Quest

Foglight® 8.1.0

Integration with SAML 2.0 in ADFS

© 2025 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight® 8.1.0 – Integration with SAML 2.0
in ADFS Foglight Version– 8.1.0

Contents

Foglight and SAML 2.0 Integration in ADFS 4

Before you begin 5

Step 1: Adding Relying Party Trust in ADFS 5

Step 2: Editing Claim Rules 8

Step 3: Configuring Endpoints 10

Step 4: Configuring Signature and Hash Algorithm 12

Step 5: Exporting the Certificate 14

Step 6: Configuring the Trust Relationship 15

Step 7: Setting up SAML in Foglight 15

About us 17

Foglight and SAML 2.0 Integration in ADFS

Starting with release 5.9.3, Foglight® Management Server supports Active Directory Federation Services (ADFS) 2.0 and PingFederate 8.x (and later) using the Security Assertion Markup Language (SAML) 2.0 protocol. Follow the below steps in sequence to completely integrate SAML SSO with the Foglight Management Server on the ADFS sever.

NOTE: ADFS requires https protocol, so Foglight's http SAML login cannot be used on ADFS. Foglight https SAML login could be using either IP address or the host name. For detailed configurations about IP or host name logon, see Before you begin, step 8 & 9 in the Step 1: Adding Relying Party Trust in ADFS section, and step 3 in the Step 3: Configuring Endpoints section.

- Before you begin
- Step 1: Adding Relying Party Trust in ADFS
- Step 2: Editing Claim Rules
- Step 3: Configuring Endpoints
- Step 4: Configuring Signature and Hash Algorithm
- Step 5: Exporting the Certificate
- Step 6: Configuring the Trust Relationship
- Step 7: Setting up SAML in Foglight

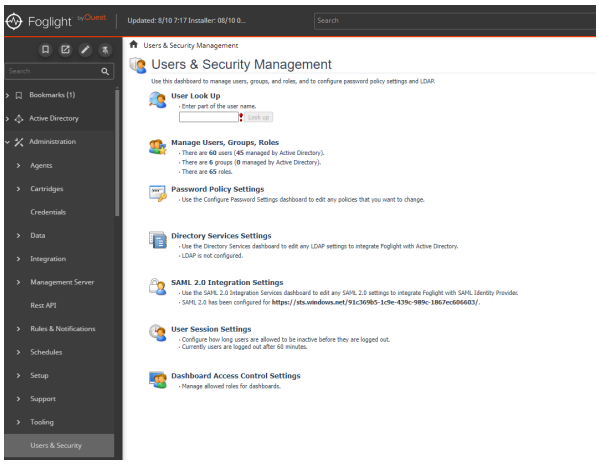
Before you begin

NOTE:

- If you are about to use SAML IP login, make sure to run the following command: "`-Dquest.saml.hostname=<foglight-server-ip>`" to start up your Foglight Management Server.
- When logging into your Foglight Management Server, make sure to keep using the same approach as what you configured during the SAML integrations. For example, if you set up the HTTPS SAML login using the IP address, you must log in to your Management Sever with https://<foglight-server-ip>:<foglight-server-port>.

You need to enable SAML 2.0 SSO Configuration in your Foglight Management Server prior to setting up the SAML integration. Follow the steps below to enable SAML 2.0 SSO Configuration:

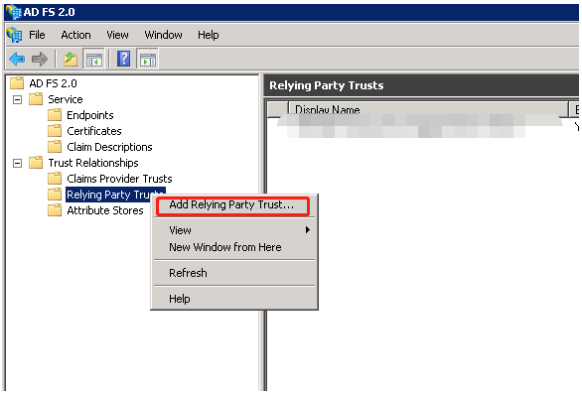
1. Log into the Foglight Management Server as a Security Administrator.
2. Under **Dashboards**, click **Administration** > **Users & Security**, and then click **SAML 2.0 Integration Settings.** The *SAML 2.0 SSO Configuration* dashboard appears.
3. Click **Enable**.



