Sentry SSO with ADFS

Contents

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.

swivelsecure

-
- Log Viewer
- ⊞ Server
- ⊞ Policy
- ⊞ Logging
- ⊞ Transport
- ⊞ Database
- ⊞ Mode
- ⊟ Repository
  - ○ Servers
  - ○ Types
  - ○ Groups
  - ○ Attributes
  - ○ Repos_Admin
  - ○ AD
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Windows GINA
- ⊞ Appliance
- ⊞ OATH
- ⊞ Config Sync
- ⊞ Reporting
- User Administration
- Save Configuration
- Administration Guide
- Logout

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".

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".

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application

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

Name	ADFS

Image	ADFS.png

Points	0

Portal URL	https://<ADFS_HOST>/ac

Endpoint URL	https://<ADFS_HOST>/ac

Entity ID	http://<ADFS_HOST>/adf

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.

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

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:

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

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.

< Previous   Next >   Cancel

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

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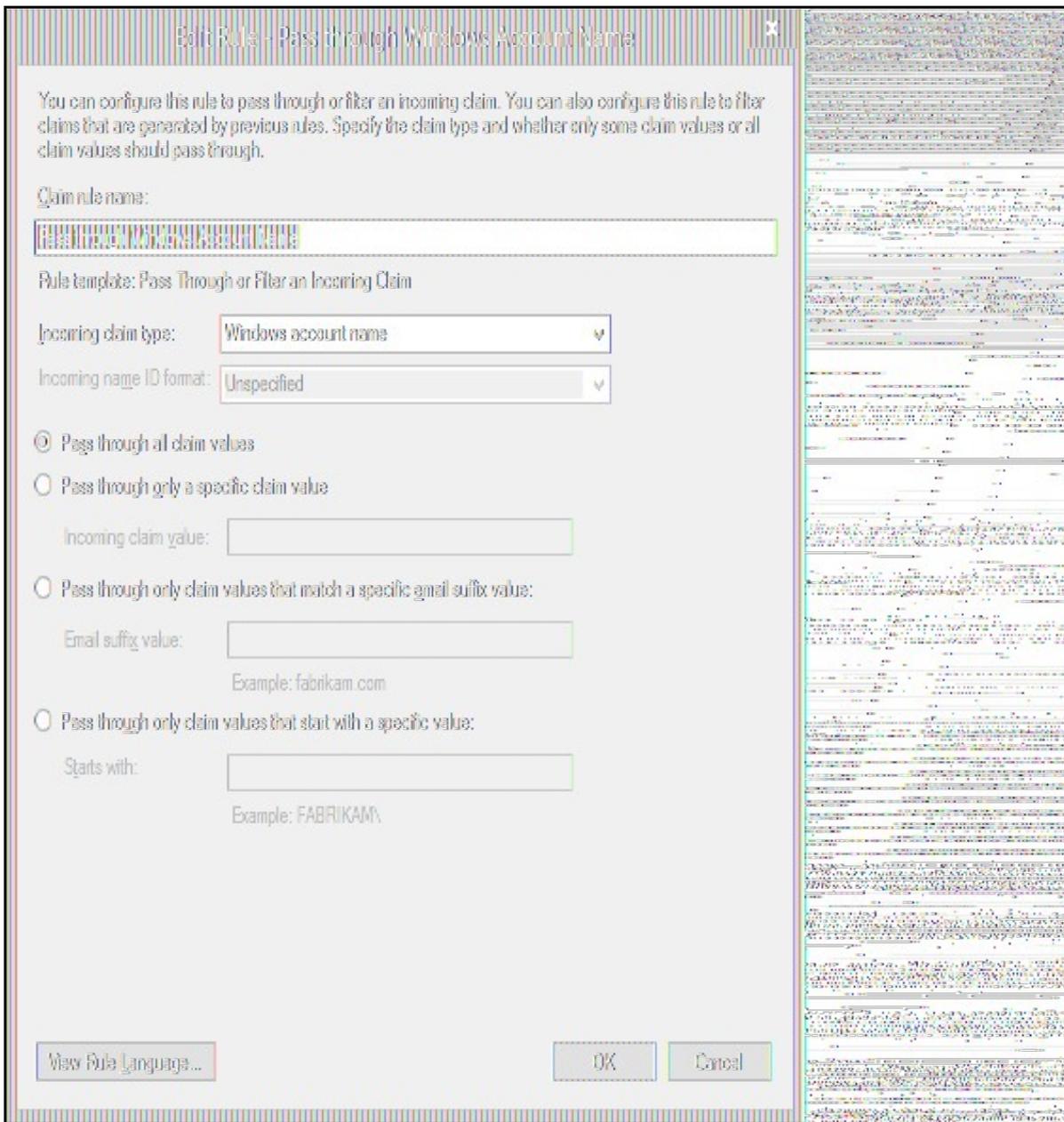
Settings:

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.
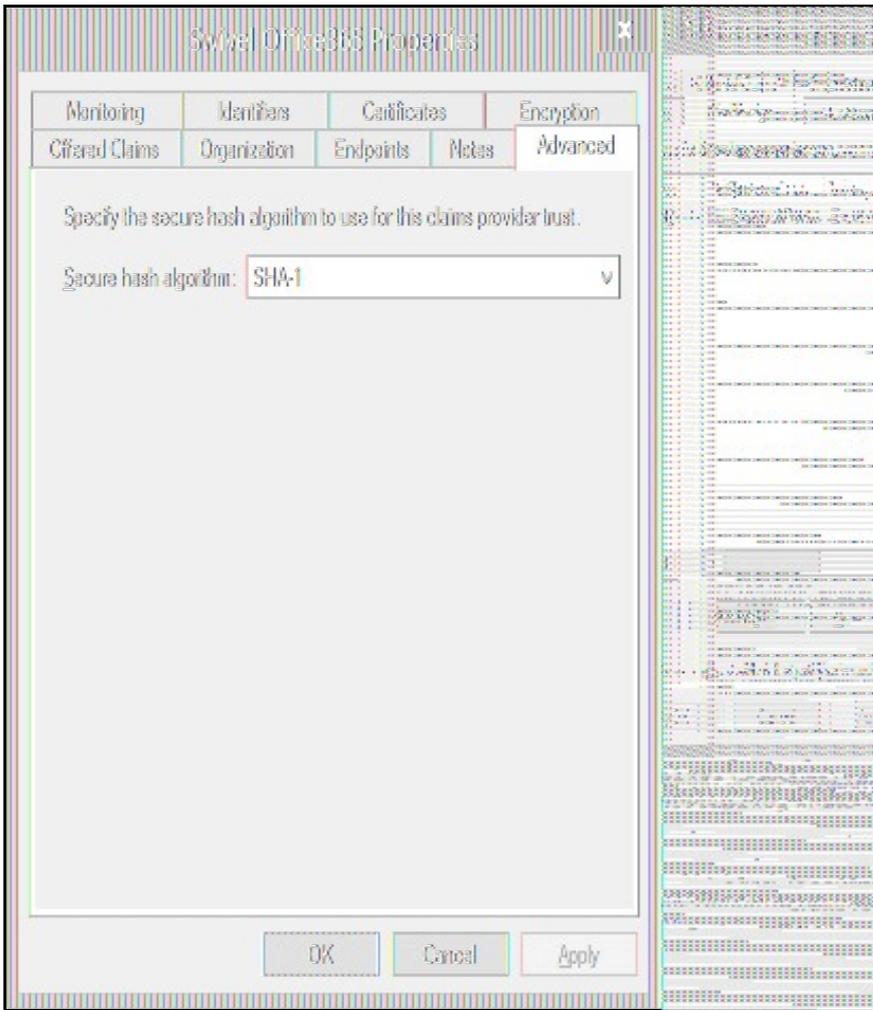
• Under Endpoints, there should be two endpoints configured.
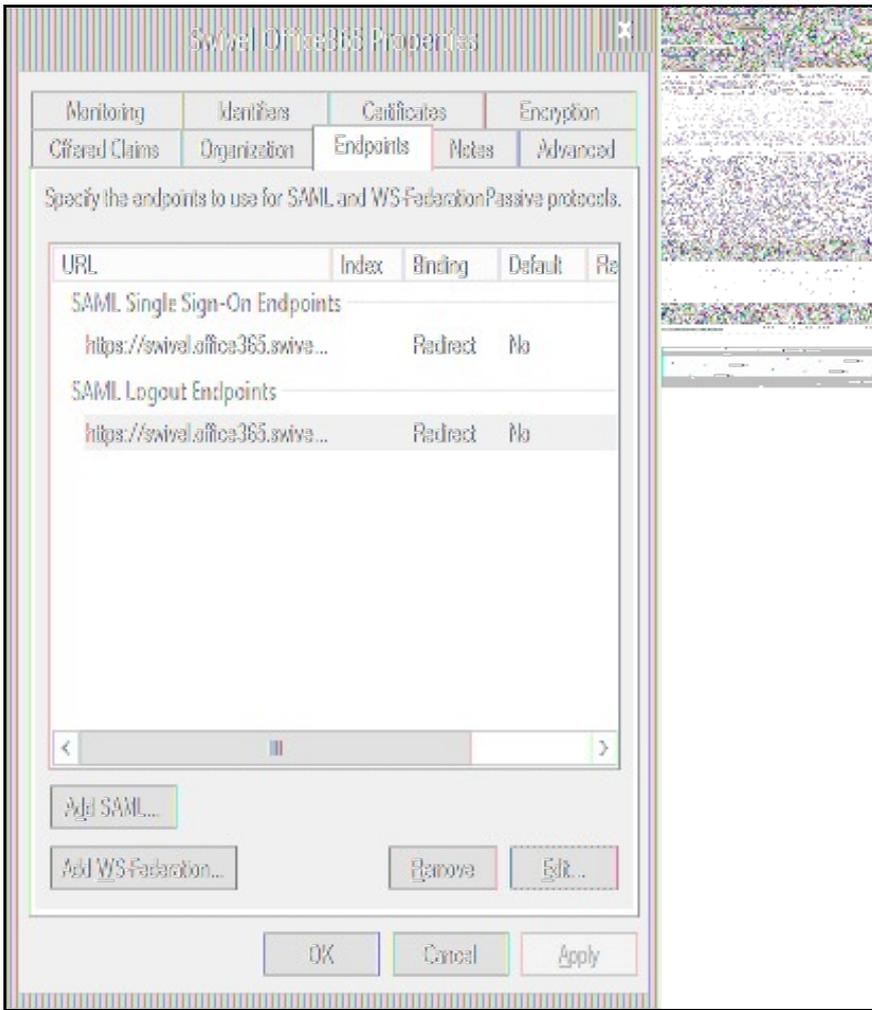
If not, create them as follows. If they have been created, check that they match the following. Both are SAML endpoints:

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

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

- Under Certificates,
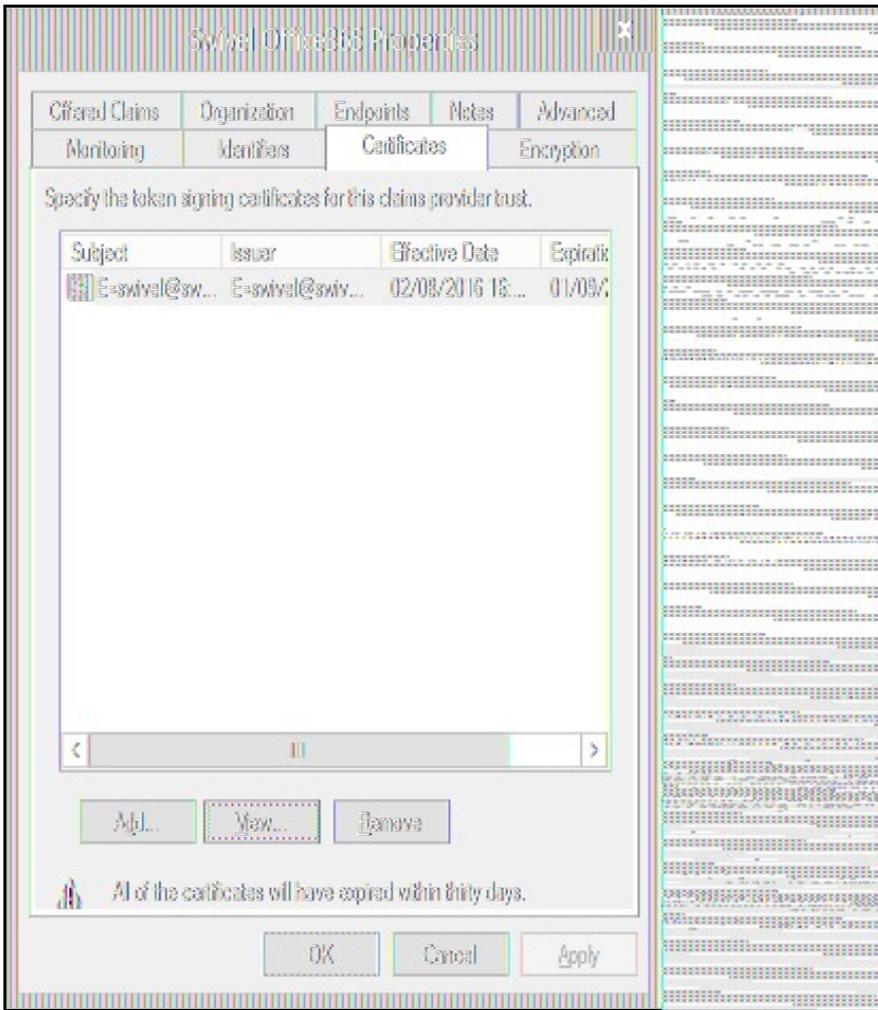
view the imported certificate,

Certificate

General | Details | Certification Path

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

[Install Certificate...] [Issuer Statement]

OK

then click on **Install Certificate**.

