Sentry SSO with ServiceNow

Contents

- 1 Introduction

- 1 Introduction
 2 Setup AuthControl Sentry Keys
 3 Setup SSO on ServiceNow
 4 Configure Check Password with Repository on the Swivel Core
 5 Setup AuthControl Sentry Application definition
 6 Setup AuthControl Sentry Authentication definition
 7 Testing connection with ServiceNow tool
 9 Testing authentication to ServiceNow via Swivel AuthControl Set

- 8 Testing authentication to ServiceNow via Swivel AuthControl Sentry
- 9 Troubleshooting

Introduction

service

This document describes how to configure ServiceNow to work with Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on yourdomain.service-now.com, you will need to setup some Keys if they were not set up already. Please see a separate article: HowToCreateKeysOnCmi. You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

Setup SSO on ServiceNow

To configure SSO setting on your ServiceNow accounts you have to access your Admin console by simply going to https://yourdomain.servicenow.com You should see an Admin console.

On the left menu you will see a User Administration section. When you click on the Single Sign-On you will be see the following screen. You have to enable the options displayed on the right, which are: "Enable multiple provider SSO" and "Enable Auto Importing of users from all identity providers into the user table". Click on the button "Add New IdP" and select the User group for which to use SSO. For this example we are using "Swivel Users".

Pilter navigator			Single Sign-On		
T	*	0	Identity Providers (IdP)		
Application Co Incident Problem Change Service Catal		I	SAML2 Update1 Pr		
Knowledge B Live Feed Survey	lase		Certificates		
User Adminis Web Servic Getting Sta API Explor REST Mess Business R REST Logs	ces Larted rer Sages Rules		Trust Store Cert InCommon_Meta_Signing Valid until 2037-12-18	SAML 2.0 Valid unbli 2016-08-17	SAML 2.0 SP Keystore
User Administr SSO provided Users Groups Roles Logged in use V Authentica Single Sign LDAP	d by Okta, Inc. ers ation				
Departments Locations Companies Location Map					

G

Click on the button "Add New IdP" and click "Manually enter metadata XML".

Plitter navigator	Add New Identity Provider			
e * 0	Configure Identity Provider			
Application Configuration				
Incident	IdP Metadata URL			
Problem	Ex. http://dp.soocircle.com			
Change	Manually enter metadata XM			
Service Catalog	Fetch Cancel			
Knowledge Base				
Live Feed Survey	and the second se			
User Administration	Name			
▼ Web Services				
Getting Started	Identity Provider URL			
API Explorer		Configuration Identify Description		
REST Messages	Identity Provider's AuthnRequest	Configure your Identity Provider		
Business Rules				
REST Logs				
User Administration	Identity Provider's SingleLogoutRequest			
SSO provided by Okta, Inc.				
Users				
Groups Roles	Identity Provider Certificate			
Logged in users				
▼ Authentication	Active			
Single Sign-On				
LDAP	Default			
Departments	Primary			
Locations	Prinary			
Companies	the state of the s			
Location Map	Advanced Settings			
Delegates				
<u>^</u>	Save			

Now navigate to your AuthControl Sentry metadata page as below(https://<FQDN_OF_SENTRY_SERVER>/sentry/metadata/generatedMetadata.xml) and copy the content of this page.

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://172.23.9.35:8443/sentry/saml20endpoint">
      kmd:IDPSSODescriptor WantAuthnRequestsSigned="false" errorURL="https://172.23.9.35:8443/sentry/errorsaml" protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0:protocolSupportEnumeration="urn:oasis:names:tc:SAUL:2.0

