Sentry SSO with ADFS

Contents

- 1 Configuring ADFS Support for Sentry
    - 1.1 Introduction
    - 1.2 Requirements
    - 1.3 Configuration Procedure
        - 1.3.1 In Swivel Core
        - 1.3.2 In Swivel Sentry
            - 1.3.2.1 Edit settings.properties
            - 1.3.2.2 Application settings
            - 1.3.2.3 Certificates
            - 1.3.2.4 In ADFS Management
                - 1.3.2.4.1 Claims Provider Trust
        - 1.3.3 Disable Active Directory Authentication
        - 1.3.4 Implement Sentry Authentication Selectively

Configuring ADFS Support for Sentry

Introduction

This article describes how to configure an ADFS server to use Sentry to replace the standard Active Directory authentication. This allows a suitably configured environment to support Swivel authentication for Office 365, for example.

Requirements

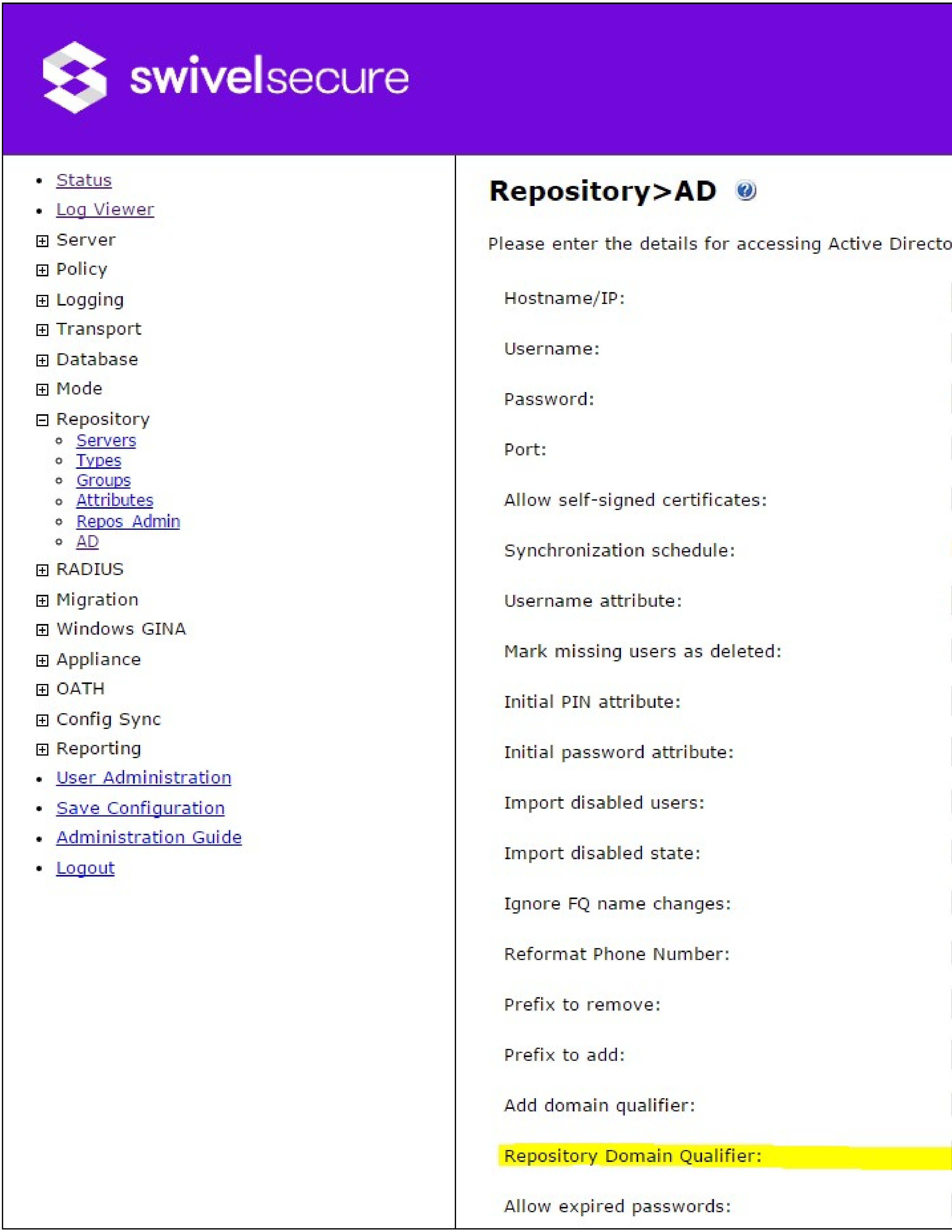
ADFS integration requires version 4.x of Sentry.

Configuration Procedure

In Swivel Core

ADFS requires the username to be in the format domain\username. To do this, you need to create a Swivel attribute that includes the prefix.

In the Swivel admin console, under the repository details for the relevant AD repository, set the domain qualifier to be the short-form domain name, followed by "\" - don't forget the backslash at the end.



Repository>AD

Please enter the details for accessing Active Directo

Hostname/IP:

Username:

Password:

Port:

Allow self-signed certificates:

Synchronization schedule:

Username attribute:

Mark missing users as deleted:

Initial PIN attribute:

Initial password attribute:

Import disabled users:

Import disabled state:

Ignore FQ name changes:

Reformat Phone Number:

Prefix to remove:

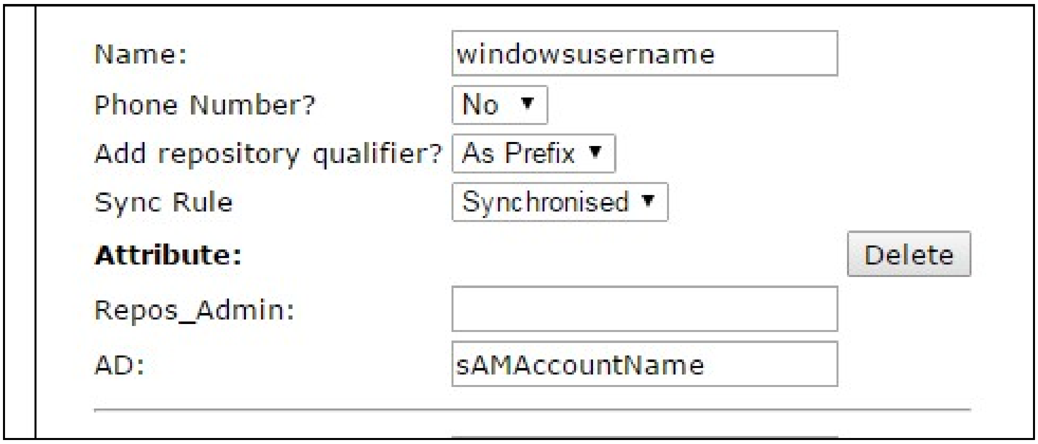
Prefix to add:

Add domain qualifier:

Repository Domain Qualifier:

Allow expired passwords:

Under Repository -> Attributes, create an attribute - for example, call it "windowsaccountname". In the definition for the AD repository, put the AD attribute name "sAMAccountName", and under domain qualifier, select "As Prefix".



Name: windowsusername

Phone Number? No

Add repository qualifier? As Prefix

Sync Rule Synchronised

Attribute:

Repos_Admin:

AD: sAMAccountName

Finally, synchronise the AD repository, to ensure that all users have an attribute in the form domain\username.

In Swivel Sentry

Edit settings.properties

NOTE: this step is not usually necessary when using version 4.0.3 or later: the correct settings are chosen automatically for ADFS, and can be overridden in the configuration anyway. This assumes that you have added a domain prefix to the repository, and have created an attribute that uses it.

