Entrust Datacard™

Trusted Identities | Secure Transactions

# Technical Integration Guide for Entrust IdentityGuard Federation Module 10.2 and Cisco ASA

Document issue: 3.0

May 2017

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

# Contents

# Introduction

This Technical Integration Guide provides an overview of how to integrate Entrust® IdentityGuard Federation Module with Cisco ASA using SAML 2.0. The aim of this integration is to add Entrust IdentityGuard multifactor authentication and single sign-on (SSO) to Cisco ASA.

More specifically, this guide describes how to enable the following features:

- Entrust IdentityGuard password for first-factor authentication
- Grid for second-factor authentication at level 1

To achieve the above functionality, this integration guide will have you configure the Cisco ASA as a SAML Service Provider (SP) and the Federation Module as a SAML Identity Provider (IDP).

While basic configuration examples are presented, complete documentation on SAML 2.0 including its functionality in Entrust IdentityGuard Federation Module and Cisco is not described. Consult the official documentation set of each product for details.

## Integration information

**Entrust IdentityGuard product** : Entrust IdentityGuard 10.2 Feature Pack 1 Patch 202062 (1289)

**Entrust IdentityGuard Federation Module** : Entrust IdentityGuard Federation Module Version 10.2 (580)

**Partner name** : Cisco Systems

**Partner product version** : Cisco ASAv 9.5 (2)

Check entrust Datacard Trusted Care for the latest supported version information at:

https://trustedcare.entrustdatacard.com

## Partner contact information

Contact Cisco at www.cisco.com, or by calling (800)553-NETS or (800)553-6387.

## Supported authentication methods

The Cisco software supports the Entrust IdentityGuard authentication methods and authentication protocols listed in Table 1.

### Table 1: Authentication methods

| Authentication method | Notes | Supported protocols |
|---|---|---|
| Password | Password authentication is first-factor authentication with Entrust IdentityGuard’s password feature. | SAML2.0 |
| Grid* | Two-step authentication only. | SAML2.0 |

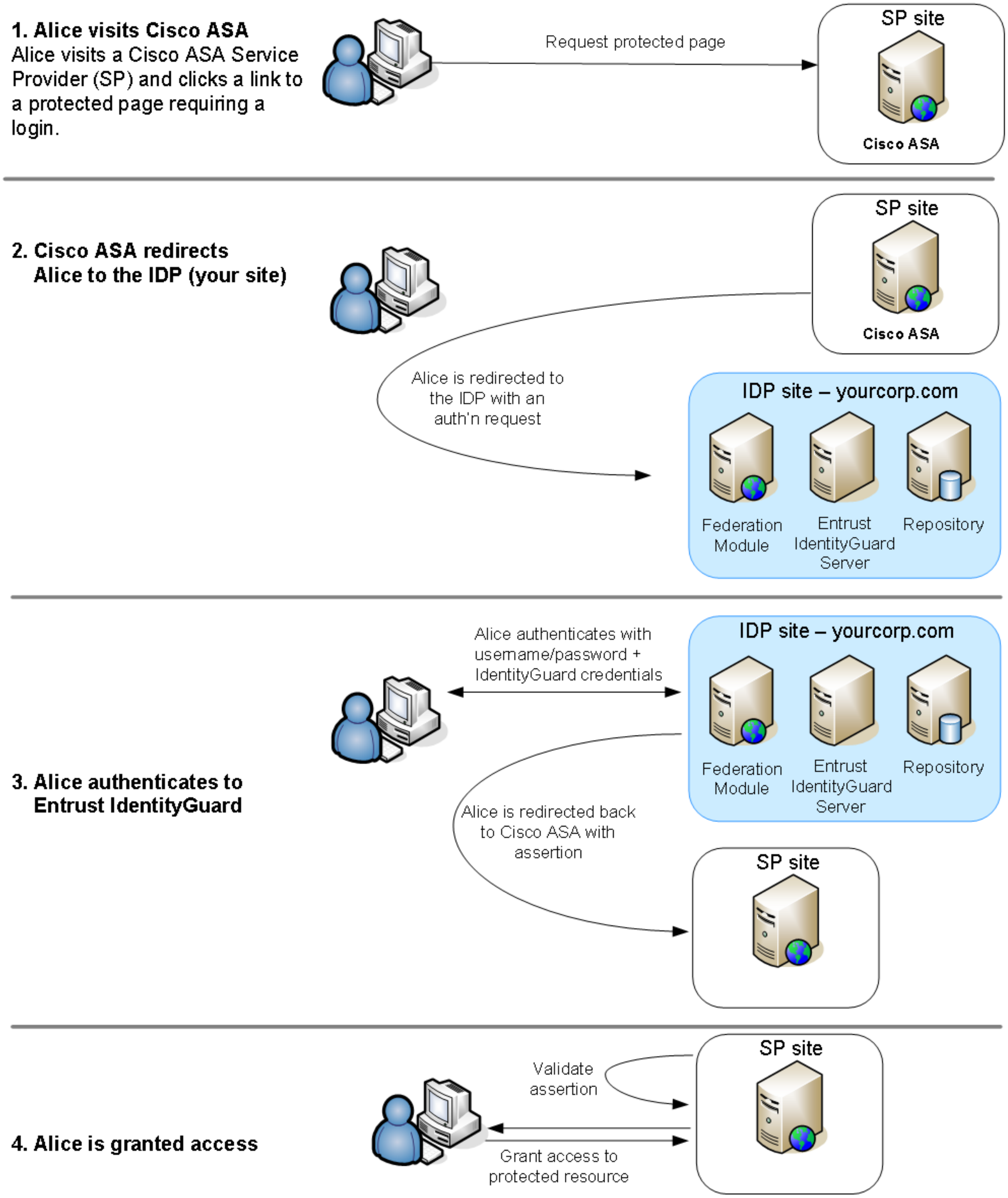
| Authentication method | Notes | Supported protocols |
|---|---|---|
| Token*[1] | Entrust IdentityGuard supports both response-only tokens and challenge/response tokens. | SAML2.0 |
| Temporary PIN* | Grid or token authentication must be configured. Supported over two step. | SAML2.0 |
| One-time password* | Two-Step Authentication supported | SAML2.0 |
| Knowledge-based questions and answers | The Radius proxy only supports a single question and answer. | SAML2.0 |
| Risk-based | IP/Geolocation only. Machine authentication must be disabled from the risk-based policies.<br>Normal or enhanced security level (not both).<br>Use IP-enabled method for Cisco SAML and put X-Forwarded-For as the Remote IP Header Name | SAML 2.0 |

[1] *Can also include a personal verification number (PVN). A PVN is an additional authentication feature that can be added to other authentication methods. Grid, token, or one-time password authentication must be configured.

# Integration overview

To integrate Cisco and the Federation Module, you must add Cisco URLs and key to the Federation Module, and vice versa. After the integration is complete, the login process occurs as shown in Figure 1.

### Figure 1: Logon process


1. Alice visits Cisco ASA
Alice visits a Cisco ASA Service Provider (SP) and clicks a link to a protected page requiring a login.
Request protected page
SP site
Cisco ASA
2. Cisco ASA redirects Alice to the IDP (your site)
SP site
Cisco ASA
Alice is redirected to the IDP with an auth'n request
IDP site – yourcorp.com
Federation Module
Entrust IdentityGuard Server
Repository
Alice authenticates with username/password + IdentityGuard credentials
IDP site – yourcorp.com
Federation Module
Entrust IdentityGuard Server
Repository
3. Alice authenticates to Entrust IdentityGuard
Alice is redirected back to Cisco ASA with assertion
SP site
Validate assertion
SP site
4. Alice is granted access
Grant access to protected resource

# Prerequisites

Before integrating the Federation Module with Cisco, install the Federation Module as an IDP following the instructions in the *Entrust IdentityGuard Federation Module Installation and Configuration Guide*, noting the following:

- Perform all pre-installation tasks, as outlined in the guide.
- Get your installation to the point where you can export the IDP Metadata, but do not actually export the data—it is not necessary to do so. After that, stop reading the *Federation Module Installation and Configuration Guide*, and follow the instructions in this document to complete the integration.

# Configuring the integration

This section contains the following topics:

- Installing the Federation Module and configuring the SAML keys
- Exporting the Federation Module verification certificate
- Exporting the IDP metadata file to Service Provider
- Configuring Cisco SAML server
- Configuring Entrust IdentityGuard Federation server authentication

## Installing the Federation Module and configuring the SAML keys

### To install the Federation Module and configure SAML keys

1. Install the Entrust IdentityGuard Federation Module according to the instructions in the *Entrust IdentityGuard Federation Module Installation and Configuration Guide*.
2. Stop at the section, "Generate SAML keys" and read the note below about generating SAML keys before proceeding further.

   **Note:** When you perform the steps in section 5, "Generate SAML keys," create a signing key pair using `the -signalias` key pair. Encryption is not required for Cisco. When the procedure directs you to run the `setSAMLKey` command, specify the signing key pair (`–signalias`) instead of an encryption key pair (`–encalias`).

3. Follow the instructions in section 5, "Generate SAML keys" of the *Entrust IdentityGuard Federation Module Installation and Configuration Guide* to generate the SAML keys using the guidance provided in the notes in step 2.
4. After generating the SAML keys, follow the procedures in the section, Exporting the Federation Module verification certificate" of this integration guide.

## Exporting the Federation Module verification certificate

### To export the verification certificate

1. From a command prompt on the Federation Module, navigate to

   ```
   <IGFMROOT>/jre1.6.0_24/bin/keytool.
   ```

2. Enter the following command all on one line:

   ```
   keytool -export -file "../../identityguardfederation92/etc/idp-scert.crt" –
   keystore "../../identityguardfederation92/etc/fm.keystore" -alias
   <signing_alias>
   ```

   Where `<signing_alias>` is the `–alias` value you specified when you installed the Federation Module and configured the SAML keys.

