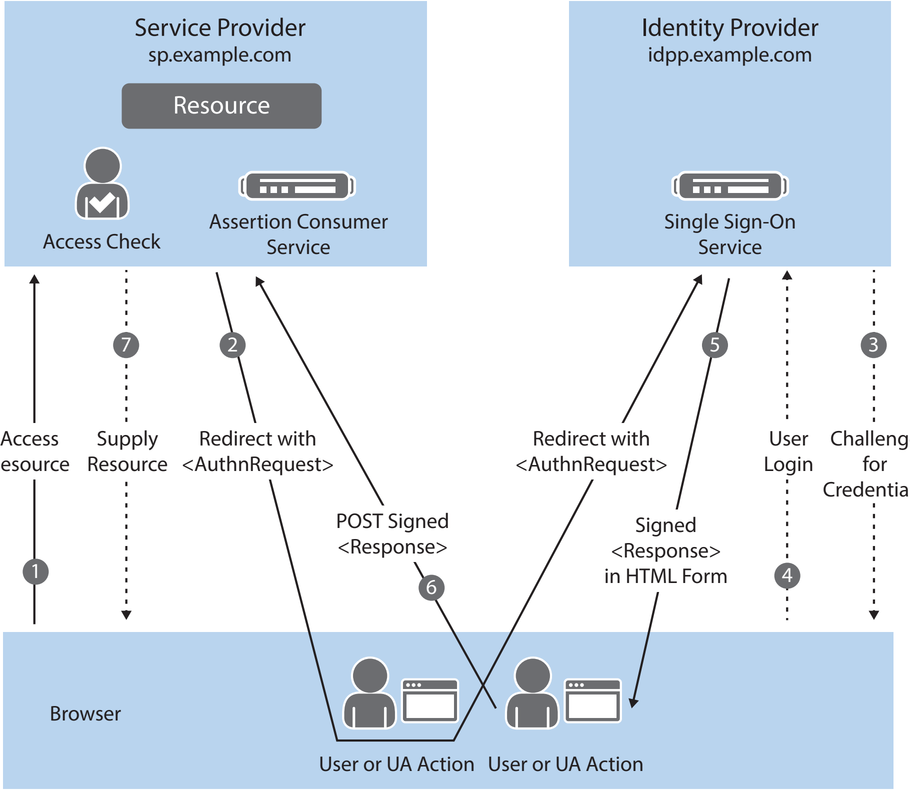


Figure 20. Frontend/service provider initiated

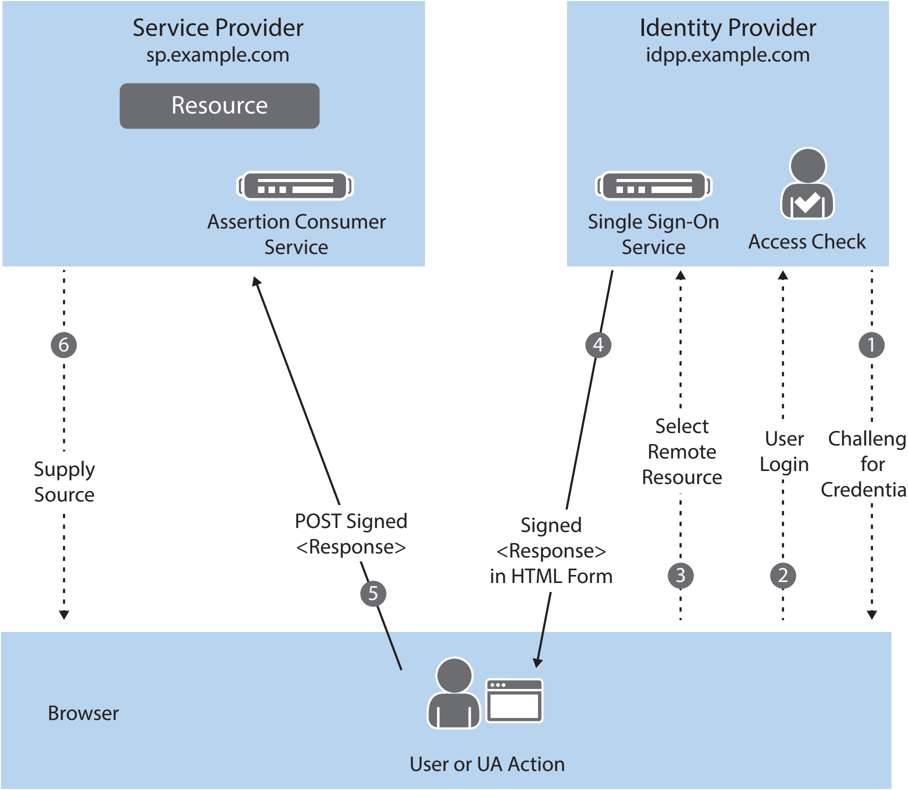


Figure 21. Backend/IdP initiated

Export Metadata

Once the service provider connection settings have been completed, you must export the metadata information. Within the main console page of PingFederate, navigate to the Service Provider Connections interface and click "Manage all SPs." Click "Export Metadata" and save.

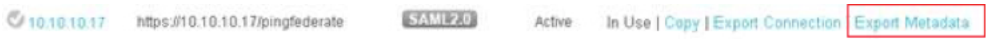
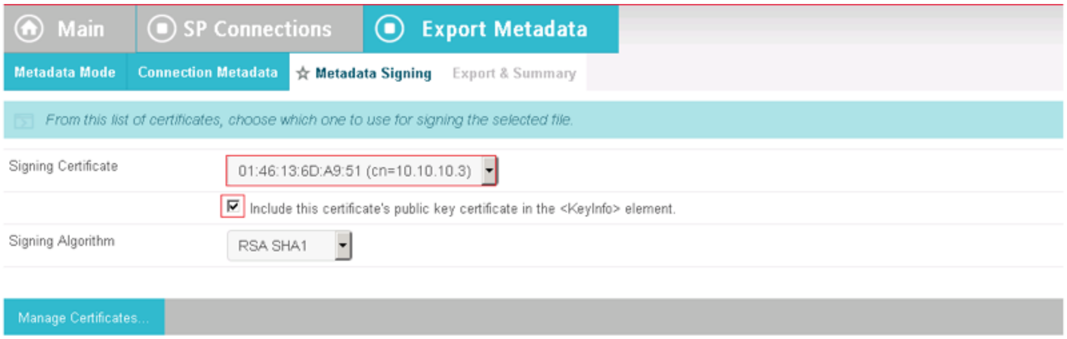

10.10.10.17
https://10.10.10.17/pingfederate
SAML2.0
Active
In Use | Copy | Export Connection
Export Metadata

Figure 22. Export Metadata



From this list of certificates, choose which one to use for signing the selected file.

Signing Certificate: 01:46:13:6D:A9:51 (cn=10.10.10.3)

