QualysGuard SAML & Microsoft Active Directory Federation Services Integration

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

Configuration

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

Disable encryption

AD FS 2.0 automatically configures itself to encrypt token data whenever it receives an encryption certificate from a partner. Turn off encryption in ADFS 2.0 tokens.

To disable encryption:

1. On the AD FS 2.0 computer, click Start > Administrative Tools > Windows PowerShell Modules.
2. At the PowerShell command prompt, type:
   ```bash
   set-ADFSRelyingPartyTrust -TargetName "TFIM SP Example" -EncryptClaims $False
   ```
3. Hit Enter.

Change AD FS 2.0 Signature Algorithm

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

In contrast, QualysGuard uses the SHA-1 algorithm to sign authentication requests and validate assertions. Follow the steps below to change the algorithm AD FS 2.0 uses with QualysGuard to the SHA-1 algorithm.

To change the AD FS 2.0 signature algorithm

1. In the AD FS 2.0 Management console, in the center pane under Relying Party Trusts, right-click QualysGuard SAML, and then click Properties.
2. On the Advanced tab, in the Secure hash algorithm list, select SHA-1, and then click OK.

Screenshots

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

Note: Tabs with no screenshot means they were empty or un-configured.
Identifiers:

**Qualys - Vuln Mgmt Properties**

Specify the display name and identifiers for this relying party trust.

- **Display name:**
  - Qualys - Vuln Mgmt

- **Relying party identifier:**
  - Example: https://fs.contoso.com/adfs/services/trust
  - QualysGuard_SharedPlatform-SAML20-SP

[Buttons: OK, Cancel, Apply, Help]
Encryption:

Specify the encryption certificate for this relying party trust.

Encryption certificate:

Issuer:
Subject:
Effective date:
Expiration date:

[Buttons: Browse, View, Remove]
Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: **SHA**
Endpoints:

```
Endpoints:

SAML Assertion Consumer Endpoints
https://qualysguard.qualys.com/idM/saml2/  0  POST
```

Specify the endpoints to use for SAML and WS-FederationPassive protocols.
Edit Endpoint:

Endpoint type: SAML Assertion Consumer

Binding: POST

Index: 0

URL:
https://qualysguard.qualys.com/IdM/saml2/
Example: https://sts.conlso.com/adfs/ls

Response URL:
Example: https://sts.conlso.com/logout

[OK] [Cancel] [Help]
Issuance Transform Rules:

The following transform rules specify the claims that will be sent to the relying party.

<table>
<thead>
<tr>
<th>Order</th>
<th>Rule Name</th>
<th>Issued Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Send Email Address</td>
<td>E-Mail Address</td>
</tr>
<tr>
<td>2</td>
<td>Send qualysguard_external_id</td>
<td>qualysguard_external_id</td>
</tr>
<tr>
<td>3</td>
<td>Send NameID</td>
<td>Name ID</td>
</tr>
</tbody>
</table>

Add Rule...  Edit Rule...  Remove Rule...  OK  Cancel  Apply  Help
Edit Rule -- Send Email Address:

**Edit Rule - Send Email Address**

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: **Send Email Address**

Rule template: Send LDAP Attributes as Claims

Attribute store: **Active Directory**

Mapping of LDAP attributes to outgoing claim types:

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail Addresses</td>
<td>E-Mail Address</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
Edit Rule -- Send NameID:

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Send NameID

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-MailAddresses</td>
<td>Name ID</td>
</tr>
</tbody>
</table>

View Rule Language...  OK  Cancel  Help
Edit Rule -- Send ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Send qualysguard_external_id

Rule template: Transform an Incoming Claim

- Incoming claim type: E-Mail Address
- Incoming name ID format: Unspecified
- Outgoing claim type: qualysguard_external_id
- Outgoing name ID format: Unspecified

- Pass through all claim values
- Replace an incoming claim value with a different outgoing claim value
  - Incoming claim value: 
  - Outgoing claim value: Browse...
- Replace incoming e-mail suffix claims with a new e-mail suffix
  - New e-mail suffix: Example: fabrik-am.com

[View Rule Language... OK Cancel Help]