   Example: `"idp-skey"`

   Sample output:

   ```
   Enter keystore password:
   ```

```
Certificate stored in file
<../../identityguardfederation92/etc/idpscert.crt>
```

# Exporting the IDP metadata file to Service Provider

## To export the metadata file

1. Log into the Entrust IdentityGuard Federation Module Configuration Editor.

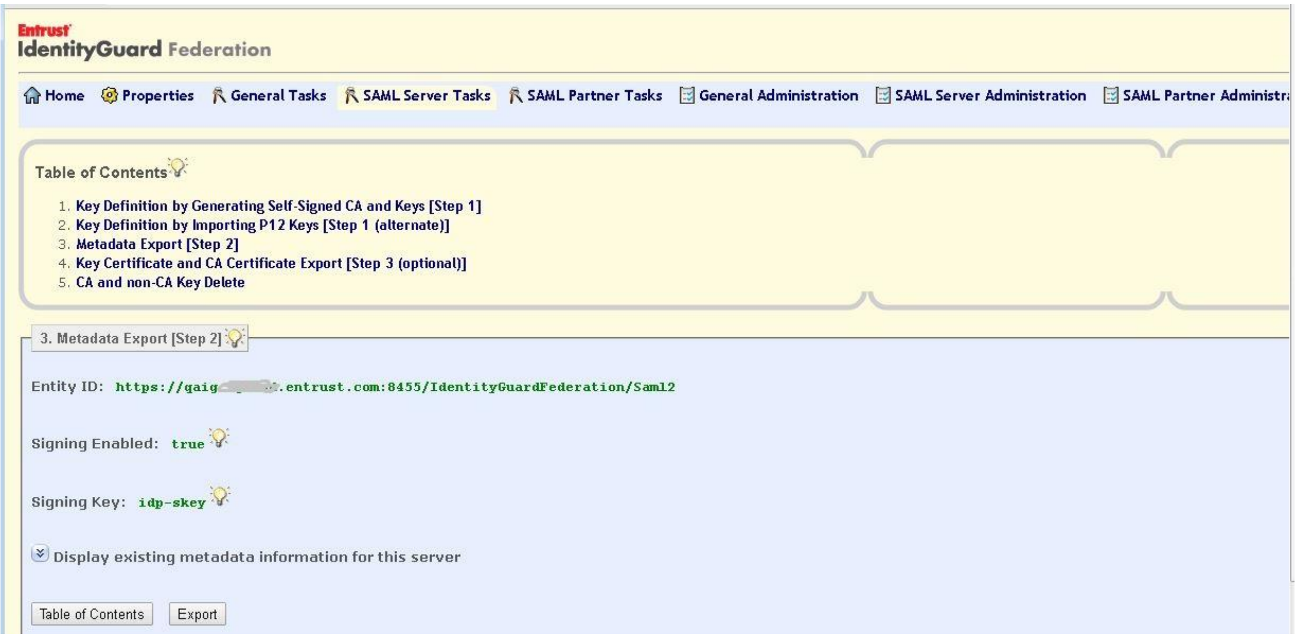


Table of Contents

1. Key Definition by Generating Self-Signed CA and Keys [Step 1]
2. Key Definition by Importing P12 Keys [Step 1 (alternate)]
3. Metadata Export [Step 2]
4. Key Certificate and CA Certificate Export [Step 3 (optional)]
5. CA and non-CA Key Delete

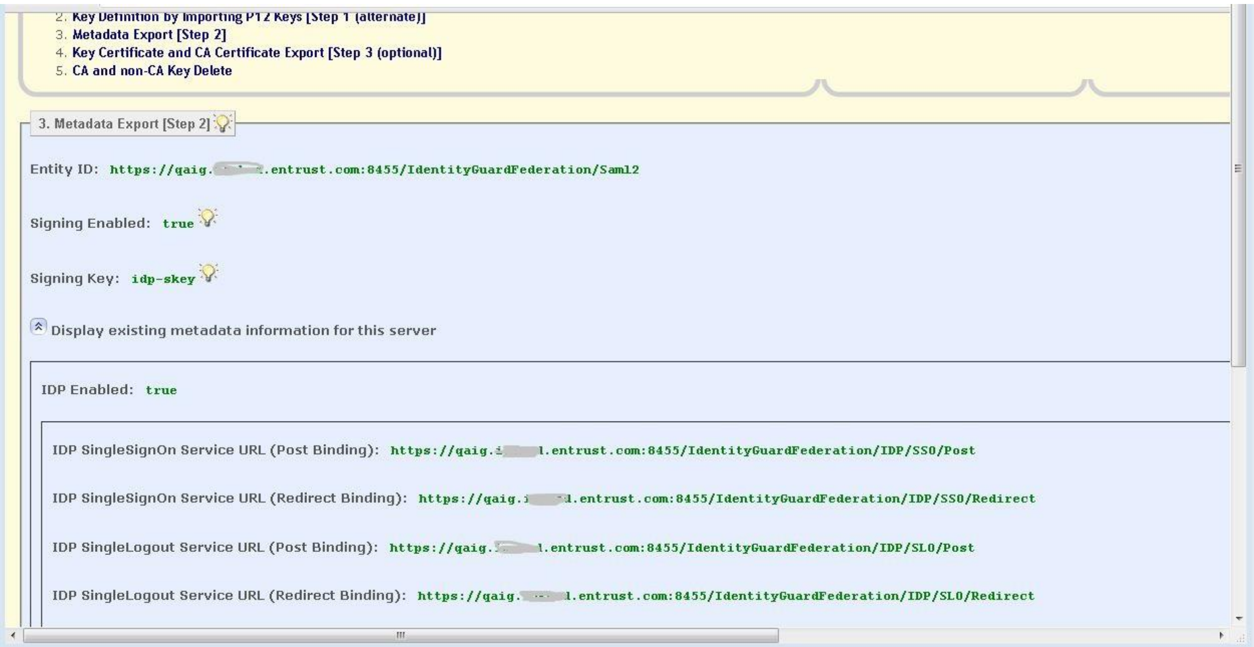
3. Metadata Export [Step 2]

Entity ID: `https://gaig[redacted].entrust.com:8455/IdentityGuardFederation/Saml2`

Signing Enabled: `true`

Signing Key: `idp-skey`

2. From the menu, click **SAML Server Tasks**.
3. Copy the Entity ID url to a text file and save it to a local folder, for example C:\IDP Metadata.
4. Click **Display existing metadata information for this server**. The following information appears.



2. Key Definition by Importing P12 Keys [Step 1 (alternate)]
3. Metadata Export [Step 2]
4. Key Certificate and CA Certificate Export [Step 3 (optional)]
5. CA and non-CA Key Delete

3. Metadata Export [Step 2]

Entity ID: https://qaig.[redacted].entrust.com:8455/IdentityGuardFederation/Saml2

Signing Enabled: true

Signing Key: idp-skey

Display existing metadata information for this server

IDP Enabled: true

IDP SingleSignOn Service URL (Post Binding): https://qaig.[redacted].entrust.com:8455/IdentityGuardFederation/IDP/SSO/Post

IDP SingleSignOn Service URL (Redirect Binding): https://qaig.[redacted].entrust.com:8455/IdentityGuardFederation/IDP/SSO/Redirect

IDP SingleLogout Service URL (Post Binding): https://qaig.[redacted].entrust.com:8455/IdentityGuardFederation/IDP/SLO/Post

IDP SingleLogout Service URL (Redirect Binding): https://qaig.[redacted].entrust.com:8455/IdentityGuardFederation/IDP/SLO/Redirect

5. Copy the **IDP SingleSignOn Service URL (Redirect Binding)** url to a text file and save it to a local folder**,** for example, `https://igfm.example.com:8455/IdentityGuardFederation/IDP/SSO/Redirect`.
6. Copy the **IDP SingleLogout Service URL (Redirect Binding)** url to a text file and save it to a local folder**,** for example, `https://igfm.example.com:8455/IdentityGuardFederation/IDP/SLO/Redirect`.

# Configuring Cisco SAML server

It is assumed that you are familiar with the administration interface of the Cisco ASAv appliance and you already have a working SSL VPN setup.

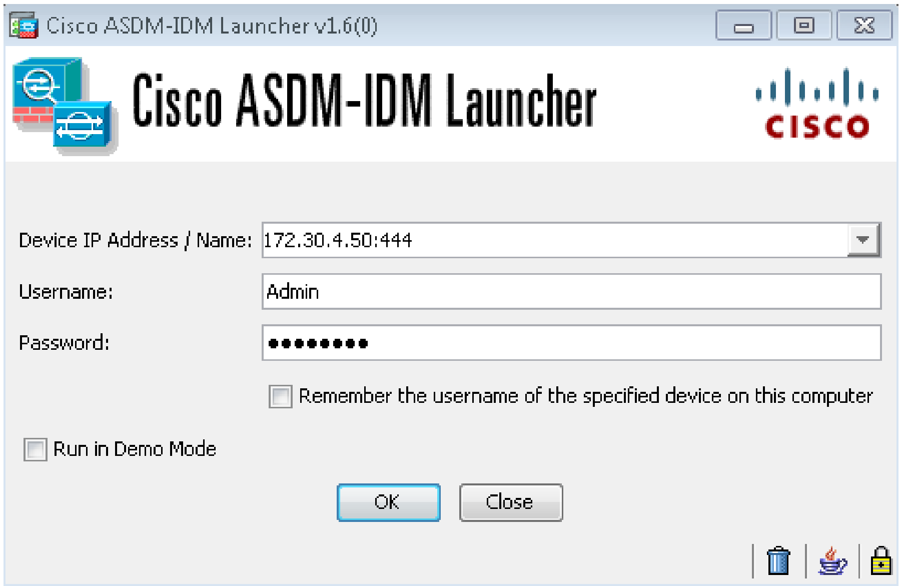
This section contains the following topics:

- Configuring Cisco ASA as a SAML 2.0 Service Provider (SP)
- Configuring a clientless Web SSL VPN connection profile
- Exporting Cisco SAML metadata file and certificate
- Configuring Entrust IdentityGuard Federation SAML Partner

## Configuring Cisco ASA as a SAML 2.0 Service Provider (SP)

### To configure Cisco as a SAML service provider

1. Log into the Cisco ASDM Version 7.5(2) or later.



Cisco ASDM-IDM Launcher v1.6(0)