Step 1: Adding Relying Party Trust in ADFS

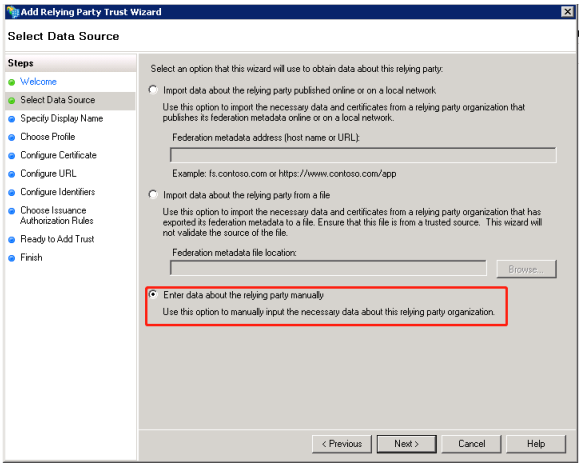
To add Relying Party Trust:

1. Open the ADFS Management Console.
2. Navigate to **Trust Relationships** > **Relying Party Trusts**. Right click **Relying Party Trusts**, and then select **Add Relying Party Trust…** from the context menu.



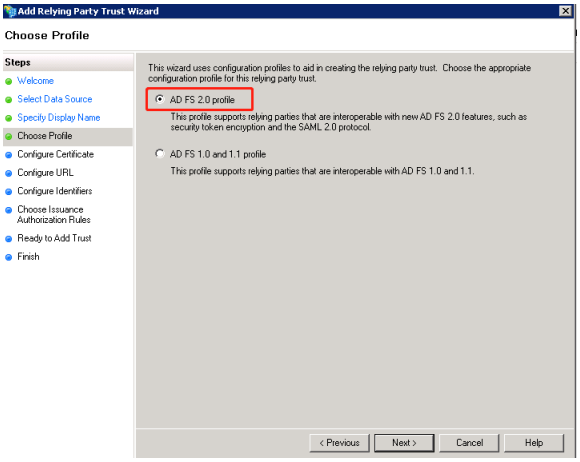
3 Click **Start** on the *Add Relying Party Trust Wizard*.

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



5 *Specify Display Name*: Specify a display name and click **Next**.

6 *Choose Profile*: Select AD FS 2.0 and click **Next**.

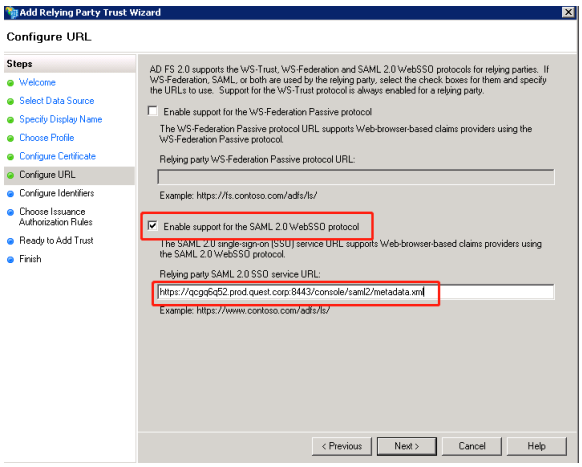


7 *Configure Certificate*: Click **Next**.