This file is located under /home/swivel/.swivel/sentry on an appliance. Check the following entries:

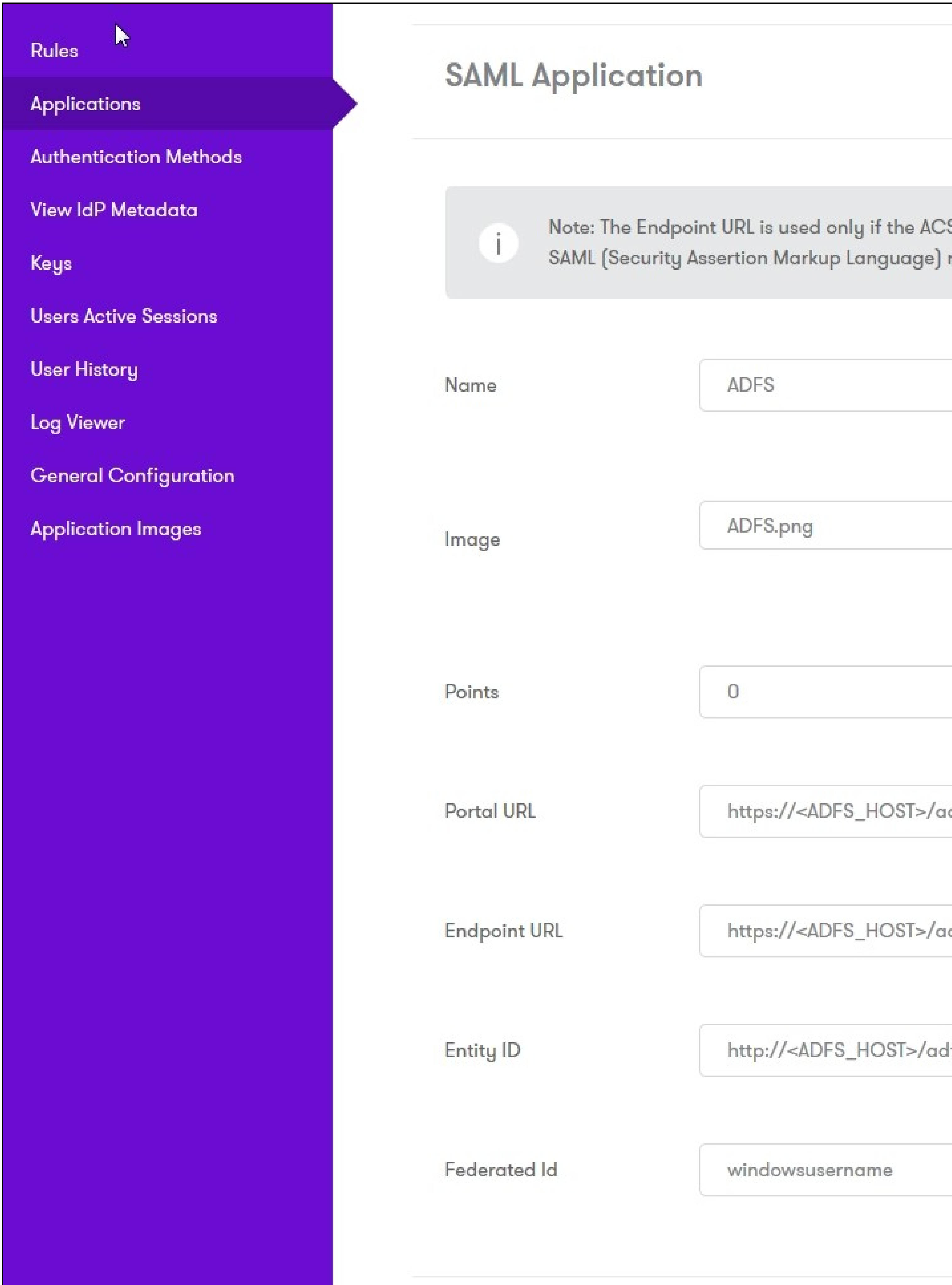
- certificateIssuer ? this must be in the form of a valid URI. It is recommended that you use the public URL of Sentry, but it doesn?t have to be a real web location.
- windowsaccountnamefield=username. This configures the Swivel attribute field to be used to import the username for ADFS. If you have configured a prefixed attribute above, use the name of that attribute. Otherwise, use an attribute mapped to sAMAccountName without a prefix, and set the prefix below. This latter option is the only possibility for Swivel version 3.10.5 or earlier.
- windowsdomainprefix=domain. This configures the domain name to be prefixed to the ADFS username. If the attribute above already has a prefix, this should be blank. If not, make sure the ?\? is included. Do not set a prefix if your attribute is already prefixed.

Application settings

In the Sentry admin console, create a new application with the following settings:

- Service Provider = ADFS
- Endpoint URL = https://<ADFS_HOST>/adfs/ls/
- Entity ID = http://<ADFS_HOST>/adfs/services/trust

Replace <ADFS_HOST> with the public host name of your ADFS server / proxy. Other than that, the format should not be changed: Endpoint URL should have a / on the end, Entity ID should not. Also, note that Entity ID starts with "http", **NOT** "https".



SAML Application

Note: The Endpoint URL is used only if the ACS
SAML (Security Assertion Markup Language) r

Name	ADFS
Image	ADFS.png
Points	0
Portal URL	https://<ADFS_HOST>/ad
Endpoint URL	https://<ADFS_HOST>/ad
Entity ID	http://<ADFS_HOST>/ad
Federated Id	windowsusername

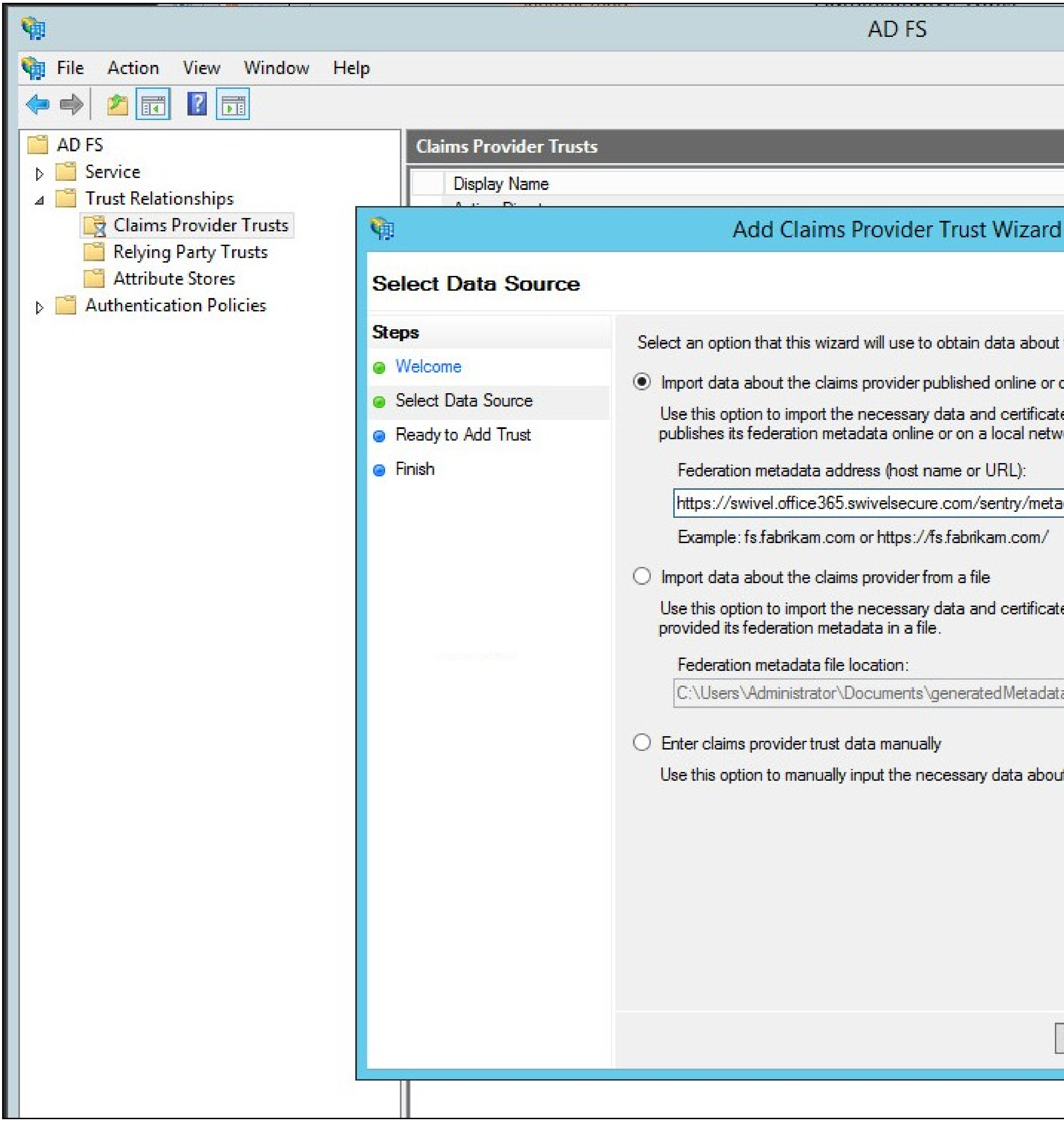
Certificates

Ensure that you generate a certificate for Sentry that is current.

In ADFS Management

Claims Provider Trust

Create a new Claims provider trust.



Select Data Source

Steps
- Welcome
- Select Data Source
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about

● Import data about the claims provider published online or o

Use this option to import the necessary data and certificate publishes its federation metadata online or on a local netw

Federation metadata address (host name or URL):

https://swivel.office365.swivelsecure.com/sentry/meta

Example: fs.fabrikam.com or https://fs.fabrikam.com/

○ Import data about the claims provider from a file

Use this option to import the necessary data and certificate provided its federation metadata in a file.