           cds:X509Data>
                             <ds:X509Certificate>HIID+TCCAuGgAwIBAgIJAIZGvqiocU+7MA0GCSqGSIb3DQEB8QUAMIGSMQswCQYDVQQGEwJHQjES
MBAGA1UECAwJWW9ya3NoaXJ1MREwDwYDVQQMDAhXZXRoZXJieTEPMA0GA1UECgwGU2VudHJ5MQv
CgYDVQQLDANEZXYxDzANBgNVBAPHB1N3aXZ1bDEsPCo6CSq65Ib3DQE3ARYdaS5nYW51b6V2aW2
QHN3aX21bHN1Y3Vy255jb20wHhcNNTYwNz12MDkyNzJyNhcNNTYwOD1HDkyNzJyNjC8kjEUAAKG
A1UEBhMCR0I×EjAQBgNVBAgHCV1vcmtzaG1y2TERMA8GA1UEBwwIV2V0aGVyYnkxDzANBgNVBAoM
BINIbnRyeTEHMAoGAIUECnmDRGV2MQ8mDQYDVQQDDAZTd2l2ZWxxLDAq8gkqhkiG9w88CQEHMiku
22Fudixldmljc88zd2l2ZixzZiNlcmUuY29tHIIBIjAN8gkqhkiG9w88AQEFAAOCAQ8ANII8CgKC
AQEAy95hRfJF6eQ/RsyBLdKP75yS0LY5+eAv09N6hgVIIAHCH8zJ1EpAffr/5950cysg4kQ86o9/
r3GUTTc0STy7HYczguGzXhBRv1qGX4NPUUN0HwQ7kyyIkPNt8/Gv81xKUqKAC36i1cN+3M4rs+zp
z24PKLN+GNcQoghPYT4RJe00DSHA1LSToRLm1T5/VTTwov3Gp3jp9Skous0sZ8hbS2/mKBdSH2QY
SHeLOLQq2Vg5KFNSjRb5A0w4VKtGd+QfnhxDDXfLOVhsF5dvh0WNdEm0FKJbJmt5T1vM/d2qNzAE
BsNShwqSSaZrs2Fx5FlS7yN4iyF4eRgex5qw+a5WywIDAQABo1AwTjAdBgNVHQ4EFgQUpJutrEey
DpvWvd5algIUmP+XQ5IwHwYDVR0j8BgwFoAUpJutrEeyDpvWvd5algIUmP+XQ5IwDAYDVR0TBAUw
AwEB/zANBgkqhki69w08AQUFAAOCAQEAfqLUdNZRY6ZnmrdPcd8+itu+dEfNQ6rUI8k36/MKiMDv
BudBzFBphZqSED069nNNTFIvyaR8+I/bmbXzrHQ2SoRHDX7/L78pQn3nDXAV4ZjxHELvmL0FeQo3
ZoQfgEtoNyf3nUQHmPxxL/1X8qfpD96cIQ793bjTs7XSVkckt4erN+D3+njv4LaAg/27qh2CcQKp
SbQUy+48p37NoaErbs7hYkzZPtzFU6YDx2dyCSb9Ek3nZNMqBbrmLF9c9LxAZT0BCIHNRFPYa2o
aRvybslv9fIvghucOrsmyPtPmSgLxI34ZqThMSz7MoCEJ3qchbHjCOlaqLqHh864jDVDvg==</ds:X509Certificate>
                        </ds:X509Data>
                  </ds:KeyInfo>
            </md:KeyDescriptor)
            (md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://172.23.9.35:8443/sentry/singleLogout"/>
            <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://172.23.9.35:8443/sentry/saml20endpoint"/>
      </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Return back on the ServiceNow setup

IdP Metadata XML - Paste copied metadata from your AuthControl Sentry and click Fetch. After that the following fields will be set automatically

Identity Provider URL

Identity Provider's SingleLogoutRequest

Identity Provider Certificate

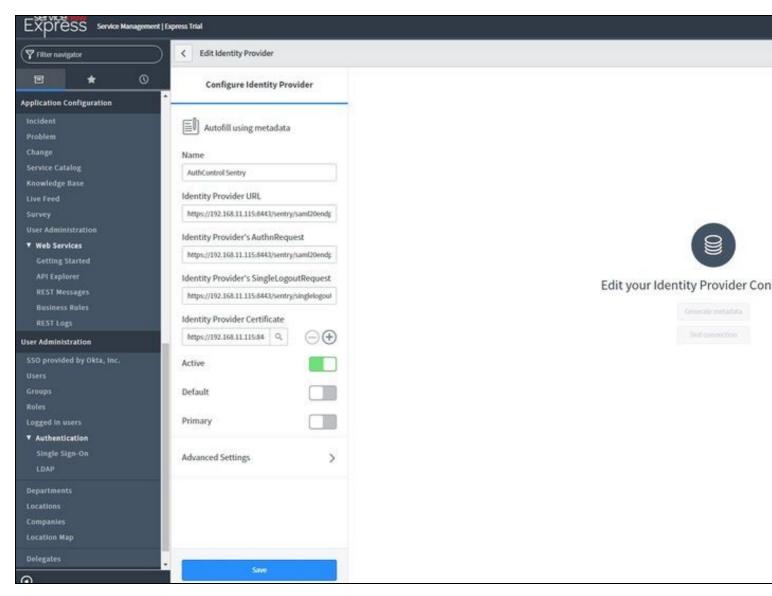
You will have to fill the following ones for your AuthControl Sentry such as:

Identity Provider's AuthnRequest - Copy and paste the value set on "Identity Provider URL"

Active - Enabled

Default - Enabled

Primary - Enabled



After you have entered all the details as above click Save. You can test the connection after setting up Auth Control Sentry

Configure Check Password with Repository on the Swivel Core

In order to check the user?s Active Directory password, ensure that the local Agent defined under Server -> Agents has got the Check Password with repository checkbox enabled. When an authentication occurs in AuthControl Sentry, the Active Directory password will then be passed to Active Directory for verification.

Setup AuthControl Sentry Application definition

Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for ServiceNow, click the Add Provider button and select ServiceNow SAML.

Rules	SAML Applicati	on
Applications		
Authentication Methods		
View IdP Metadata	Note: The End	dpoint URL is used only if the ACS (Assertion Consume
Keys		ty Assertion Markup Language) request.
Users Active Sessions		
User History	Name	ServiceNow
Log Viewer		
General Configuration	Image	ServiceNow.png V
	Points	0
	Portal URL	https://yourdomain.service-now.com/navpage.c
	Endpoint URL	
	Entity ID	https://yourdomain.service-now.com
	Federated Id	email
		Save

Name: ServiceNow(Type an Arbitrary name for this Application) Image: ServiceNow.jpg(selected by default) Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: (this Portal URL is ServiceNow login URL which you can usually access on: https://yourdomain.service-now.com/navpage.do

Endpoint URL: N/A

Entity ID: https://yourdomain.service-now.com (Entity ID is the one defined on ServiceNow > User Administration > Single Sign-On > AuthControl Sentry Idp > Advanced Settings: Entity ID)

Federated Id: email

Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for ServiceNow authentication.

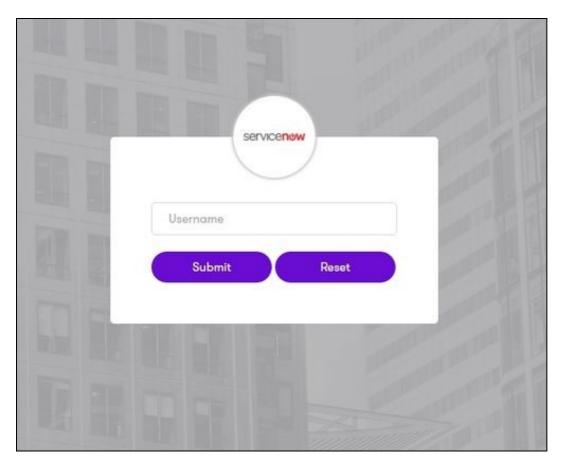
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the ServieNow Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry here)

Testing connection with ServiceNow tool

ServiceNow provides a tool to test the connection. Go to User Administration > Single Sign-On and click AuthControl Sentry ldp. After that click Test connection.

Pilter navigator	Edit Identity Provider	
e \star 0	Configure Identity Provider	
Application Configuration		
Incident Problem	Autofill using metadata	
Change	Name	
Service Catalog	AuthControl Sentry	
Knowledge Base Live Feed	Identity Provider URL	
Survey	https://192.168.11.115:8443/sentry/sami20endp	
User Administration	Identity Provider's AuthnRequest	9
▼ Web Services	https://192.168.11.115.8443/sentry/sami20endp	
Getting Started API Explorer	Identity Provider's SingleLogoutRequest	Edit your Identity Provider Co
REST Messages	https://192.168.11.115.8443/sentry/singlelogout	
Business Rules	Identity Provider Certificate	Generate metadata
REST Logs	https://192.168.11.115.84 Q	Test connection 5
User Administration		13
SSO provided by Okta, Inc. Users	Active	
Groups	Default	
Roles		
Logged in users	Primary	
▼ Authentication		
Single Sign-On	Advanced Settings >	
LOAP		
Departments		
Locations		
Companies		
Location Map		
Delegates		
System Policy		
0	Save	

A new window will be displayed that will redirect to AuthControl sentry username page.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the ServiceNow Application definition.

