

SAML

Feature Description

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **5**

1.1 Document Purpose 5

1.2 Intended Audience 5

2 SAML Authentication Flow **6**

3 AD FS Settings **9**

3.1 Terminology Differences 9

3.2 Ensure the Services are Running 9

3.3 Service Settings 12

3.4 Endpoint Settings 15

3.5 Certificate Settings 16

3.6 Claim Description Settings 19

3.7 Trust Relationships Settings 19

3.7.1 Ensure Active Directory is Enabled 19

3.7.2 Add a Relying Party Trust 20

3.7.3 Add End Points 30

3.7.4 Import the Certificate 34

3.7.5 Configure the Identifiers 35

3.7.6 Claim Rules 36

3.8 Authentication Policies Setting 38

4 Configure SAML Authentication in the LoadMaster **41**

4.1 Limitations 41

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4.1.1 Certificate Signature Verification 41
4.1.2 Persistent Cookies 41
4.2 Configure the SSO Domain 41
4.3 Configure the Virtual Service 44
5 Appendix A: Logging 47
References 50
Last Updated Date 51

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

Security Assertion Markup Language (SAML) is a standards-defined protocol. The specification defines the syntax and semantics for assertions made about a subject. Subjects are typically end users of a system. SAML assertions and protocol messages are XML-encoded but rely on HTTP-based mechanisms for transport between entities.

SAML enables web-based Single Sign On (SSO). It also provides for centralized federated identity and authentication management. Microsoft Active Directory Federation Services (AD FS) is the SAML-based Identity Provider (IdP) which has been tested and which is referred to in this document. However, other IdPs may also work. AD FS is a standards-based service running on a Microsoft box that allows the secure sharing of identity information between trusted parties. In general terms, this is known as a federation. AD FS supports SAML, essentially playing the role of a SAML IdP. The LoadMaster supports SAML, playing the role of a SAML service provider. The service provider provides secure, gated access to a resource.

1.1 Document Purpose

The purpose of this document is to provide information and instructions on how to configure SAML authentication with the Kemp LoadMaster.

1.2 Intended Audience

This document is intended to be used by anyone who is interested in finding out further information about using SAML authentication with the LoadMaster.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 SAML Authentication Flow

When using other Edge Security Pack (ESP) authentication protocols in the LoadMaster, end users are presented with the standard Kemp login form. This is not displayed by LoadMaster when using SAML because a login form is not provided by Kemp. The LoadMaster instead redirects the client to a login form which is located at the IdP.

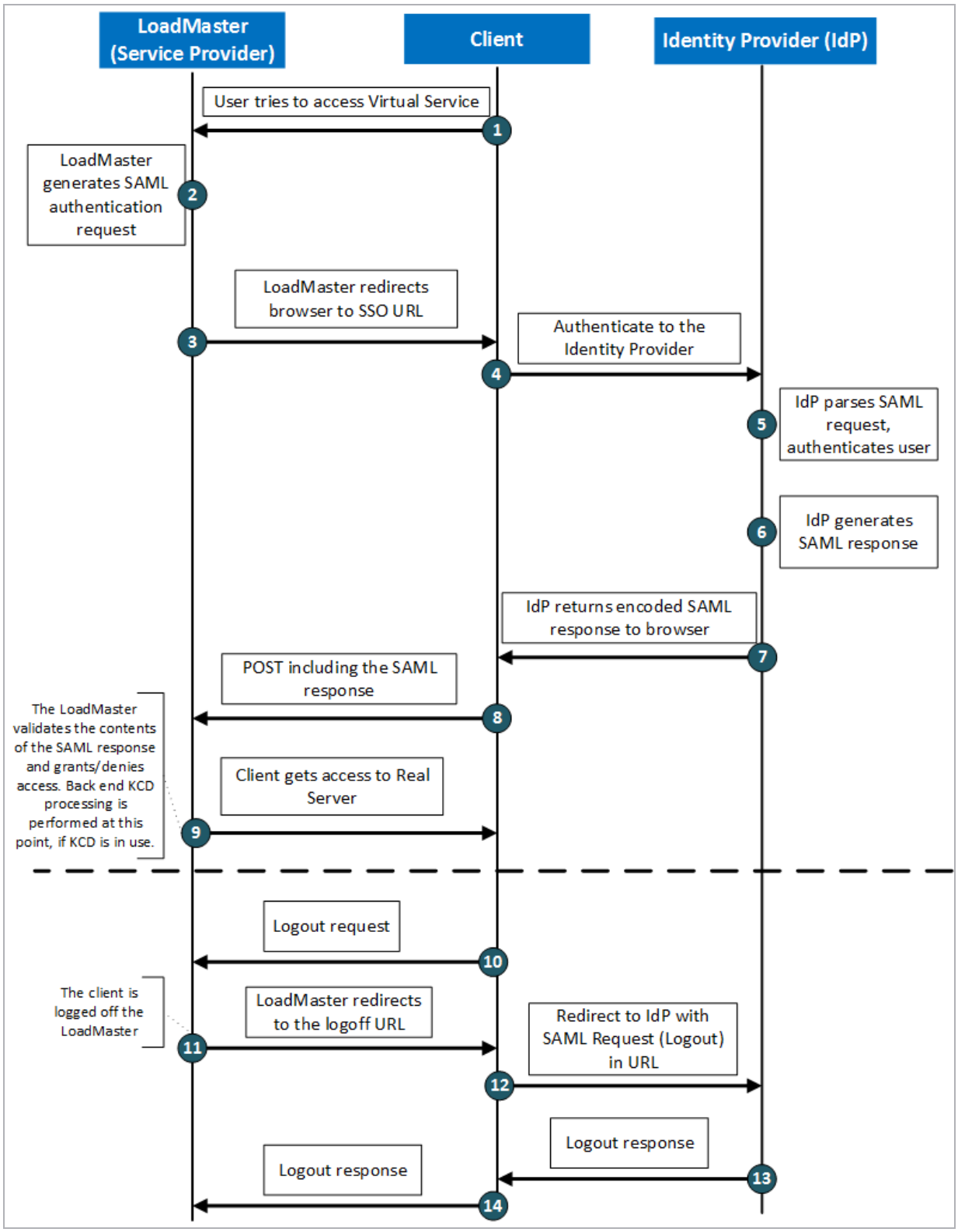
The LoadMaster implementation relies on protocol bindings for HTTP redirect which is used for redirections to a claims provider, alternatively known as an IdP. The LoadMaster also has a dependency on HTTP POST – the LoadMaster expects HTTP POST messages for IdP responses, where applicable.

The domain is fundamentally different to other types of SSO domain that are configurable on the LoadMaster because the LoadMaster does not interact directly with the authentication server (AD FS in this scenario). The LoadMaster redirects and informs the client to interact directly with AD FS so that the client can input the credentials that are required for authentication.

The URL provided in the original request from L7 is preserved. This URL is given precedence over the destination URL from the SAML response. For example, if a user logs in to a URL such as **https://sharepoint.kemptest.com/personal/admin**, they are directed to **https://sharepoint.kemptest.com/personal/admin** and not **https://sharepoint.kemptest.com**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 SAML Authentication Flow



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Here is a description of the flow:

1. The client attempts to connect to the Virtual Service on the LoadMaster.

2. The LoadMaster identifies that there is no cookie for the session. As this is a SAML-based domain – the authentication request is built.

3. The client is informed to redirect to the IdP.

4. The client sees the login form from the IdP federation server and enters their credentials. This interaction is between the client and the IdP. The credentials are passed between the client and the Federation Server.

5. The IdP parses the SAML request and authenticates the user.

6. The IdP generates the SAML response.

7. The IdP returns the encoded SAML response to the browser in the URL.

8. A POST request, including the SAML response is passed back to the Service Provider (the LoadMaster).

9. The LoadMaster validates the contents of the SAML response and grants/denies access. Back-end KCD processing is performed at this point, if KCD is in use.

Logging out results in another series of events:

10. The user signs out.

11. The client gets logged out of the LoadMaster and redirected to the IdP again to allow the user to log back in, if necessary.

12. A logout response is passed from the IdP to the client.

13. A logout response is passed from the client to the LoadMaster.

> This flow is known as SP-initiated authentication; IdP-initiated authentication is not supported.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 AD FS Settings

Some information is provided below on some of the key AD FS settings. The AD FS settings can be configured using the AD FS management console which is available in the Server Manager by going to **Tools > AD FS Management**.

3.1 Terminology Differences

There is a difference in terminology between AD FS terms and SAML terms. AD FS supports SAML and implements SAML but the terminology associated with AD FS varies in comparison to the terminology that is used in the context of SAML.

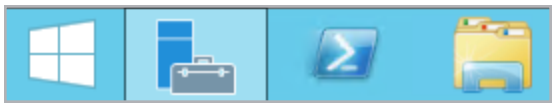
Some examples of these terminology differences are provided in the table below.

AD FS Name	SAML Name	Concept
Security Token	Assertion	A package of security information, describing a user, created and consumed during a federated access request.
Claims Provider	Identity Provider (IdP)	Partner in a federation that creates security tokens for users.
Relying Party	Service Provider (SP)	Partner in a federation that consumes security tokens for providing access to applications.
Claims	Assertion attributes	Data about users that is sent inside security tokens.

3.2 Ensure the Services are Running

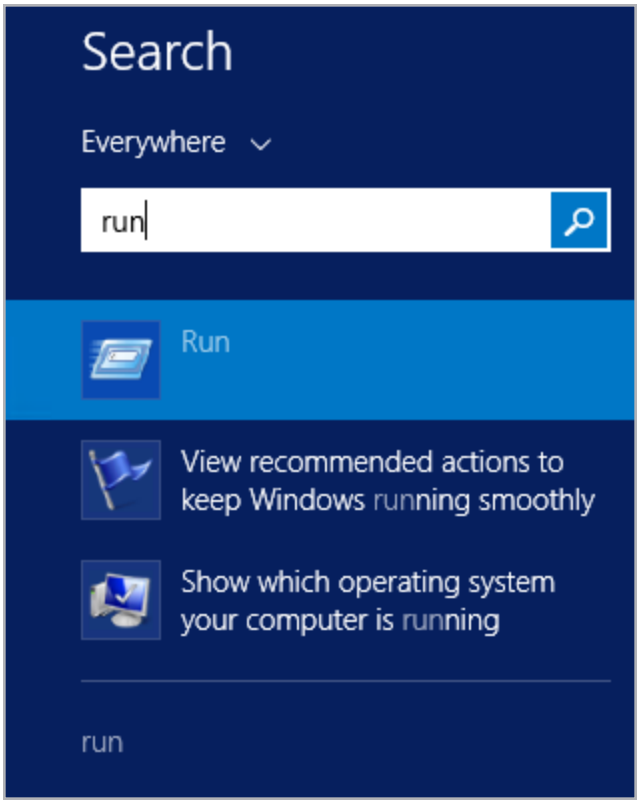
Before making changes to the AD FS settings, ensure the Active Directory Federation Services and Device Registration Service are running.

To do this, follow the steps below:

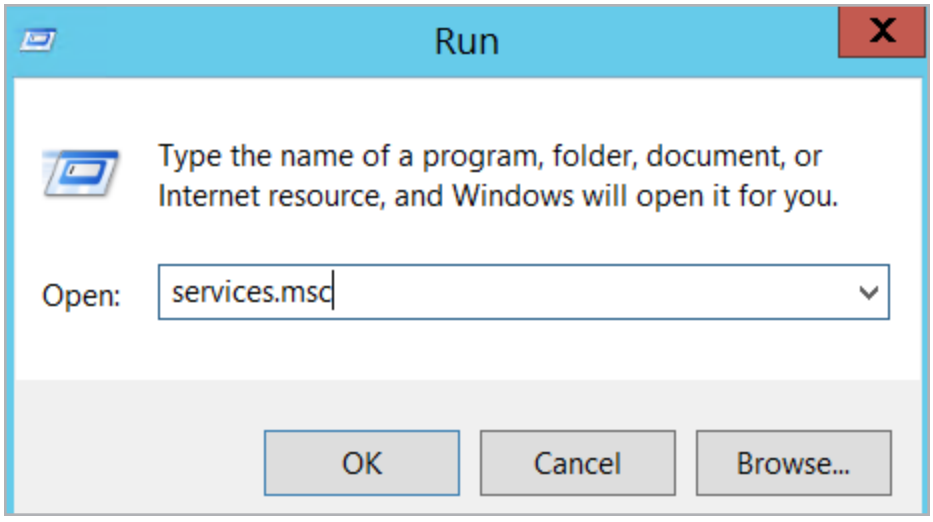


1. Click the **Start** menu in the bottom-left corner of the screen.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

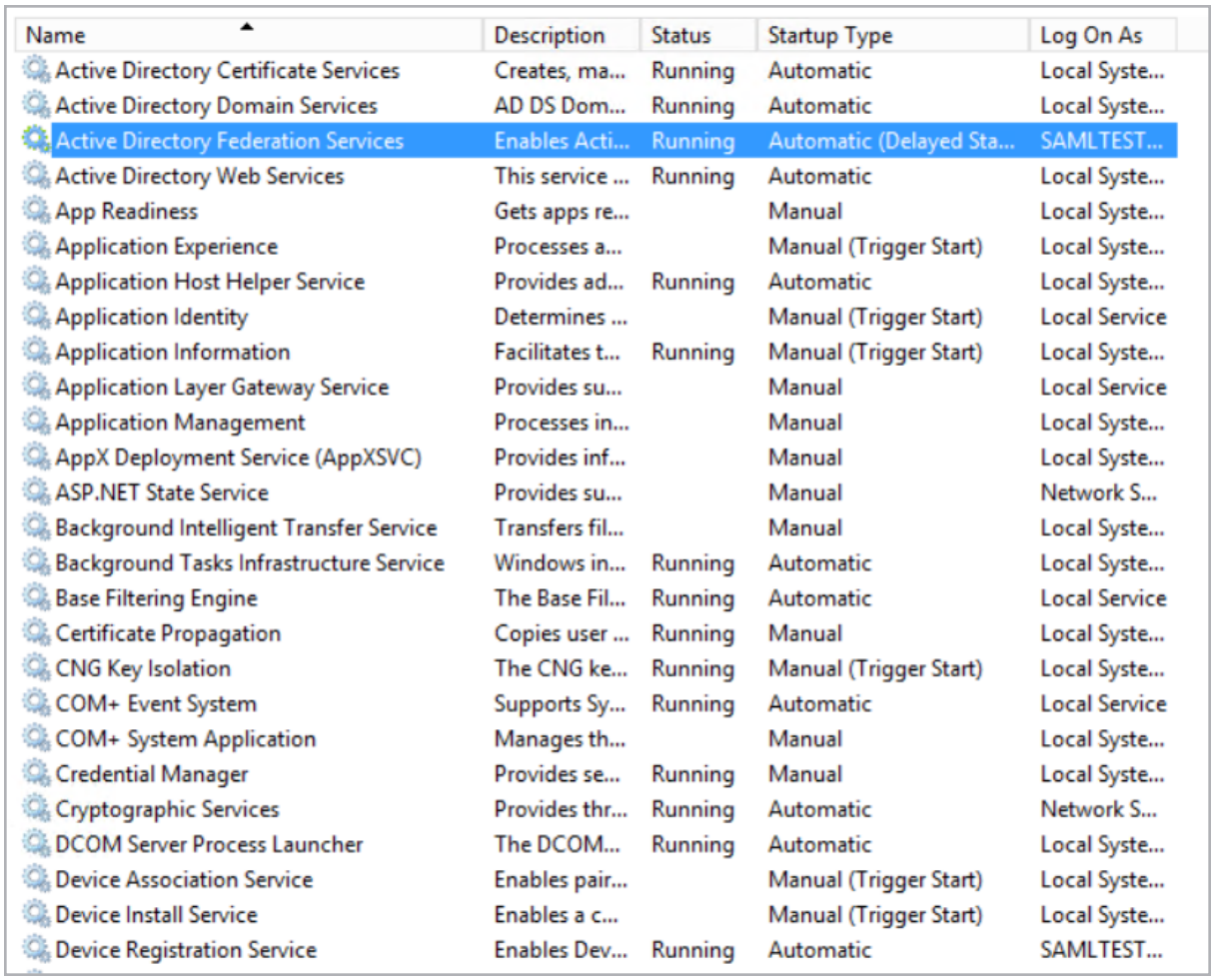


2. Type **run** and click the **Run** option.



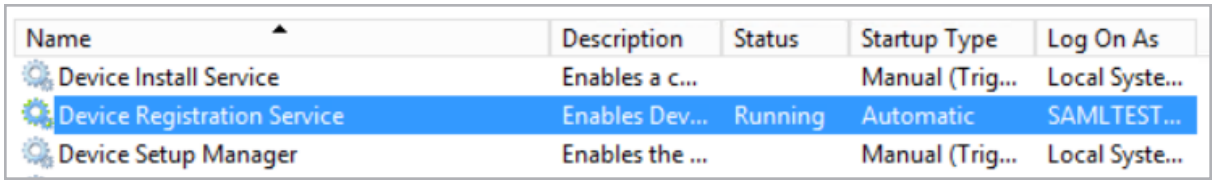
3. Enter **services.msc** and click **OK**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



Name	Description	Status	Startup Type	Log On As
Active Directory Certificate Services	Creates, ma...	Running	Automatic	Local Syste...
Active Directory Domain Services	AD DS Dom...	Running	Automatic	Local Syste...
Active Directory Federation Services	Enables Acti...	Running	Automatic (Delayed Sta...	SAMLTEST...
Active Directory Web Services	This service ...	Running	Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...		Manual (Trigger Start)	Local Syste...
Application Host Helper Service	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trigger Start)	Local Service
Application Information	Facilitates t...	Running	Manual (Trigger Start)	Local Syste...
Application Layer Gateway Service	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (AppXSVC)	Provides inf...		Manual	Local Syste...
ASP.NET State Service	Provides su...		Manual	Network S...
Background Intelligent Transfer Service	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastructure Service	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trigger Start)	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Credential Manager	Provides se...	Running	Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
DCOM Server Process Launcher	The DCOM...	Running	Automatic	Local Syste...
Device Association Service	Enables pair...		Manual (Trigger Start)	Local Syste...
Device Install Service	Enables a c...		Manual (Trigger Start)	Local Syste...
Device Registration Service	Enables Dev...	Running	Automatic	SAMLTEST...