☑ Include this certificate's public key certificate in the <KeyInfo> element.

Signing Algorithm: RSA SHA1

Figure 23. Metadata signing

On the Metadata Signing tab, select the Signing Certificate that matches with the PingFederate host address. Check to include the certificate's public key certificate in the element and select RSA SHA 1 option for Signing Algorithm. Click Next and export the metadata file to your local machine. Once the file has been saved, you must import the metadata file to the Thunder Series device by using this command:

```
vThunder#import auth-saml-idp pingfederate tftp://example.com/metadata
```

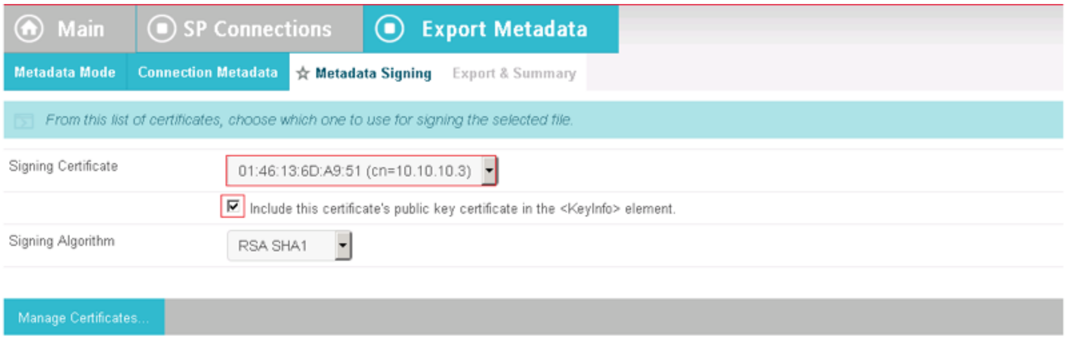
Thunder Series Configuration

This section of the guide explains how to configure the AAM SAML portion of the Thunder Series configuration. On the AAA Policy section of the GUI, navigate to AAM -->Policies and Templates.