In this login example we are using the email as a username

	servicenuv	.)	
	user@email.com		and F
	Password		100
	OTC		
	TURing	Υ.	and the
	1 2 3 4 5 6 S 2 4 1 3 U	7 8 9 0 S 8 7 5	AL AN
	Login	Refresh Image	Part I
M. D. T.			Barris

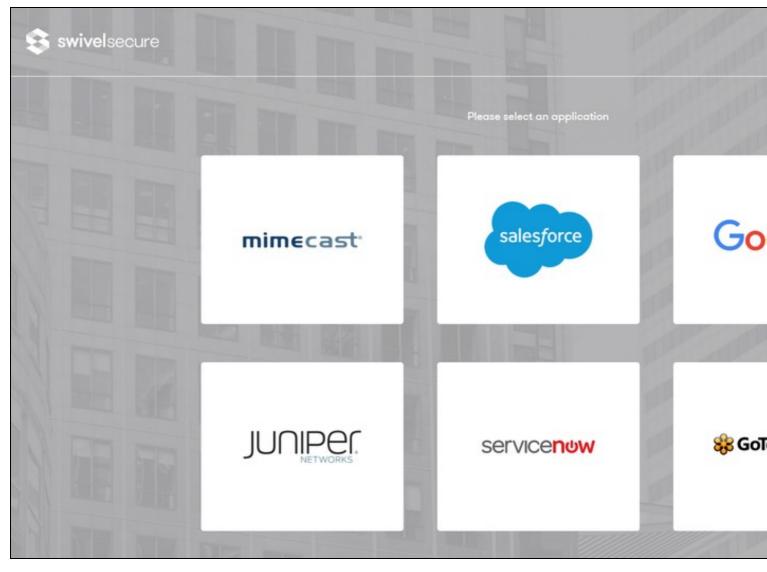
After we enter our authentication credentials we will see a logout screen. Close that window and on the ServiceNow page click View Log. Check that the logs indicate that the SAML authentication was successful.

Testing authentication to ServiceNow via Swivel AuthControl Sentry

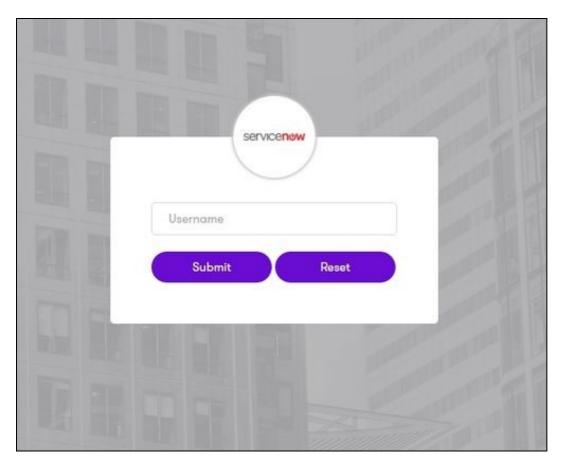
This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. https://yourdomain.service-now.com/navpage.do

Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. https://mycompanysentrydomain/sentry/startPage On a Start Page you will be able to see a new ServiceNow Icon on which you can click and proceed with authentication (as you would by going straight to the ServiceNow page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the ServiceNow Application definition.

In this login example we are using the email as a username

	servicenov	•)	
	user@email.com		
	Password		1 32
	OTC		
	TURing	~	and the fi
	1 2 3 4 5 6 S 2 4 1 3 0	7 8 9 0 S 8 7 5	Terra La
	Login	Refresh Image	ALC: NOT OF
II IN G			R. M.

After we enter our authentication credentials we successfully will see the ServiceNow account that we tried to access.

Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from ServiceNow
- The ServiceNow has a Test Connection feature that provides details about the SAML response received from AuthControl Sentry

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

If you have issues login in with then SAML authentication to the admin console you can always access by https://yourdomain.service-now.com/side_door.do

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 Can AuthControl Sentry find the Certificate locally, is it the correct one?
 Has the correct Metadata been uploaded to the ServiceNow?

 - Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?