# 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.



 Status Repository>AD @ Log Viewer Server Please enter the details for accessing Active Directo Policy Hostname/IP: Username: Database Mode Password: Repository Servers Port: Types Groups Attributes Allow self-signed certificates: Repos Admin · AD Synchronization schedule: E RADIUS Username attribute: F Windows GINA Mark missing users as deleted: H OATH Initial PIN attribute: Config Sync Initial password attribute: User Administration Import disabled users: Save Configuration Administration Guide Import disabled state: Logout 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 <b>▼</b>	
Attribute:		Delete
Repos_Admin:		
40.	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:

- certificatelssuer ? 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".



### 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

https://swivel.office365.sw ×
← → C 🏠 https://swivel.office365.swivelsecure.com/sentry/metadata/generatedMetadata.xml
🔢 Apps 🖁 Google 📋 Cinemas 📋 Financial 📋 Games 📋 Home 🌐 Java Sites 🌐 Music 📋 One and One 🏥 Reference 🌐 Shopping 🌐 TV 👘 Tra
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<pre>* (md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://swivel.office365.sudvelsecure.com/sentry/s * (md:IDPS500escriptor WantAuthnRequestSSigned="false" errorURL="https://swivel.office365.sudvelsecure.com/sentry/errorsaml" protocolSupportEnumention="urn:oasis:names:tc:SAML:2.0:protocol" validUntil="2017-00-05700:20:55.2632"&gt; * <ds:keyinfo xmlns:ds="http://uww.w3.org/2000/09/xmldsig#"> * <ds:keyenfo xmlns:ds="http://uww.w3.org/2000/09/xmldsig#"> * <ds:keyenfo xmlns:ds="http://uww.w3.org/2000/09/xmldsig#"> * <ds:x5000ercificate> MILEFTCCArdgwaRMAg(IAAoNBFTopXI]MA0CCSq6STb3DQE88QUANEG840swCQYDVQQGewDHQ]EX_MBUGAUUECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUECAutR0v2ZbkvcGllbnQxE/AA0E3UMECAUUEBAUCBAUUECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUECAutR0v2ZbkvcGllbnQxE/AA0E3UMECAUUEBAUCBAUUECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUECAutR0v2ZbkvcGllbnQxE/AA0E3UMECAUUEBAUCBAUUECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUECAutR0v2ZbkvcGllbnQxE/AA0E3UMEADV2UECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUEGAutR0vzDkvcGllbnQxE/AA0E3UMEADV2UECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUEGAutR0vzDkvcGllbnQxE/AA0E3UMEADV2UECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUUEGAutR0vzDkvcGllbnQxE/AA0E3UMEADV2UECAUUECAuGV2VzdC82b3Jrc2hpcmUkETAP8gUM&amp; ZNwgUzyJdXIIE820EUH8IGAUEG8/AA0E3UMECAUUESAuUEBAUCAUBAUUEUH21LLNB3AUUEAUEAZUMB/SDWTUAUTAUUMUEAUAAUEAUZUAUEAUEAUEAUUEU/SD/SDWTUAUUUUUAUAAUEAUEAUEAUEAUUEU/SD/SDWTUAUUUUUUUUUAUAAUEAUEAUEAUEAUEAUEAUEAUEAU</ds:x5000ercificate></ds:keyenfo></ds:keyenfo></ds:keyinfo></pre>

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:

staps	Select the template for the claim rule that you want to create from the following list. The description provides	a state of the second s
() Choose Rule Type	details about each claim rule template.	
Ø Configure Claim Rule	Claim rule template:	All Milly, on a solution of marks and all should be a solution of the solution
	Pass Through or Filter an Incoming Claim 👻	
	Claim rule template description:	
	Using the Pass Through or Fiter an Incoming Claim rule template you can pess through all incoming claims with a selected claim type. 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 and 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 adted. Fermione 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.

	Add Tran	storn Claim Rule Wiz	ard		×	and the second second second second
Configure Rule						
Steps © Choose Rule Type © Configure Claim Pule	You can configure this rule claims that are generated to claim values should pass the Qlaim rule name: Pass through Name ID	e to pass through or illier an inc by previous rules. Specify the r recugh.	centing claim. Yeu ca daim type and wheth	in also configure t ter only some clair	his rule to filter n values or al	
	Rula templata: Pass Throu	gh or Alter an Incorring Claim				And the second s
	Incoming claim type:	Name ID		v		
	O Page through al claim o	alues		· ·		
	<ul> <li>Pass through grily a spinor incoming claim value:</li> </ul>	ecific claim value				
	Pass through only claim	i values that match a specific	gmail suñix value:			
	Email suifig value:	swivel.cffice365.swivelsecu	ingo.en			
	O Pass through only claim Starts with:	Example: fabrikam.com i values that start with a speci	lic value:	_		
		Example: FABRIKAM\				
			< Previous	Finish	Cancel	
			V LIVING		Series	