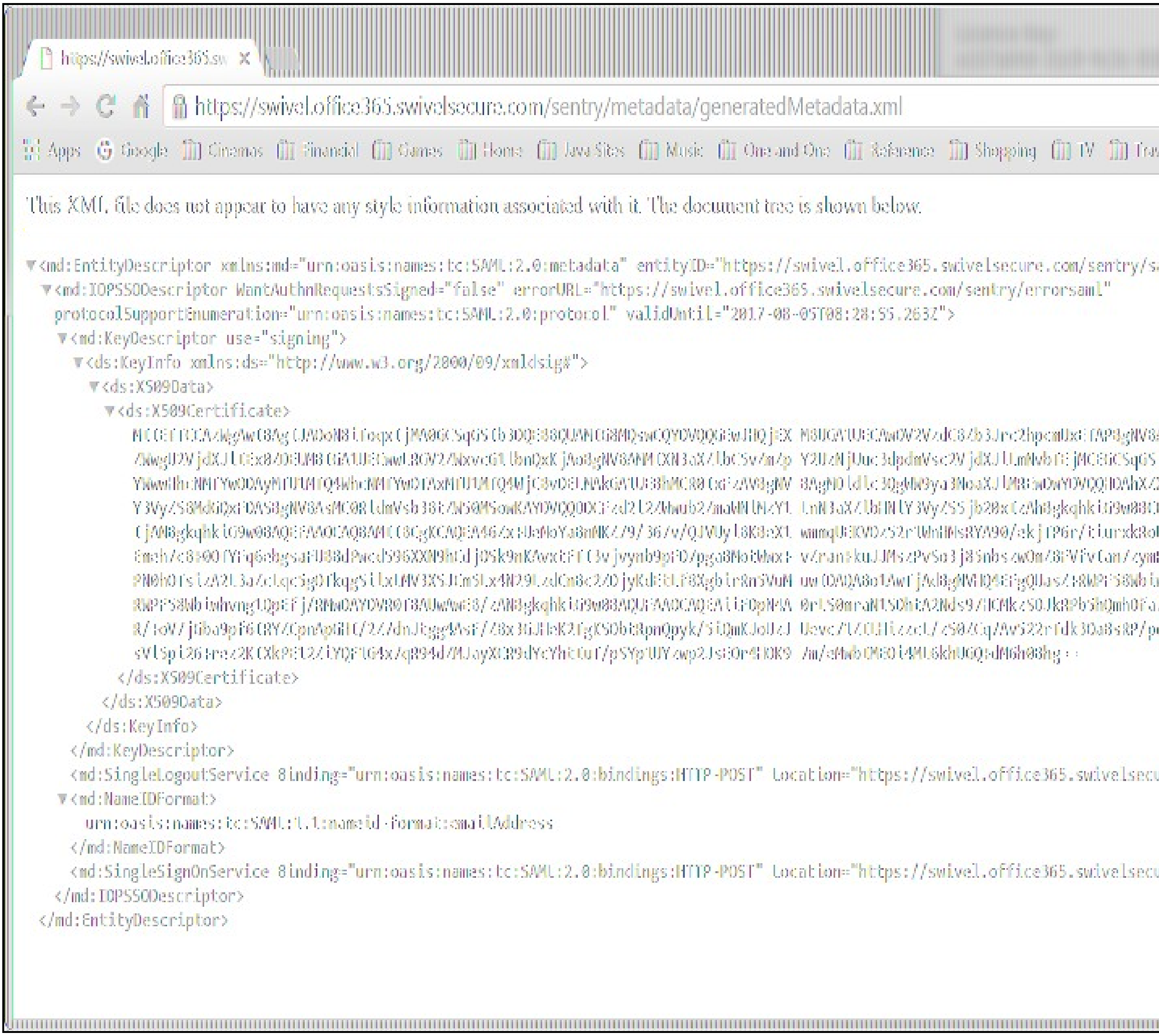
Federation metadata file location:

C:\Users\Administrator\Documents\generatedMetadat

○ Enter claims provider trust data manually

Use this option to manually input the necessary data about

If you can import the metadata directly from the Sentry URL: that is simplest, but it may not work, due to SSL handshaking issues. In which case, download the metadata to a file



https://swivel.office365.sw ×
https://swivel.office365.swivelsecure.com/sentry/metadata/generatedMetadata.xml
Apps
Google
Cinemas
Financial
Games
Home
Java Sites
Music
One and One
Reference
Shopping
TV
Trav

This XML file does not appear to have any style information associated with it. The document tree is shown below.