4. Ensure the Active Directory Federation Services is running. If it is not, right-click it and click **Start**.

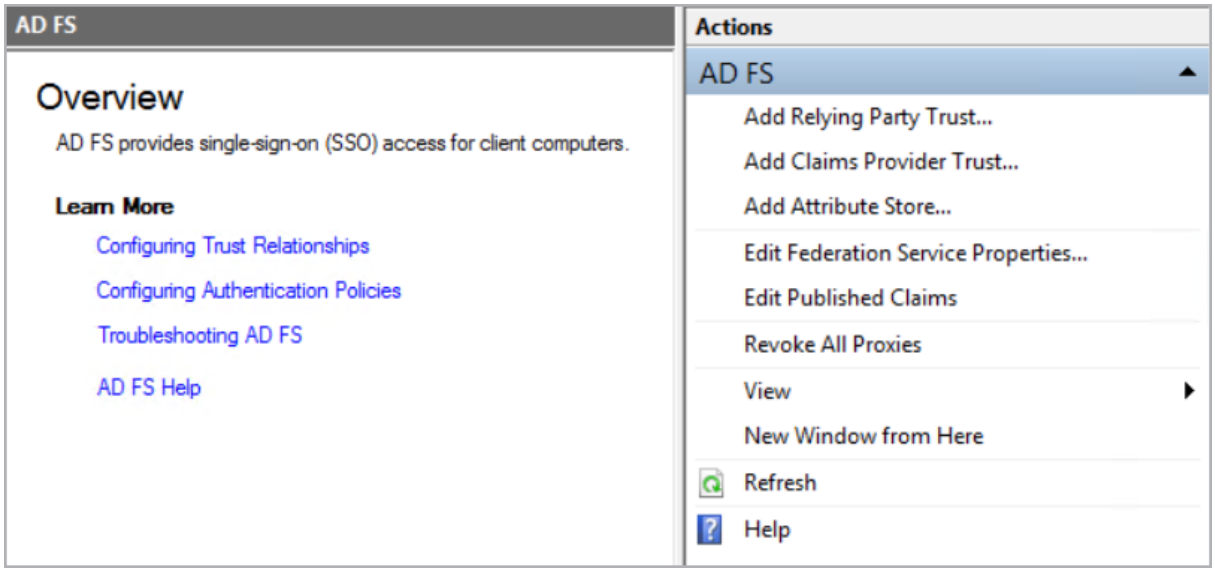


Name	Description	Status	Startup Type	Log On As
Device Install Service	Enables a c...		Manual (Trig...	Local Syste...
Device Registration Service	Enables Dev...	Running	Automatic	SAMLTEST...
Device Setup Manager	Enables the ...		Manual (Trig...	Local Syste...

5. Ensure the Device Registration Service is running. If it is not, right-click them and click **Start**.

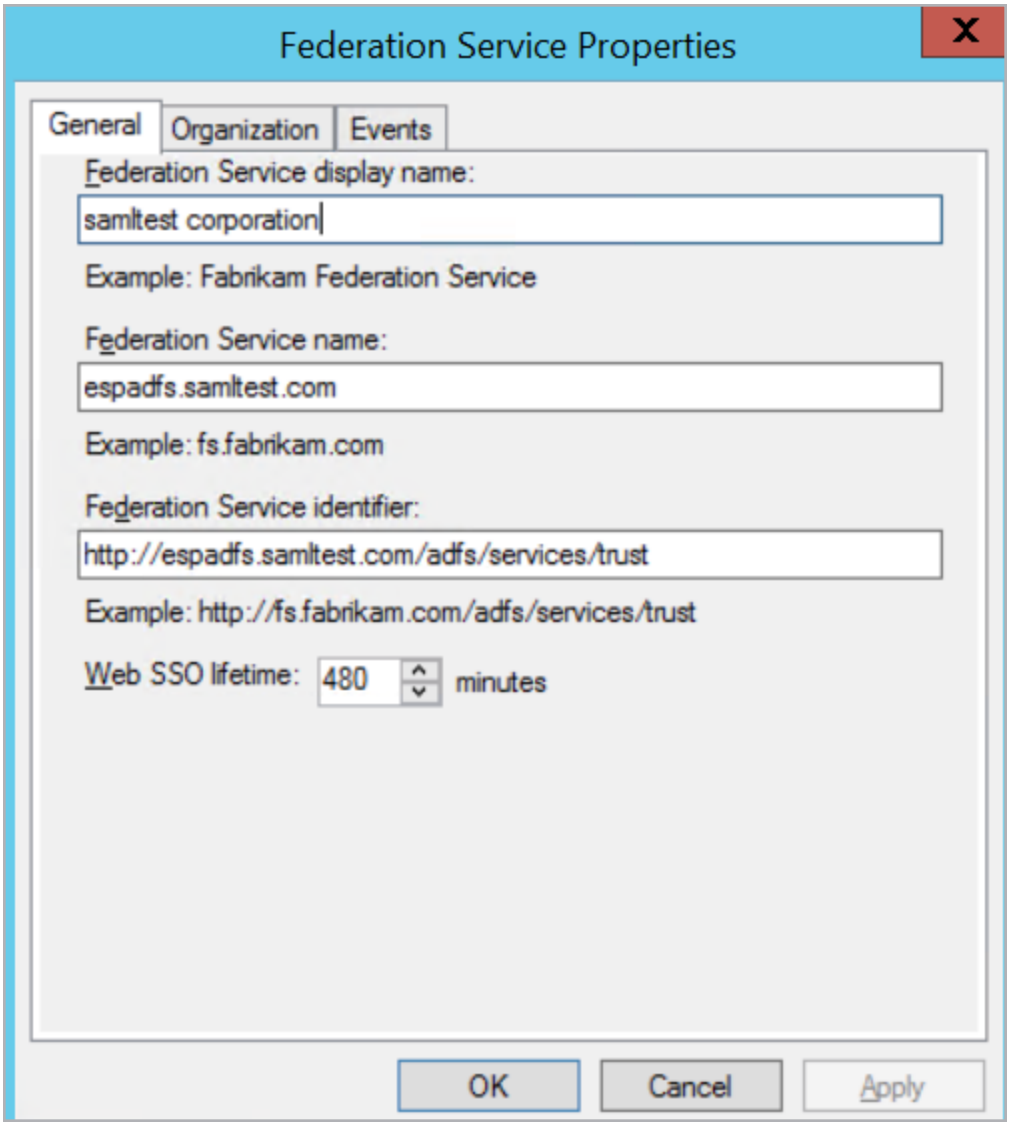
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.3 Service Settings

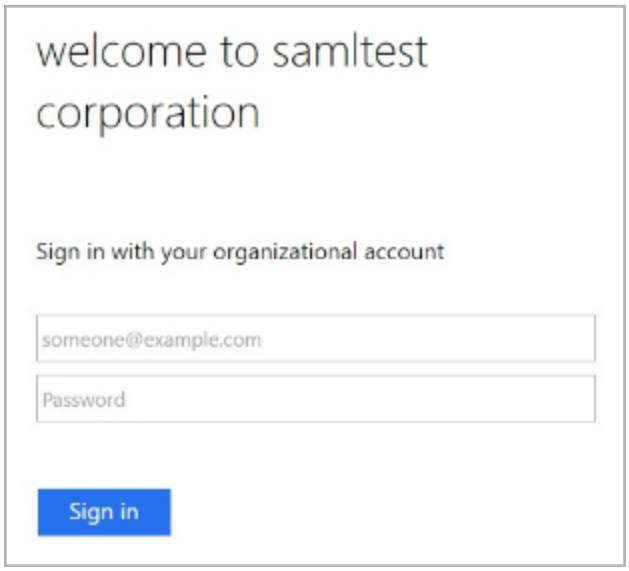


To access the Federation Service Properties, click the **AD FS folder** and click **Edit Federation Service Properties** on the right.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

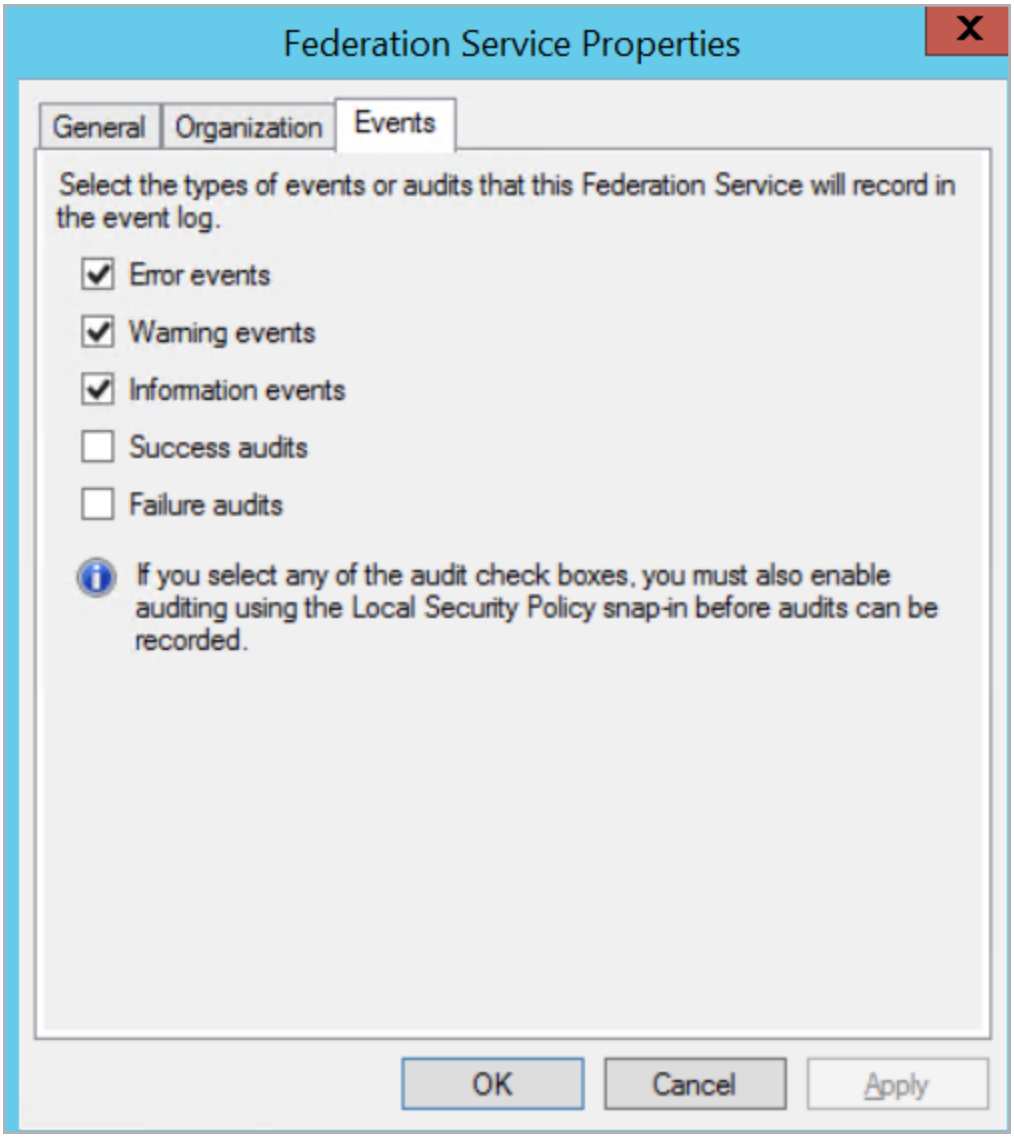


The Federation Service display name is the corporation name. This is shown on the log on screen when the client is redirected to the form-based authentication on the IdP. In the example screenshot above, the Federation Service display name is set to samltest corporation.

The Federation Service name is the qualified server name (Fully Qualified Domain Name (FQDN)) for this federation service (AD FS).

The Federation Service identifier is the IdP entity ID, such as http://<FQDN>/adfs. This must match the IdP entity ID in the context of SAML.

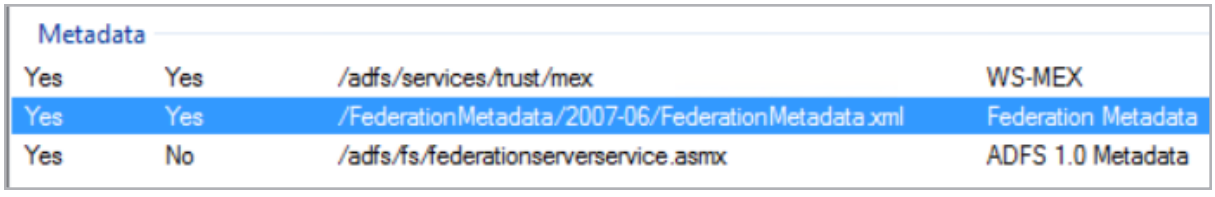
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



In the Events tab, the first three options should be selected.

3.4 Endpoint Settings

The Services > Endpoints folder contains a list of the endpoints that are served by AD FS.

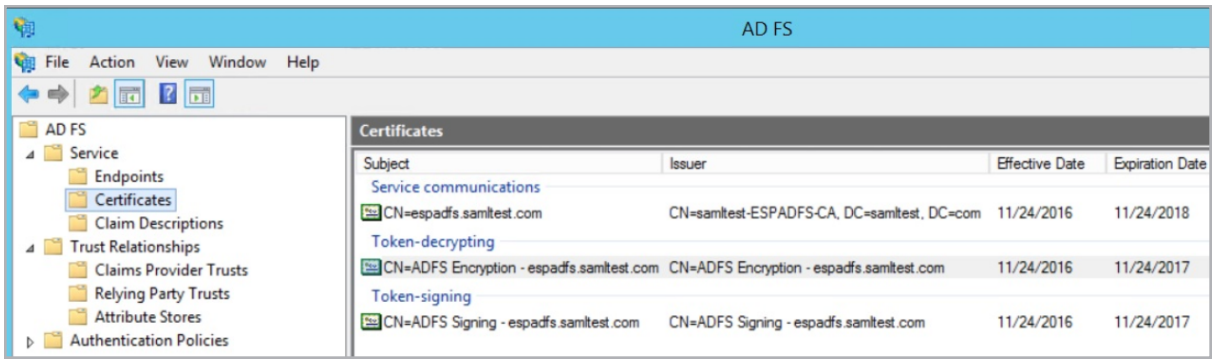


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The Metadata section contains a path to the FederationMetadata.xml file which can be imported into the LoadMaster when configuring the SAML domain. This path will form part of a full URL which includes the federation service server. Go to this URL (for example, https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml) in a web browser to download the metadata file which can then be imported using the IdP Metadata File field in the LoadMaster. Importing this file automatically populates the IdP Entity ID, IdP SSO URL and IdP Logoff URL fields with the relevant data.

3.5 Certificate Settings

All communications between the service provider and the IdP (AD FS in this case) must be secure. The certificate infrastructure must be in place on AD FS. Kemp assumes that this is in place in the case of production environments. If setting up AD FS for the first time, please ensure the correct certificate infrastructure is in place.