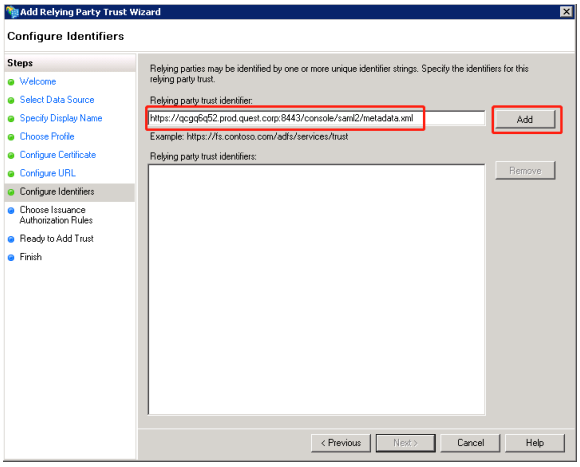
8 *Configure URL*: Select **Enable support for the SAML 2.0 WebSSO protocol**, and then input Foglight's SAML 2.0 metadata URL in https, which is:

NOTE: ADFS requires https protocol, so Foglight's http SAML login cannot be used on ADFS.

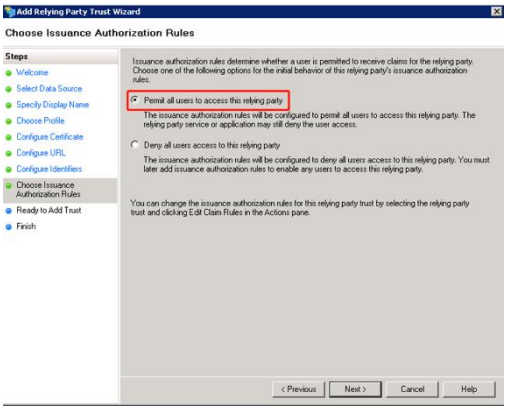
- IP logon: https://<foglight-server-ip>:<foglight-ssl-port>/console/saml2/metadata.xml. Click **Next**.
- Host name logon: https://<foglight-server-host-name>:<foglight-ssl-port>/console/saml2/metadata.xml. Click **Next**.



9 *Configure Identifiers*: Input Foglight's SAML 2.0 metadata https URL used in step 8 in the **Relying party trust identifier** field, click **Add**, and then click **Next**.

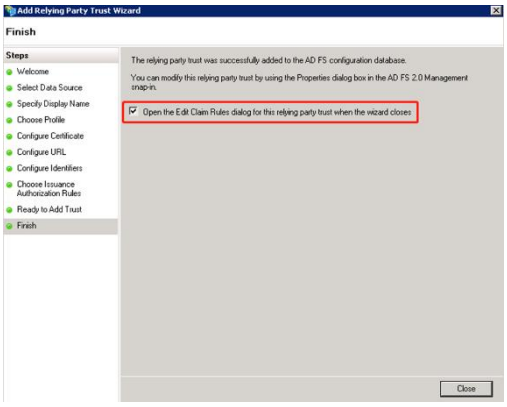


10 *Choose Issuance Authorization Rules*: Select **Permit all users to access this relying party** and click **Next**.



11 *Ready to Add Trust*: Click **Next**.

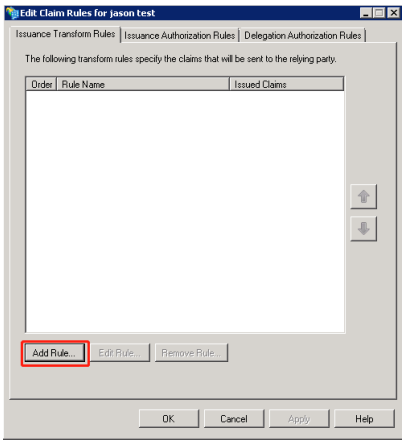
12 *Finish*: Make sure to select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, and then click **Close**.



