Cisco AnyConnect VPN on ASA (IdP-initiated) integration guide

Introduction

Use this guide to integrate Cisco AnyConnect VPN (SAML) with SecureAuth IdP on Cisco Adaptive Security Appliance (ASA).

Prerequisites

- SecureAuth IdP version 9.1 or later with a realm ready for the Cisco ASA integration
- Cisco account
- Supported on Cisco ASA version 9.7.1 or later for both AnyConnect client and clientless SSL VPN

Cisco ASA configuration steps

This section provides the information you need to configure SecureAuth IdP on Cisco ASA.

1. Log in to the Cisco ASA box.

2. From the command line, run the following commands below and in the remaining steps:

    – sh run webvpn saml

3. Create a SAML identity provider, where *UniqueName* can be any name. This name is used in the SecureAuth IdP configuration section for the WSFed /SAML Issuer field on the Post Authenticaton tab.

    saml idp *UniqueName*

4. Configure the SecureAuth IdP URLs.

    url sign-in *https://yourVPNaddress.com/SecureAuth#*

    url sign-out *https://yourVPNaddress.com/SecureAuth#*

5. Configure the Clientless VPN base URL.

    base-url *https://yourCisco-server.com/samltest*

6. Configure trustpoints between the SecureAuth IdP and ASA.

    trustpoint idp *UniqueName*

    trustpoint sp *asa_saml_sp*

7. Configure SAML timeout.

    timeout assertion *7200*

SecureAuth IdP configuration steps

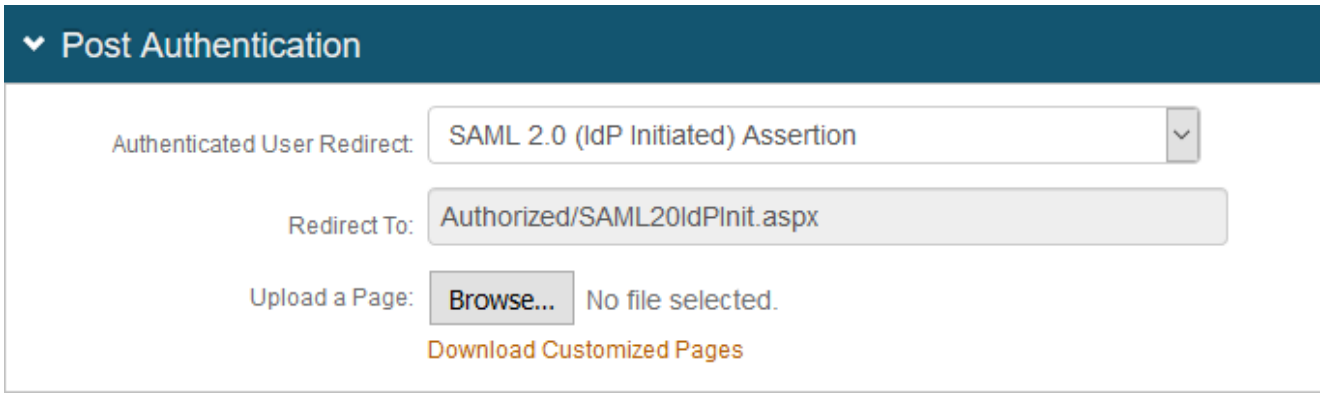
1. Log in to your **SecureAuth IdP Admin** console.

Post Authentication tab

2. Select the **Post Authentication** tab.

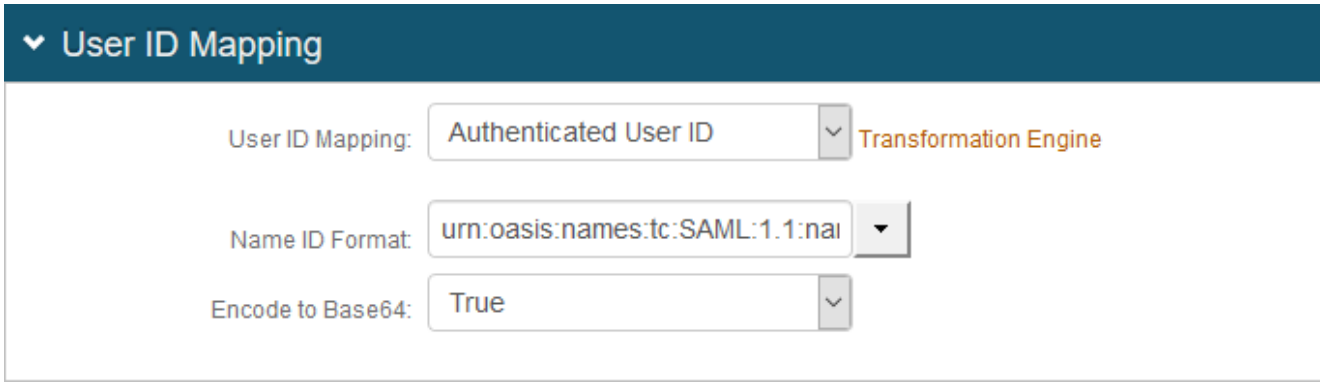
3. In the **Post Authentication** section, make the following entry:

    a. Set **Authenticated User Redirect** to **SAML 2.0 (IdP Initiated) Assertion**.



4. In the **User ID Mapping** section, make the following entries:

   a. Set **User ID Mapping** to **Authenticated User ID**.



5. In the **SAML Assertion / WS Federation** section, make the following entries:

   a. Set the **WSFed Reply To / SAML Target URL** to the absolute URL of the application, to where end-users are redirected upon successful authentication.

      For example, https://yourCisco-server.com/samltest

   b. Set the **SAML Consumer URL** to the Cisco URL used to accept a SAML assertion.

      For example, https://yourCisco-server.com/+CSCOE+/saml/sp/xxxxx

   c. Set the **WSFed/SAML Issuer** to a unique name that identifies the SecureAuth IdP to the application (as the SAML ID).

      This value is shared with the application and can be any word, phrase, or URL, but must match exactly in the SecureAuth IdP and Cisco ASA configurations.

      For example, *UniqueName* is used in step 3 of the Cisco ASA configuration steps

   d. Set the **SAML Recipient** to the identifiable information of the SAML Recipient, which usually maps to the SAML Consumer URL.

      For example, https://yourCisco-server.com/+CSCOE+/saml/sp/xxxxx

   e. Set the **SAML Audience** to the base domain of the application.

      For example, https://yourCisco-server.com/+CSCOE+/samltest/saml/sp/xxxxx

   f. Set the **SP Start URL** to the login URL for the application.

      This value enables appropriate redirection for normal login and SSO login experiences.

      For example, https://yourCisco-server.com/+CSCOE+/samltest

SAML Assertion / WS Federation

WSFed Reply To/SAML Target URL:	https://yourCisco-server.com/samltest
SAML Consumer URL:	https://app.company.com/owahttps://yourCisco-server.com/+CS(
WSFed/SAML Issuer:	UniqueName
SAML Recipient:	https://yourCisco-server.com/+CSCOE+/saml/sp/xxxxx
SAML Audience:	https://yourCisco-server.com/+CSCOE+/samltest/saml/sp/xxxxx
SP Start URL:	https://yourCisco-server.com/+CSCOE+/samltest
WS-Fed Version:	1.2
WS-Fed Signing Algorithm:	SHA1
SAML Signing Algorithm:	SHA1
SAML Offset Minutes:	100
SAML Valid Hours:	24
Append HTTPS to SAML Target URL:	True
Generate Unique Assertion ID:	True
Sign SAML Assertion:	True
Sign SAML Message:	False
Encrypt SAML Assertion:	False