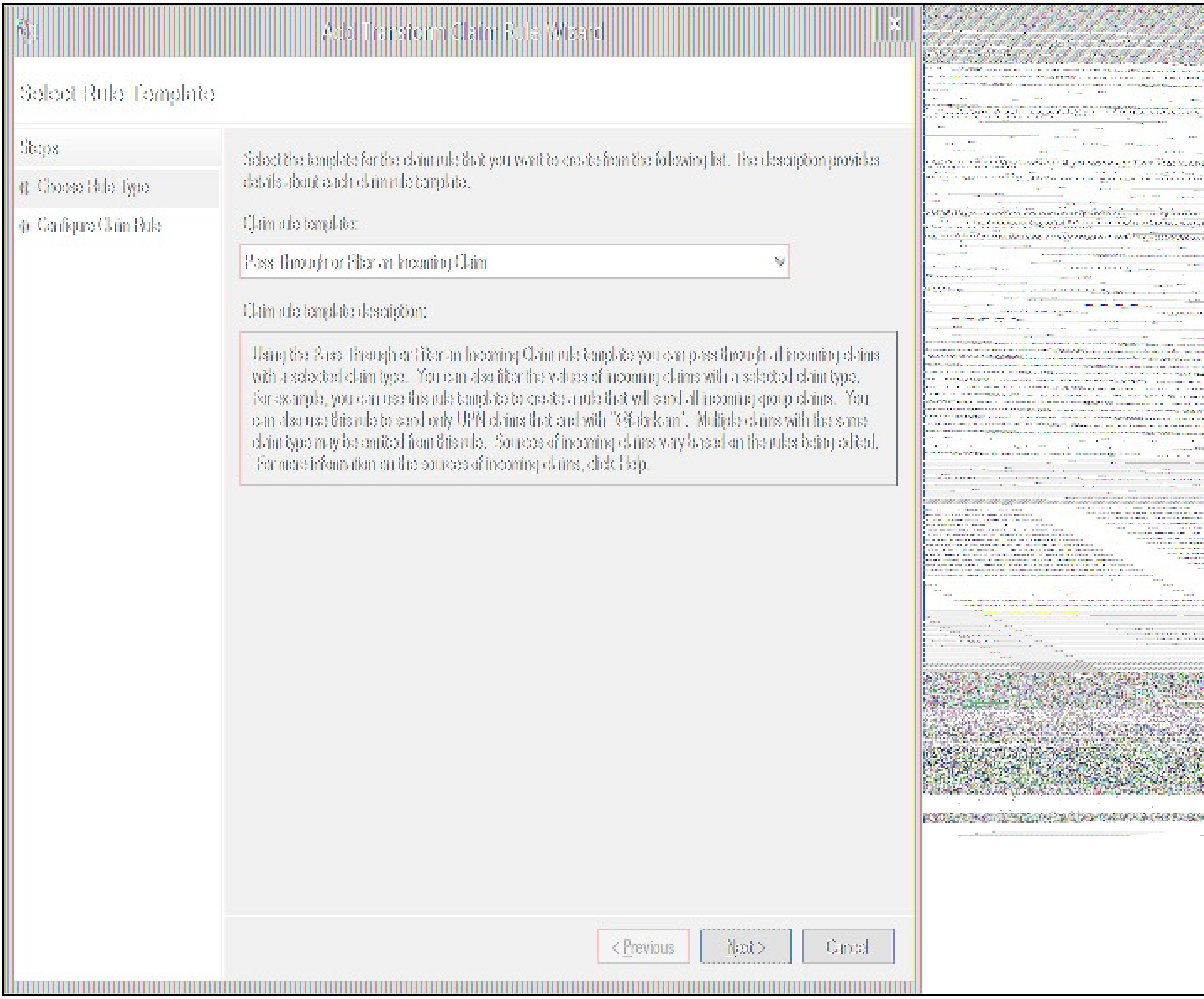
```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://swivel.office365.swivelsecure.com/sentry/s
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" errorURL="https://swivel.office365.swivelsecure.com/sentry/errorsaml"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" validUntil="2017-08-05T08:28:55.263Z">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
          ▼<ds:X509Certificate>
              MIIEFTCCAv2gAwIBAgIJAOoN8iToqxCjMA0GCSqGSIb3DQEBBQUAMIGBMQswCQYDVQQGEwJHQjEX MBUGA1UECAwOV2VzdCBZb3Jrc2hpcmUxETAPBgNVBA
              /AwgU2VjdXJlIExBZDEUMBIGA1UECwwLRGV2ZWxvcG1lbnQxKjAoBgNVBAMMIXN3aXZlbC5vZmZp Y2UzNjUuc3dpdmVsc2VjdXJlLmNvbTEjMCEGCSqGS
              YWwwHhcNMTYwODAyMTU1MTQ4WhcNMTYwOTAxMTU1MTQ4WjCBvDELMAkGA1UEBhMCR0IxFzAVBgNV BAgMDldlc3QgWW9ya3NoaXJlMREwDwYDVQQHDAhXZ
              Y3VyZSBMdGQxFDASBgNVBAsMC0RldmVsb3BtZW50MSowKAYDVQQDDCFzd2l2ZWwub2ZmaWNlMzY1 LnN3aXZlbHNlY3VyZS5jb20xIzAhBgkqhkiG9w0BC
              CjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA46/xHUoMoYa8nMKZ/9/36/v/QJVUyl8K8eXl wmmqUEKVDz52rWnHMsRYA90/ekjIP6r/tiurxkRo
              Emeh/c8+00fYFq6ebgsaFU88dPwcd596XXN9hCdjOSk9nKAvxtFfC3vjvynb9pFD/pga8MotWwx+ v/ran+kuJJMszPvSo3j8Snbs/wOm/8FVfvCan/zym
              PN0hOTsIzA2L3a/cLqcig0TkqgSilxLMV3XSJCm5Lx4N29LzdCm8c2/DjyKdEELf8Xgbir8n5VuM uwIDAQABo1AwTjAdBgNVHQ4EFgQUasZ+RWPF58Wbi
              RWPF58WbiwhvngUQpEfj/8MwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAiLFOpNKA 0rLS0mraN1SOhtA2Nds9/ICMkzS0Jk8Pb5hQmh0fa
              8/+oV/jUba9pf6CRYZCpnApGHC/2Z/dnJtgg4AsF/Z8x3GJHeK2fgKSObtRpnQpyk/5iQmKJoUzJ Uevc/UZCHizzcL/zS0ZCq/Av522rfdk3Oa8s8P/p