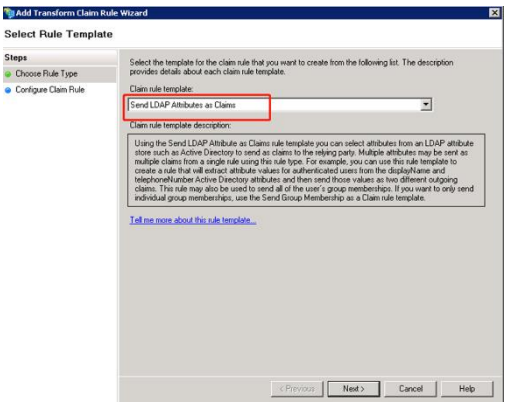
Step 2: Editing Claim Rules

To edit Claim Rules:

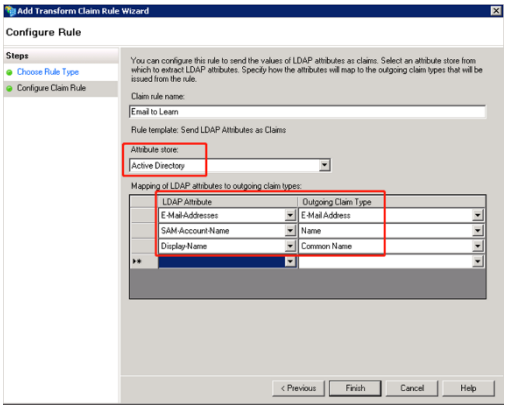
1 On the prompted **Edit Claim Rules** dialog box, click **Add Rule…**



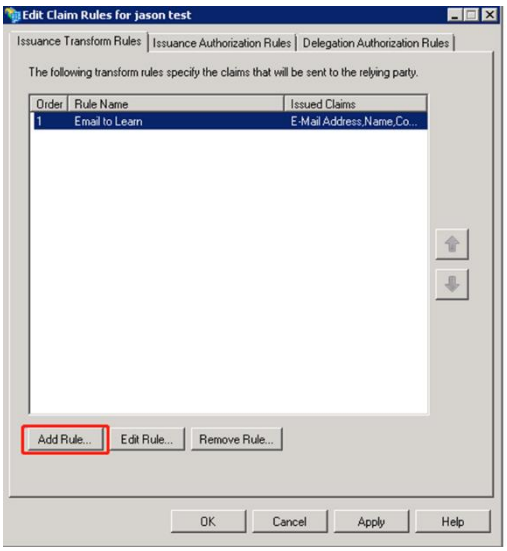
2 *Choose Rule Type*: Select **Send LDAP Attributes as Claims** and click **Next**.



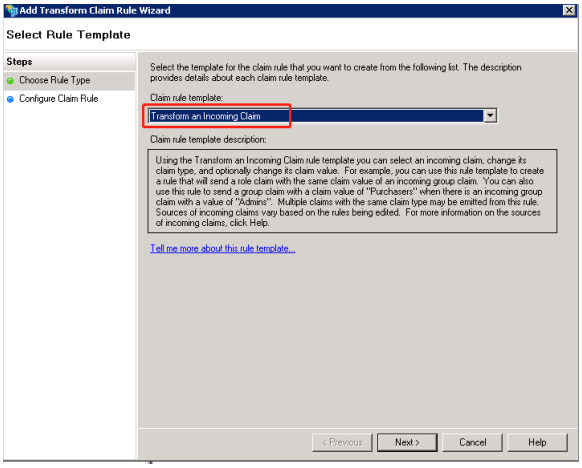
3 *Configure Claim Rule*: Specify a rule name, and select **Active Directory** as the **Attribute store**. Add LDAP attributes mapping as below, and then click **Finish**.