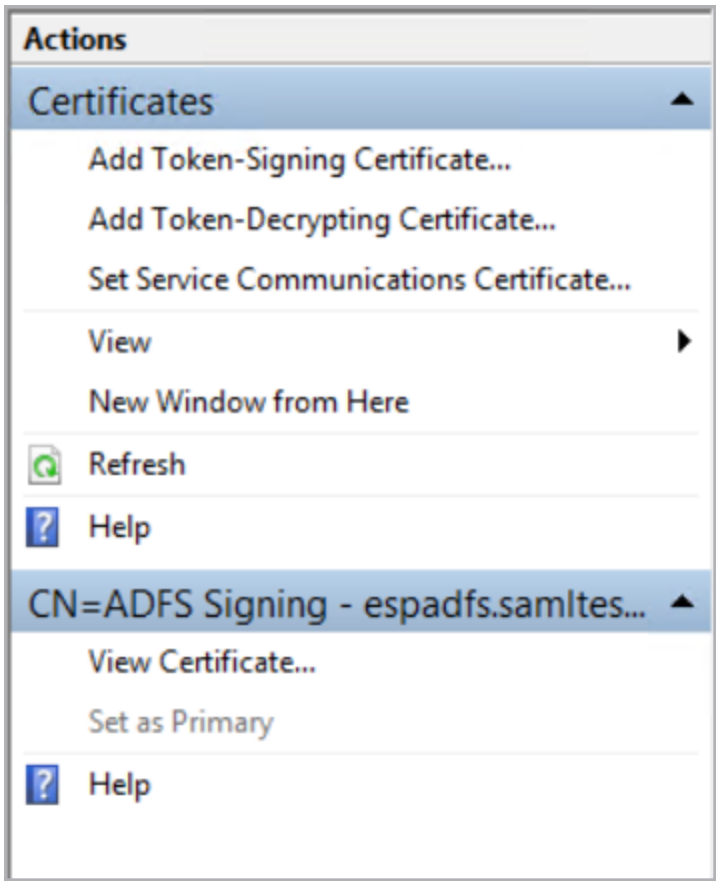


In the Certificates folder, there are certificates for service communication, token decrypting and token signing. The token signing certificate is important. When referring to tokens in AD FS, they generally map to assertions in the context of SAML. The token signing certificate is used for signing any response data from the AD FS. The LoadMaster requires this certificate to verify the signature on the service provider side (that is, on the LoadMaster side).

Export the token signing certificate from AD FS by following the steps below:

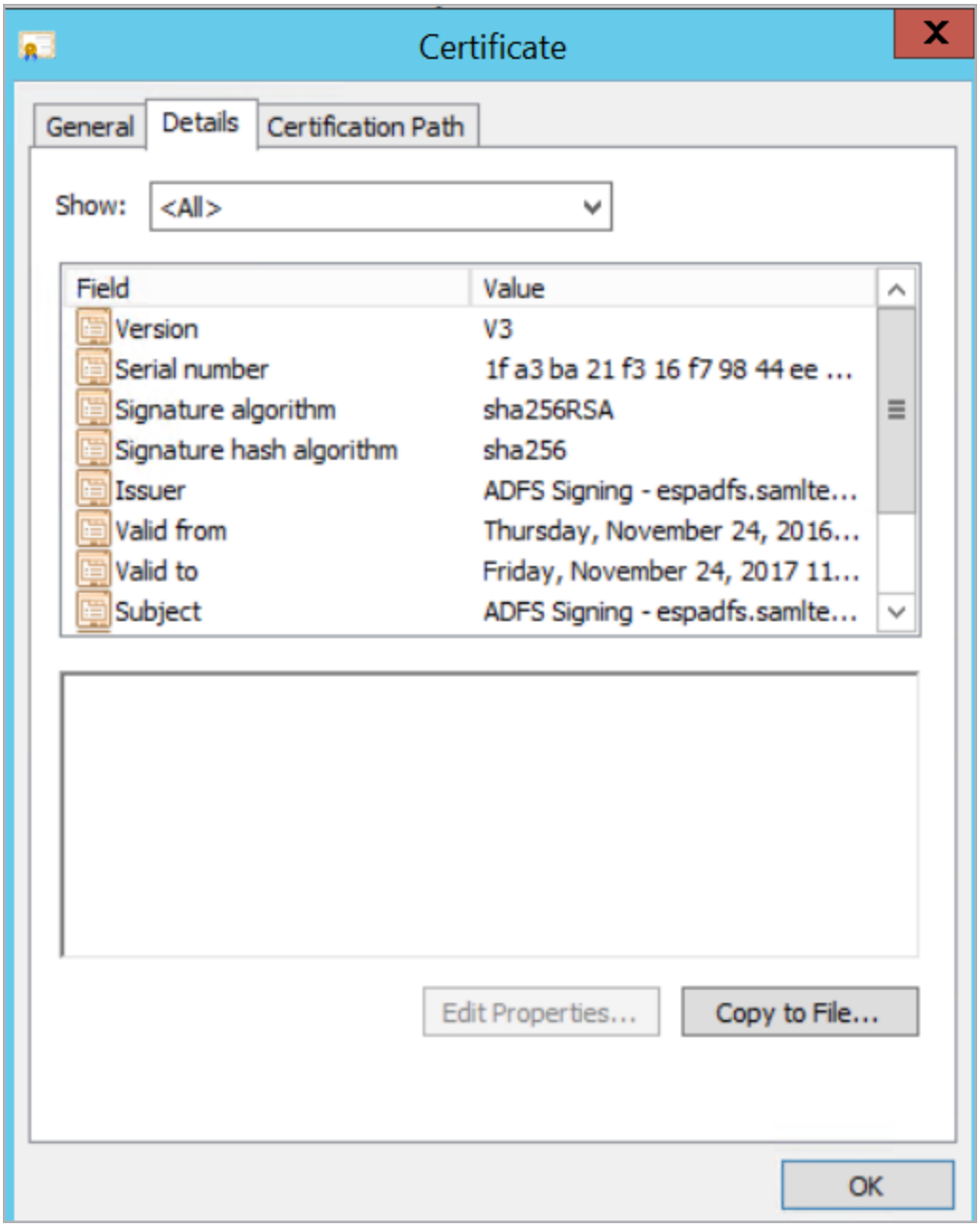
1. Go to **Services > Certificates** in AD FS.
2. Select the **Token-signing** certificate.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



3. Click **View Certificate**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



4. Click **Copy to File**.
5. Follow the steps in the certificate export wizard.
6. Provide a filename for the certificate.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

You must convert the certificate to a .pem format before importing it to the LoadMaster. There are many certificate converters available online. Alternatively, you can use an openssl command to perform the conversion.

Import the .pem certificate into the LoadMaster by following the steps below in the LoadMaster Web User Interface (WUI):

7. In the main menu, go to **Certificates & Security > Intermediate Certs**.
8. Click **Choose File**.
9. Browse to and select the certificate file.
10. Enter a Certificate Name and click **Add Certificate**.

This token signing certificate is now available to select in the IdP Certificate drop-down list in the SAML SSO domain in the LoadMaster.

3.6 Claim Description Settings

The Claim Descriptions folder contains a list of all the claims that can be asked and provided for. Usually this is backed up by Active Directory. There is a mapping between LDAP attributes and the claims that can be provided by AD FS.

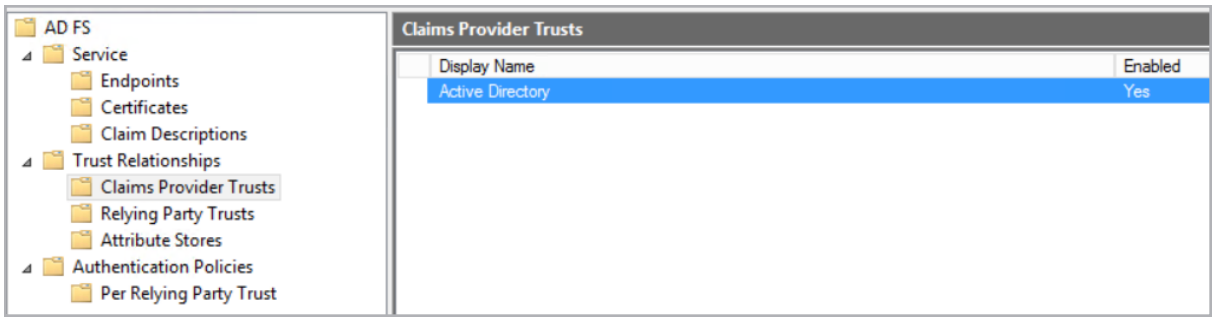
3.7 Trust Relationships Settings

The trust relationship is about establishing trust between an IdP and a service provider. In AD FS terminology – the relying party is the service provider (the LoadMaster).

Identifiers are configured here in AD FS which are used when building request messages from the service provider.

3.7.1 Ensure Active Directory is Enabled

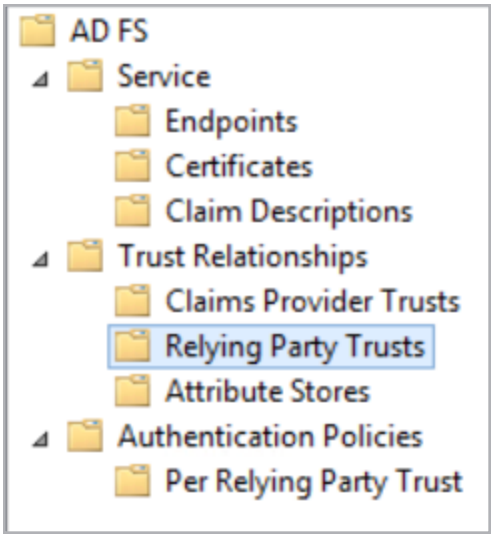
To ensure Active Directory is enabled, click the **Claims Provider Trusts** folder.



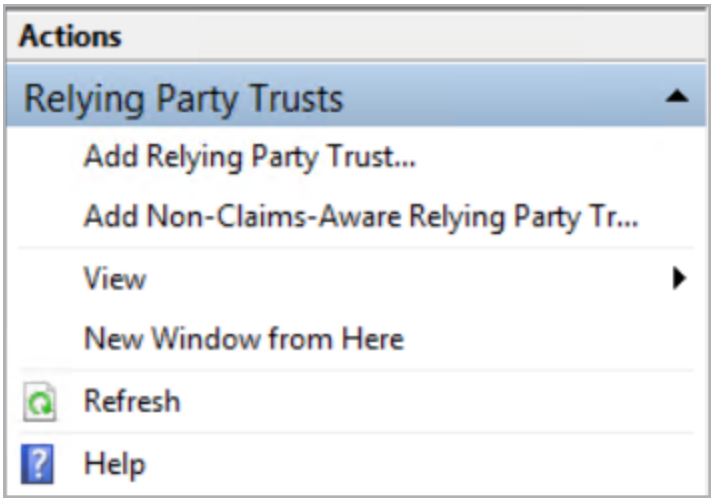
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3.7.2 Add a Relying Party Trust

To add a Relying Party Trust, follow the steps below:

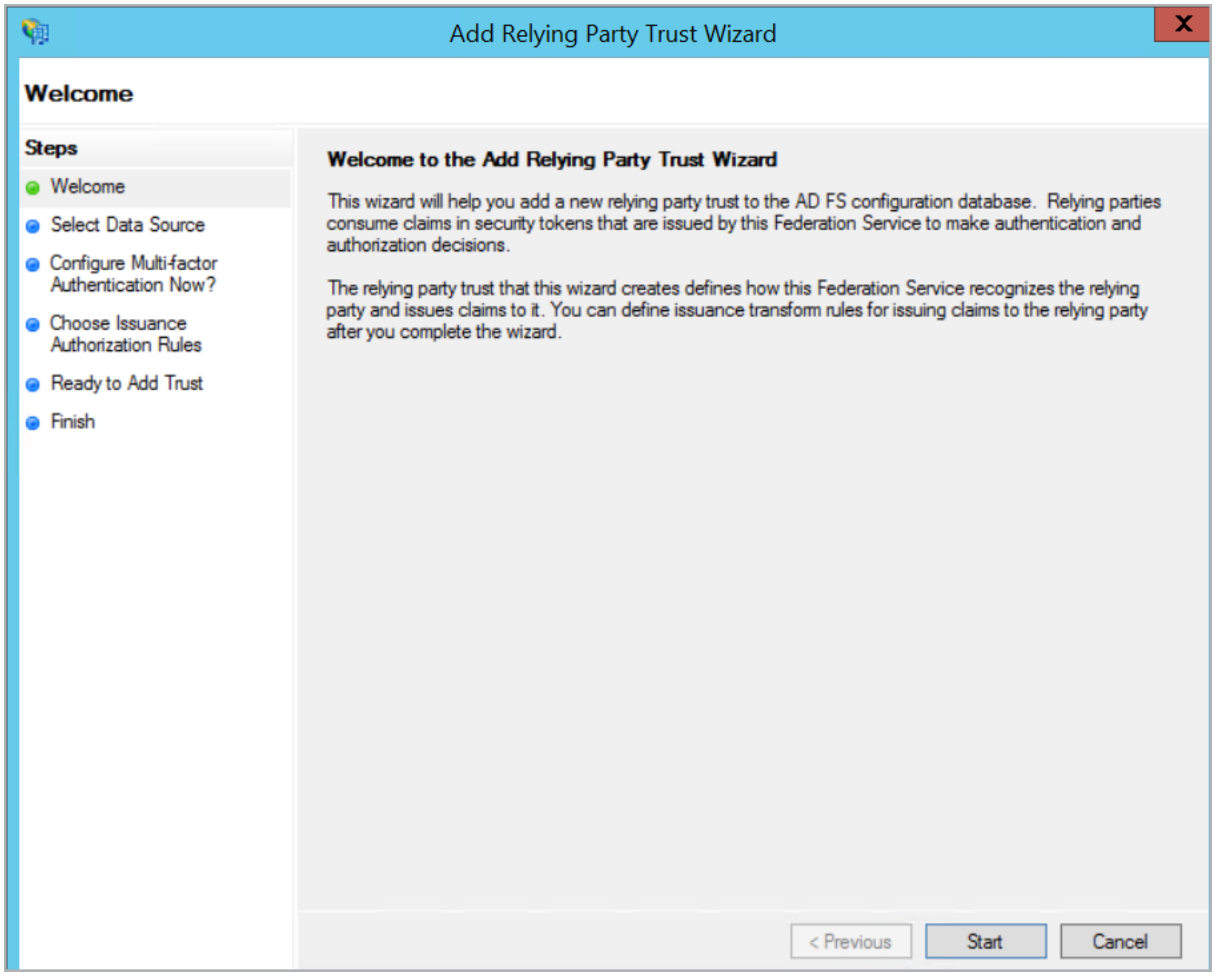


1. Click the **Relying Party Trusts folder**.



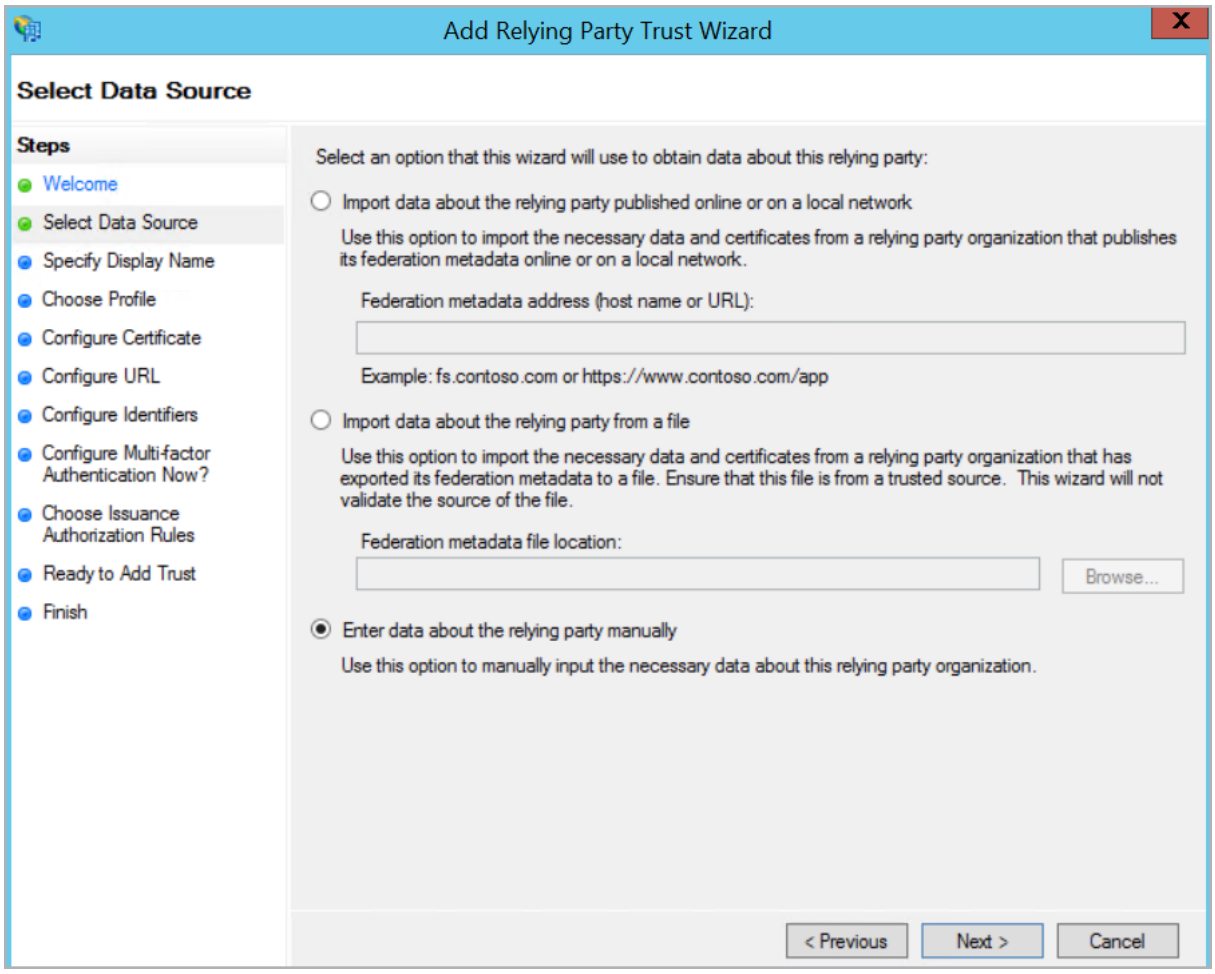
2. Click **Add Relying Party Trust**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