              sVlSpi26+rez2KCXkPEl2ZiYQFtG4x/qR94d/MJayXCR9dYcYhtCuf/pSYpUYzwp2Js+Or4HOK9 /m/eMwbCMEOi4MU6khUGQ+dM6h08hg==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://swivel.office365.swivelsecu
  ▼<md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://swivel.office365.swivelsecu
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

and import the settings from that file.

Once you have created the new trust, you will be given the opportunity to add claim rules:

Claim Rules:

Create two rules using the template ?Pass Through or Filter an Incoming Claim?, as follows:



Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

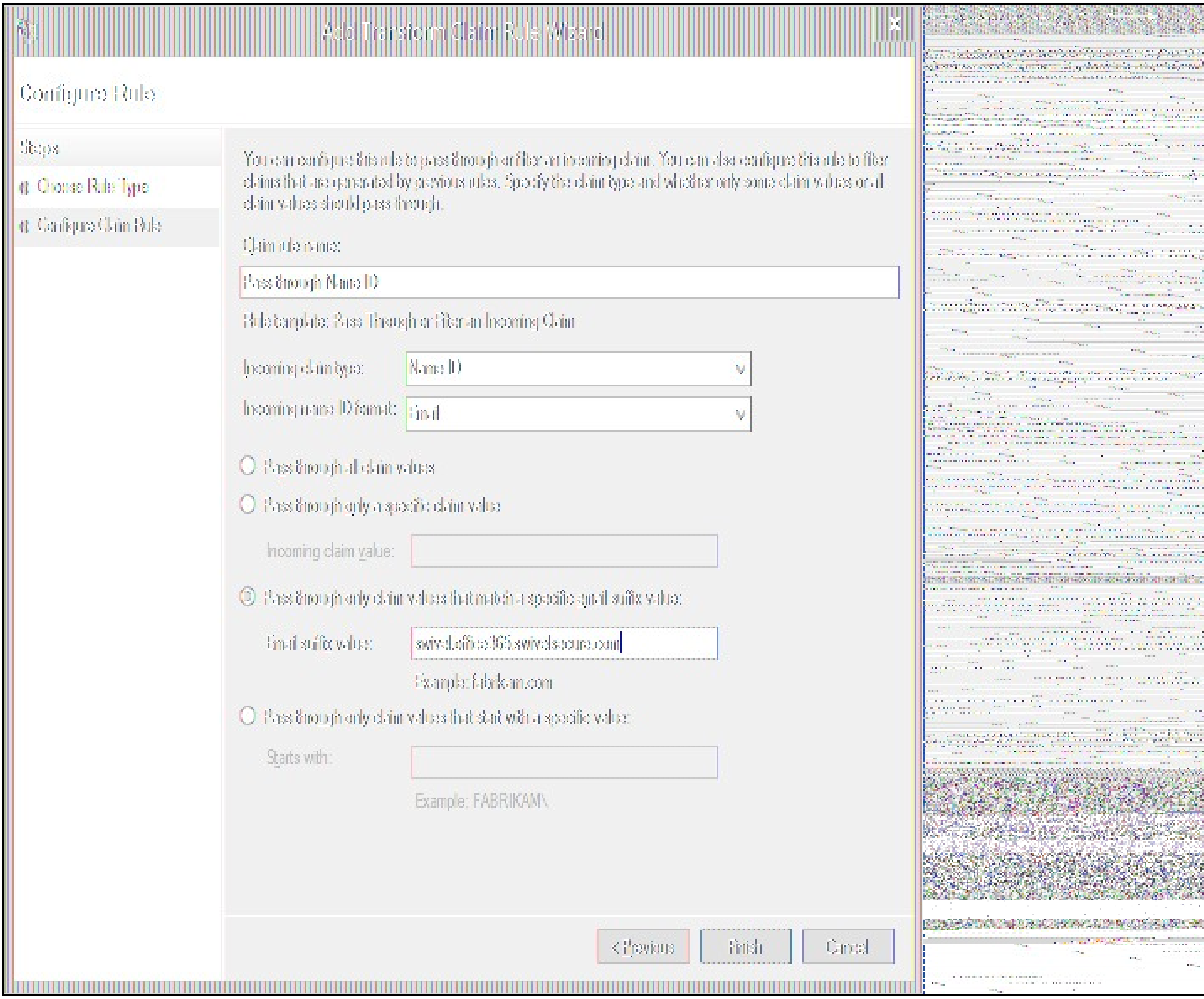
Claim rule template:

Pass Through or Filter an Incoming Claim

Claim rule template description:

Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

- Incoming claim type = Name ID: it is recommended that you specify the format as Email, and only pass through claims matching your domain suffix.



Configure Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Pass through Name ID

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Name ID

Incoming name ID format: Email

○ Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

● Pass through only claim values that match a specific email suffix value:

Email suffix value: swivel.office365.swivelsecure.com

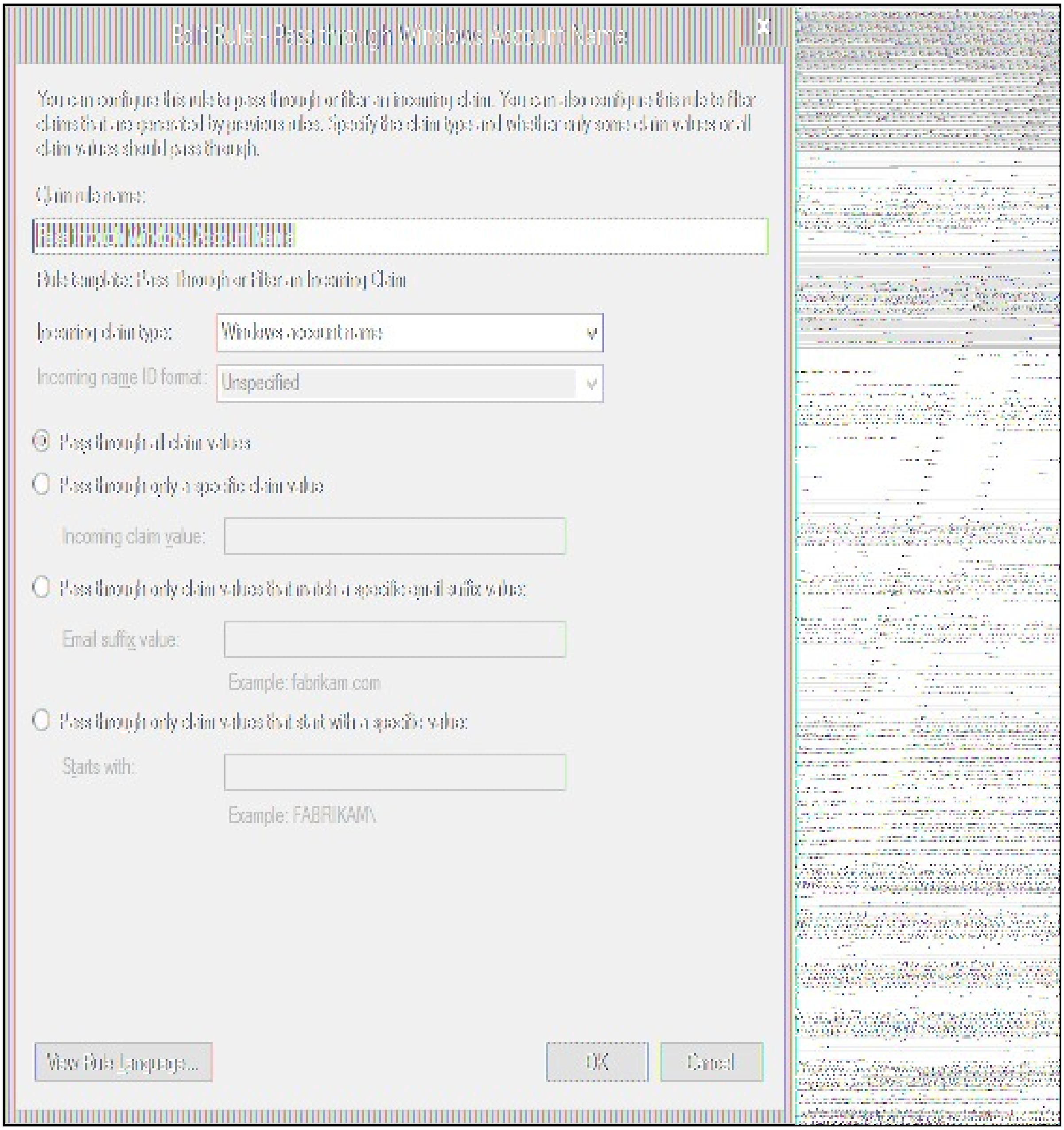
Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

- Incoming claim type = Windows Account Name. There is no need to specify any other restrictions on this claim rule.



Edit Rule - Pass through Windows Account Name

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Pass through Windows account name

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format: Unspecified

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