The AAA Policy section of the GUI is the section where the site administrator configures the allow/deny rules of a client. Client policies can be configured based on domain and access list to control access within an application or site using these variables:

1. Index
2. Domain Name
3. Access List
4. Action
5. Authentication Template

AAA Policy



From this list of certificates, choose which one to use for signing the selected file.

Signing Certificate: 01:46:13:6D:A9:51 (cn=10.10.10.3)

☑ Include this certificate's public key certificate in the <KeyInfo> element.

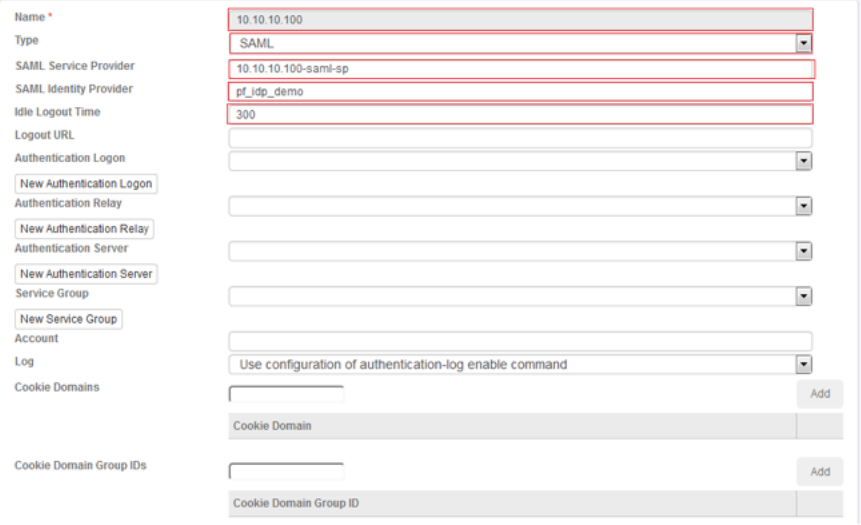
Signing Algorithm: RSA SHA1

Figure 24. ACOS AAA Policy

Authentication Template Configuration

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

1. Name
2. Type
3. SAML Service Provider
4. SAML Identity Provider
5. Idle Logout Time



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
Logout URL	
Authentication Logon	
Authentication Relay	
Authentication Server	
Service Group	
Account	
Log	Use configuration of authentication-log enable command
Cookie Domains	
Cookie Domain Group IDs	

Figure 25. Authentication Template

Configuration Samples

```
AAM Configuration Sample via HTTP VIP
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/pingfederate
  service-url http://10.10.10.100
aam authentication template 10.10.10.100
  type saml
  saml-sp 10.10.10.100-saml-sp
  saml-idp pingfederate
aam aaa-policy 10.10.10.100-policy
  aaa-rule 1
    authentication-template 10.10.10.100
aam aaa-policy 1010.10.10.100-policy
slb virtual-server VIP-HTTP-AAM 10.10.10.100 /24
  port 80 http
    name HTTP-AAM
    snat-on-vip
    source-nat auto
    service-group http-sg
    aaa-policy 10.10.10.100-policy
```

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-16142-EN-01
Nov 2014

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.

©2014 A10 Networks, Inc. All rights reserved. The A10 logo, A10 Lightning, A10 Networks, A10 Thunder, aCloud, ACOS, ACOS Policy Engine, ACOS Synergy, Affinity, aFleX, aFlow, aGalaxy, aVCS, AX, aXAPI, IDaccess, IDsentrie, IP-to-ID, SoftAX, SSL Insight, Thunder, Thunder TPS, UASG, VirtualN, and vThunder are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.