

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

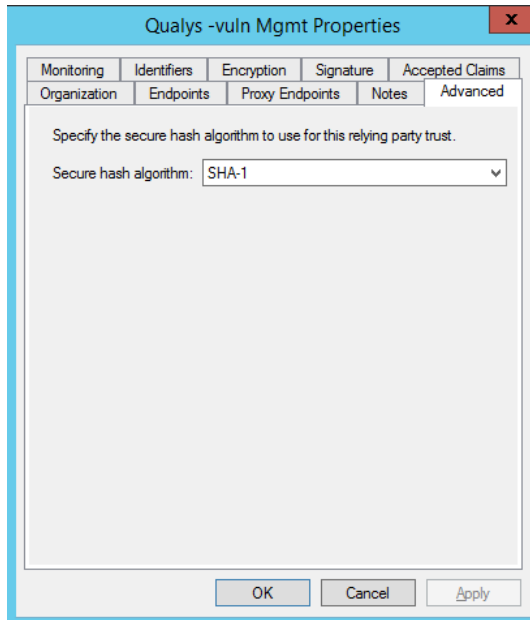
The identifier is QualysGuard_SharedPlatform-SAML20-SP, as shown in this example.

The screenshot shows the 'Qualys -vuln Mgmt Properties' dialog box with the 'Identifiers' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs: 'Organization', 'Endpoints', 'Proxy Endpoints', 'Notes', 'Advanced', 'Monitoring', 'Identifiers', 'Encryption', 'Signature', and 'Accepted Claims'. The 'Identifiers' tab is active, showing the text 'Specify the display name and identifiers for this relying party trust.' Below this, there is a 'Display name:' label and a text box containing 'Qualys -vuln Mgmt'. There is a 'Relying party identifier:' label and an empty text box, with an 'Add' button to its right. Below that is an 'Example:' label with the text 'https://fs.contoso.com/adfs/services/trust'. There is a 'Relying party identifiers:' label and a list box containing 'QualysGuard_SharedPlatform-SAML20-SP', with a 'Remove' button to its right. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Encryption

The screenshot shows the 'Qualys -vuln Mgmt Properties' dialog box with the 'Encryption' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs: 'Organization', 'Endpoints', 'Proxy Endpoints', 'Notes', 'Advanced', 'Monitoring', 'Identifiers', 'Encryption', 'Signature', and 'Accepted Claims'. The 'Encryption' tab is active, showing the text 'Specify the encryption certificate for this relying party trust.' Below this, there is an 'Encryption certificate:' label and a text box containing 'Issuer:', 'Subject:', 'Effective date:', and 'Expiration date:'. There are 'Browse...', 'View...', and 'Remove' buttons below the text box. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Advanced



Qualys -vuln Mgmt Properties

Monitoring Identifiers Encryption Signature Accepted Claims
Organization Endpoints Proxy Endpoints Notes Advanced

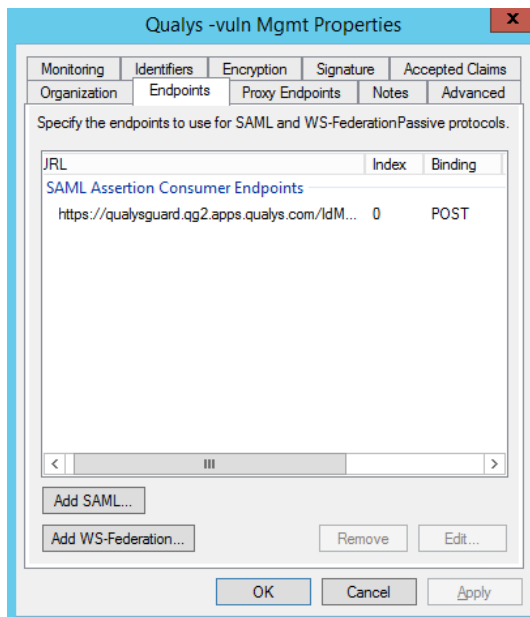
Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

OK Cancel Apply

Endpoints

The URL is based on the Qualys Cloud Platform for your subscription. [Click here](#) to learn more.



Qualys -vuln Mgmt Properties

Monitoring Identifiers Encryption Signature Accepted Claims
Organization Endpoints Proxy Endpoints Notes Advanced

Specify the endpoints to use for SAML and WS-Federation Passive protocols.