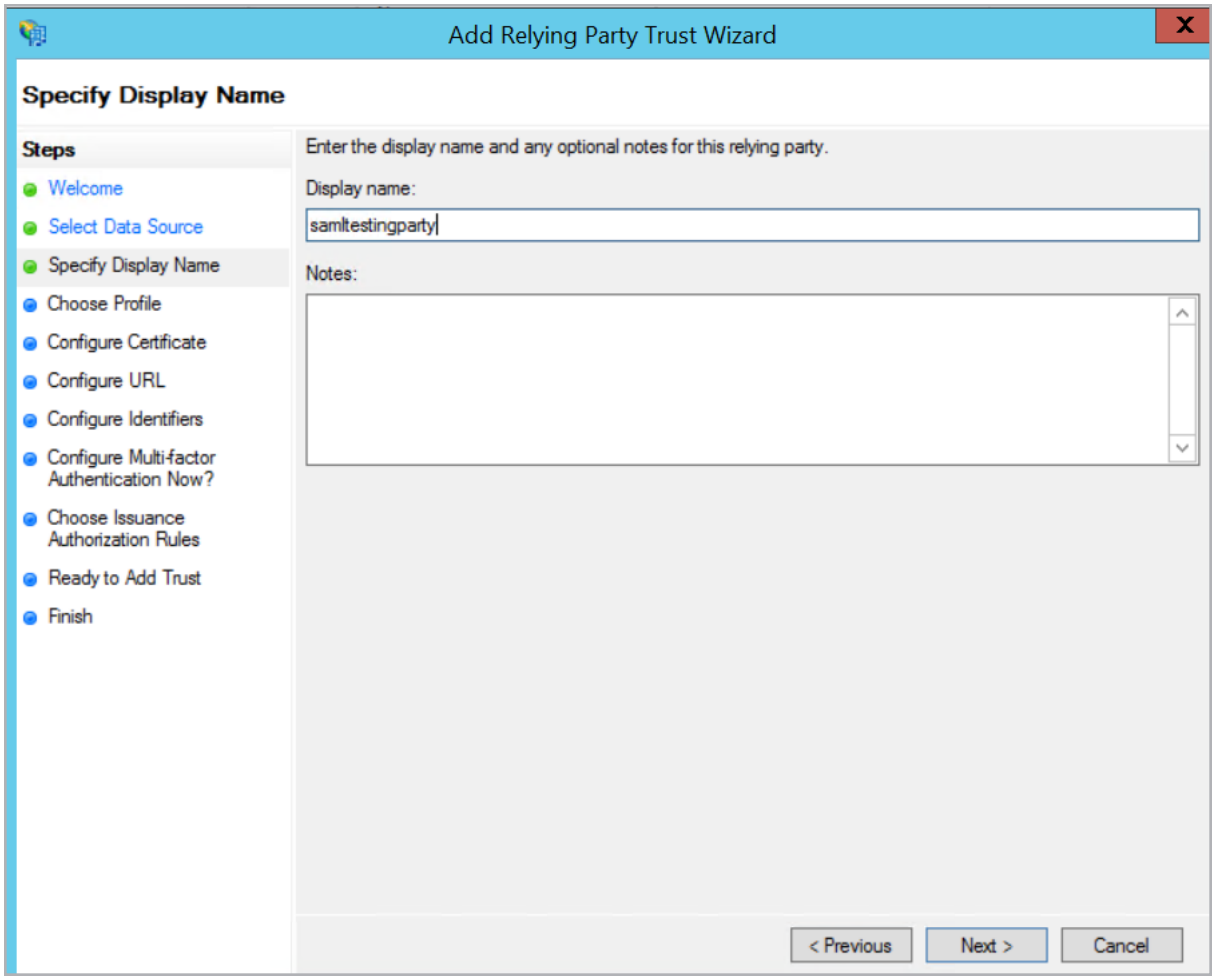
3. Click **Start**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



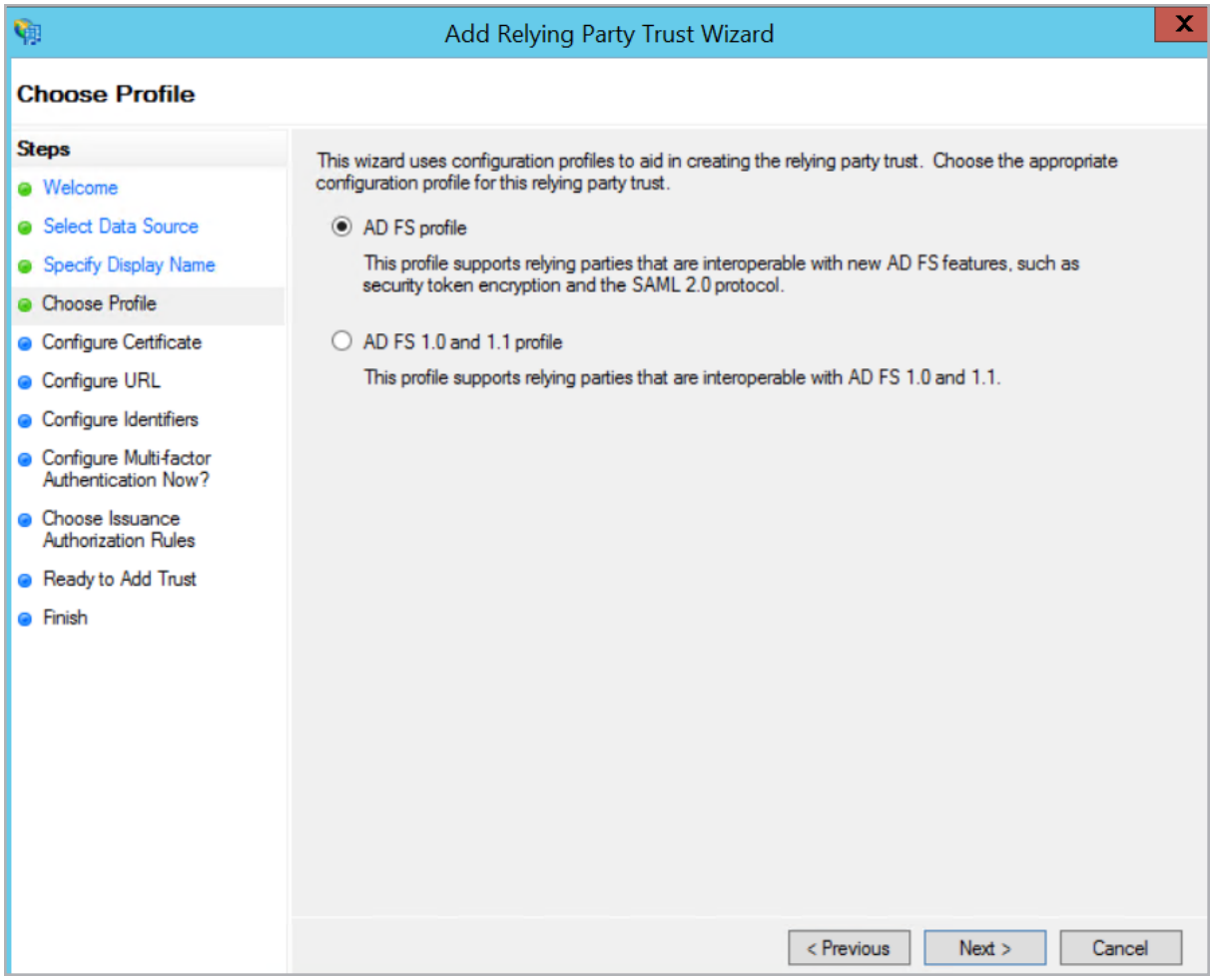
4. Select **Enter data about the relying party manually** and click **Next**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



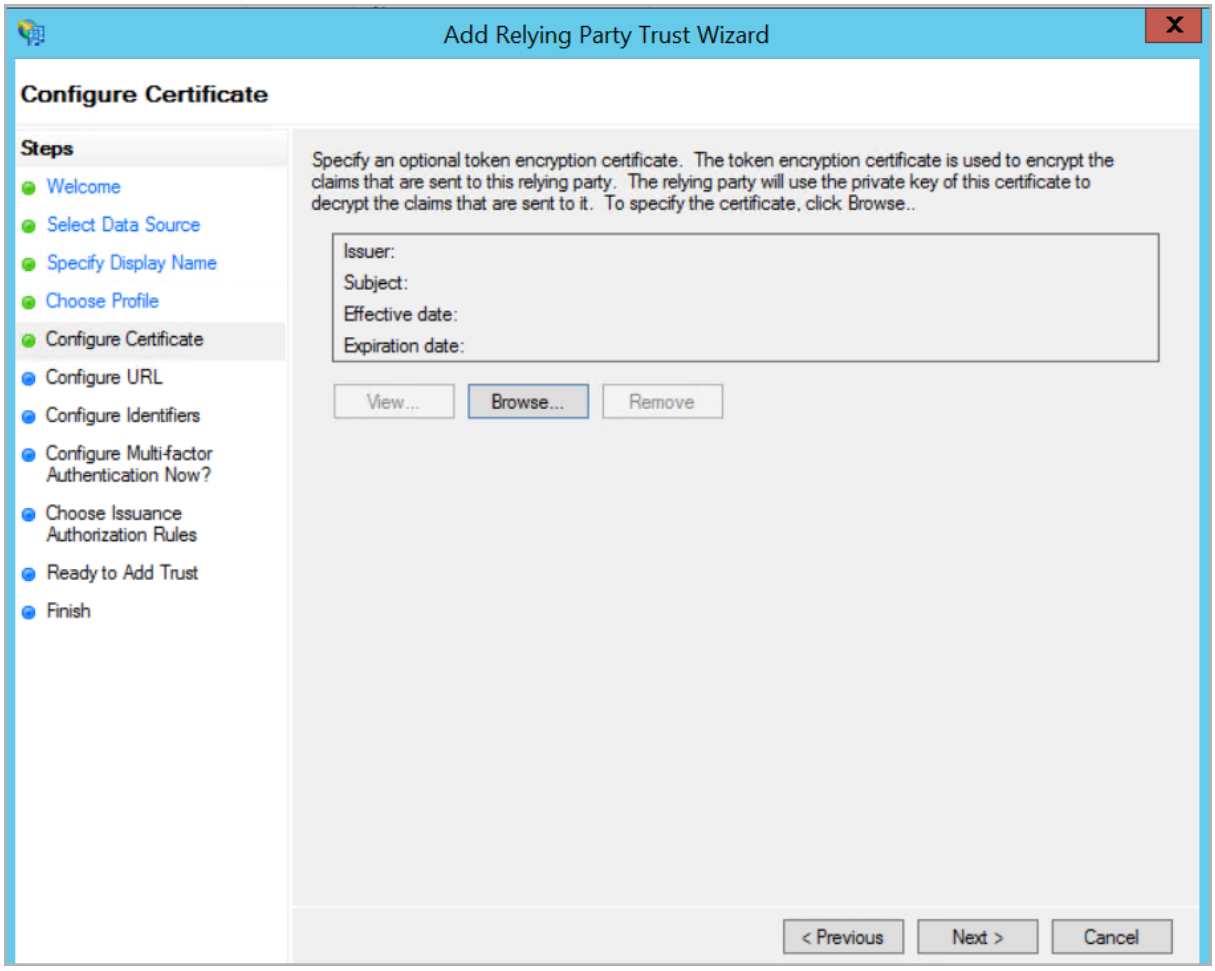
5. Enter a Display name for the Relying Party Trust and click **Next**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



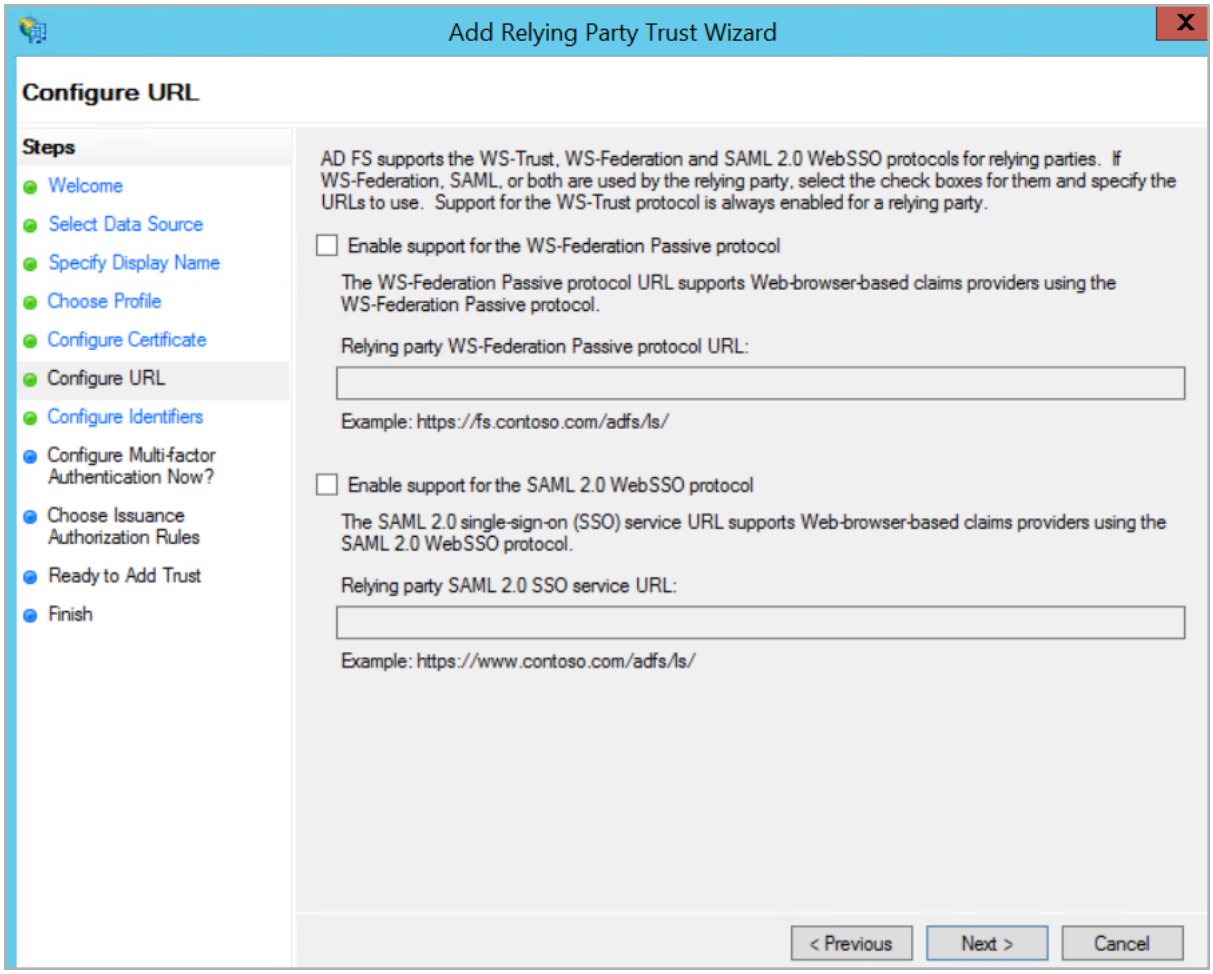
6. Select the **AD FS profile** option (this supports SAML 2.0) and click **Next**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

