Qualys SAML & Microsoft Active Directory Federation Services Integration

Microsoft Active Directory Federation Services (ADFS) is currently supported for authentication. The Qualys ADFS integration must be configured as SP initiated.

Configuration

Microsoft ADFS 2.0 defaults to values that are incompatible with Qualys SAML 2.0. The following configuration changes will enable Qualys SAML to integrate with your ADFS.

Disable Encryption

ADFS 2.0 automatically configures itself to encrypt token data whenever it receives an encryption certificate from a partner.

Qualys SAML supports encrypted assertions when this option is enabled for your subscription. Please contact Qualys Support or your Technical Account Manager to have support for encrypted assertions enabled.

If you do not have encrypted assertions enabled, then you must turn off encryption in ADFS 2.0 tokens following the steps below.

1) On the ADFS 2.0 computer, click Start > Administrative Tools > Windows PowerShell Modules.

2) At the PowerShell command prompt, type:

   set-ADFSRelyingPartyTrust -TargetName "TFIM SP Example"
   -EncryptClaims $False

3) Hit Enter.

Change ADFS 2.0 Signature Algorithm

When acting as an identity provider, ADFS 2.0 defaults to using the Secure Hash Algorithm 256 (SHA256) to digitally sign assertions sent to relying parties. In addition, in cases where relying parties sign authentication requests, ADFS 2.0 defaults to expecting those requests to be signed using SHA256.

In contrast, Qualys uses the SHA1 algorithm to sign authentication requests and both SHA1 and SHA256 to validate assertions. Follow the steps below to change the algorithm ADFS 2.0 uses with Qualys to the SHA1 algorithm.

How to change the ADFS 2.0 signature algorithm:

1) In the ADFS 2.0 Management console, in the center pane under Relying Party Trusts, right click Qualys SAML, and then click Properties.

2) On the Advanced tab, in the Secure hash algorithm list, select SHA1, and then click OK.
Samples

Below are screenshot examples of an ADFS configured to integrate with Qualys SAML. You may use your proxy system to forward qualys.your_organization.com to your assigned system generated SSO login URL.

Note – If a tab is not shown below then that means the tab was empty or not configured.

Identifiers

The identifier is QualysGuard_SharedPlatform-SAML20-SP, as shown in this example.
Advanced

The URL is based on the Qualys Cloud Platform for your subscription. Click here to learn more.

Endpoints
The trusted URL you enter for the endpoint is based on the Qualys Cloud Platform for your subscription. Tip – You can identify the platform by the separator in your Qualys username. Your username is formatted in this way: 5 letters from your company name followed by a separator (shown in red below), your initials and an increment number.

<table>
<thead>
<tr>
<th>Account Location</th>
<th>URL</th>
<th>Sample Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysguard.qualys.com/IdM/saml2/">https://qualysguard.qualys.com/IdM/saml2/</a></td>
<td>quays_ab1</td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysguard.qg2.apps.qualys.com/IdM/saml2/">https://qualysguard.qg2.apps.qualys.com/IdM/saml2/</a></td>
<td>quays2ab1</td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysguard.qg3.apps.qualys.com/IdM/saml2/">https://qualysguard.qg3.apps.qualys.com/IdM/saml2/</a></td>
<td>quays3ab1</td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysguard.qualys.eu/IdM/saml2/">https://qualysguard.qualys.eu/IdM/saml2/</a></td>
<td>quays-ab1</td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysguard.qg2.apps.qualys.eu/IdM/saml2/">https://qualysguard.qg2.apps.qualys.eu/IdM/saml2/</a></td>
<td>quays5ab1 or quayslab1</td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysguard.qg1.apps.qualys.in/IdM/saml2/">https://qualysguard.qg1.apps.qualys.in/IdM/saml2/</a></td>
<td>quays8ab1</td>
</tr>
<tr>
<td>Private Cloud Platform</td>
<td>https://qualysguard.BASE_URL/IdM/saml2/</td>
<td></td>
</tr>
</tbody>
</table>
**Issuance Transform Rules**

To leverage ADFS for authentication, follow these steps:

1) Click ADFS > Relying Party Trusts > Edit Claim Rule > Add rule.
2) Configure 3 rules as described in the sections that follow.
3) Click Apply and OK.
Rule #1 – Send Email Address

Choose Rule Type > Claim Rule Template > Send LDAP Attributes as Claims.

Configure the rule as follows:
Claim rule name = Send Email Address
Attribute store = Active Directory
LDAP Attribute = E-mail-Addresses
Outgoing Claim Type = E-mail Address
Rule #2 – Send qualysguard_external_id

Choose Rule Type > Claim Rule Template > Transform an Incoming Claim.

Configure the rule as follows:
Claim rule name = Send qualysguard_external_id
Incoming claim type = E-mail Address
Outgoing claim type = qualysguard_external_id (Needs to be manually entered)
Rule #3 – Send Name ID

Choose Rule Type > Claim Rule Template > Transform an Incoming Claim.

Configure the rule as follows:
Claim rule name = Send NameID
Incoming claim type = E-mail Address
Outgoing claim type = Name ID
Outgoing name ID format = Transient Identifier

Last updated: March 11, 2019