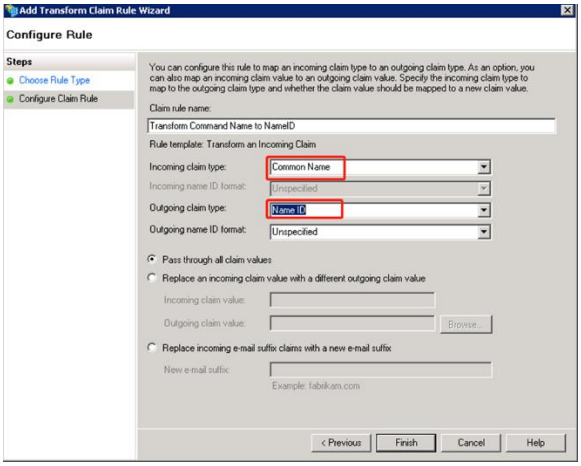
4 Click **Add Rule…** button again to add another rule on the **Edit Claim Rules** wizard.



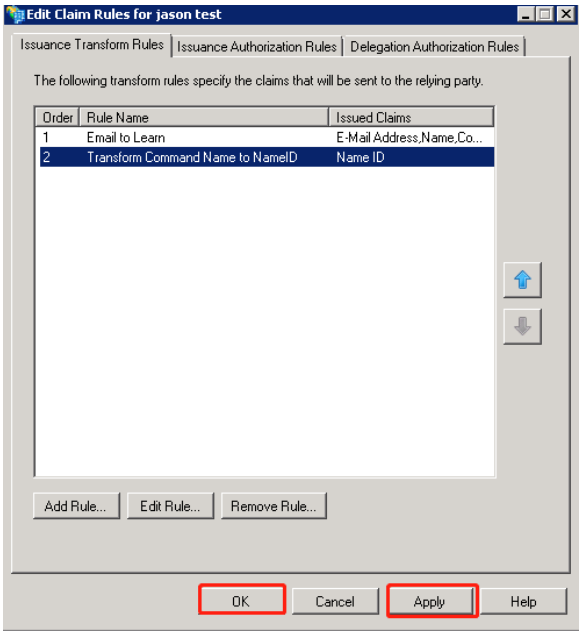
5 *Choose Rule Type*: Select **Transform an Incoming Claim** and click **Next**.



6 *Configure Claim Rule*: Specify a rule name and configure it as below, and then click **Finish**.



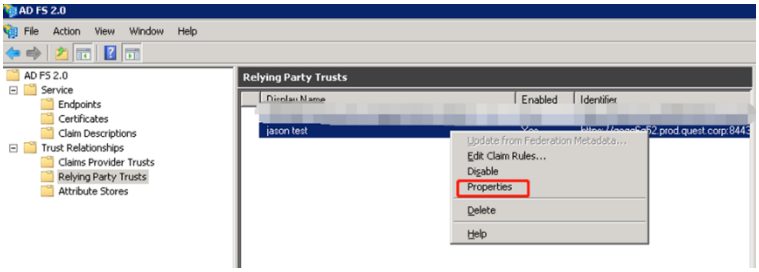
7 Click **Apply** to apply the configuration then click **OK** to close the **Edit Claim Rules** wizard.



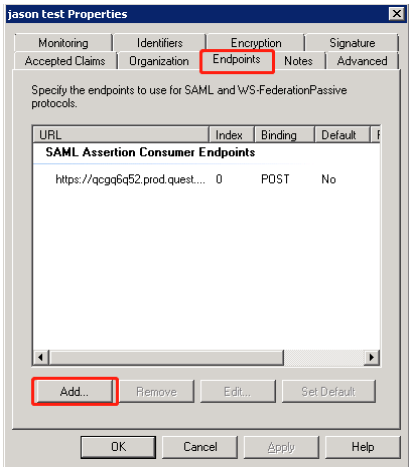
Step 3: Configuring Endpoints

To configure endpoints:

1 Right click the Relying party Trusts item that you added above, and then click **Properties**.



2 Select **Endpoints** on the **Properties** wizard, and then click **Add**.

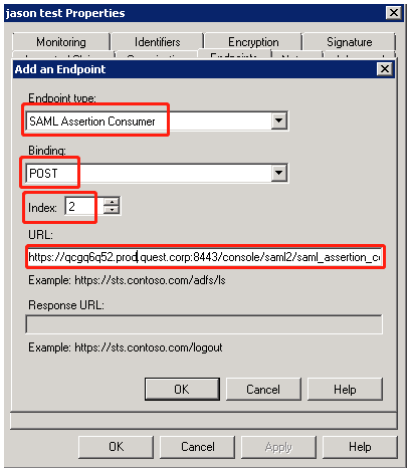


3 You need add two Endpoints, including SAML Assertion Consumer endpoint and SAML Logout endpoint.

a For the URL field of SAML Assertion Consumer endpoint, the value is:

- IP logon: https://<foglight-server-ip>:<foglight-ssl-port>/console/saml2/saml_assertion_consumer
- Host name logon: https://<foglight-server-host-name>:<foglight-ssl-port>/console/saml2/saml_assertion_consumer

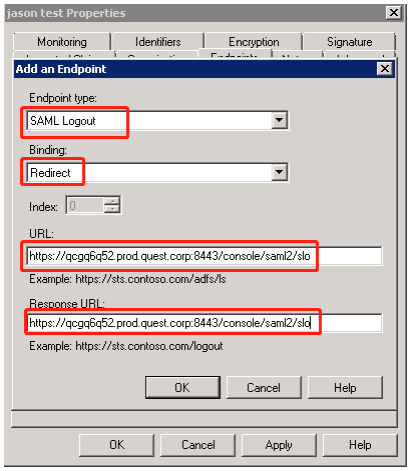
Configure the other fields as below, and then click **OK** when you finish.



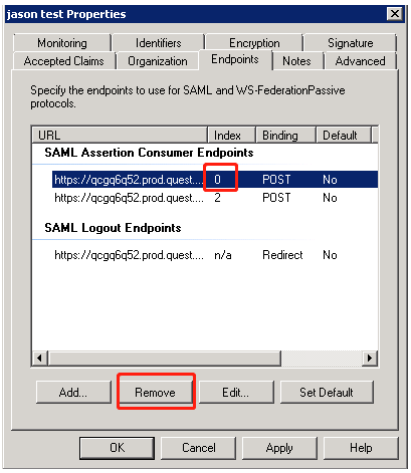
b Both the URL and Response URL fields of SAML Logout endpoint are:

- IP logon: https://<foglight-server-ip>:<foglight-ssl-port>/console/saml2/slo
- Host name logon: https://<foglight-server-host-name>:<foglight-ssl-port>/console/saml2/slo

Configure the other fields as below, and then click **OK** when you finish.



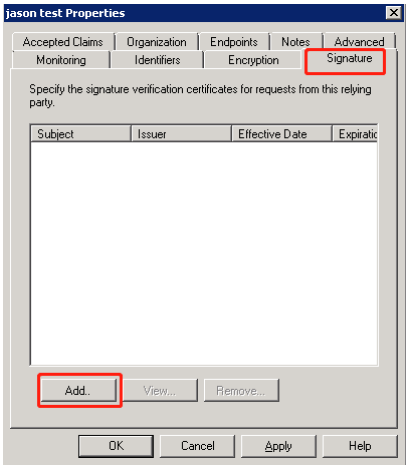
c Select the default **SAML Assertion Consumer Endpoint** which index is 0, and then click **Remove** to delete it.