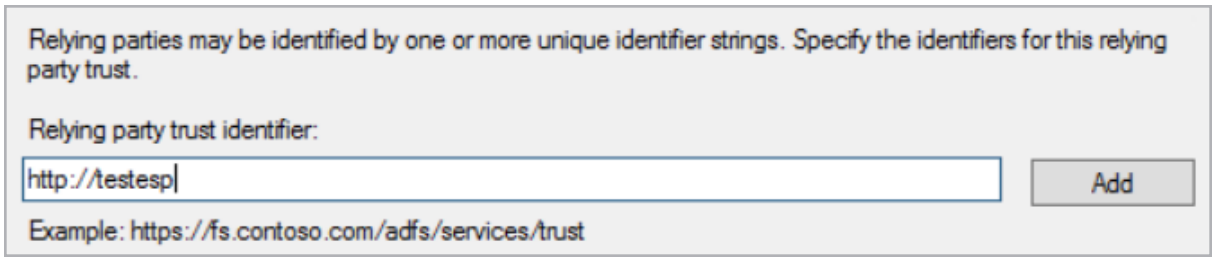


7. Click **Next** and do not add a token encryption certificate. Encryption is not supported.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

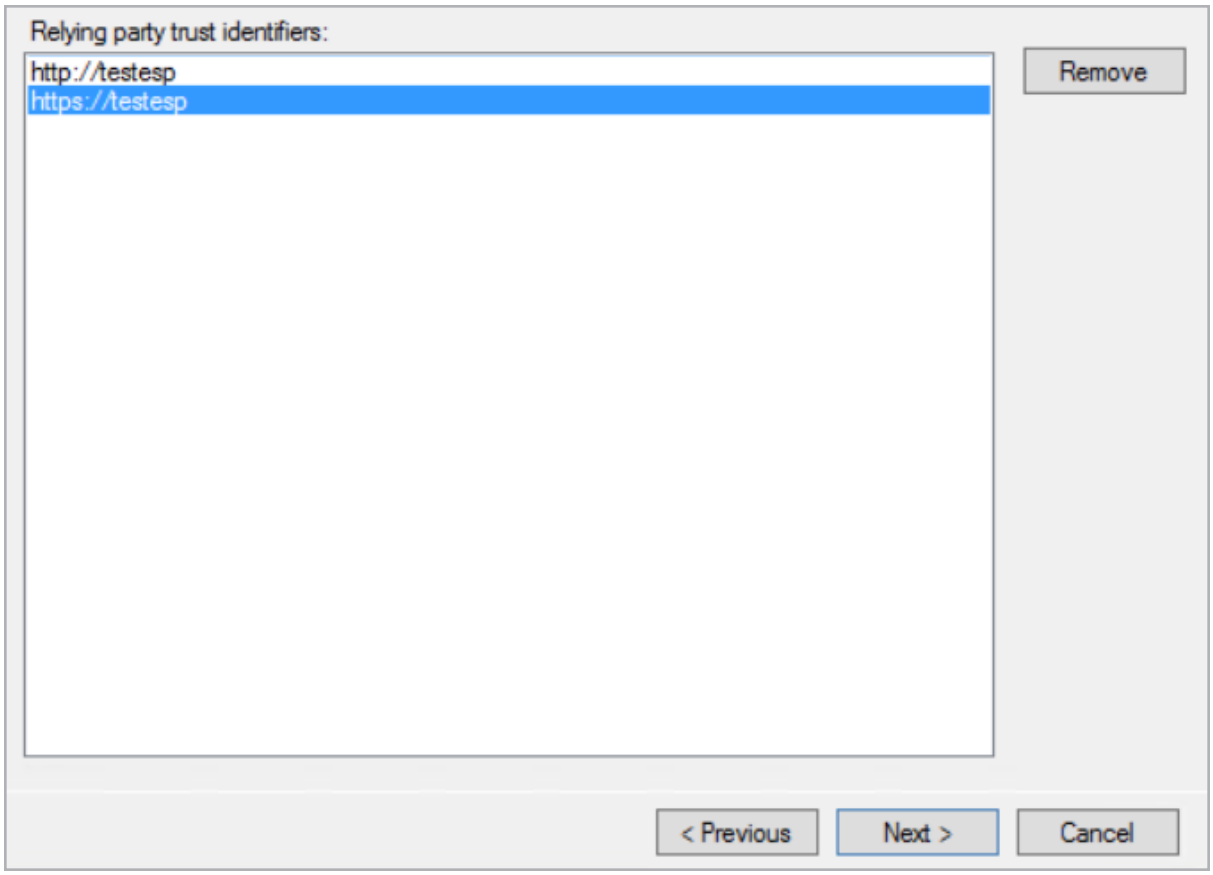


8. Do not select either option on the Configure URL screen and click **Next**.



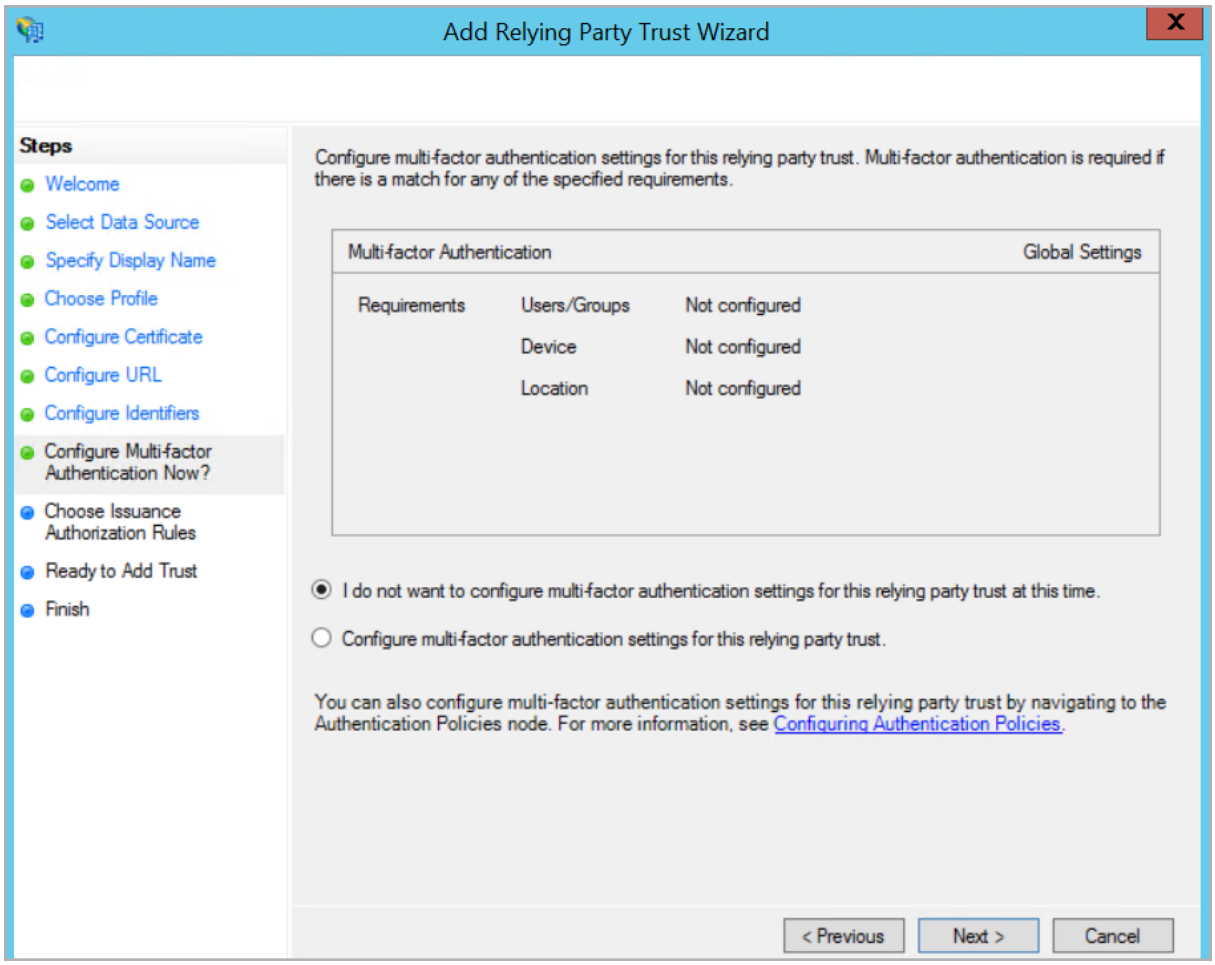
9. Enter the Relying party trust identifier in the form of a URL and click **Add**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



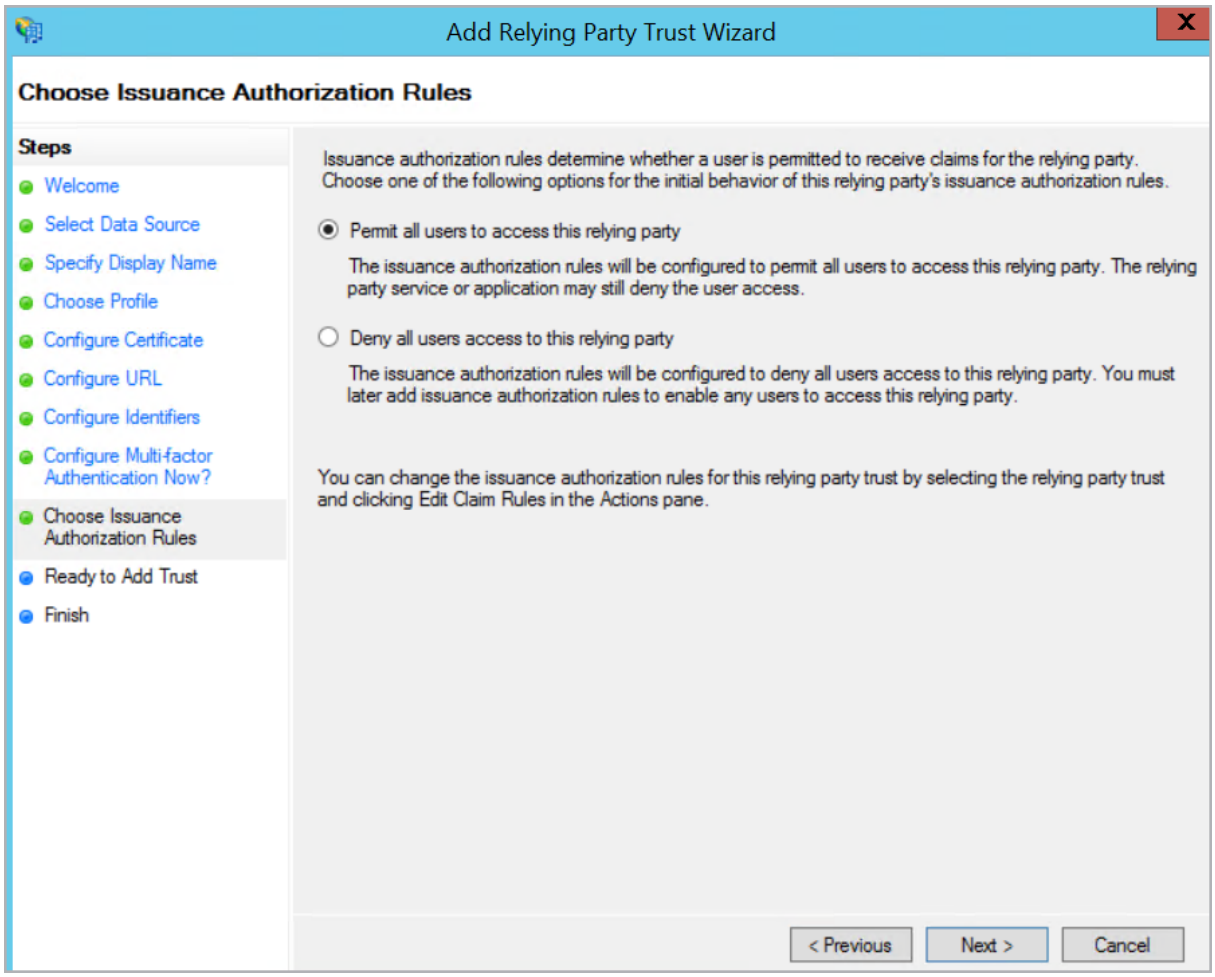
10. Click **Next**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



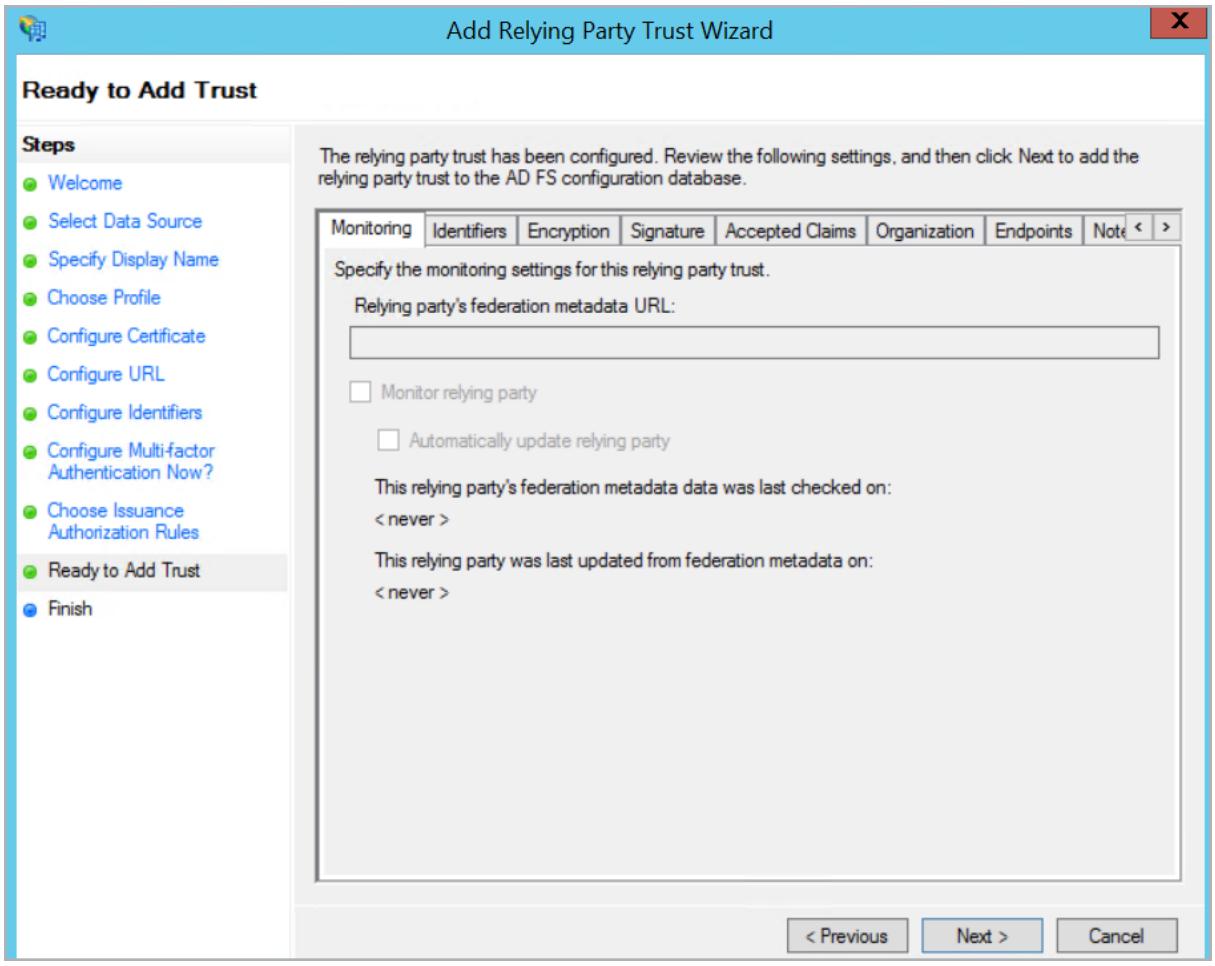
11. Select I do not want to configure multi-factor authentication settings for this relying party trust at this time and click **Next**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



12. Select **Permit all users to access this relying party** and click Next.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