Cisco ASDM-IDM Launcher

Device IP Address / Name: 172.30.4.50:444

Username: Admin

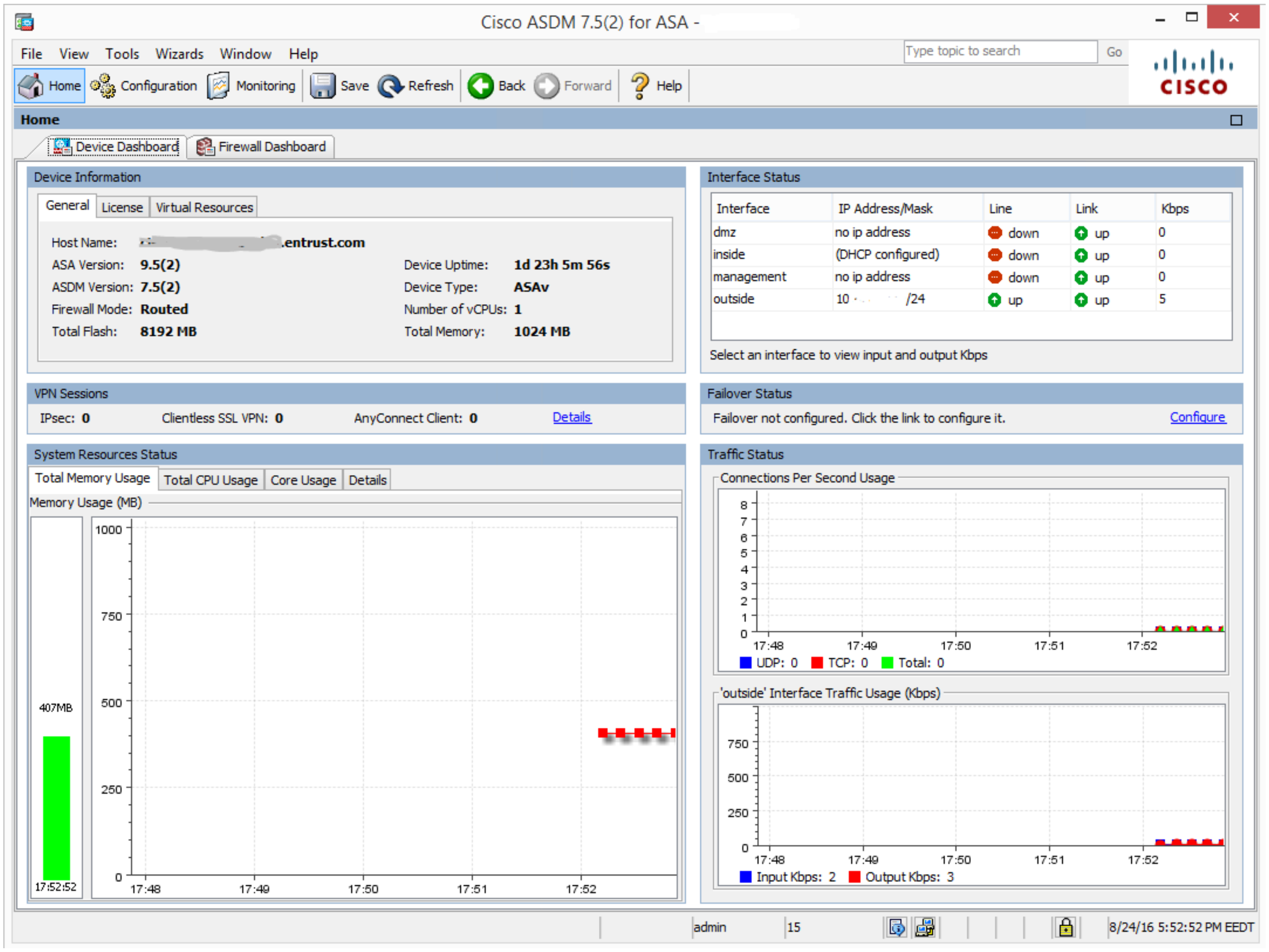
Password: ●●●●●●●●

□ Remember the username of the specified device on this computer

□ Run in Demo Mode

**Note:** Use the Cisco documentation to for information on downloading the ASDM setup.

The following Cisco ASA management console page appears.



Cisco ASDM 7.5(2) for ASA - [redacted]

File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
Home
Device Dashboard
Firewall Dashboard

Device Information

General | License | Virtual Resources

Host Name: [redacted].entrust.com

ASA Version: 9.5(2)

ASDM Version: 7.5(2)

Firewall Mode: Routed

Total Flash: 8192 MB

Device Uptime: 1d 23h 5m 56s

Device Type: ASAv

Number of vCPUs: 1

Total Memory: 1024 MB

Interface Status

| Interface | IP Address/Mask | Line | Link | Kbps |
|---|---|---|---|---|
| dmz | no ip address | down | up | 0 |
| inside | (DHCP configured) | down | up | 0 |
| management | no ip address | down | up | 0 |
| outside | 10 [redacted] /24 | up | up | 5 |

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details

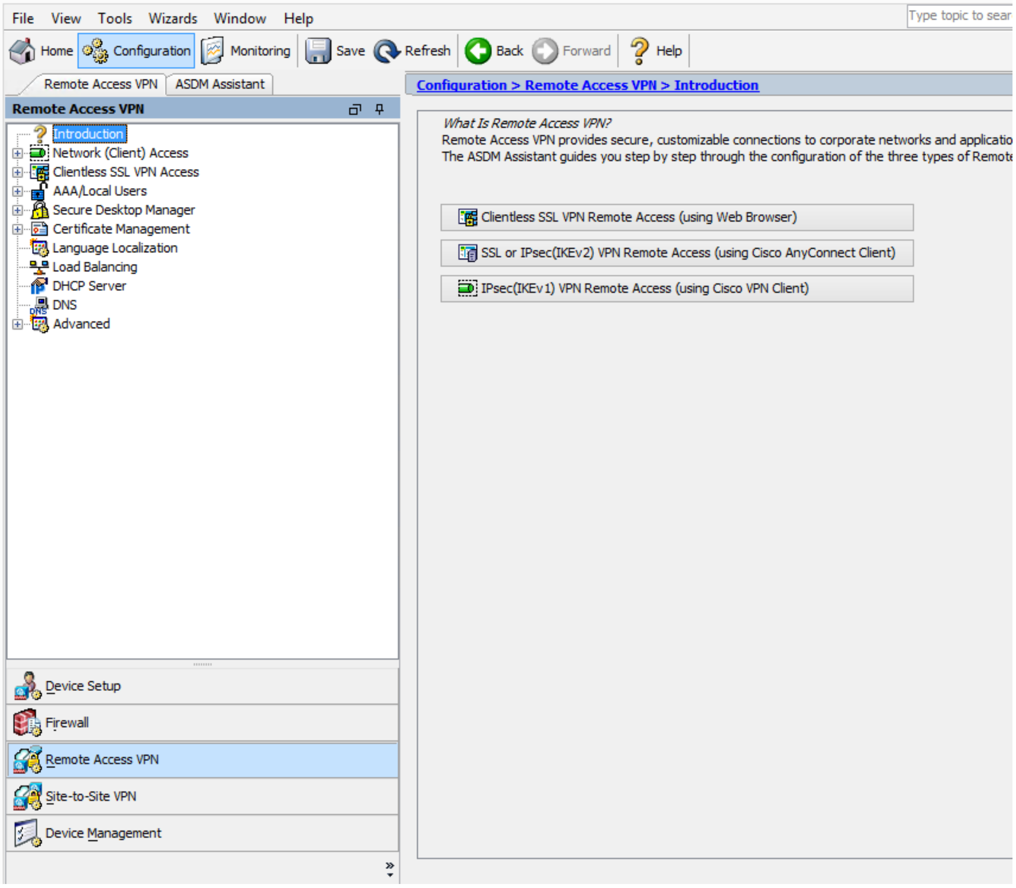
Failover Status

Failover not configured. Click the link to configure it. Configure

System Resources Status

Traffic Status

2. Select the **Configuration** tab. The following ASDM page appears.

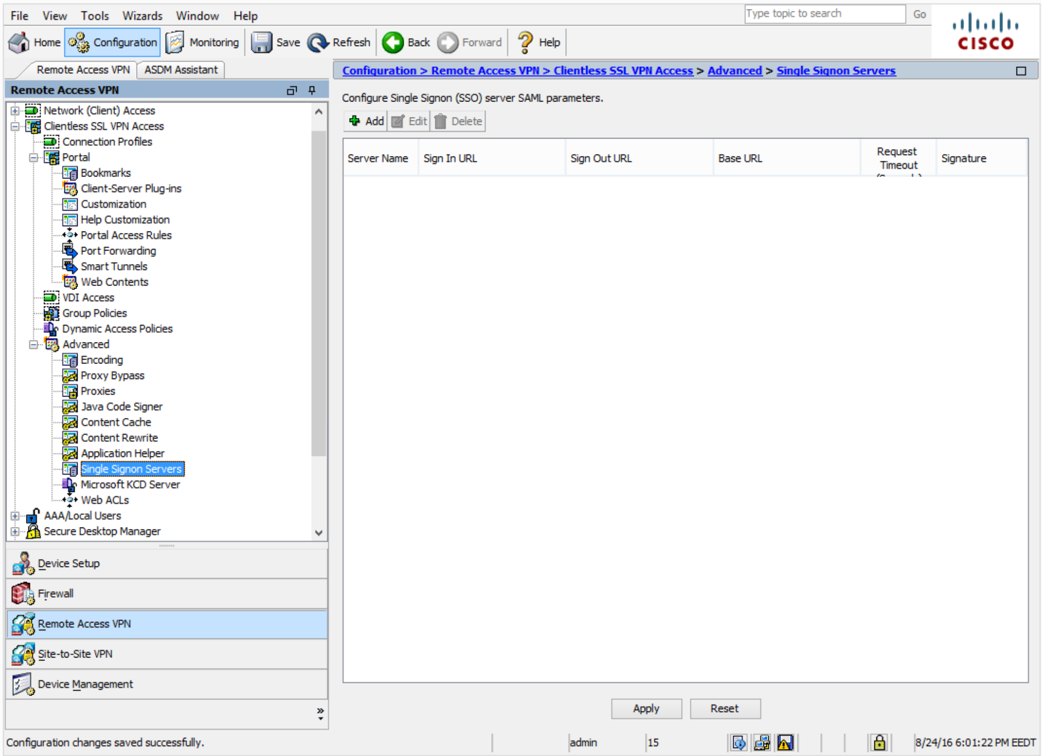


*What Is Remote Access VPN?*

Remote Access VPN provides secure, customizable connections to corporate networks and applicatio

The ASDM Assistant guides you step by step through the configuration of the three types of Remote

3. Click **Remote Access VPN** > **Clientless SSL VPN Access** in the left-pane of ASDM.



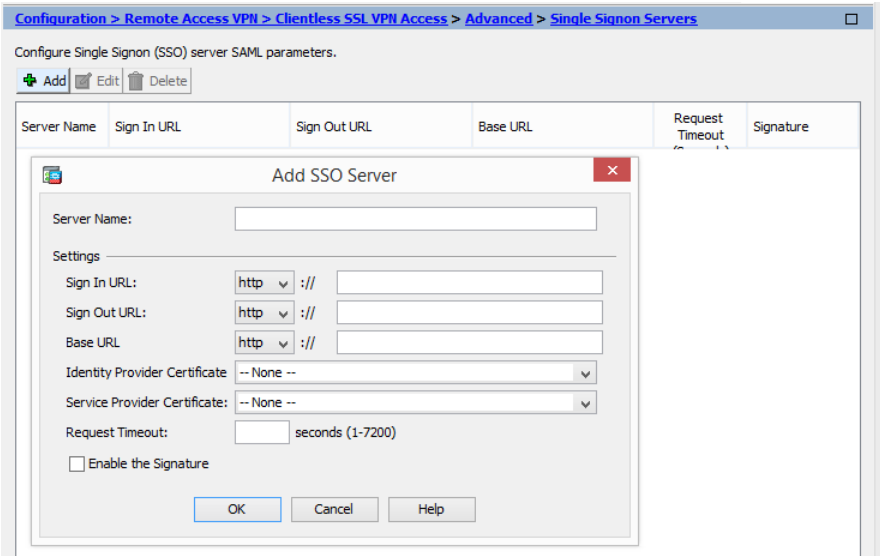
Configure Single Signon (SSO) server SAML parameters.

| Server Name | Sign In URL | Sign Out URL | Base URL | Request Timeout | Signature |
|---|---|---|---|---|---|

Configuration changes saved successfully.

