How to Integrate StoreFront 2.6 and NetScaler Gateway for Pass-through Access with SAML Authentication through Microsoft AD FS
Contents

1. Requirements ....................................................................................................................................................................3
2. Configuration .....................................................................................................................................................................4
3. Issues Seen During Implementation .................................................................................................................................21
1. Requirements

- XenApp and Web Interface servers must be domain members
- Only as of December 2014, XenApp 6.5 is supported
- XenApp XML service must be running with IIS on the XenApp farm. This is because Kerberos authentication is done by IIS on the user's behalf
- StoreFront 2.6 or later must be used
- StoreFront must not be installed on a Domain Controller
- StoreFront must have a SSL certificate installed and configured
- Active Directory domain functional level must be 2003 or 2008
- Single Forest and Single Domain used in this example
- Additional services such as network file shares, login scripts, and network printers will need additional Kerberos delegation configuration which is not covered in this document
- NetScaler, Microsoft AD FS, and StoreFront must all have their time in sync. It is recommended that they all use the same NTP server to guarantee this behavior
2. Configuration

2.1. Active Directory Configuration

- Delegation must be configured for XenApp and StoreFront servers.
- StoreFront must delegate http service to all XML servers.
- The XenApp server then must delegate http and host service to themselves and host and http service to all XenApp servers.
- Each XenApp server must also delegate cifs and ldap services to the Domain Controllers.
2.2. StoreFront Configuration

1. Create a store for Kerberos authentication.

2. Define the XenApp 6.5 servers with their fully qualified domain name (FQDN). This cannot be its IP address or any other DNS alias.

3. Enable Kerberos Delegation for Delivery Controllers.

**Note:** “Subnet IP address” is the IP configured on NetScaler for the NetScaler Gateway virtual server. It is not the NATed public/private IP, and it has to be the actual IP address configured.

5. Ensure Remote Access is configured with the preceding Gateway configuration.
6. Locate the file `C:\Program Files\Citrix\Receiver\StoreFront\Services\ProtocolTransitionService\AccessList.txt` and add domain users/groups that should have access to this functionality.

7. Restart StoreFront server after creating and configuring the store/site.
2.3. XenApp Configuration

Each XenApp server must trust XML requests which can be configured in a server policy as follows:
2.4. NetScaler Configuration

1. Import SSL certificate from AD FS server for its Token-Signing Certificate.
2. Create SSL certificate by referencing the previously imported certificate.
3. Create Session Profile and specify Web Receiver URL with **https** and server Fully Qualified Domain Name (FQDN).

4. Create Session Policy and link it to be Session Profile.
5. Create SAML authentication server.

**Note:** Signing Certificate Name is an optional configuration. When not configured on NetScaler, do not configure it on AD FS. In this example, the signing certificate is an already installed server certificate on the NetScaler. It must be installed on the AD FS server as well and referenced in the **Signature** tab. The issuer name is the subject name of the certificate being used.
6. Create SAML authentication policy and link to the preceding profile.

```
Create Authentication SAML Policy

Name*
adfs2012

Authentication Type
SAML

Server*
adfs2012

Expression*
ns_true
```

7. Link authentication and session policy to the NetScaler Gateway virtual server.

```
Authentication SAML Policy

VPN Virtual Server
Basic Settings

Name: accesss-dev
IP Address: 192.168.1.234
Port: 4443

NetScaler Gateway Session Policy

Priority | Policy Name
---------|------------
0         | adfs2012

Expression: REQ.HTTP.HEADER User-Agent NOT CONTAINS Client
```
8. Ensure that proper STAs have been configured on the NetScaler Gateway virtual server.

2.5. AD FS Configuration

1. Export Token-Signing Certificate with its private key (used in Step 1, NetScaler Configuration).

2. Adjust SSO lifetime and Service Identifier as required.

3. Create a Relying Party Trust.
4. Select the radio button to enter data manually.

![Enter data about the relying party manually](image1)

Use this option to manually input the necessary data about this relying party organization.

5. Choose a display name.

![Add Relying Party Trust Wizard](image2)

Specify Display Name

Steps: Welcome, Select Data Source, Specify Display Name

Display name: NetScalpel

Notes:

6. Choose profile type (in this example, AD FS profile was chosen).

![Choose Profile](image3)

Steps: Welcome, Select Data Source, Specify Display Name, Choose Profile

Choose Profile

- AD FS profile: This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.
- AD FS 1.0 and 1.1 profile: This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

7. If encryption is needed, enter certificate information (in this example, it was not used).

![Configure Certificate](image4)

Steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate

Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

Issuer: [box]
Subject: [box]
Effective date: [box]
Expiry date: [box]

View... Browse... Remove...
8. Leave all options unchecked under Configure URL.

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

- Enable support for the WS-Federation Passive protocol
  
The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

  Relying party WS-Federation Passive protocol URL:

  Example: https://fs.contoso.com/adfs/ls/

- Enable support for the SAML 2.0 WebSSO protocol

  The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

  Relying party SAML 2.0 SSO service URL:

  Example: https://www.contoso.com/adfs/ls/

9. Enter Relying Party Identifier, which is the FQDN of the AD FS server being used. An example would be adfs.company.com
10. Do not configure Multi-factor.

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

<table>
<thead>
<tr>
<th>Multi-factor Authentication</th>
<th>Global Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Users/Groups</td>
</tr>
<tr>
<td>Device</td>
<td>Location</td>
</tr>
<tr>
<td>Not configured</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

I do not want to configure multi-factor authentication settings for this relying party trust at this time.

11. Choose to permit all users to use this relay or configure it later using authorization rules (in this example, Permit all is selected).

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party’s issuance authorization rules.

- Permit all users to access this relying party
  The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

- Deny all users access to this relying party
  The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
12. Click **Next**.

13. Leave **Open the Edit Claim Rules**... unchecked and click **Close**.
14. Go to the properties of the newly created relaying party trust and click the **Signature** tab. Import the certificate, which is mentioned on the NetScaler SAML server profile, if configured.

15. Click the **Endpoints** tab and add an SAML endpoint where the trusted URL is the FQDN of the Access Gateway virtual server and /cgi/samlauth.

16. Click **OK** to close all dialog boxes.
17. Go to NetScaler Relaying Party trust and select **Edit Claim Rules**.

18. Add the following rule:

19. Click **OK** to close all dialog boxes.
3. Issues Seen During Implementation

While launching a published application the user would start the session, logon to the server, but the server would quickly report “Access is denied” before displaying the application. The same user would be able to log on through RDP or through an explicit logon to StoreFront. This issue is currently under investigation but to get around the problem the registry DWORD *IgnoreRegUserConfigErrors* was created under *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server*.