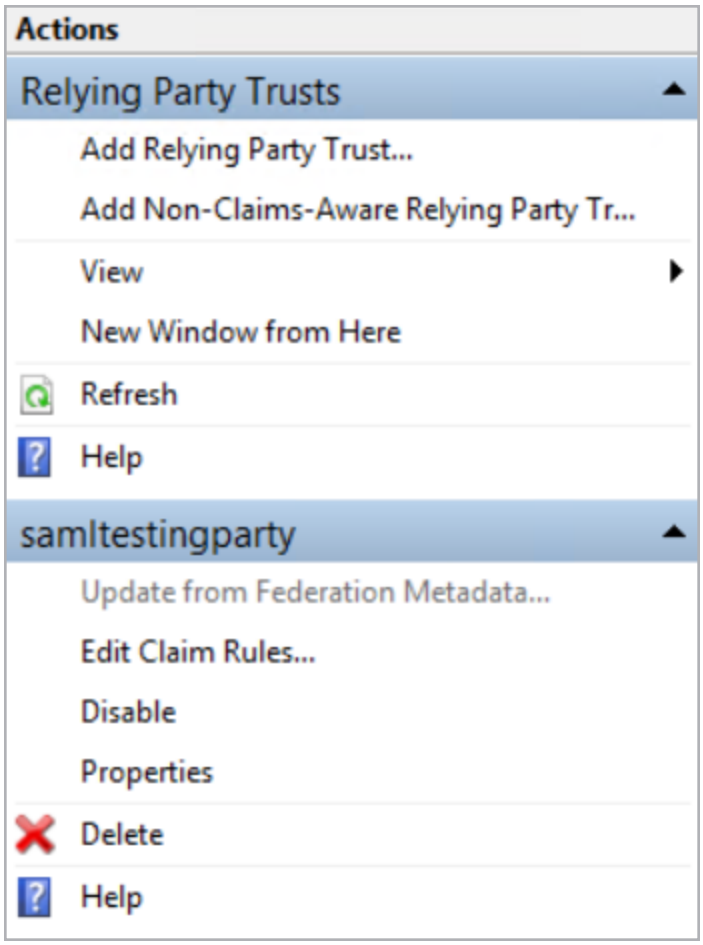


13. Click **Next**.
14. Click **Finish**.

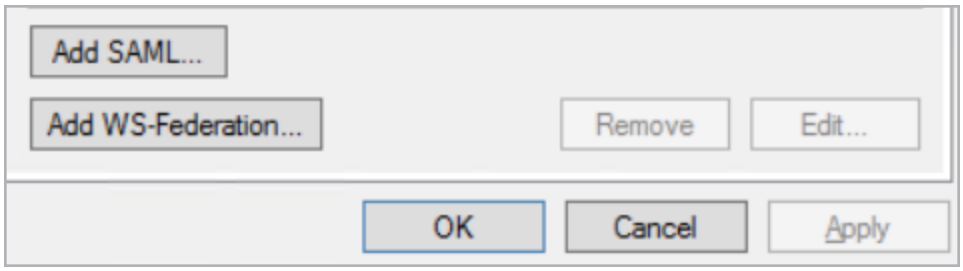
3.7.3 Add End Points

Now, add the end points by following the steps below:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

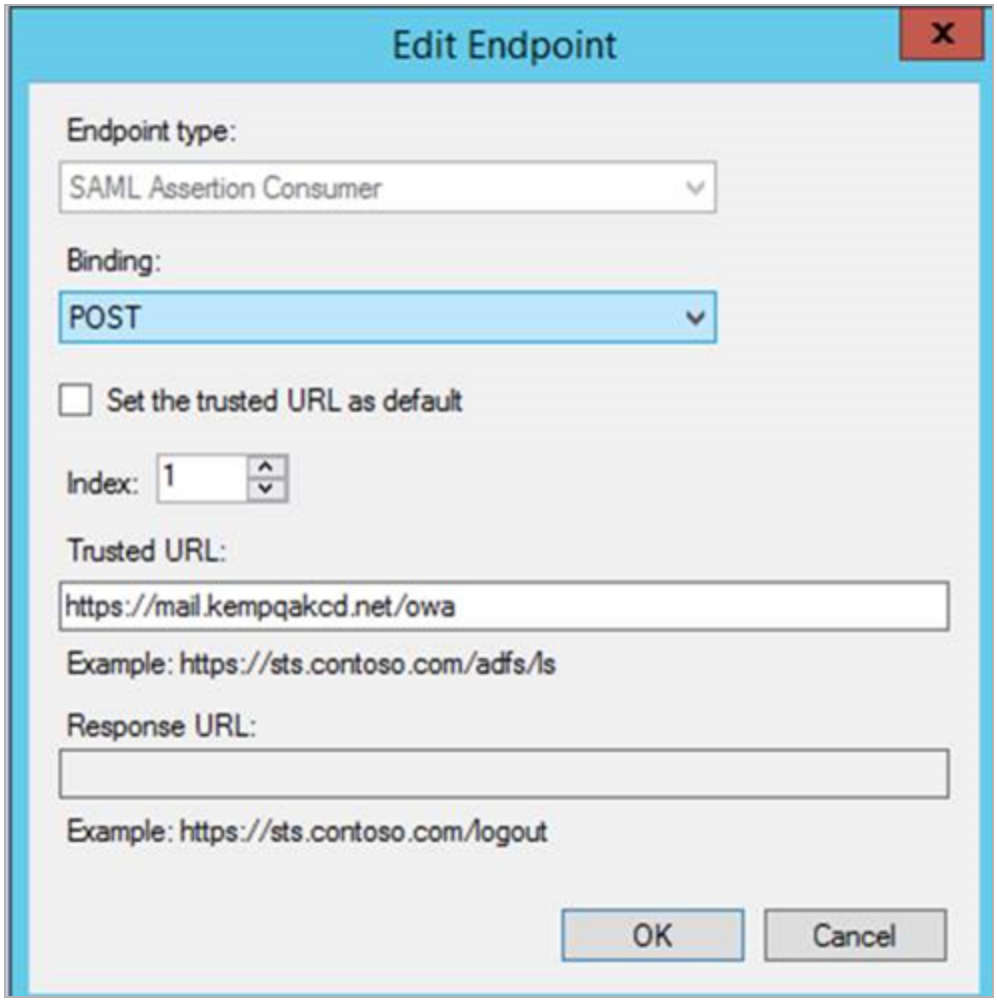


1. Go to the Properties of the relying party trust.
2. Select the **Endpoints** tab.

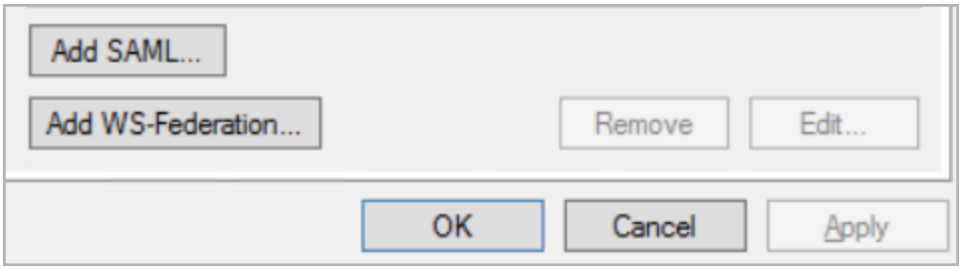


3. Click **Add SAML**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

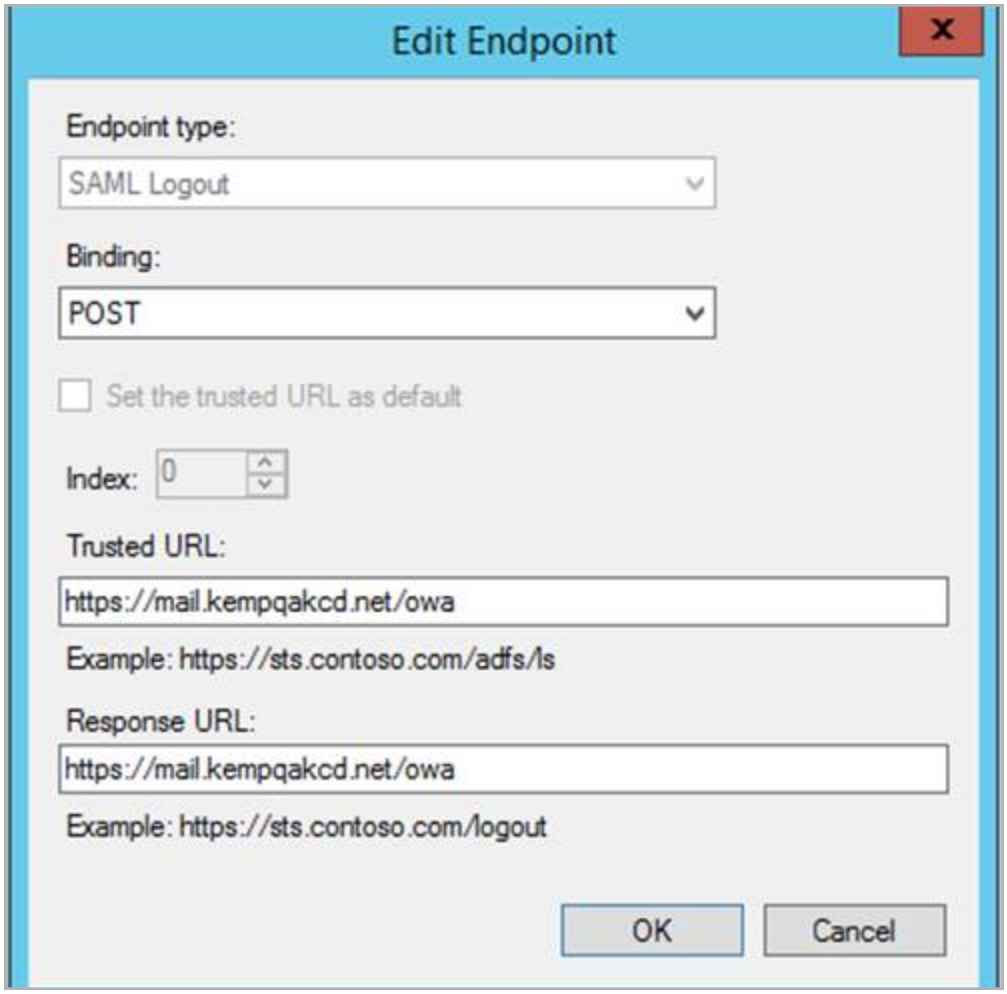


4. Select **SAML Assertion Consumer** from the **Endpoint type** drop-down list.
5. Select **POST** as the Binding.
6. Enter the **Virtual Service FQDN** in the **Trusted URL** text box. Then, click OK.



7. Click **Add SAML** again to add the logout endpoint.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



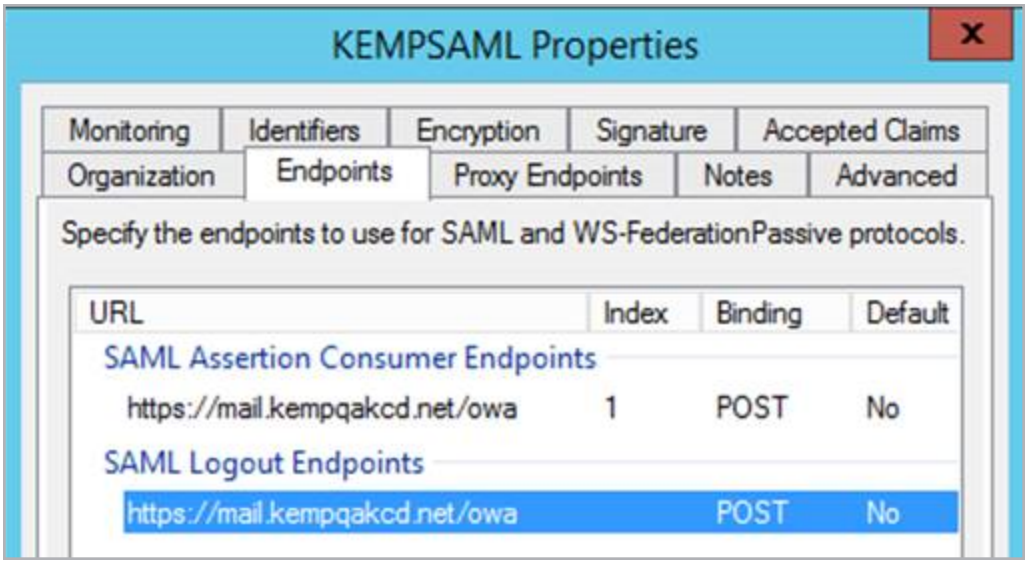
8. Select **SAML Logout** as the Endpoint type.

9. Select **POST** as the Binding.

10. Enter the logout URL in the **Trusted URL** text box, for example https://<VirtualServiceFQDN>/<LogoutURL>.

11. Copy the URL from the **Trusted URL** text box into the **Response URL** text box. Then, click **OK**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



Both URLs should point towards the Virtual Service.

3.7.4 Import the Certificate

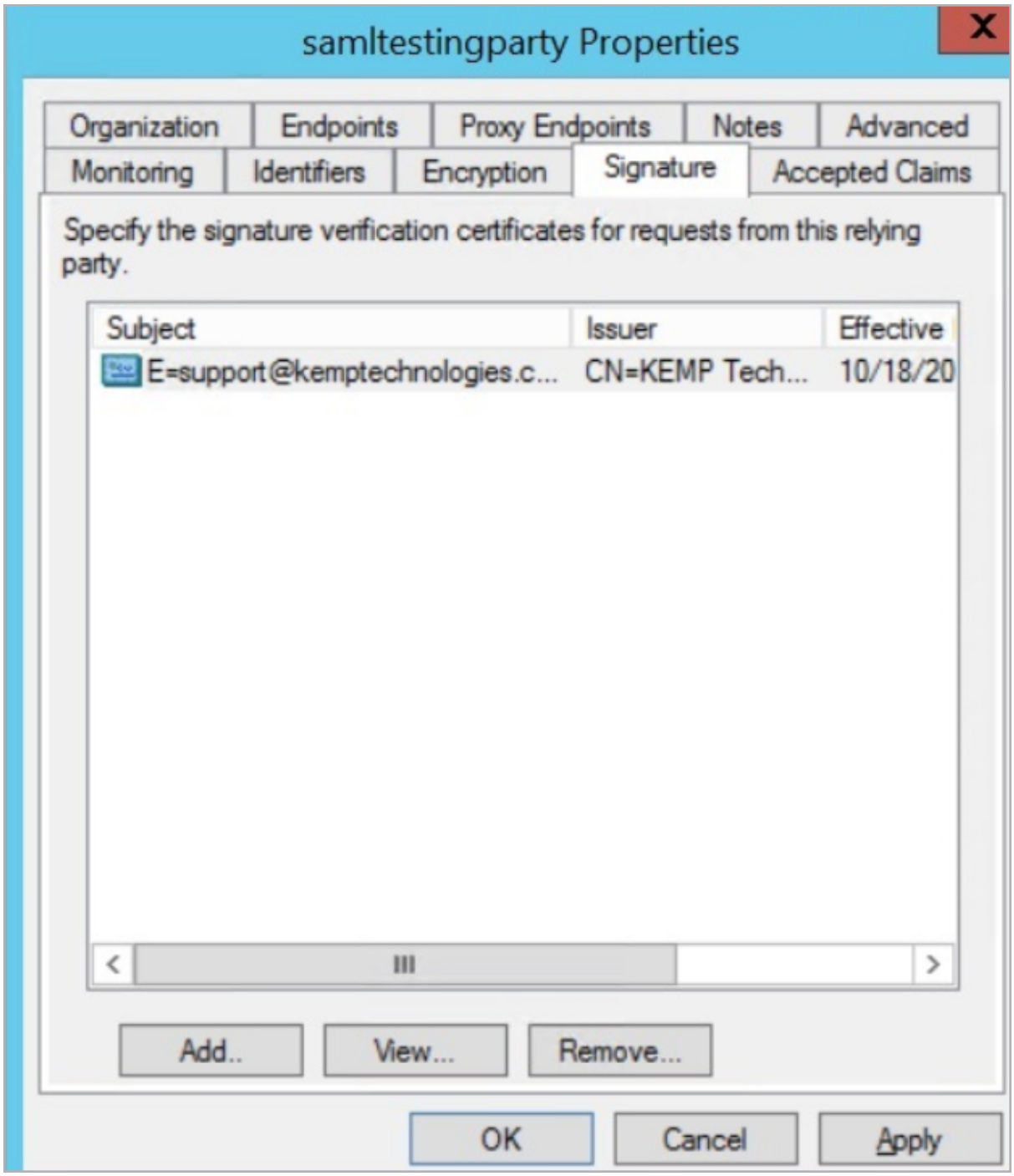
Export the certificate from the LoadMaster by going to **Virtual Services > Manage SSO**, clicking **Modify** on the SAML SSO domain and clicking **Download**.

To import the certificate in AD FS, follow the steps below:

1. Select the **Signature** tab.
2. Click **Add**.
3. Browse to and select the certificate that was downloaded from the LoadMaster.