4. Expand the **Clientless SSL VPN access > Advanced> Single Signon Servers**.

5. In the **Configure Single Signon (SSO) Server SAML** parameters pane click **Add**. The **ADD SSO server** page appears.


Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Signon Servers
Add
Edit
Delete
OK
Cancel
Help

Configure Single Signon (SSO) server SAML parameters.

| Server Name | Sign In URL | Sign Out URL | Base URL | Request Timeout | Signature |
|---|---|---|---|---|---|

Add SSO Server

Server Name:

Settings

Sign In URL: http ://

Sign Out URL: http ://

Base URL: http ://

Identity Provider Certificate: -- None --

Service Provider Certificate: -- None --

Request Timeout: seconds (1-7200)

□ Enable the Signature

6. In the **Server Name** field, enter the IDP Entity Id that you exported in the section, "Exporting the IDP metadata file to Service Provider."

7. In the **Settings** field, do the following:

   a. In the **Sign In URL** field, select **https** from the drop down list, and then enter the IDP SingleSignOn Service URL (Redirect Binding) url (without `https://`) that you exported in the section, "Exporting the IDP metadata file to Service Provider."

b. In the **Sign Out URL** field, select **https** from the drop-down list, and then enter the IDP SingleLogout Service URL (Redirect Binding) url (without `https://`) that you exported in the section, "Exporting the IDP metadata file to Service Provider."

c. In the **Base UR**L field, select **https** from the drop-down list, and then enter the Cisco FQDN name, for example, `ciscoasa.yourdomain.com`.

d. In the **Identity Provider Certificate** field, select Entrust IdentityGuard certificate from the drop-down list.

   **Note**: It assumed that you have already uploaded the Identity Provider certificate into Cisco ASA using the Certificate management option in Cisco ASA. See the Cisco ASA documentation for more information on certificate installations.

e. In the **Service Provider Certificate** field, select Cisco ASA self-sign or CA certificate from the drop down list.

f. In the **Request Timeout** field, enter the timeout assertion, for example, 7200.

g. Select **Enable the Signature** option if you want to verify the signature, else deselect it (Recommended).

h. Click **OK** to return to the Cisco ASA main console.

8. Click **Apply** on the Cisco ASA main console page

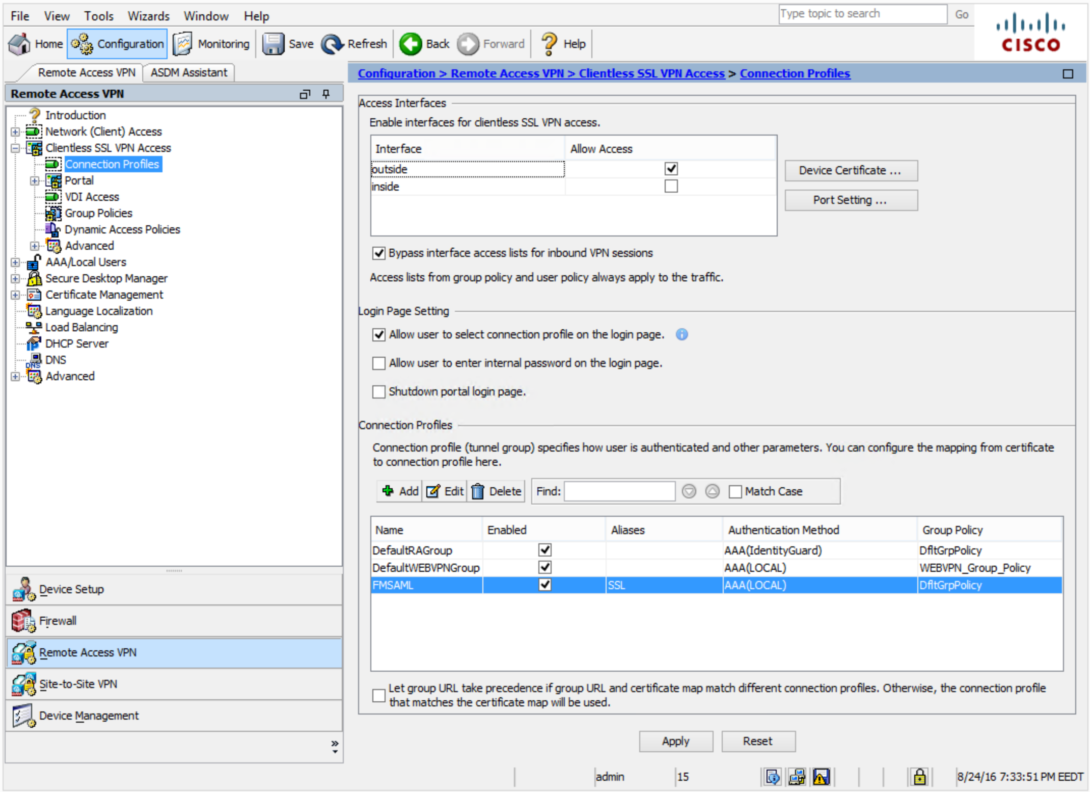
You have now completed the Cisco ASA SAML server configurations.

## Configuring a clientless Web SSL VPN connection profile

This configuration lets users establish a secure, remote-access VPN tunnel to the corporate network using a web browser.

### To configure a clientless Web SSL connection profile

1. On the Cisco ASA management console, navigate to **Configuration>Remote Access VPN** > **Clientless SSL VPN Access>Connection Profiles** on the left-pane in ASDM. The **Connections Profile** page appears.



Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|---|---|
| outside | ☑ |
| inside | ☐ |

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

☐ Allow user to enter internal password on the login page.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

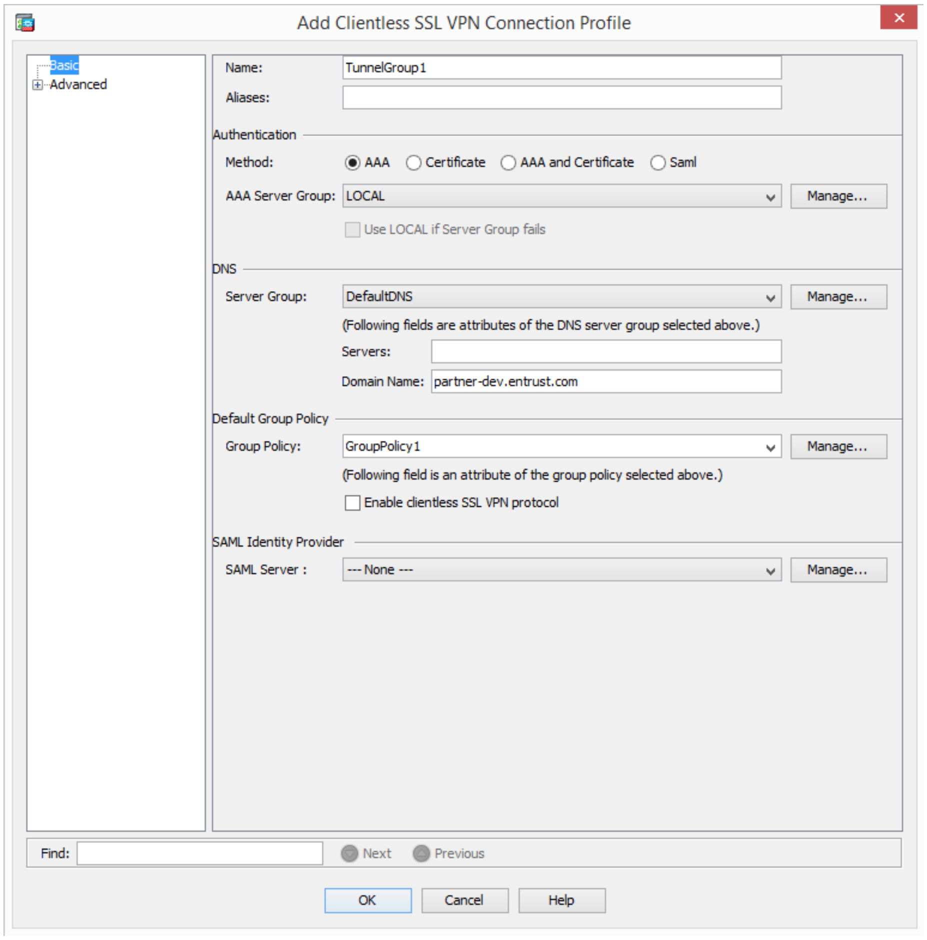
☐ Match Case

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|---|---|---|---|---|
| DefaultRAGroup | ☑ | | AAA(IdentityGuard) | DfltGrpPolicy |
| DefaultWEBVPNGroup | ☑ | | AAA(LOCAL) | WEBVPN_Group_Policy |
| FMSAML | ☑ | SSL | AAA(LOCAL) | DfltGrpPolicy |

☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

2. In the **Access Interface** pane, select the **Outside** checkbox.
3. Select the **Allow user to select connection profile on the login page** checkbox.
4. In the **Connections Profile** pane, click **Add**.

The **Add Clientless SSL VPN Connection Profile** page appears.



Name: TunnelGroup1

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ AAA and Certificate ○ Saml

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers:

Domain Name: partner-dev.entrust.com

Default Group Policy

Group Policy: GroupPolicy1

(Following field is an attribute of the group policy selected above.)