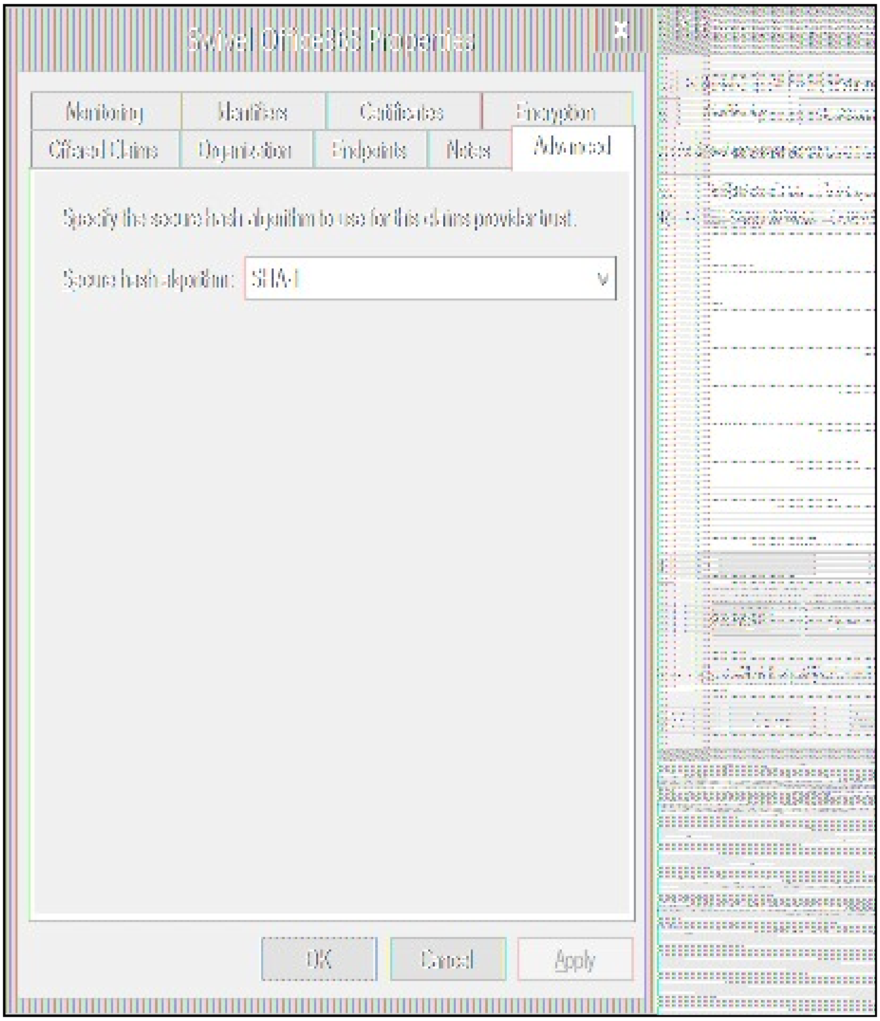
Starts with:

Example: FABRIKAM\

Settings:

You will need to edit the properties of this trust:

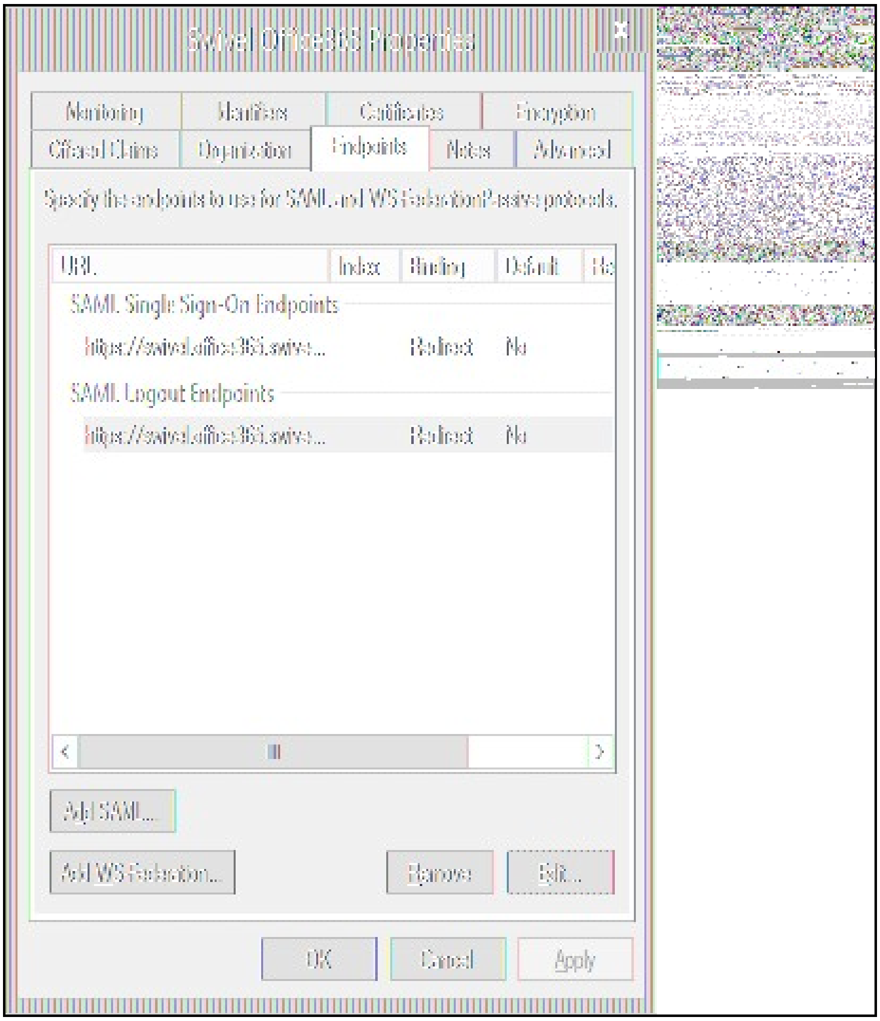
- Under Advanced, Secure hash algorithm must match the signing algorithm for the Sentry certificate. Version 4 supports SHA-256, but if you have an older version of Sentry SSO, you must select SHA-1.



Specify the secure hash algorithm to use for this claims provider trust.

Secure hash algorithm: SHA-1

- Under Endpoints, there should be two endpoints configured.

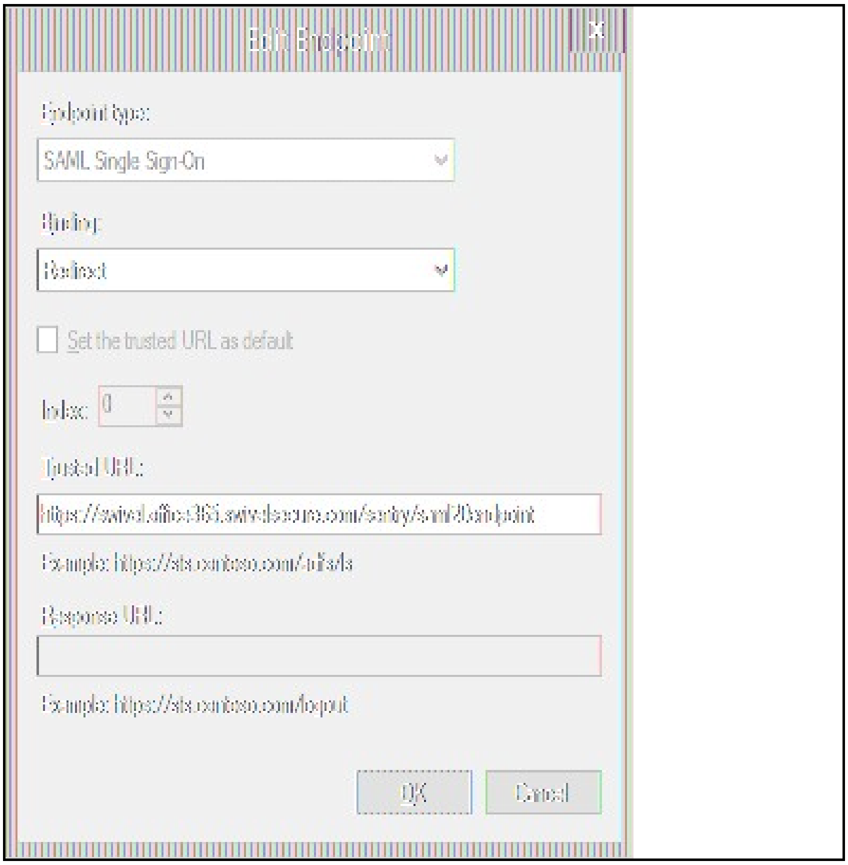


Specify the endpoints to use for SAML and WS-Federation Passive protocols.

URL	Index	Binding	Default	Re
SAML Single Sign-On Endpoints				
https://swivel.office365.swivel...		Redirect	No	
SAML Logout Endpoints				
https://swivel.office365.swivel...		Redirect	No	

If not, create them as follows. If they have been created, check that they match the following. Both are SAML endpoints:

- Endpoint Type = SAML Single Sign-On, Binding = redirect, Trusted URL = https://<sentry_URL>/sentry/saml20endpoint



Edit Endpoint

Endpoint type:

SAML Single Sign-On

Binding:

Redirect

□ Set the trusted URL as default

Index: 0

Trusted URL:

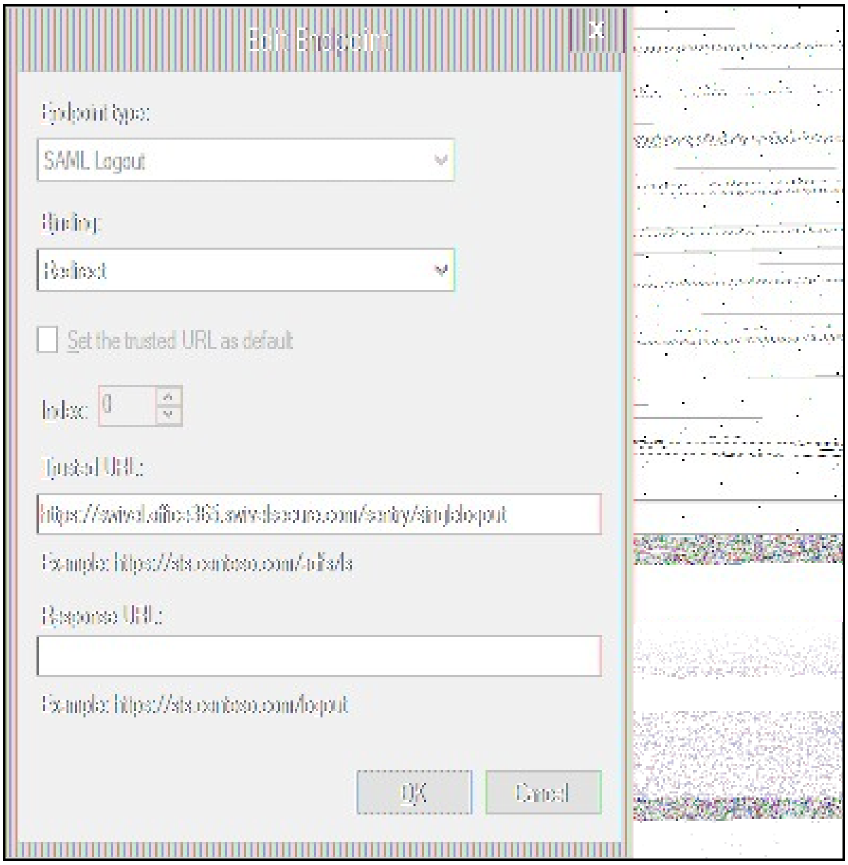
https://swivel.office365.swivelsecure.com/sentry/saml20endpoint

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

Response URL:

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

- Endpoint Type = SAML Logout, Binding = redirect, Trusted URL = https://<sentry_URL>/sentry/singlelogout, Response URL = https://<sentry_URL>/sentry/singlelogout



Edit Endpoint

Endpoint type:

SAML Logout

Binding:

Redirect

□ Set the trusted URL as default

Index: 0

Trusted URL:

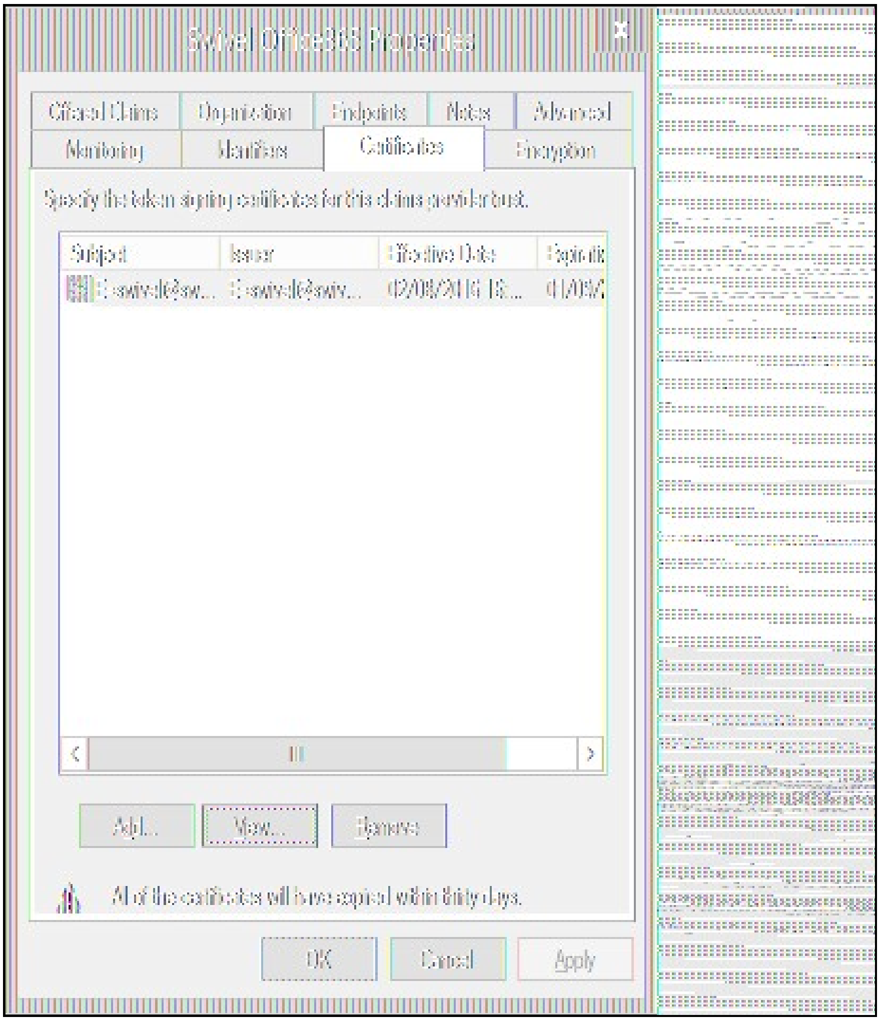
https://swivel.office365.swivelsecure.com/sentry/singlelogout

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

Response URL:

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

- Under Certificates,

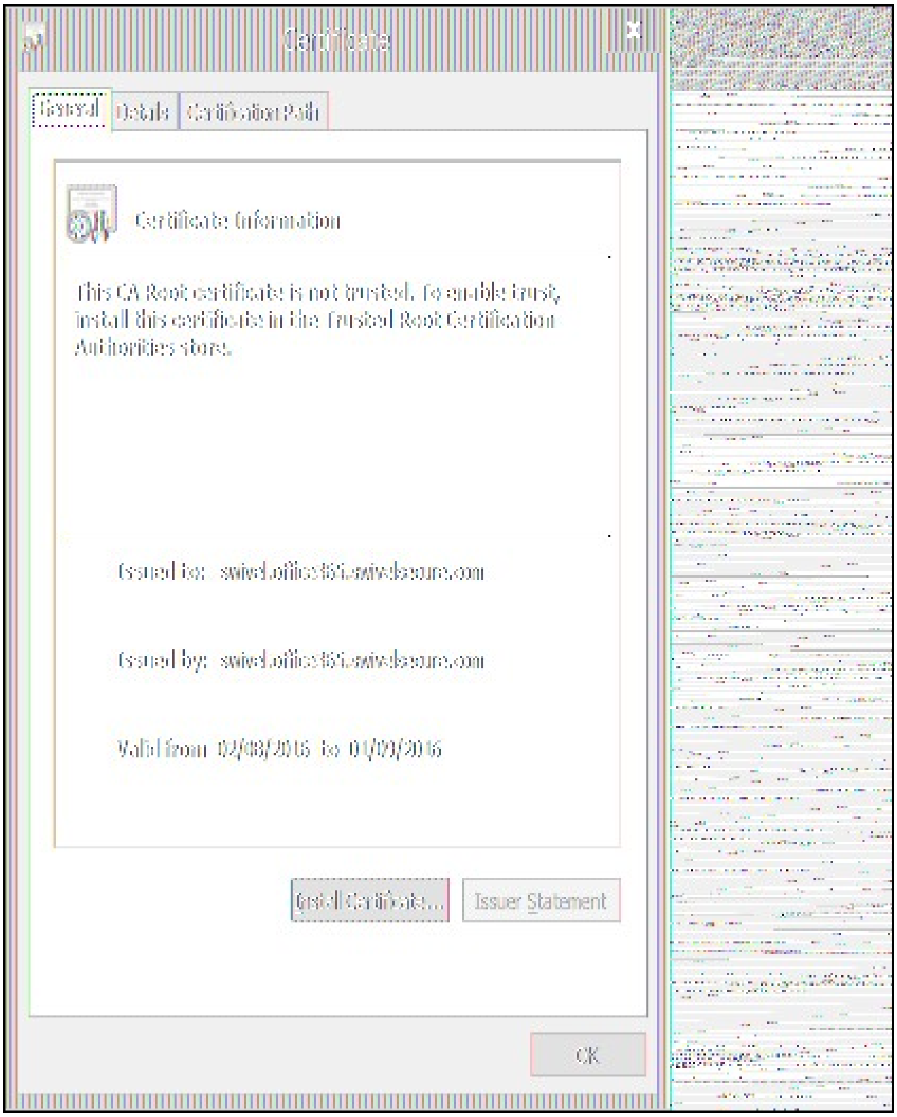


Specify the token signing certificates for this claims provider trust.

Subject	Issuer	Effective Date	Expiratio
E=swivel@sw...	E=swivel@swiv...	02/08/2016 16:...	01/08/

All of the certificates will have expired within thirty days.

view the imported certificate,



Certificate Information

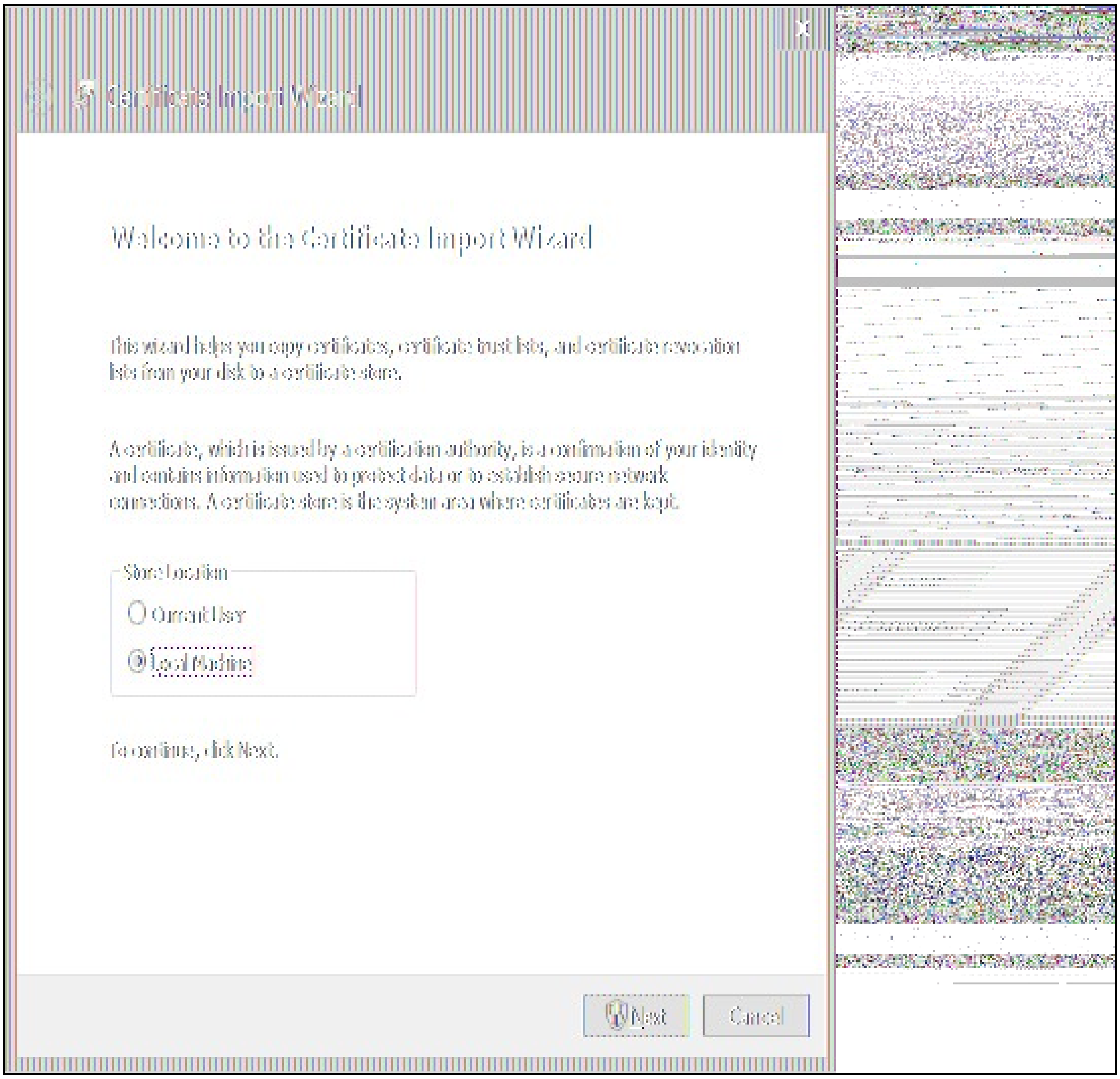
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: swivel.office365.swivelsecure.com

Issued by: swivel.office365.swivelsecure.com

Valid from 02/08/2016 to 01/09/2016

then click on **Install Certificate**.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

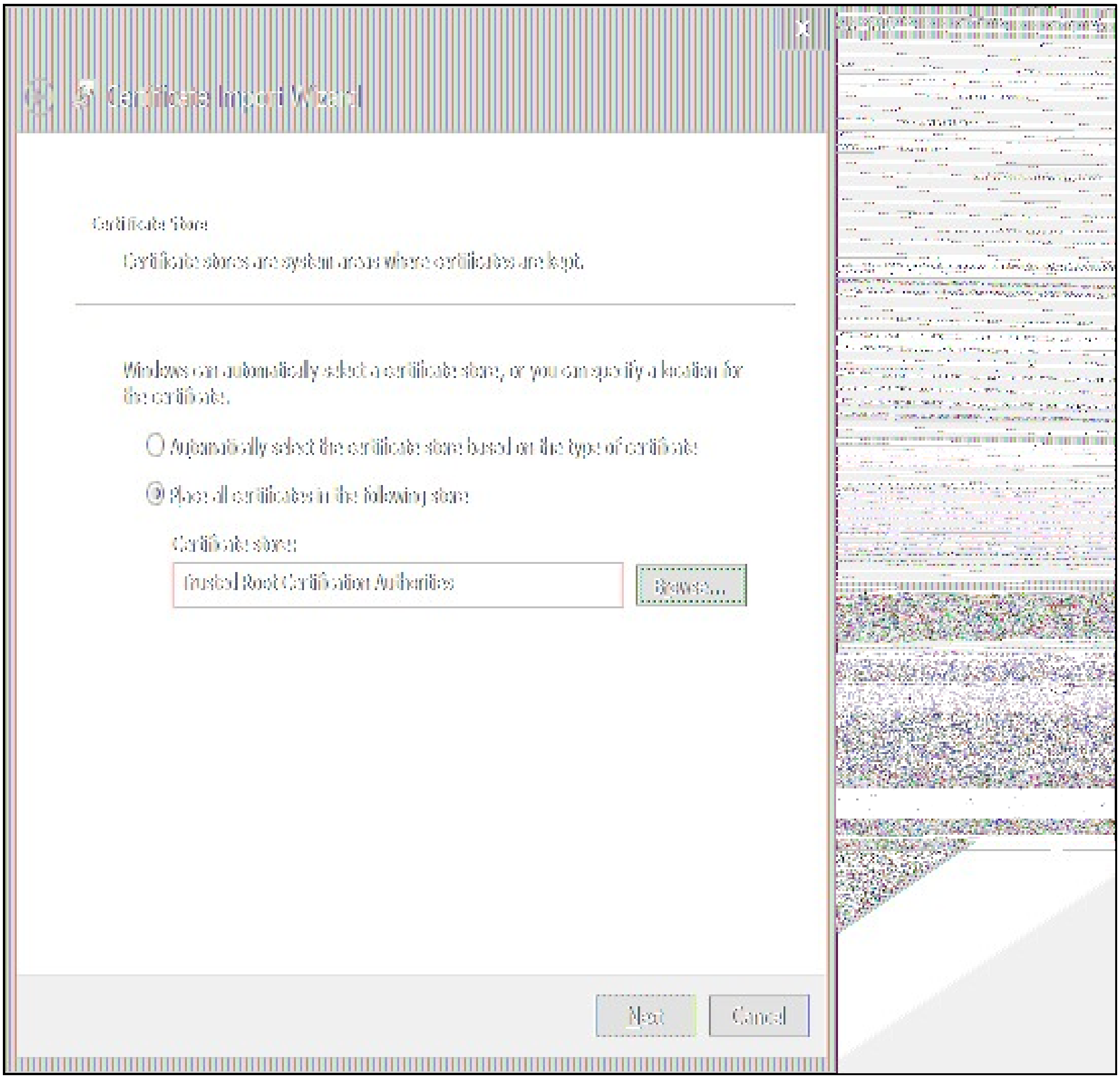
Store Location

○ Current User

● Local Machine

To continue, click Next.

Select **Local Machine** on the next page,



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

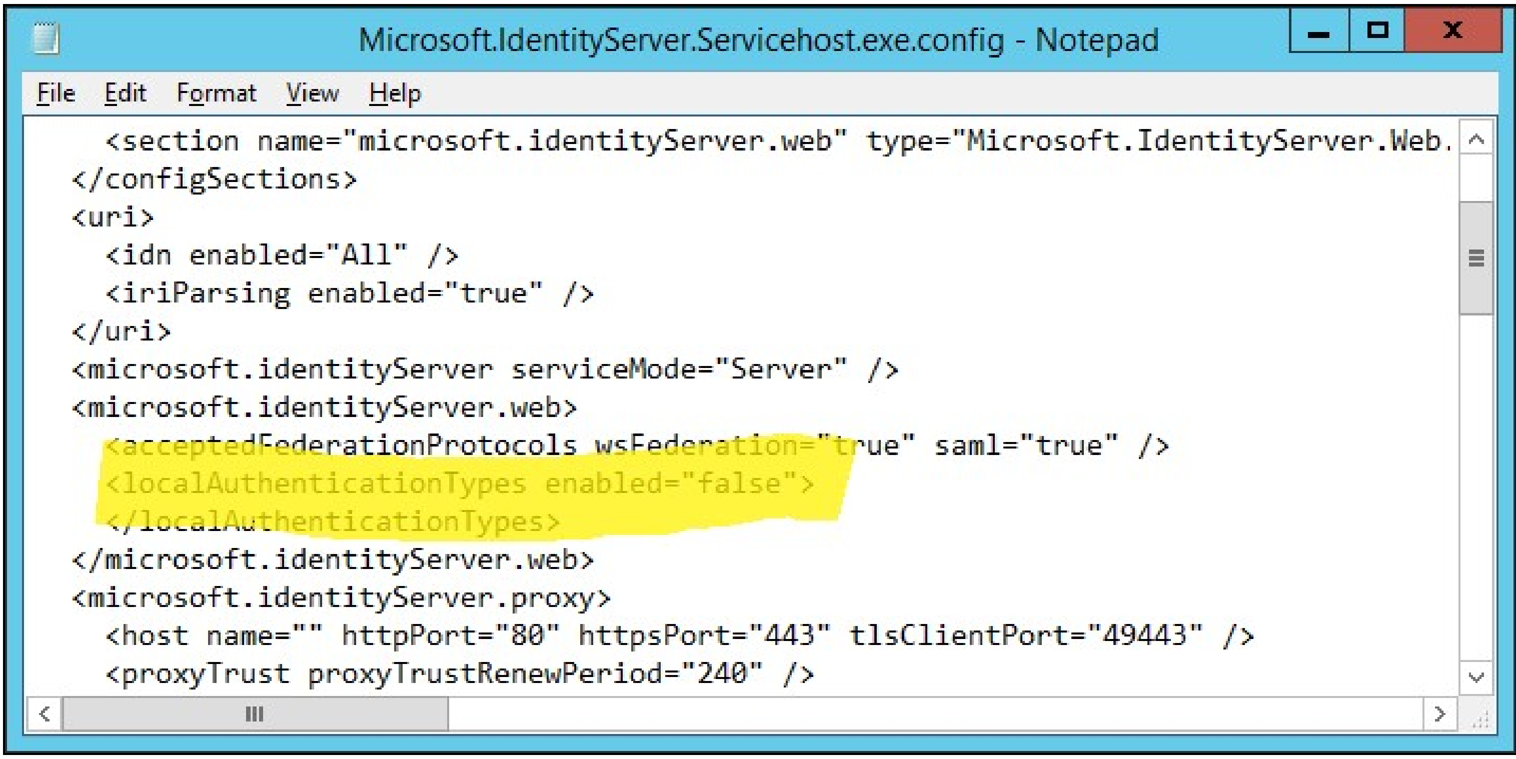
and on the following page, **Place all certificates in the following store**. Browse and select **Trusted Root Certification Authorities**.

Disable Active Directory Authentication

As ADFS is currently configured, you will now have a choice of Active Directory or Swivel authentication. To disable Active Directory authentication:

- Edit C:\Windows\ADFS\Microsoft.IdentityServer.Servicehost.exe.config.

Note that you must open your text editor (for example Notepad) as administrator, or you will not be able to save the changes.


Microsoft.IdentityServer.Servicehost.exe.config - Notepad
File Edit Format View Help