> In the context of log out processing – the service provider signs the log out request message. Therefore, on the AD FS side – there must be a certificate to verify that the signature is accurate and correct for the message that was signed on the service provider.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



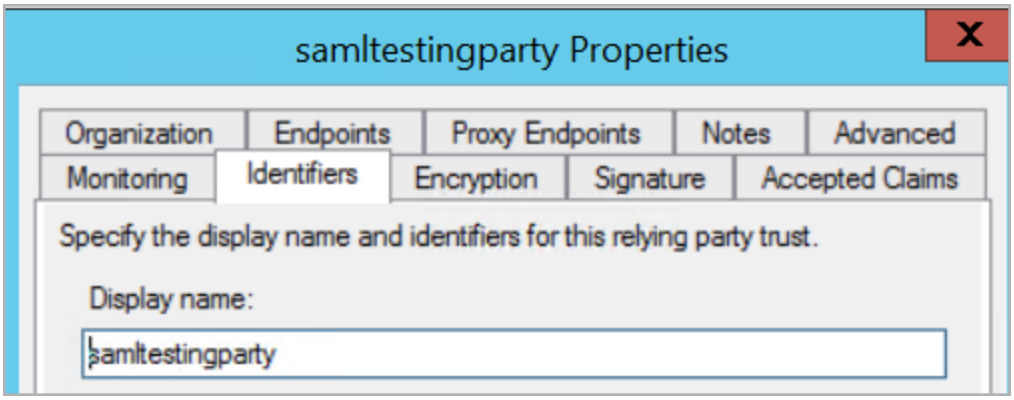
4. Click **OK**.

3.7.5 Configure the Identifiers

Configure the identifiers by following the steps below:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1. Select the **Identifiers** tab.



2. Enter the Display name. This value should be entered as the **SP Entity ID** in the LoadMaster.

3. For the Relying party identifiers, include all possible connotations of the URL, for example http://<ID>, https://<ID>.

4. Click **OK**.

3.7.6 Claim Rules

A single claim is required. While multiple claims may be configured, it is recommended you use a single claim only, which should be most appropriate for the environment. In the Claim Rule, the LDAP attributes are mapped to the outgoing claim types. The LoadMaster supports:

- The User-Principal-Name which maps to the UPN (which is the outgoing claim type)

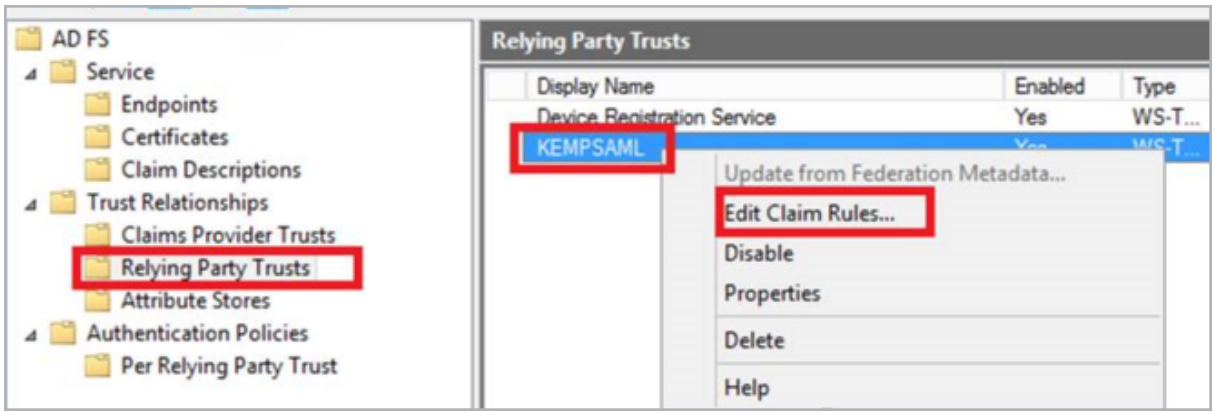
- The SAM-Account-Name (which is the typical Windows samAccountName attribute from an LDAP perspective) which maps to the Windows account name

- The User-Principal-Name which maps to the Name ID outgoing claim type

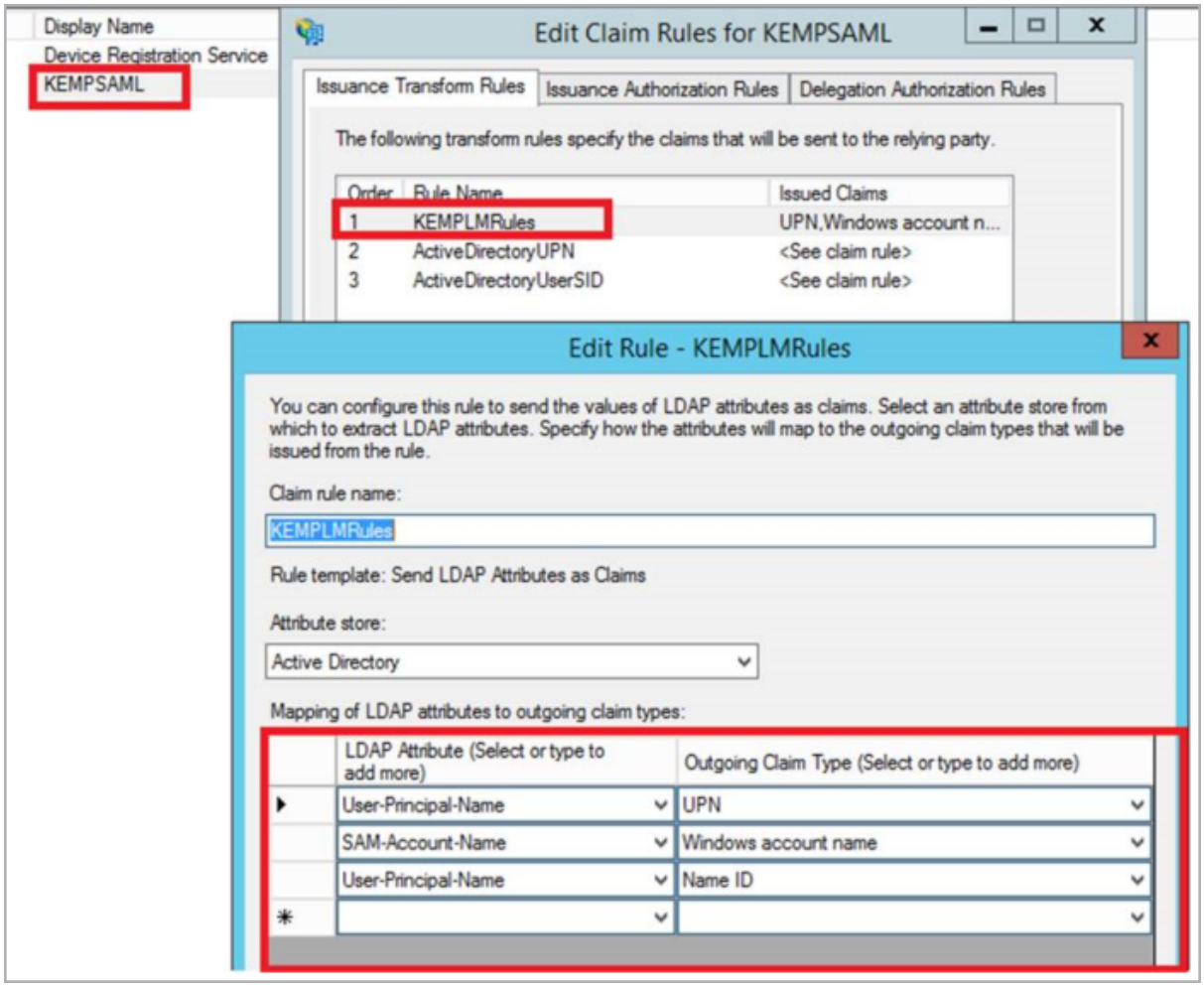
> The User-Principal-Name is important because without it – a session index is not included in the SAML response. The session index is very important to correlate an existing session and a log out operation.

To add the Claim Rule, follow the steps below:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



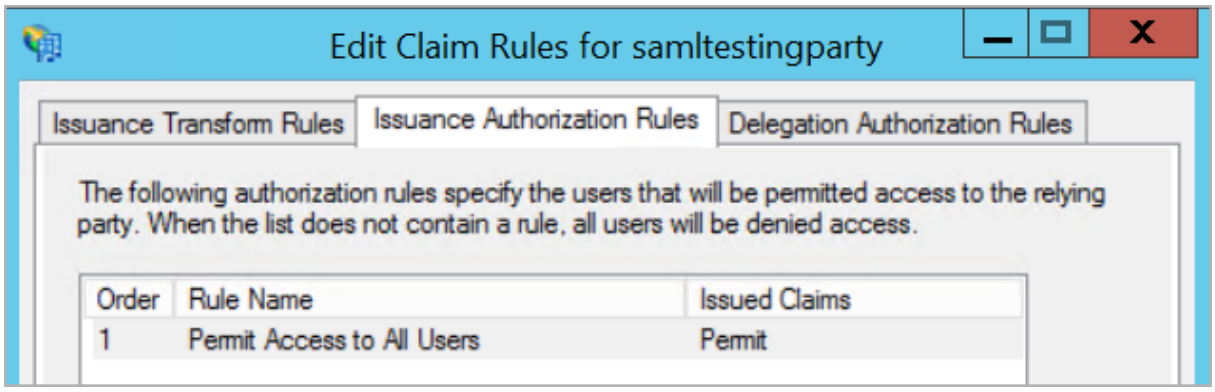
1. Select the **Relying Party Trusts folder**.
2. Right-click the relevant Display Name and select **Edit Claim Rules**.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Edit the relevant rule.

4. Add the attribute mappings.

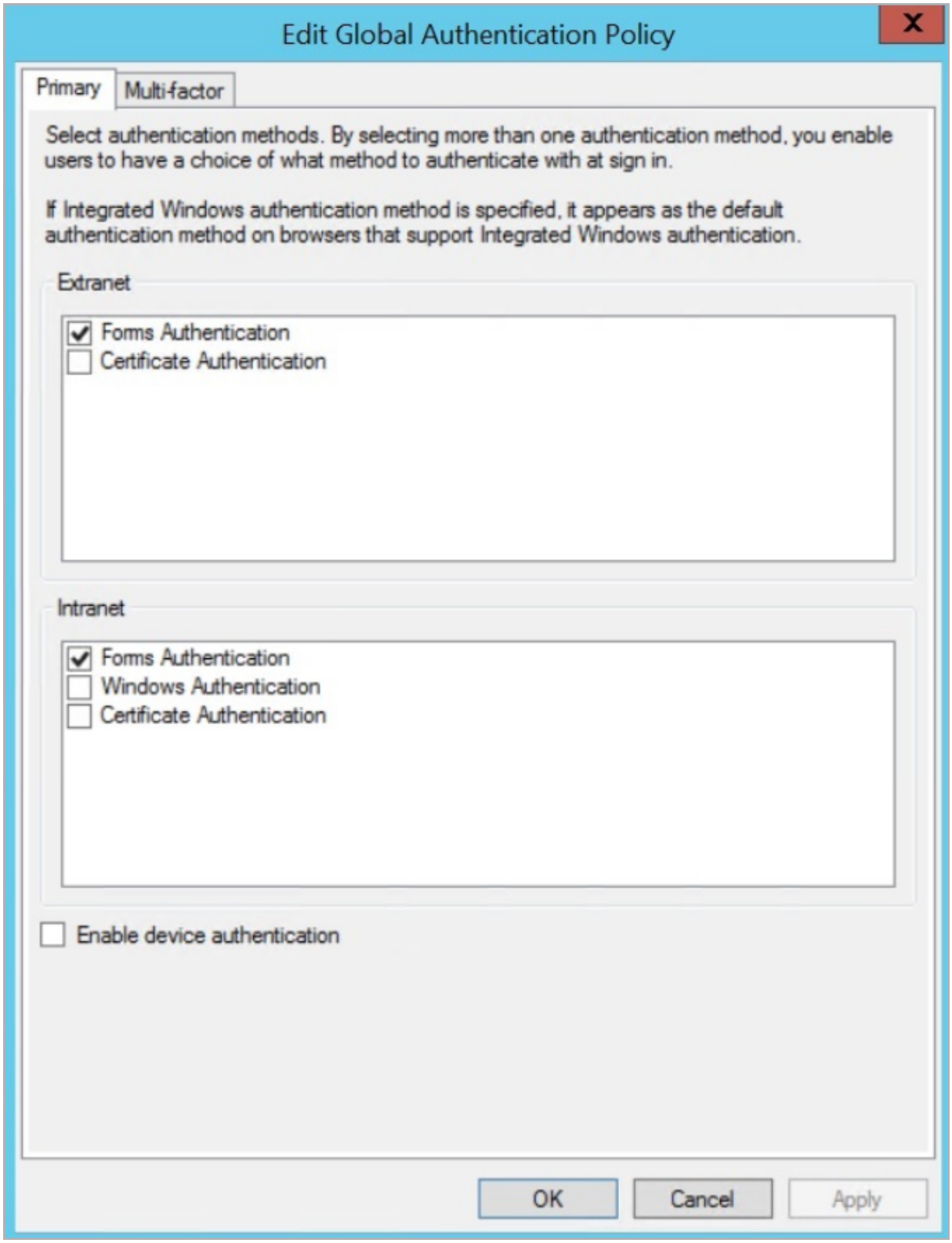


5. Ensure that all users are permitted access by selecting the Issuance Authorization Rules tab.

3.8 Authentication Policies Setting

Right-click the **Authentication Policies** folder and select **Edit Global Primary Authentication**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Select the **Primary** tab. Depending on production requirements (external/internal, and so on), Forms Authentication may need to be enabled for both the Extranet and Intranet. Deselect the other options. Click **OK** to save the settings.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4 Configure SAML Authentication in the LoadMaster

Follow the steps in the sections below to configure the options for SAML in the LoadMaster.

4.1 Limitations

Refer to the sections below for information on some limitations when using SAML.

4.1.1 Certificate Signature Verification

Since LoadMaster firmware version 7.2.40, the signature verification in the case of having a SAML IDP Token Signing certificate, which was signed by your Root Certificate, will not (should not) work.

In previous versions, you could set your SAML IDP Token Signing Certificate on your IDP Provider. The Root certificate configured in your SSO Domain was then used to verify the signature and trust was established.

Since 7.2.40, the certificate in the response must match the certificate assigned in the SAML SSO domain. This means that your certificate can not be created by a Third Party Provider, such as Go Daddy, and it should be a trusted Root Cert.

4.1.2 Persistent Cookies

The persistent cookie feature works with SAML. However, it is susceptible to browser behavior and may be effective to use with Internet Explorer only. Also, depending on testing performed and multiple cookies being in use, the cookie that can be used varies.

4.2 Configure the SSO Domain

SAML SSO domains are fundamentally different from other SSO domains which can be configured on the LoadMaster. This is because the LoadMaster does not directly interact with the authentication server. In the context of SAML, the LoadMaster performs redirections. The LoadMaster asks the client to redirect to an IdP to issue some claims and get the required assertions back.

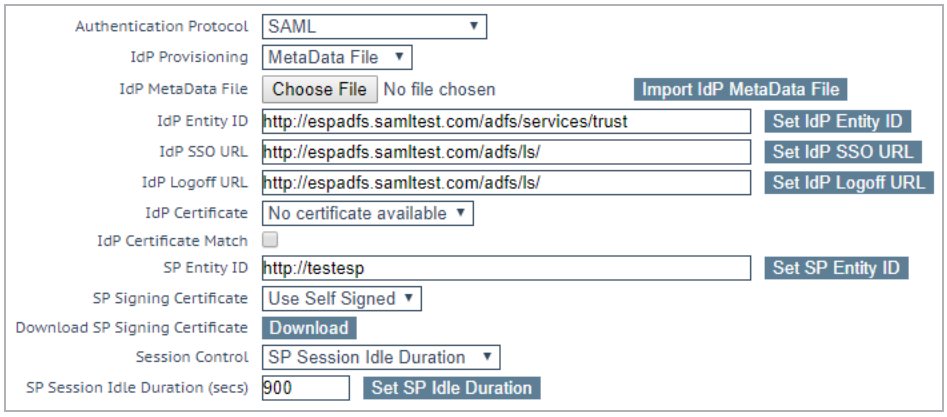
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To configure a SAML-based SSO domain in the LoadMaster, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Manage SSO**.



2. Enter a name for the SSO domain in the Add new Client Side Configuration text box and click **Add**.



3. Select **SAML** as the Authentication Protocol.

4. Select the relevant IdP Provisioning option.

The Manual option enables you to manually input details into the IdP fields.

The MetaData File option enables you to upload an IdP MetaData File. This simplifies the configuration of the IdP attributes, including the IdP Entity ID, IdP SSO URL and IdP Logoff URL. The metadata file can be downloaded from the IdP. For further information, refer to the **Endpoint Settings** section. To upload the file - click **Browse**, navigate to and select the relevant file and click **Import IdP MetaData File**.

5. Select an IdP Certificate for use in the context of assertion verification.

> The certificate can be exported from the IdP and imported in the LoadMaster in the **Certificates & Security** section.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The IdP Certificate is very important in terms of verification of the assertions that must be contained in the SAML response that is received from the IdP. Without the certificate, verification cannot proceed.

6. Decide whether or not to enable the **IdP Certificate Match** check box.

> If this option is enabled, the IdP certificate assigned must match the certificate in the IdP SAML response.