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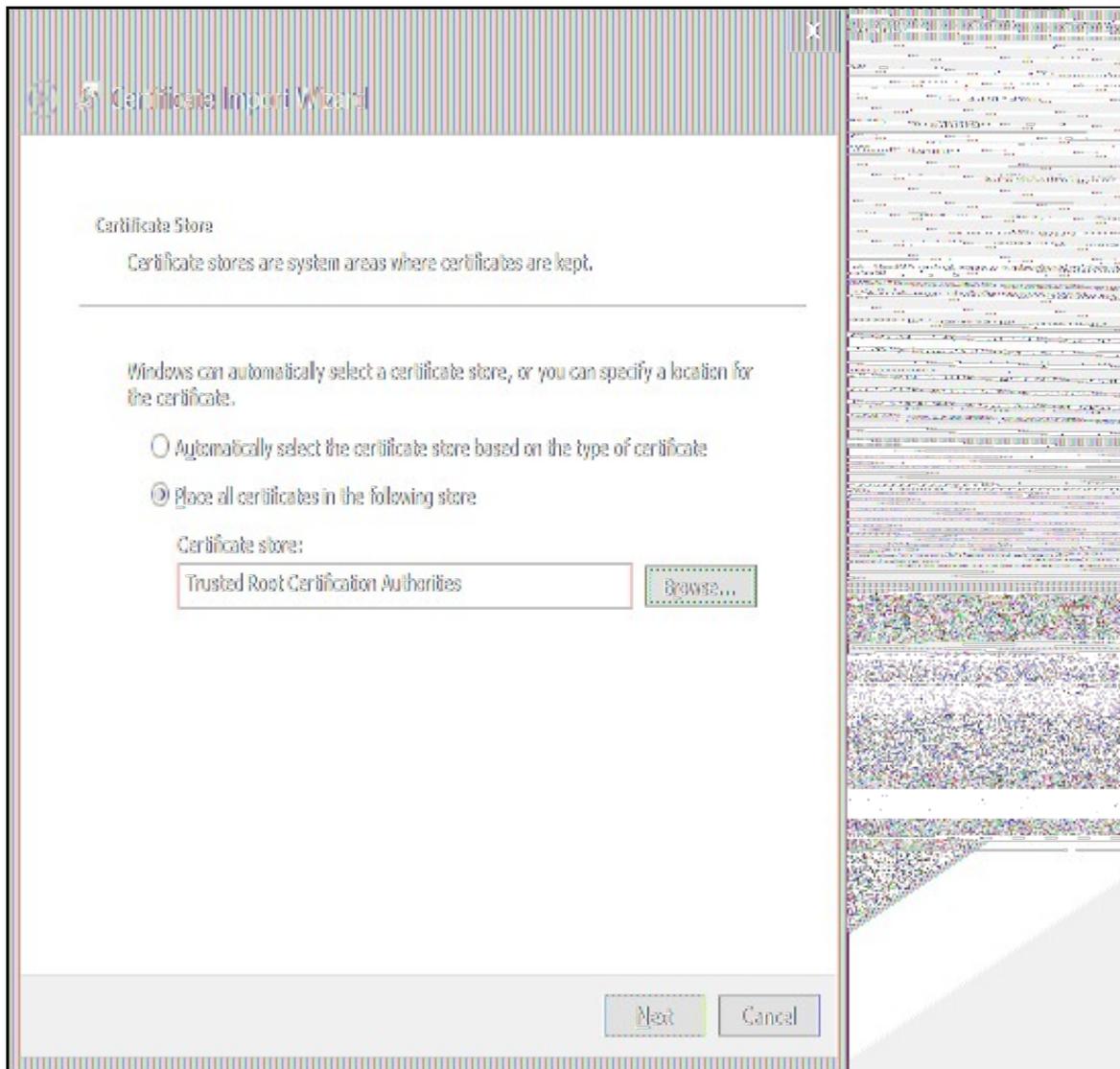
and on the following page, **Place all certificates in the following store**. Browse and select **Trusted Root Certification Authorities**.

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.

- 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")
```