□ Enable clientless SSL VPN protocol

SAML Identity Provider

SAML Server : --- None ---

5. In the tree view, select **Basic** and then complete the following:
   - **a.** In the **Name** field, enter a name for the clientless connection profile.
   - **b.** In the **Aliases** field, enter an alias for the connection profile. The alias is what the user will select from on the Web SSL login page. If the alias contains a space, enclose it in quotation marks (for example, `"SAML Alias"`).
   - **c.** For the Authentication Method, select SAML.
   - **d.** From the **DNS Server Group** drop-down list, select the **DefaultDNS** server group.
   - **e.** In the **Servers** field, enter the IP address of the DNS server group.
   - **f.** In the **Domain Name** field, enter the DNS domain name.
   - **g.** From the **Group Policy** drop-down list, select a group policy or leave at default GroupPolicy1.
   - **h.** Select **Enable clientless SSL VPN protocol** check box.
   - **i.** In the **SAML Identity Provider** field, select the SAML server you have configured in the section "Configuring Cisco ASA as a SAML 2.0 Service Provider (SP)."
6. Click **OK** to return the Cisco ASA main console page.
7. Click **Apply** on the Cisco ASA main console page.

# Exporting Cisco SAML metadata file and certificate

### To download Cisco SAML metadata XML file

1. In the browser enter `https://ciscoasa.yourdomain.com/saml/sp/metadata/SSLVPN`.

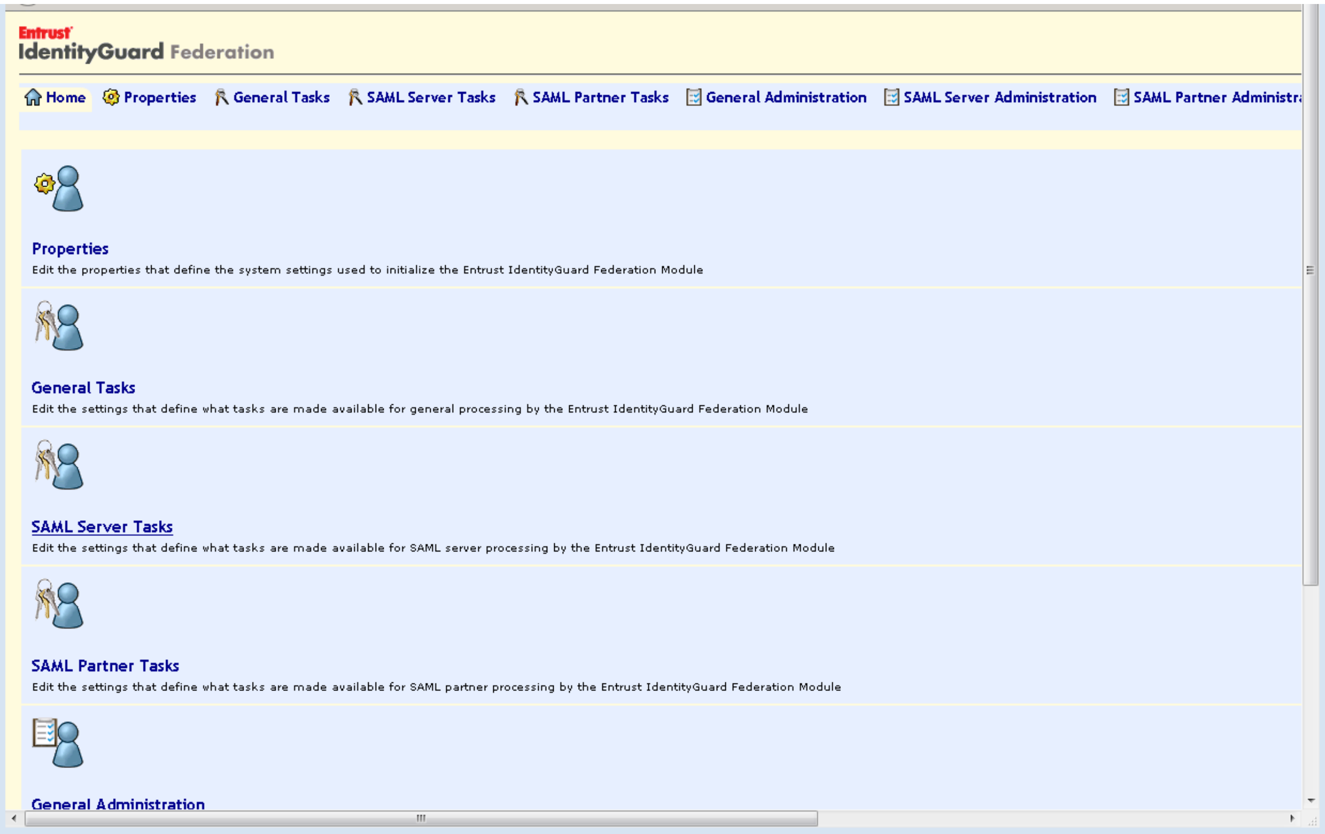
   In this URL, the SSLVPN is the Tunnel group name or SSL VPN connection profile name that you configured in the section "Configuring Cisco ASA as a SAML 2.0 Service Provider (SP)."

2. Download the Cisco SAML metadata file and Cisco certificate.
3. Export the Cisco SAML metadata file and Cisco certificate into the local folder of Entrust IdentityGuard Federation server.

# Configuring Entrust IdentityGuard Federation SAML Partner

### To configure SAML partner or Service Providers (SP) metadata and certificate

1. Login to Entrust IdentityGuard Federation Configuration Editor. The **Configuration Editor** appears.



Properties
Edit the properties that define the system settings used to initialize the Entrust IdentityGuard Federation Module

General Tasks
Edit the settings that define what tasks are made available for general processing by the Entrust IdentityGuard Federation Module

SAML Server Tasks
Edit the settings that define what tasks are made available for SAML server processing by the Entrust IdentityGuard Federation Module

SAML Partner Tasks
Edit the settings that define what tasks are made available for SAML partner processing by the Entrust IdentityGuard Federation Module

General Administration

2. From the menu bar, click **SAML Partner Tasks**. The **SAML Partner Task** page appears.

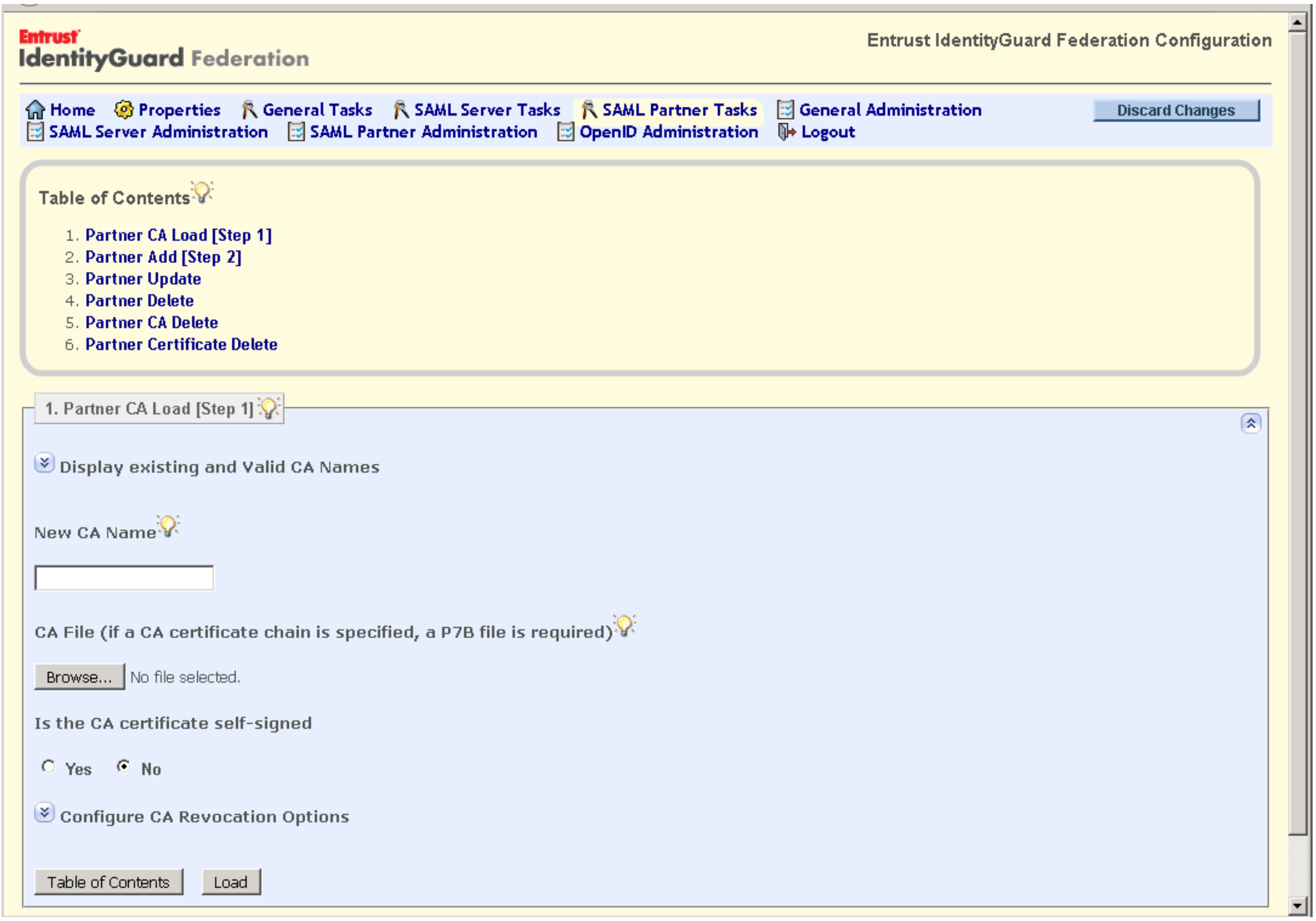


Table of Contents

1. Partner CA Load [Step 1]
2. Partner Add [Step 2]
3. Partner Update
4. Partner Delete
5. Partner CA Delete
6. Partner Certificate Delete

1. Partner CA Load [Step 1]

Display existing and Valid CA Names

New CA Name

CA File (if a CA certificate chain is specified, a P7B file is required)

Browse... No file selected.