7. Enter the **SP Entity ID** and click **Set SP Entity ID**.

> This is an identifier that is shared to enable the IdP to understand, accept and have knowledge of the entity when request messages are sent from the LoadMaster. This must correlate to the identifier of the relying party on the AD FS server.

8. Select the relevant SP Signing Certificate option.

It is optional to sign requests that are sent in the context of logon. Currently, the LoadMaster does not sign those requests.

In the context of log off requests – it is mandatory and these requests must be signed. This is to avoid any spoofing and to provide extra security in relation to log off functionality. This ensures that users are not being hacked and not being logged off unnecessarily.

In the **SP Signing Certificate** field, you can use a self-signed certificate to perform the signing.

9. If using a self-signed certificate, click the **Download** button to download the certificate. This certificate must be installed on the IdP server (for example AD FS) to be added to the relying party signature.

The AD FS server requires this certificate for use of the public key to verify the signatures that the LoadMaster generates.

10. Select the relevant Session Control option.

> The IdP maximum duration value cannot be set in the LoadMaster. The value is taken from the IdP protocol. If the value is not already set in the IdP authentication response, the

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

default value of 30 minutes is assigned as the IdP maximum duration.

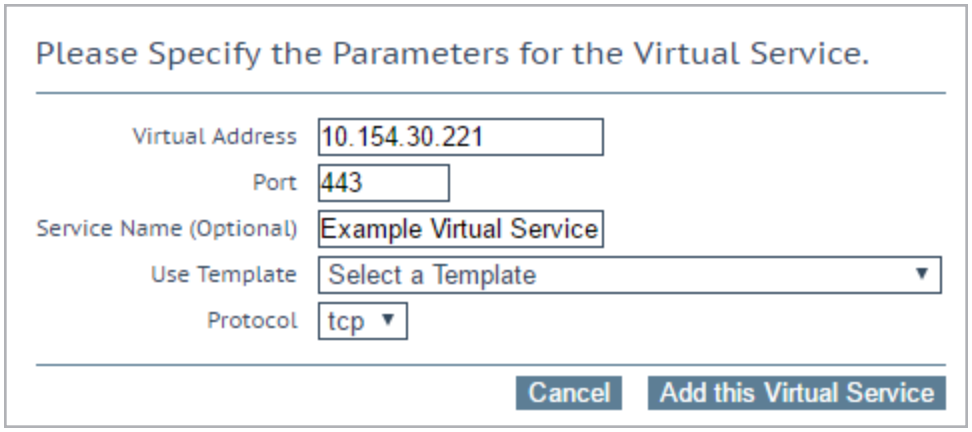
11. If using SP Session Idle Duration, enter the SP Session Idle Duration and click **Set SP Idle Duration**.

12. If using SP Session Max Duration, enter the SP Session Max Duration and click **Set SP Max Duration**.

4.3 Configure the Virtual Service

Follow the steps below to configure the Virtual Service to use SAML authentication:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.



2. Enter a valid IP address in the **Virtual Address** text box.

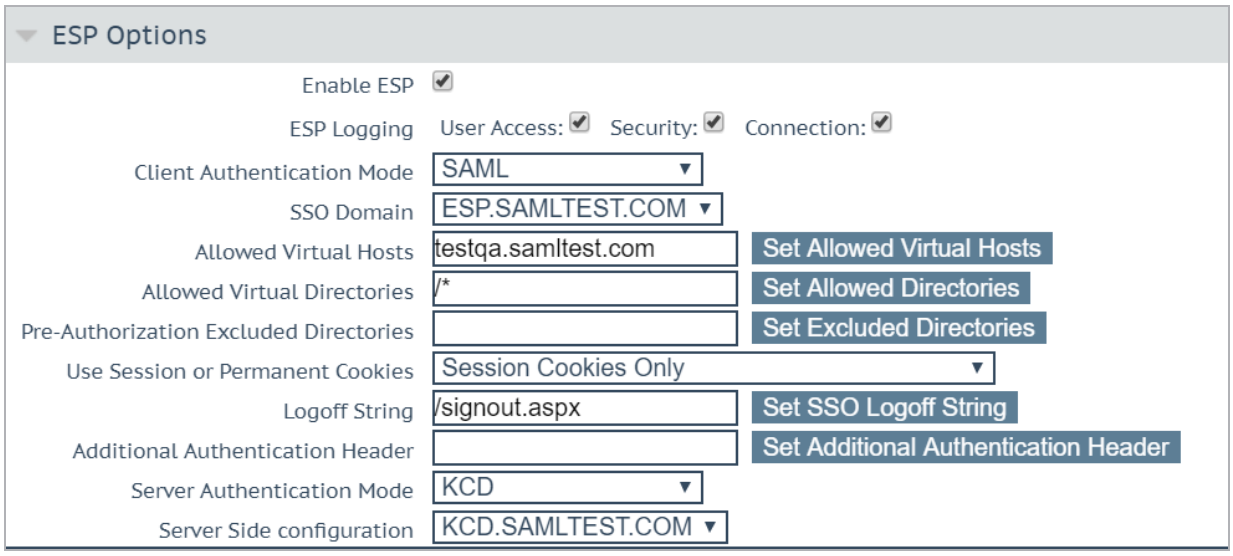
3. Enter the **Port**.

4. Enter a **Service Name**.

5. Click **Add this Virtual Service**.

6. Expand the **ESP Options** section.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



7. Select the **Enable ESP** check box.
8. Select **SAML** as the Client Authentication Mode.
9. Select the SAML **SSO Domain**.
10. Enter any Allowed Virtual Hosts, as needed.
11. Enter the **Logoff String** and click **Set SSO Logoff String**.

> The Logoff String is important. The Logoff String has a special protocol flow associated with it in the context of SAML. Not only do you want to log out of the Service Provider on the LoadMaster, but the user also must be logged out of the IdP.

12. If required, enter the **Additional Authentication Header** and click **Set Additional Authentication Header**.

> The **Additional Authentication Header** specifies the name of the HTTP header. This header is added to the HTTP request from the LoadMaster to the Real Server and its value is set to the user ID for the authenticated session.

13. Select the **Server Authentication Mode**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The **Server Authentication Mode** can be set to **None**, **KCD**, or **Server Token**. **Basic Authentication** is not supported because the LoadMaster does not have access to the username and password.

> If you select **Server Token** as the **Server Authentication Mode** on reception and verification of the SAML response, the LoadMaster requests a long-lived token. The LoadMaster then builds a redirection URL with the token specified.

14. If using KCD as the **Server Authentication Mode**, please select the relevant option for Server Side configuration.

> For further information on KCD, refer to the Kerberos Constrained Delegation, Feature Description.

15. Configure any other settings as needed.

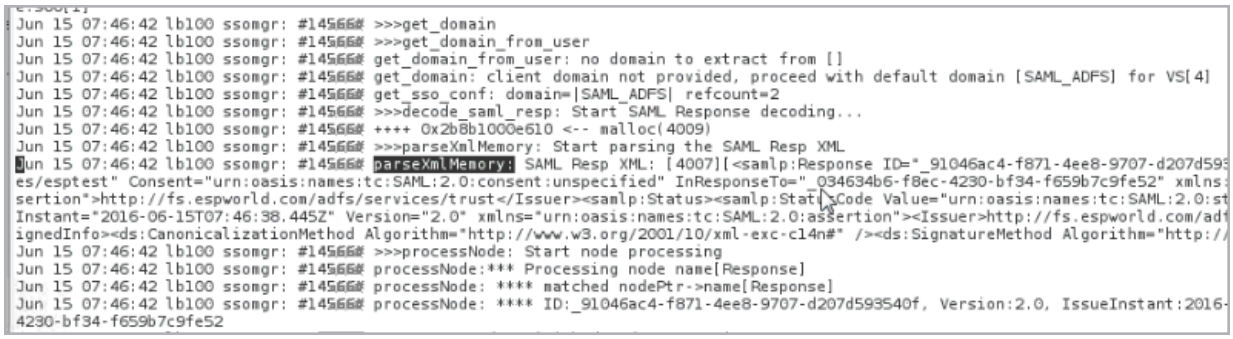
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5 Appendix A: Logging

There are very detailed logs available to assist in investigating issues. Some things to look out for in the logs are:



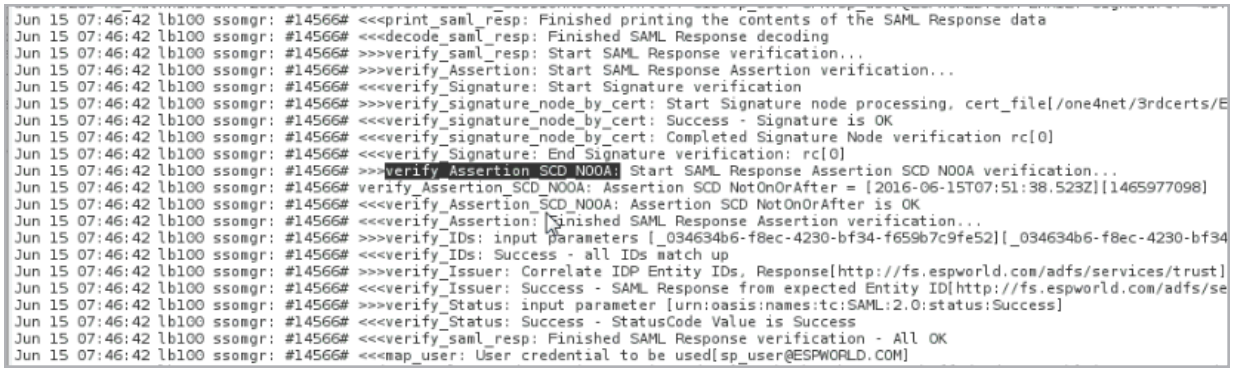
- Ensure there is a SAML domain assigned
- An ID must be generated for the request
- The SAML request is encoded
- The authentication request is built up and sent back down to L7



- At some point later, a response is received
- An XML-encoded SAML response gets parsed
- Some of the information which is in the SAML response is displayed
- That information is processed

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- The required pieces are extracted to perform a significant amount of verification checks



- When finished processing the XML, the verification steps begin

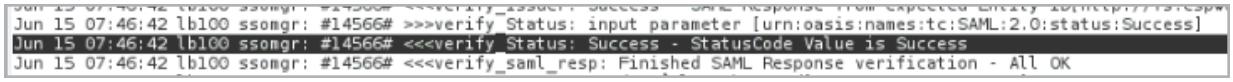
- As part of the verification:

- The signature is checked to ensure it is OK

- The “Not On Or After” (NOOA) time is checked to ensure that time has not passed because the assertion has a lifetime associated with it

- All of the IDs are checked to ensure they match. There is an original ID which is allocated as part of a request. That ID is received back as part of a response so it is checked to ensure it matches in two places in the response document.

- The issuer is verified to ensure that the response is received from the IdP which was configured previously



- A success code is displayed in the response. That has to be successful to indicate that the user was successfully authenticated at the IdP.

- The username entered when signing in is displayed

- Next, the KCD processing occurs (if relevant)

- Once the KCD processing is finished, the site is browsed

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



```
Jun 15 07:47:21 lb100 ssomgr: #14566# operation == L7_AUTH_SAML_LOGOUT
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>get_domain
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>get_domain_from_user
Jun 15 07:47:21 lb100 ssomgr: #14566# get_domain_from_user: no domain to extract from []
Jun 15 07:47:21 lb100 ssomgr: #14566# get_domain: client domain not provided, proceed with default domain [SAML_ADFS] for VS[4]
Jun 15 07:47:21 lb100 ssomgr: #14566# get_sso_conf: domain=|SAML_ADFS| refcount=2
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>generate_ID: Generate ID for SAML AuthnReq
Jun 15 07:47:21 lb100 ssomgr: #14566# ++++ 0x2b8b1000a5e0 <-- malloc(42)
Jun 15 07:47:21 lb100 ssomgr: #14566# generate_random_sequence: sequence [172040bf-4029-44fd-a67d-808199c6c6e4]
Jun 15 07:47:21 lb100 ssomgr: #14566# <<<generate_ID: ID string generated [_172040bf-4029-44fd-a67d-808199c6c6e4]
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>build_saml_logout_req: Start processing to build Logout Request for SAML
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>generate_IssueInstant: Generate IssueInstant for SAML Req
Jun 15 07:47:21 lb100 ssomgr: #14566# ++++ 0x2b8b1000a640 <-- malloc(21)
Jun 15 07:47:21 lb100 ssomgr: #14566# <<<generate_IssueInstant: IssueInstant generated [2016-06-15T07:47:21Z]
Jun 15 07:47:21 lb100 ssomgr: #14566# ---- 0x2b8b1000a640 --> free()
Jun 15 07:47:21 lb100 ssomgr: #14566# build_saml_logout_req: Logout Request XML string:[<samlp:LogoutRequest xmlns:samlp="urn:oas
040bf-4029-44fd-a67d-808199c6c6e4" Version="2.0" IssueInstant="2016-06-15T07:47:21Z" Destination="https://fs.espworld.com/adfs/ls
> <samlp:SessionIndex>_369b28b4-abc0-4608-b0ff-d28da567128b</samlp:SessionIndex> </samlp:LogoutRequest>]
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>encode_saml_req: Start SAML LogoutReq Request encoding...
Jun 15 07:47:21 lb100 ssomgr: #14566# ++++ 0x2b8b10008820 <-- malloc(906)
Jun 15 07:47:21 lb100 ssomgr: #14566# encode_saml_req: Encoded blob:fZFRT4MwFIX%2FCul7oWBXoNmIRnwg2ZwZRhNflkKLLoG2ckvcz7fbMJk%2B%
BaBRU5Qrt4zQhlDQdpiTJMaWdxIKlEmcki%2FO8ZS1TFAUvagTvrJCv8CLApCoNTmjnTyRmmDAcL55JymnKk%2FgNBaXfcdDCna0P5yzwKOogVGC%2FzNjLsDVDJGQHUQ
WiaQmmjGS4IV2HZZJJsWBp7MNLzx8z%2BLn%2B%2Bq%2FiGw%3D%3D
Jun 15 07:47:21 lb100 ssomgr: #14566# <<<encode_saml_req: Finished LogoutReq Request encoding
Jun 15 07:47:21 lb100 ssomgr: #14566# build_saml_logout_req: SAMLRequest Blob:[436][SAMLRequest=fZFRT4MwFIX%2FCul7oWBXoNmIRnwg2Zw
23WPAkJt6NxpjU9ulL%2BNwSAGt3BaBRU5Qrt4zQhlDQdpiTJMaWdxIKlEmcki%2FO8ZS1TFAUvagTvrJCv8CLApCoNTmjnTyRmmDAcL55JymnKk%2FgNBaXfcdDCna0P
PzM3HhLa8VnAZUWqpjsb9heZNkDcWiaQmmjGS4IV2HZZJJsWBp7MNLzx8z%2BLn%2B%2Bq%2FiGw%3D%3D]
Jun 15 07:47:21 lb100 ssomgr: #14566# build_saml_logout_req: cfg->sp_cert:UseSelfSigned, def_samlcert:saml_self_signed
Jun 15 07:47:21 lb100 ssomgr: #14566# /one4net/certs/.saml_self_signed.pem: signing cert_file
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>query_sign: Start processing to Sign Logout Request for SAML
Jun 15 07:47:21 lb100 ssomgr: #14566# >>>query_sign: Query[SAMLRequest=fZFRT4MwFIX%2FCul7oWBXoNmIRnwg2ZwZRhNflkKLLoG2ckvcz7fbMJk%
Gt3BaBRU5Qrt4zQhlDQdpiTJMaWdxIKlEmcki%2FO8ZS1TFAUvagTvrJCv8CLApCoNTmjnTyRmmDAcL55JymnKk%2FgNBaXfcdDCna0P5yzwKOogVGC%2FzNjLsDVDJGQ
kDcWiaQmmjGS4IV2HZZJJsWBp7MNLzx8z%2BLn%2B%2Bq%2FiGw%3D%3D], SigAlg[1], Key file[/one4net/certs/.saml_self_signed.pem]
Jun 15 07:47:21 lb100 ssomgr: #14566# query_sign: Added SigAlg...[SAMLRequest=fZFRT4MwFIX%2FCul7oWBXoNmIRnwg2ZwZRhNflkKLLoG2ckvcz
%2BNwSAGt3BaBRU5Qrt4zQhlDQdpiTJMaWdxIKlEmcki%2FO8ZS1TFAUvagTvrJCv8CLApCoNTmjnTyRmmDAcL55JymnKk%2FgNBaXfcdDCna0P5yzwKOogVGC%2FzNjL
sb9heZNkDcWiaQmmjGS4IV2HZZJJsWBp7MNLzx8z%2BLn%2B%2Bq%2FiGw%3D%3D&SigAlg=http%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-
```

- At some point there is a log out operation

- An operation is seen for L7 authentication SAML logout

- The logout request is built

- The logout request is sent to L7

- The client redirects to the logout

- A digest is created and there is a full query string

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Kerberos Constrained Delegation, Feature Description

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.