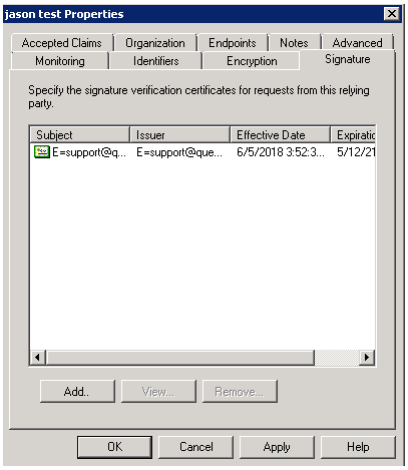
Step 4: Configuring Signature and Hash Algorithm

To configure Signature and Hash algorithm:

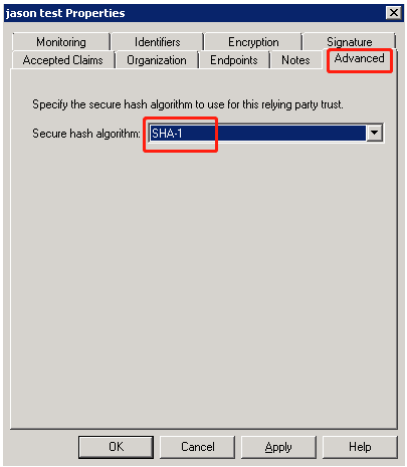
1 Select **Signature** on the **Properties** wizard, and then click **Add**.



2 Add a Foglight server's signature file. You can get a default one from *<foglight-server-directory>/config/sam_certificate.pem* or you can generate your own signature file.



3 After adding the signature file, select **Advanced** and choose **SHA-1** option for the **Secure hash algorithm** field, and then click **Apply**.

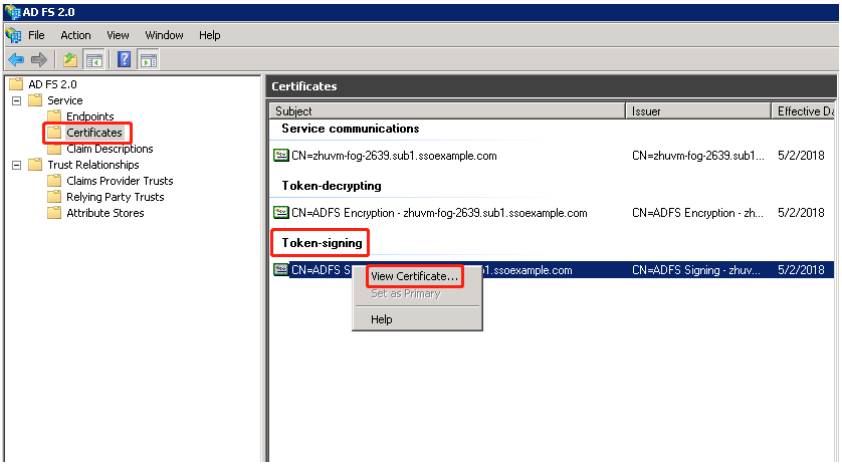


4 Click **OK** to finish the Properties configuration.

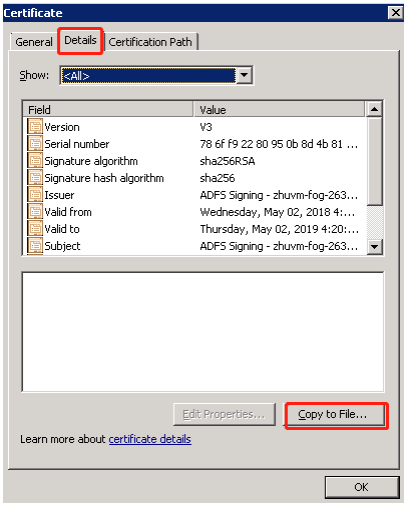
Step 5: Exporting the Certificate

To export the certificate:

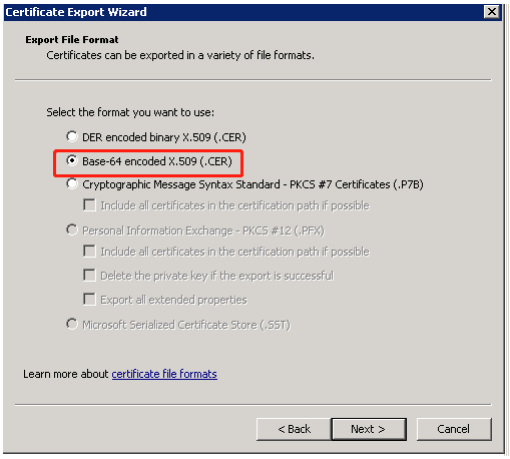
1 Navigate to **Service** > **Certificates** on the ADFS Management Console, right click the **Token-signing** item, and then click **View Certificate**…



2 Select **Details** on the pop-up **Certificate** wizard and click **Copy to File**… to export the certificate which will be used in the following Foglight SAML setup.