Is the CA certificate self-signed

○ Yes ● No

Configure CA Revocation Options

**3.** Click **Partner CA Load [Step 1]** and complete the following:

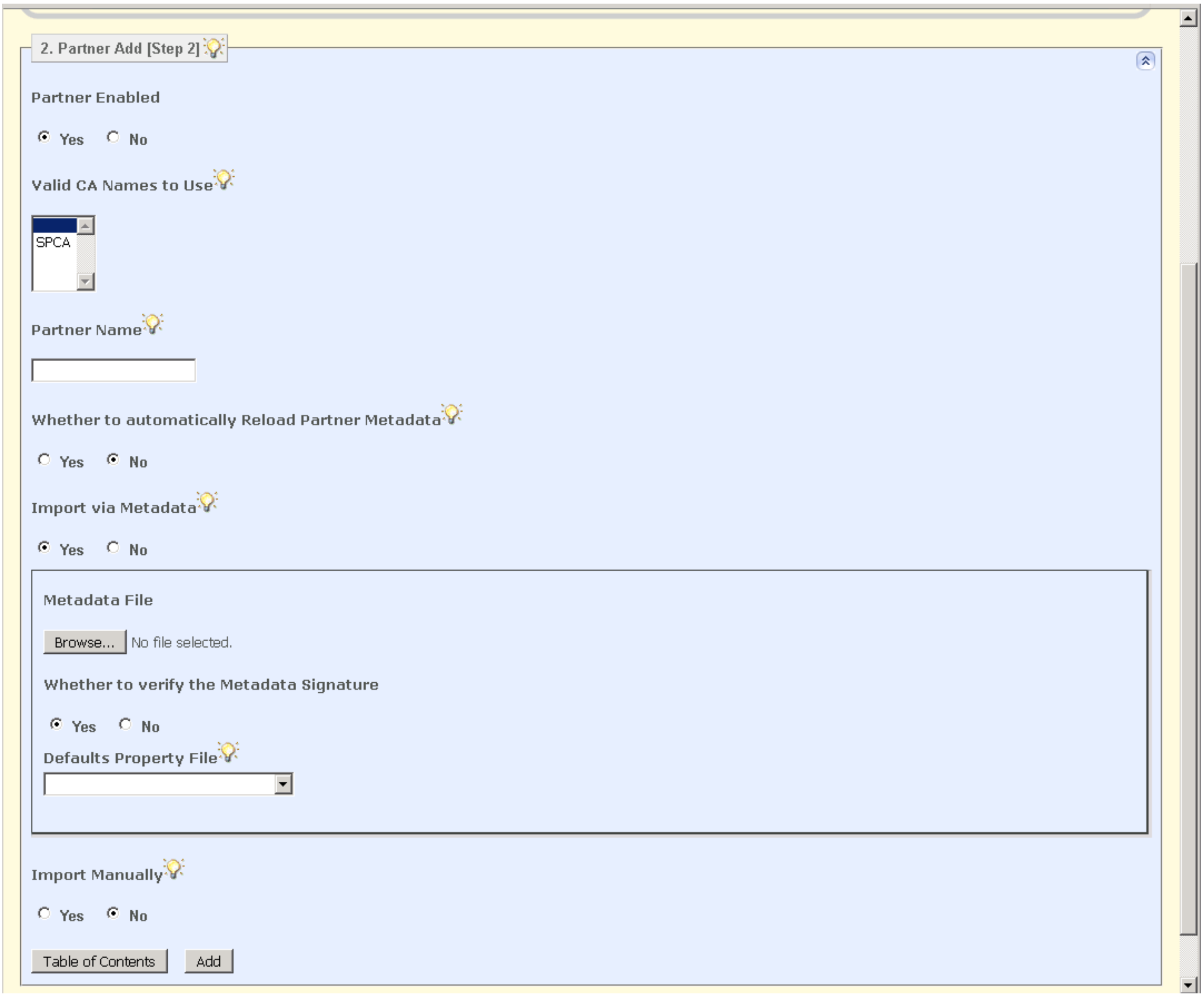
**a.** In the **New CA Name** field, enter the name for the Service Provider.

**4.** Click **Browse** and select the Cisco (Service Provider) certificate that you exported in the section," Exporting Cisco SAML metadata file and certificate".

**5.** Select **Yes** if the CA certificate is self-signed. If not, select **No**.

**6.** Click **Load**.

**7.** Click **Partner Add [Step 2]**. The following page appears.



2. Partner Add [Step 2]

Partner Enabled

● Yes ○ No

Valid CA Names to Use

SPCA

Partner Name

Whether to automatically Reload Partner Metadata

○ Yes ● No

Import via Metadata

● Yes ○ No

Metadata File

Browse... No file selected.

Whether to verify the Metadata Signature

● Yes ○ No

Defaults Property File

Import Manually

○ Yes ● No

Table of Contents Add

8. To add the partner metadata file, do the following:
   a. In the **Partner Enabled** field, select **Yes**.
   b. In the **Valid CA Names to Use** field, select the CA certificate that you configured in step 3 (**Partner CA Load [Step 1]**).
9. In the **Partner Name** field, enter the name for the Service Provider, for example, `SP_Metadata`.
10. In the **Import via Metadata** field, select **Yes**.
11. In the **Metadata File**, click **Browse** and select the SP metadata file that you exported in the section, "Exporting Cisco SAML metadata file and certificate."
12. Select **Yes**, if you want to verify the metadata signature or select No.
13. In the **Default Property File** drop-down list, select **Cisco.defaults.properties**.
14. In the **Import Manually** field, select **No**.
15. Click **Add**.

You have now exported and uploaded the Service Provider Metadata and CA certificate to Entrust IdentityGuard Federation Server (Idp).

# Configuring Entrust IdentityGuard Federation server authentication

This section includes procedures for configuring one-step and two-step authentication in Entrust IdentityGuard Federation Server.

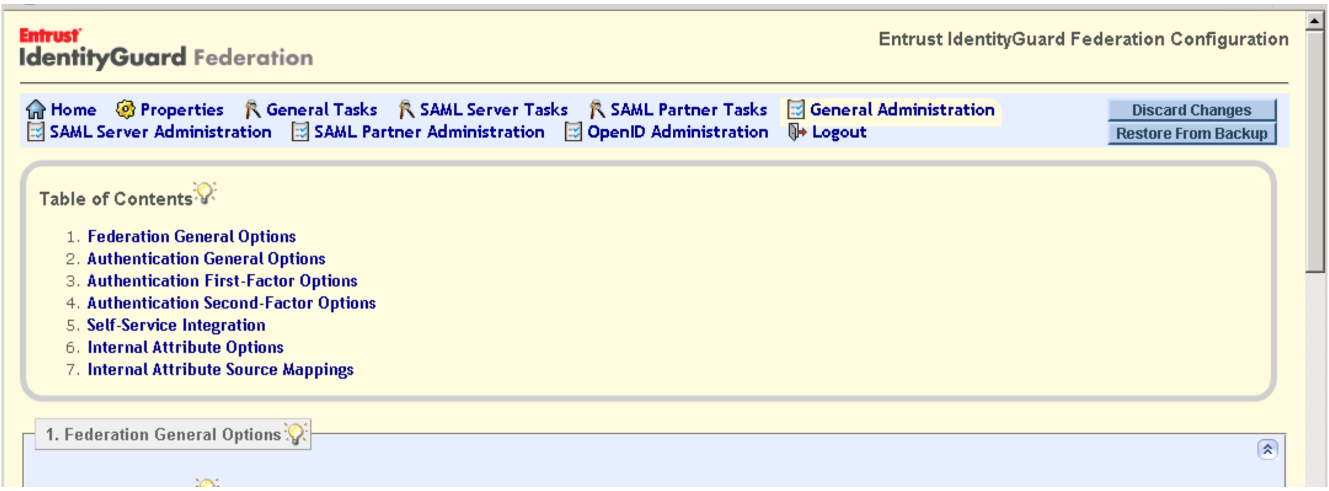
This section includes the following topics:

- Configuring Entrust IdentityGuard Federation server for one-step authentication
- Configuring Entrust IdentityGuard Federation server for two-step authentication

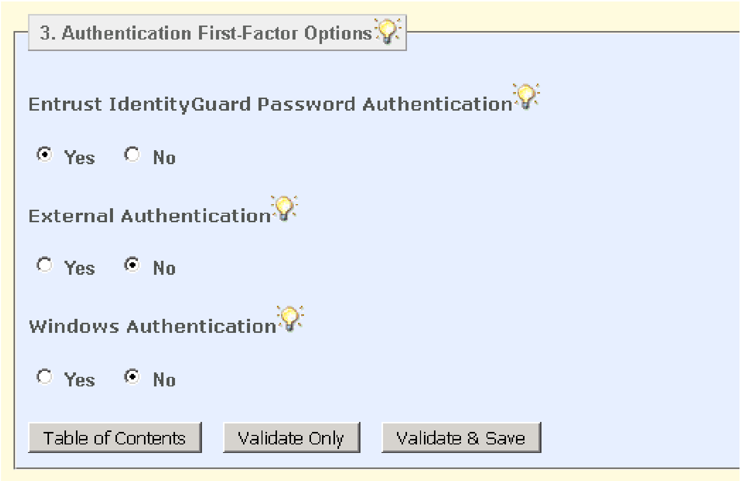
## Configuring Entrust IdentityGuard Federation server for one-step authentication

### To set up Entrust IdentityGuard Federation Server for one-step authentication

1. Login to Entrust IdentityGuard Federation Server.


Entrust
IdentityGuard Federation
Entrust IdentityGuard Federation Configuration
Home
Properties
General Tasks
SAML Server Tasks
SAML Partner Tasks
General Administration
SAML Server Administration
SAML Partner Administration
OpenID Administration
Logout
Discard Changes
Restore From Backup
Table of Contents
1. Federation General Options
2. Authentication General Options
3. Authentication First-Factor Options
4. Authentication Second-Factor Options
5. Self-Service Integration
6. Internal Attribute Options
7. Internal Attribute Source Mappings
1. Federation General Options

2. Click the **General Administration** tab.
3. Click **Authentication First-Factor Options**. The first factor authentication options appear.



3. Authentication First-Factor Options

Entrust IdentityGuard Password Authentication

● Yes ○ No

External Authentication

○ Yes ● No

Windows Authentication

○ Yes ● No

4. In the **Entrust IdentityGuard Password Authentication** field, select Yes.
5. Leave the other settings at the default values.
6. Click **Validate & Save**.
7. Restart the Entrust IdentityGuard Federation services for the changes to take effect.