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

-					
	Edit	Rule - Pass through Windows Acco	int Name	X.	Alternational and a solution and the solution of the solution
	You can configure this rule claims that are generated claim values should pass t	e to pass through or filter an incoming claim. You c by previous rules. Spacify the claim type and what hrough.	an also configure t her only some clai	his rule to filter n values or all	
	<u>Claim rule name:</u>				
	THE OWNER WATCH AND	Here and the second			
	Pule template: Pass Throu	igh ar Filter an Inconting Claim			
	Incoming claim type:	Windows account name	v		A search and a second sec
	Incoming name ID format:	Unspecified	v		
	O Page through all claim y	values			
	O Pass through grily a sp	ecific claim value			
	Incoming claim value:				and and a configuration
	O Pass through only claim	n values that match a specific email suffix value:			Section of the section of the
	Email suffix value:				
		Example: fabrikam.com			
	O Pass through only claim	n values that start with a specific value:			
	Starts with:				
		Example: FABRIKAM\			
	View Rule Language		XQ	Cancel	
					sula superior in the second states of the

## 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.

		Swizel Offi	re365 Prope	erties	×	
	Manitaring	<b>Mentifiers</b>	Cartificat	25	Encryption	A STATE OF
	Cifered Claims	Organization	Endpoints	Notes	Advanced	and the second states and
	Spacify the sac	ure hash algorith	n to use for this	claims prov	ider trust.	estriction loop 1997 - Estate Maria Second
	Secure hash ak	porithm: SHA-1			v	
			0K	Cancel	Apply	
Π						

• Under Endpoints, there should be two endpoints configured.

Manitaring	Identifiers	Cartif	ìcates	Encrypt	ion	
Cifered Claims	Organization	Endpoint	s Notes	e Adva	nced	15271275875628428427455 1954-1954827497721828
pecify the endpo	vints to use for SAM	IL and WS	Federation	<sup>2</sup> assive prol	ocols.	
URL		Index	Binding	Default	Ra	Steering and the second
SAML Single https://swiv	Sign-On Endpoi el.affice365.swive et Envlociets	nts 	Redirect	Na		
JULIA 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	LE STEEP STILLS					
hilips://swiv	aluitice365.swive		Redirect	Na		
hilps://swiv	el.añce365.swive	**	Radract	¢٩	>	
<	el.añce365.swive		Radrect	Ň	>	

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

Echt Br	opeint X	
Endpoint type:		
SAML Single Sign-On	v	
<u>Binding:</u>		
Recirect	v	
Set the trusted URL as default		
l <mark>o</mark> dex: 0 ×		
Insted URL:		
https://swivel.office365.swivelsecure.	.com/sentry/saml20endpoint	
Example: https://sts.contoso.com/adi	is/ls	
Response URL:		
Example: https://sts.contoso.com/log	out	
	<u>QK</u> Cancel	

• Endpoint Type = SAML Logout, Binding = redirect, Trusted URL = https://<sentry\_URL>/sentry/singlelogout, Response URL = https://<sentry\_URL>/sentry/singlelogout

Ecilt Endpoint	X
Endpoint type:	San 5 Chin Sand See
SAML Logout	ngarandarandara
Bailea	and the construction of the second se
Redrect V	na transmitrana ite -
Set the trusted URL as default	יייינאינטייעעיישייש איזיגיעטינעריישיישיישיישיי
lodex: 0	
Trusted VPL:	Contract of the second s
https://swivel.office365.swivelsacure.com/sentry/singlelogout	
Example: https://sta.conteso.com/aci/s/ls	
Response URL:	
Example: https://sts.conteso.com/logout	
<u>D</u> X Cancel	

• Under Certificates,

ared Claims	Organization	Endpoi	nts Note	8	Advanced	_	
anitaring	Identifiers	Car	tificates	Er	nstyption		maaliiliiliilii
iv the token ai	oning cartificates	for this c	laima provida	rtrust.			
	× ×						
ubject	SSUER		Effective Dat	18-	Expiratic		
E=swivel@s	v Esswival@	swiv	02/08/2016	15	01/09/;		
Da murangar	a ann ang		10 10 10 10				
						20	
						100	
						1	
						100	
					>		
	11						
Add	III Maw.	<u>B</u> an	1949		>		
Add	III	<u>I</u> m	1923		>		
Add	II Yow	<u>B</u> arines	1878	dana	>		

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 02/08/2015 to 01/09/2016	
gastall Cartificate Issuer Statement	
СК	

then click on Install Certificate.

🔆 - S. Cardificate Internet Misseri	A CONTRACTOR OF
	ne se series
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 O Qurrent User O Local Machine	
To continue, dick Next.	
Cancel	·

Select Local Machine on the next page,

infill) گاری این Certificate Import Witers! این این این این این این این این این این	
Cartificate Store	
Certificate stores are system areas where certificates are kept.	an in the second s
<ul> <li>Windows can automatically select a certificate store, or you can specify a location for the certificate.</li> <li>Automatically select the certificate store based on the type of certificate</li> <li>Bace all certificates in the following store</li> <li>Certificate store:</li> <li>Trusted Root Certification Authorities</li> </ul>	
Mexit Cancel	

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")