Sentry SSO with Azure

Contents

- 1 Configuring Sentry SSO with Azure Active Directory
  - 1.1 Introduction
  - 1.2 Configuring Sentry Repository
  - 1.3 Configuring Sentry
  - 1.4 Configuring Azure AD

Configuring Sentry SSO with Azure Active Directory

Introduction

WARNING: implementing this solution prevents you from adding more users to Azure Active Directory using the Azure web portal. You can still add users through Azure AD Connect or PowerShell.

This article describes how to configure Azure Active Directory to allow authentication through Swivel Secure Sentry Single Sign-On. This allows access to Office 365 and other applications that require Azure, without the need for Active Directory Federation Services (ADFS). If your Azure domain is backed by ADFS, then see the article on Sentry_SSO_with_ADFS.

Configuring Sentry Repository

It is assumed that you already have a suitable Azure domain configured for use with Sentry authentication. In order to use this domain for Sentry SSO, you need to import the users into the Sentry database. Instructions for doing that can be found under Azure AD as a Data Source.

Configuring Sentry

This article assumes that you are using Sentry version 4.0.4 or earlier. Later versions will provide a more automated process.

Log into Sentry using the **Admin Login** button, and locate the Applications page. Click on **Add Application**.

Application Types

RADIUS VPN - Cisco ASA

RADIUS VPN - Citrix Netscaler

RADIUS VPN - Juniper

RADIUS VPN - Other

SAML - ADFS

SAML - Citrix Netscaler

SAML - GoToMeeting

SAML - Google

SAML - Mimecast

SAML - Office 365

SAML - OneLogin

SAML - Other

Select either SAML - ADFS or SAML - Office 365. The following screen shot assumes Office 365.

SAML Application

Note: The Endpoint URL is used only if the
SAML (Security Assertion Markup Languag

Name	Office365
Image	Office365.png
Points	0
Portal URL	https://portal.office.co
Endpoint URL	https://login.microsoft
Entity ID	urn:federation:Microso
Federated Id	altusername

Enter the settings as shown here. The Portal URL, Endpoint URL and Entity ID must be as shown. Federated Id will depend on how your Sentry repository is configured, but will probably be either **username** or **altusername**. It should correspond to the immutable ID set in Azure AD.

Configuring Azure AD

In order to use Sentry for Azure authentication, you need to enable federated authentication on the Azure domain you are using. This applies to the entire domain: you can't enable federated authentication for some users and standard (or "managed") authentication for others. If you have multiple domains in a single Azure account, however, you can (and must) enable federated authentication for each domain separately.

The domain(s) that you use for federated authentication cannot be the primary domain, and they cannot be managed by Azure - you must manage them yourself. They must also have been verified within Azure.

The procedure below uses Microsoft PowerShell to configure Azure. It assumes you have the MSOnline powershell library installed. Note that it must be the older version referenced here. The new Azure AD module doesn't have the cmdlets referenced by the following script. If you need to install it, use the following command:

```
Install-Module -Name MSOnline
```

You should open a PowerShell command prompt with administrator privileges to carry this out. We are assuming that you are executing these commands interactively, but if you are sufficiently familiar with PowerShell, you can run it as a single script.

It is assumed that the domain you are going to federate has already been created and validated: managing this is outside the scope of this document.

First of all, connect to Azure:

```
Connect-MsolService
```

This command will prompt you for the username and password of your Azure account.

The following 3 lines need to be customized to match your environment:

Replace <my.domain.com> in the following line with the actual domain that you want to enable federated authentication on

```
$domainName="<my.domain.com>"
```

Replace <my.sentry.com> with the host name (and port if required) of your Swivel Secure Sentry server

```
$sentryUri="https://<my.sentry.com>/sentry"
```

Replace <my brand name> with the display name of your domain.

```
$brandName="<my brand name>"
```

The above line is optional - you could simply use

```
$brandName = $domainName
```

The following section extracts metadata from the Sentry server. It will only work if you can connect to your Sentry server without certificate errors. If you cannot do this, you will have to set $issuerUri and $cert by extracting them directly from the metadata: contact Swivel Secure support desk for help on this.

```
$metadataUri=$sentryUri + "/metadata/generatedMetadata.xml"
$metadata=[xml](Invoke-WebRequest -Uri $metadataUri).Content
$metadataRoot = $metadata.EntityDescriptor
$issuerUri = $metadataRoot.entityID
$cert = $metadataRoot.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certificate -replace '\s',''
```

The next two URIs are derived from the Sentry URI

```
$logonUri = $sentryUri + "/saml20endpoint"
$logoffUri = $sentryUri + "/singlelogout"
```

Finally, now we have all the information, we can enable federated authentication

```
Set-MsolDomainAuthentication -DomainName $domainName -Authentication Federated -IssuerUri $issuerUri -FederationBrandName $brandName -LogOffU
```

Make sure that the above is pasted all in one line.

It may take a while for the configuration changes to propagate, so don't worry if you don't get the expected results immediately. To check that the settings have been applied, use the following command:

```
Get-MsolDomainFederationSettings -DomainName $domainName
```

If you get no response, the domain is still using managed authentication.