Sentry SSO with Cisco ASA using SAML

Contents

Introduction

This Document describes how to integrate a Cisco ASA with Swivel Sentry SSO using SAML.

If your Cisco ASA does not support SAML or you are not licensed to do so, our Sentry SSO with Cisco ASA for RADIUS article can be used instead: it uses a custom login page to redirect to Sentry, and RADIUS to verify that the SAML claim is valid. The solution is not suitable for use with AnyConnect.

Setup AuthControl Sentry Keys

Before you are able to create a SAML configuration in Cisco ASA, you will need to setup some Keys. 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.

Convert Sentry Keys to PFX

You will need to retrieve the keys generated above from the /home/swivel/.swivel/sentry/keys folder so that you are able to convert from PEM format to a PFX file containing the private key.

The openssl command to achieve a PEM to PFX conversion is as follows:

```
openssl pkcs12 -export -out Cert.pfx -in cert.pem -inkey key.pem
```

You will be prompted for a password for the private key and a password for the PFX you are creating This command assumes:

- Cert.pfx is the file being created
- cert.pem is the cert file downloadable from the AuthControl keys GUI
- key.pem is the private key you download from the /home/swivel/.swivel/sentry/keys folder using WinSCP

Download the Sentry SSO IdP metadata

In the Sentry SSO Web GUI (running on port 8443), right click on the 'View IdP Metadata' left hand menu option and 'Save As' an xml file e.g. SwivelIdPMetadata.xml. We will upload this to the Cisco ASA in a moment.

Configure Cisco ASA

We recommend you protect your SSL VPN endpoint with an SSL certificate and ensure that it is working prior to embarking on this integration.

The below steps all assume that you are administering the Cisco ASA using the ASDM client.

Import the AuthControl Sentry IdP Certificate

In the ASDM, go to Configuration -> Remote Access VPN -> Certificate Management -> Identity certificates.

Click Add. Give the certificate an arbitrary name. Import the PFX created earlier being sure to ensure a password was set and is entered in the Decryption Passphrase field. Browse to the file and finally, click Add Certificate to validate and import the PFX.

Don't forget to Apply the changes in the ASDM client.