3 Select **Base-64 encoded X.509 (.CER)** format as the export file type.



Step 6: Configuring the Trust Relationship

To configure the trust relationship:

1. On the ADFS server machine, run PowerShell as administrator.
2. Run the following command to load the ADFS PowerShell module.

   Add-PSSnapin Microsoft.Adfs.PowerShell
3. Run the following two commands to set up the trust relationship. You need to change the *<relying-party-trust-display-name>* to the **Display Name** of the Relying Party Trust that you have added in Step 1: Adding Relying Party Trust in ADFS.

   - *Set-ADFSRelyingPartyTrust -TargetName <relying-party-trust-display-name> -SigningCertificateRevocationCheck None*
   - *Set-ADFSRelyingPartyTrust -TargetName <relying-party-trust-display-name> -EncryptionCertificateRevocationCheck None*

Step 7: Setting up SAML in Foglight

To set up SAML in the Foglight Management Server:

1. Log into the Foglight Management Server as a Security Administrator.
2. Under **Dashboards**, click **Administration** > **Users & Security** > **SAML 2.0 SSO**. The *SAML 2.0 SSO Configuration* dashboard appears.
3. Click **Edit Settings** and configure the SAML settings as below.

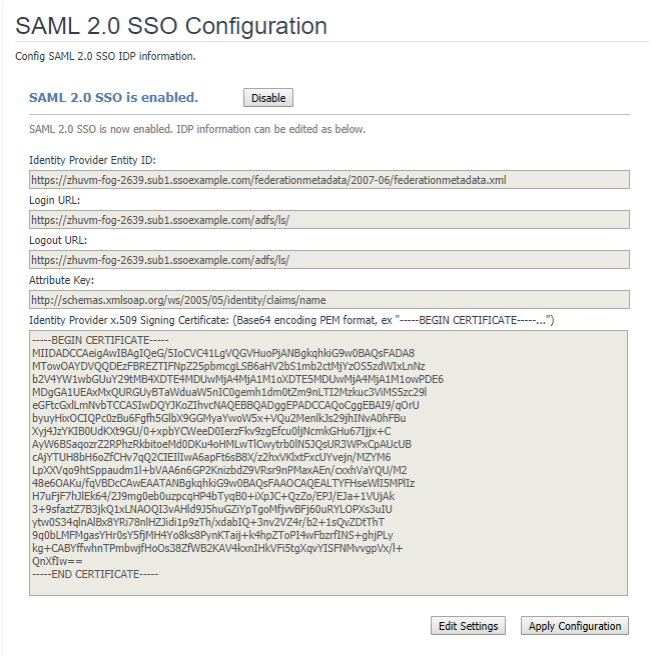
a *Identity Provider Entity ID*: The value should be https://<ADFS_SERVER>/federationmetadata/2007-06/federationmetadata.

b *Login URL:* The value should be https://<ADFS_SERVER>/adfs/ls/.

c *Logout URL*: The value should be https://<ADFS_SERVER>/adfs/ls/.

d *Attribute Key*: It depends on the identity key selected to identity the user. For example it can be http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name.

e *Identity Provider x.509 Signing Certificate*: copy the content of the certificate file which you have exported in Step 5: Exporting the Certificate.



4 Click **Apply Configuration** to save the configuration.

Then configurations of integrating SAML 2.0 SSO with the Foglight Management Server in ADFS are completed.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece – you – to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.