# Configuring Entrust IdentityGuard Federation server for two-step authentication

## To set up Entrust IdentityGuard Federation Server for two-step authentication

1. Login to Entrust IdentityGuard Federation Server.

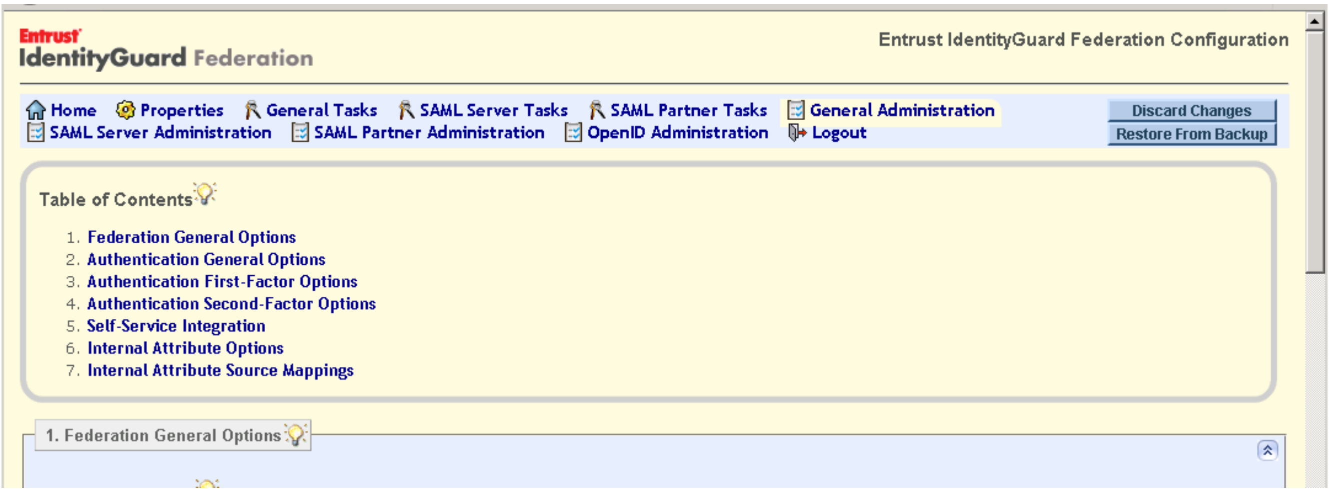
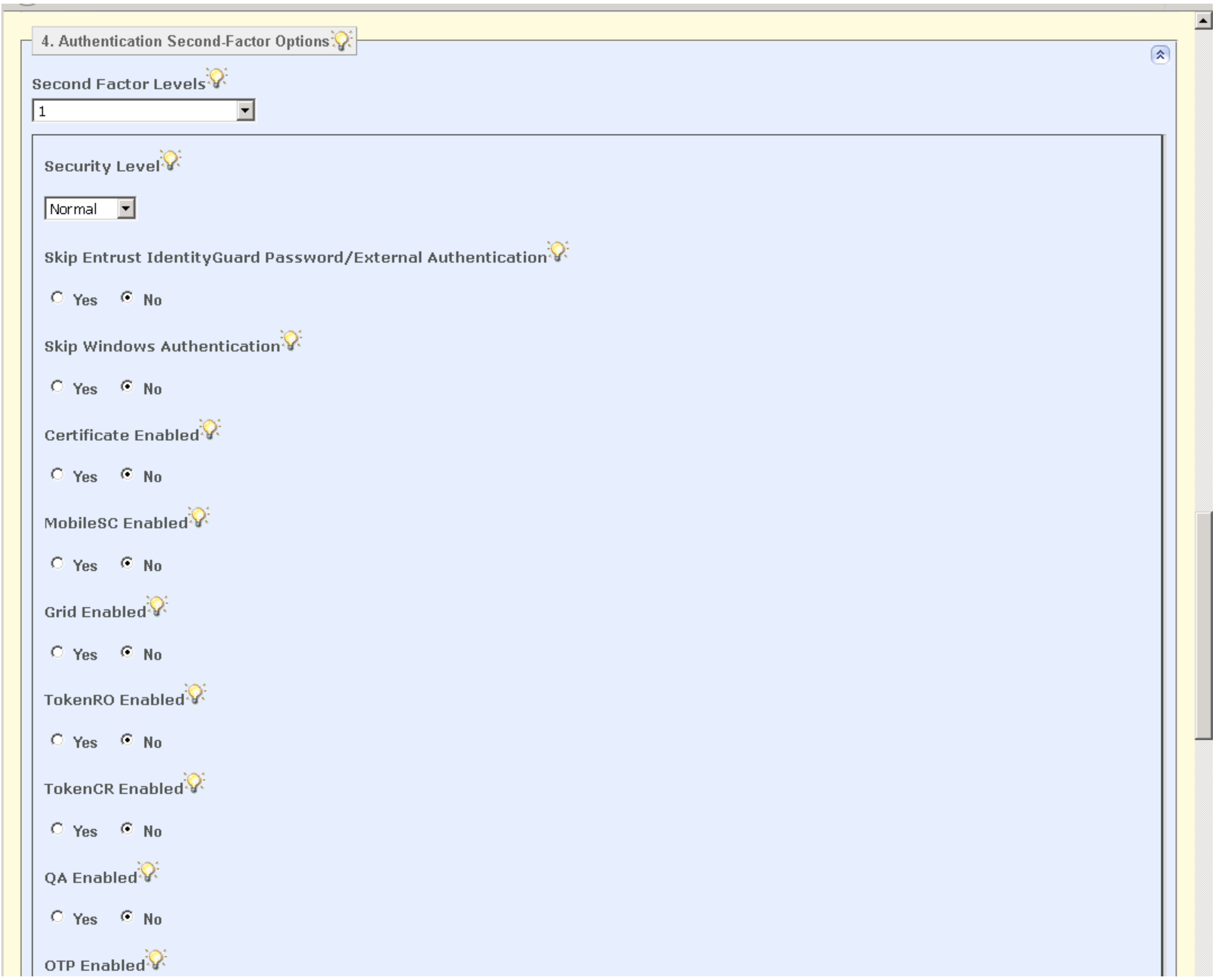


Table of Contents

1. Federation General Options
2. Authentication General Options
3. Authentication First-Factor Options
4. Authentication Second-Factor Options
5. Self-Service Integration
6. Internal Attribute Options
7. Internal Attribute Source Mappings

1. Federation General Options

2. Click the **General Administration** tab.
3. Click **Authentication Second-Factor Options**. The second factor authentication options appear.



4. Authentication Second-Factor Options

Second Factor Levels: 1

Security Level: Normal

Skip Entrust IdentityGuard Password/External Authentication

○ Yes ● No

Skip Windows Authentication

○ Yes ● No

Certificate Enabled

○ Yes ● No

MobileSC Enabled

○ Yes ● No

Grid Enabled

○ Yes ● No

TokenRO Enabled

○ Yes ● No

TokenCR Enabled

○ Yes ● No

QA Enabled

○ Yes ● No

OTP Enabled

4. In the **Security Level** field, select **Normal**.
5. Select the authentication method types, for example, select **Grid Enabled** and then select **Yes** to enable the second-factor authentication.
6. Click **Validate & Save**.
7. Restart the Entrust IdentityGuard Federation services for the changes to take effect.

# Testing the integration

This section includes the following topics:

- Testing IDP-initiated login
- Testing SP-initiated login
- Testing IDP-initiated logout
- Testing SP-initiated logout
- Testing Cisco using a PVN with your second-factor authentication response

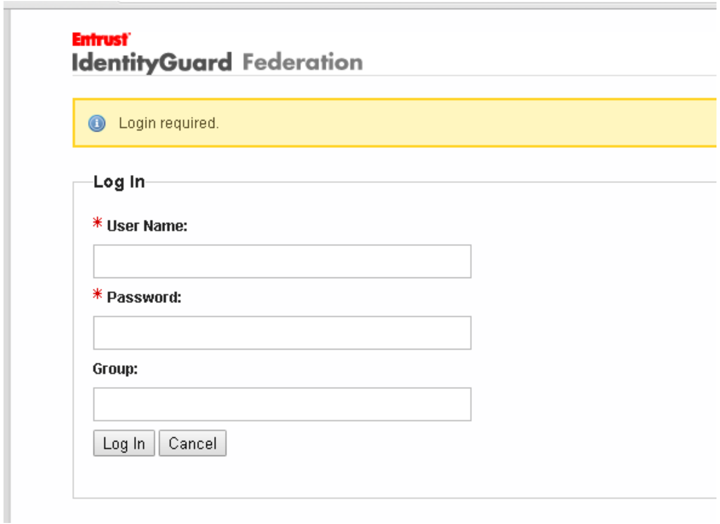
## Testing IDP-initiated login

Users may want to log in first to the Federation Module at your organization, and then switch to Cisco SSL portal. This is called an IDP-initiated login, or an unsolicited login.

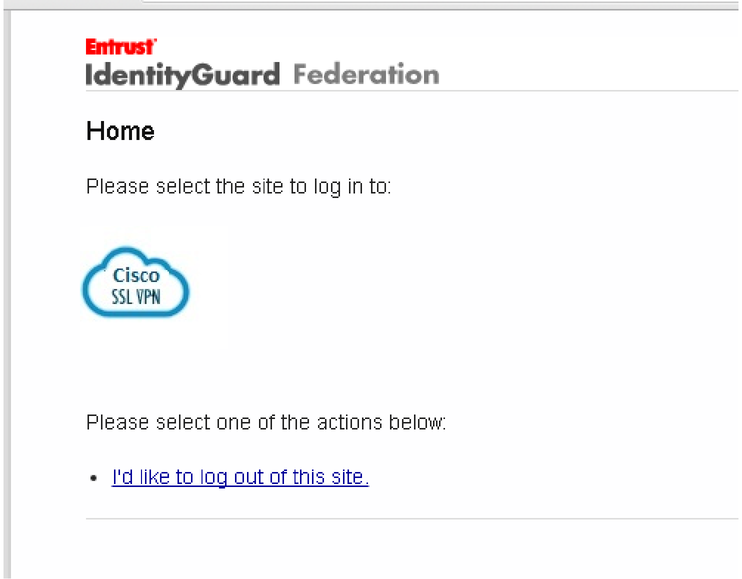
### To perform an unsolicited login

1. Log in to the Federation Module using your Web browser. For example, `https://fm.yourcorp.com:8455/IdentityGuardFederation/`

   You are redirected with the Entrust IdentityGuard Federation First Factor login window.



2. In the **User Name** field, enter the Entrust IdentityGuard server username.
3. In the **Password** field, enter the Entrust IdentityGuard server user password.
4. The **Group** field is optional. The Entrust IdentityGuard user belongs to the group.
5. Click **Login**. You are brought to the Cisco select the site log in page.