```
    <section name="microsoft.identityServer.web" type="Microsoft.IdentityServer.Web.
  </configSections>
  <uri>
    <idn enabled="All" />
    <iriParsing enabled="true" />
  </uri>
  <microsoft.identityServer serviceMode="Server" />
  <microsoft.identityServer.web>
    <acceptedFederationProtocols wsFederation="true" saml="true" />
    <localAuthenticationTypes enabled="false">
    </localAuthenticationTypes>
  </microsoft.identityServer.web>
  <microsoft.identityServer.proxy>
    <host name="" httpPort="80" httpsPort="443" tlsClientPort="49443" />
    <proxyTrust proxyTrustRenewPeriod="240" />
```

- Search for ?<localAuthenticationTypes? and set enabled to ?false?.
- Restart ADFS.

Implement Sentry Authentication Selectively

If you don't want to use Sentry authentication for all ADFS applications, or in all scenarios, you can use the PowerShell cmdlets to control it. Some examples are given in the following link:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/home-realm-discovery-customization

Potentially the most useful scenarios would be to bypass Sentry for intranet login:

```
Set-AdfsProperties -IntranetUseLocalClaimsProvider $true
```

or to use Sentry for selected relying parties only:

```
Set-AdfsRelyingPartyTrust -TargetName "Office 365" -ClaimsProviderName @("Sentry SSO")
```