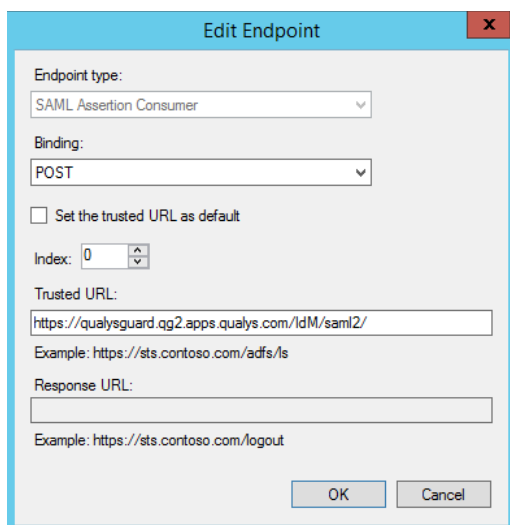
| JRL | Index | Binding |
|--|-------|---------|
| SAML Assertion Consumer Endpoints | | |
| https://qualysguard.qg2.apps.qualys.com/IdM... | 0 | POST |

< III >

Add SAML... Add WS-Federation... Remove Edit...

OK Cancel Apply

Edit Endpoint



Edit Endpoint

Endpoint type:
SAML Assertion Consumer

Binding:
POST

☐ Set the trusted URL as default

Index: 0

Trusted URL:
https://qualysguard.qg2.apps.qualys.com/IdM/saml2/
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

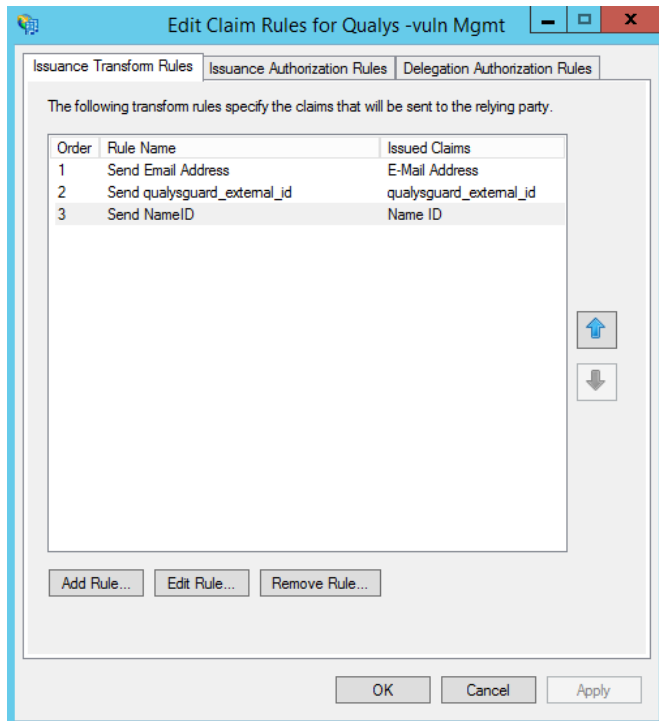
The trusted URL you enter for the endpoint is based on the Qualys Cloud Platform for your subscription. Tip – You can identify the platform by the separator in your Qualys username. Your username is formatted in this way: 5 letters from your company name followed by a separator (shown in **red** below),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

| Account Location | URL | Sample Username |
|-------------------------|--|------------------------|
| Qualys US Platform 1 | https://qualysguard.qualys.com/IdM/saml2/ | quays_ab1 |
| Qualys US Platform 2 | https://qualysguard.qg2.apps.qualys.com/IdM/saml2/ | quays2ab1 |
| Qualys US Platform 3 | https://qualysguard.qg3.apps.qualys.com/IdM/saml2/ | quays3ab1 |
| Qualys EU Platform 1 | https://qualysguard.qualys.eu/IdM/saml2/ | quays-ab1 |
| Qualys EU Platform 2 | https://qualysguard.qg2.apps.qualys.eu/IdM/saml2/ | quays5ab1 or quays!ab1 |
| Qualys India Platform 1 | https://qualysguard.qg1.apps.qualys.in/IdM/saml2/ | quays8ab1 |
| Private Cloud Platform | https://qualysguard.BASE_URL/IdM/saml2/ | |

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

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | E-Mail-Addresses | 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)

Edit Rule - Send qualysguard_external_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:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

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

Edit Rule - Send NameID

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:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Last updated: March 11, 2019