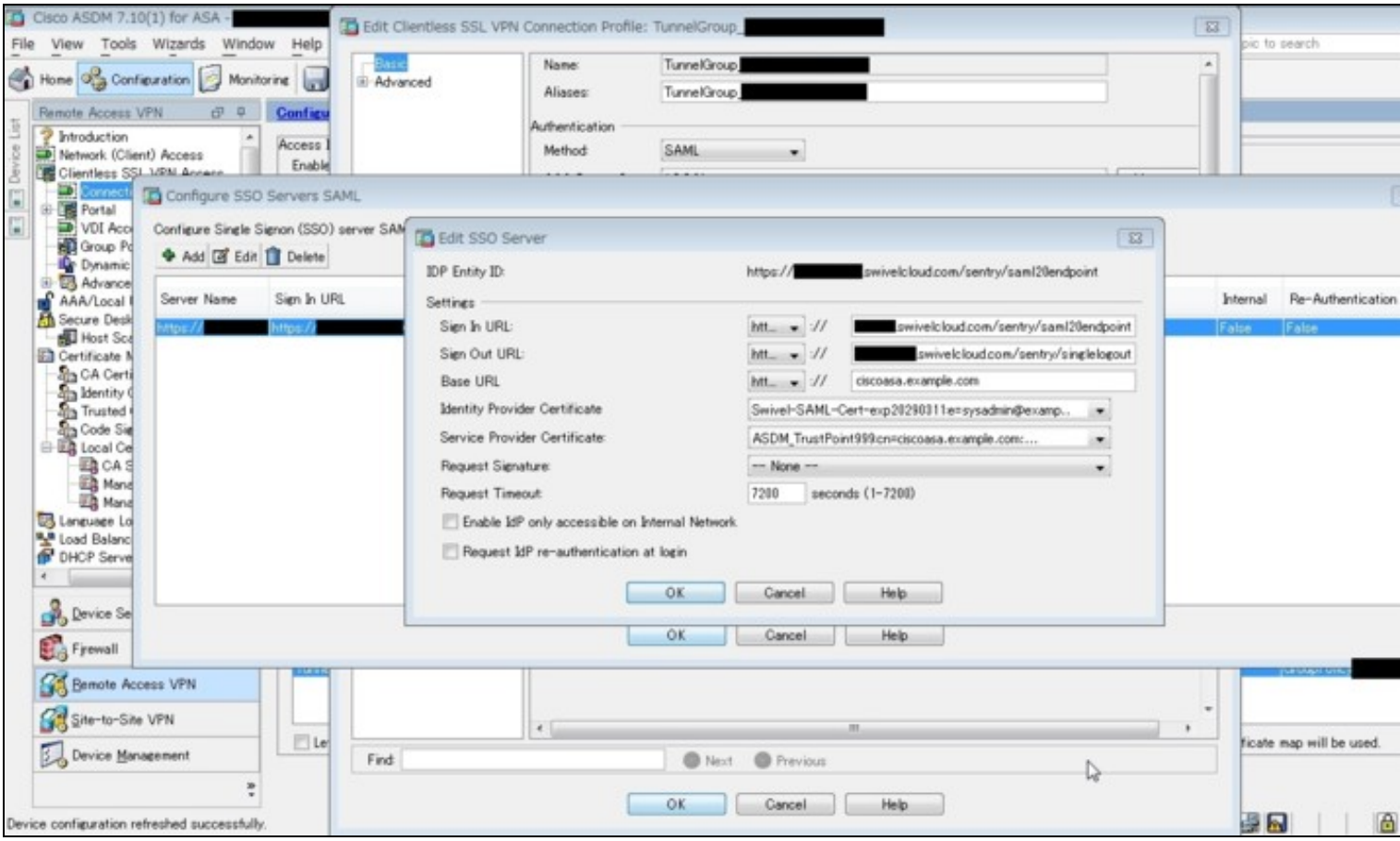
Setup the SAML IdP against the SSL VPN Connection Profile

In the ASDM, go to Configuration -> Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles, highlight the Connection Profile assigned to the SSL VPN and click the Edit button.

Under the Basic tab, SAML Identity Provider section, click Manage.

Add a new entry:

- IDP Entity ID: (needs to match the entity ID specified in Sentry SSO metadata XML file, in the AuthControl Sentry GUI -> View Metadata screen you will see the IDP's entity ID listed at the top) e.g. "**https://<AuthControlSentryHostname>/sentry/saml20endpoint**" . The FQDN of this entity ID URL should be valid. If not, login to the Swivel Secure CMI -> Main Menu -> Appliance -> Sentry and set the Base URL to be correct and restart Tomcat. Then view and export the IdP metadata again.
- Sign In URL: **https://<AuthControlSentryHostname>/sentry/saml20endpoint**
- Sign Out URL: **https://<AuthControlSentryHostname>/sentry/singlelogout**
- Base URL: (the CiscoASA FQDN hostname) e.g. **https://ciscoasa.example.com**
- Identity provider certificate (select the one imported earlier)
- Service provider certificate (select the SSL certificate assigned to the SSL VPN endpoint)



Configure AuthControl Sentry

Log into the Sentry administration console. Select **Applications**. Then click **Add Application** and select the type **SAML - Other**

Enter an arbitrary name e.g. "Cisco ASA".

Portal URL should be the public URL of your Cisco server. It is recommended that you use the same address for **Endpoint URL**, although this will usually be overridden be the address sent by the Cisco login page.

Entity ID must be the same as the value shown as *IDP Entity ID* in the Add SSO Server window shown above, so that AuthControl Sentry will recognize the request as coming from this Cisco server.