Entrust IdentityGuard Federation

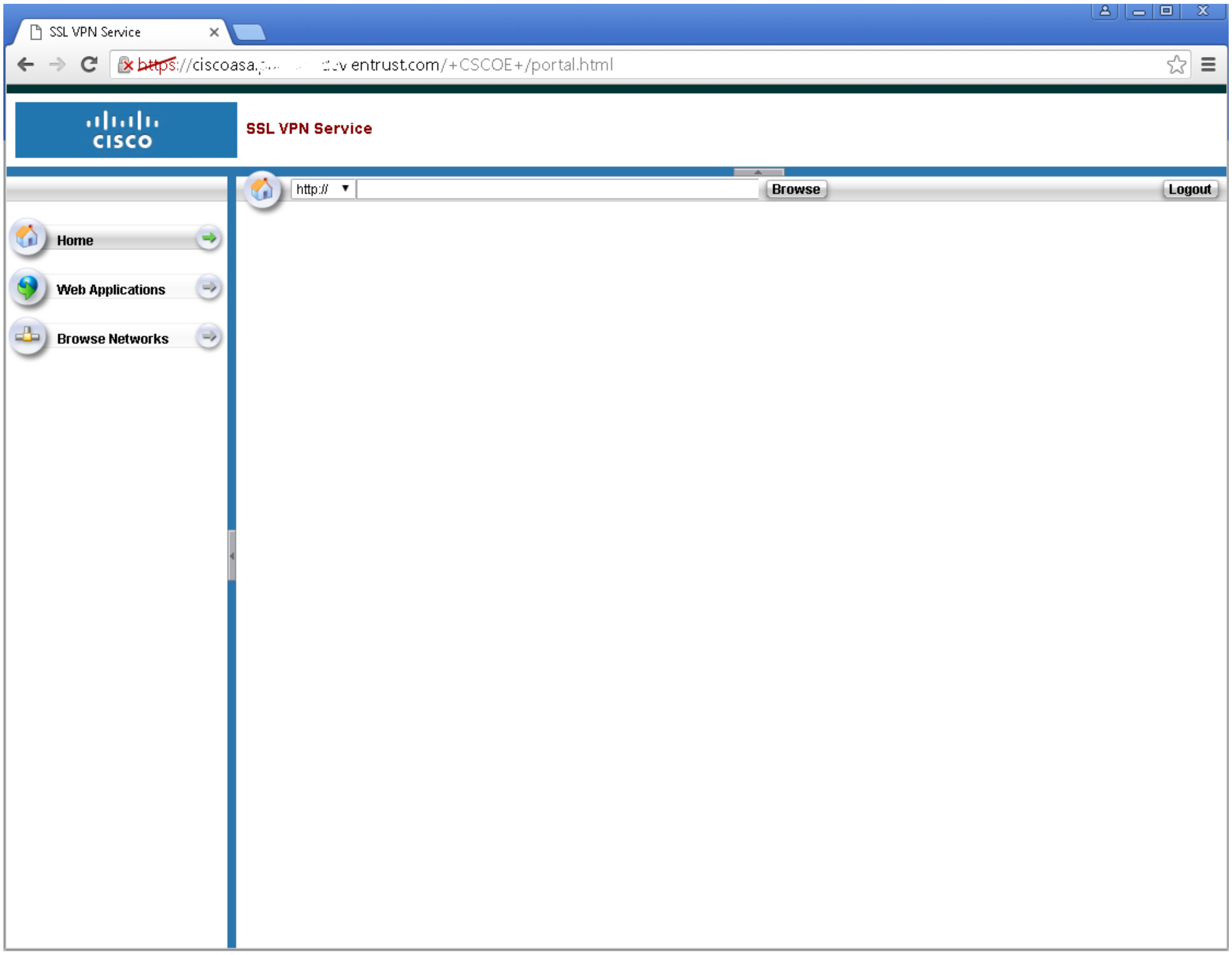
Home

Please select the site to log in to:

Please select one of the actions below:

- I'd like to log out of this site.

6. Select the site icon displayed on the page, for example, Cisco.
7. Click **OK**. You are brought to the **Cisco User Portal** page.

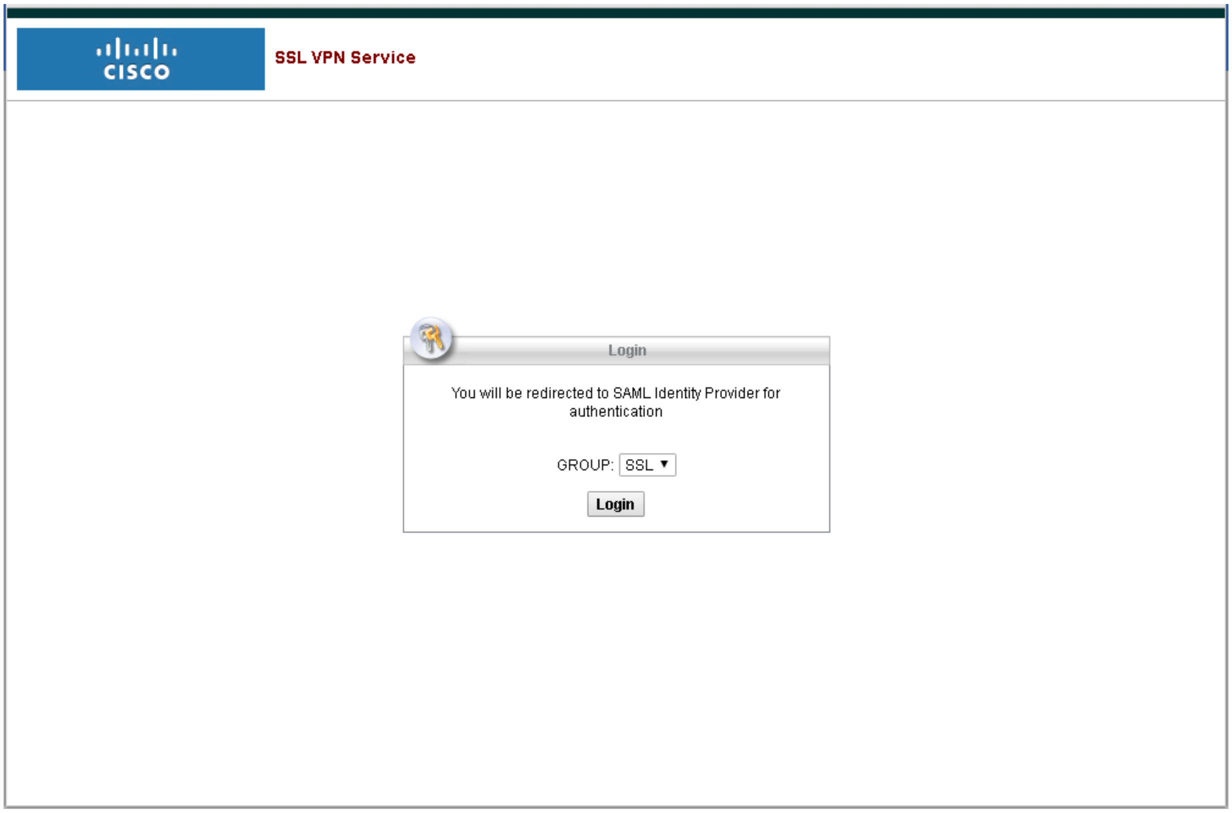


## Testing SP-initiated login

Users might want to log in directly to Cisco, without navigating to the Federation Module first. This is called an SP-initiated login, or a solicited login.

### To test Cisco SP-initiated login

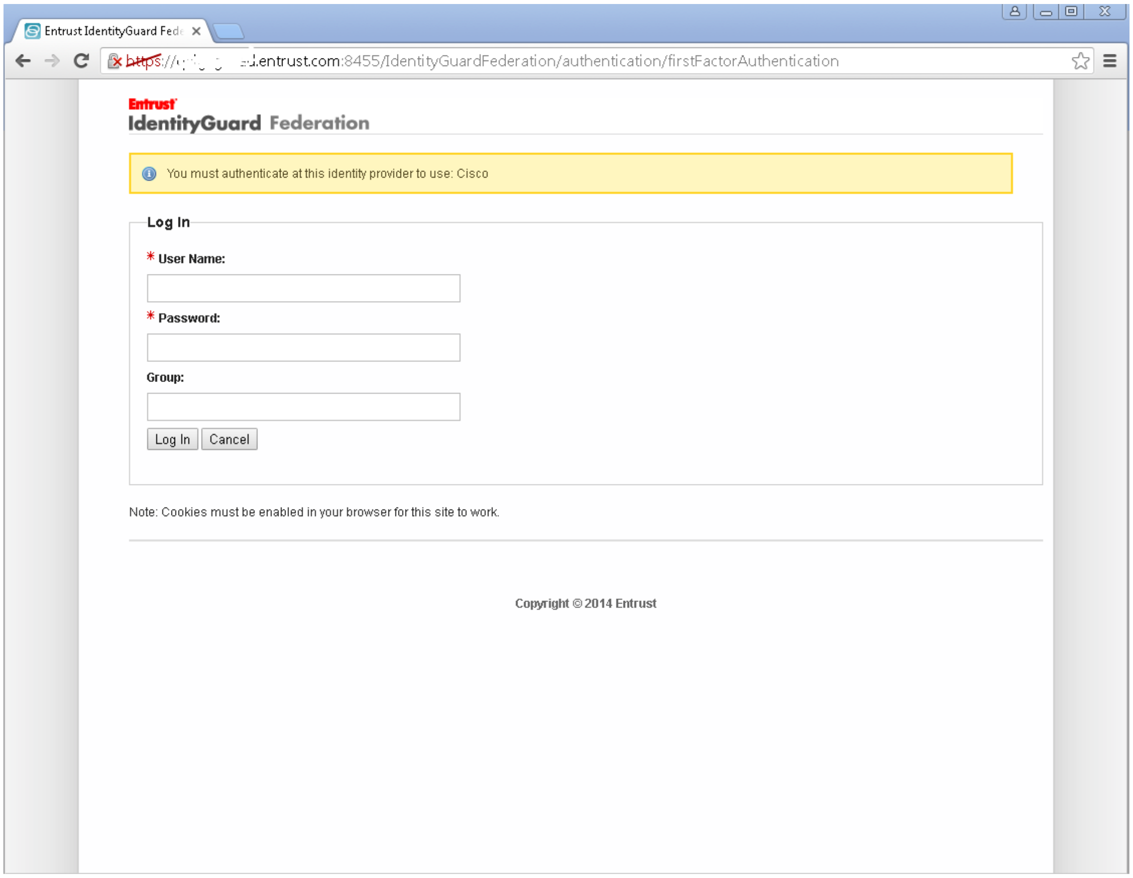
1. Open a Web browser on the client computer.
2. Enter the https://ciscoasa.yourdomain.com or `<https://172.30.20.15>` IP address (where the IP address is the Cisco SSL VPN). You are brought to the Cisco SSL login page.



You will be redirected to SAML Identity Provider for authentication

GROUP: SSL

3. Select the SSL VPN **Group** aliases from the drop-down list and click **Login**. You are redirected to the Entrust IdentityGuard Federation First Factor login window.


Entrust IdentityGuard Fed
https://[redacted].entrust.com:8455/IdentityGuardFederation/authentication/firstFactorAuthentication
Entrust
IdentityGuard Federation

You must authenticate at this identity provider to use: Cisco

Log In

* User Name:

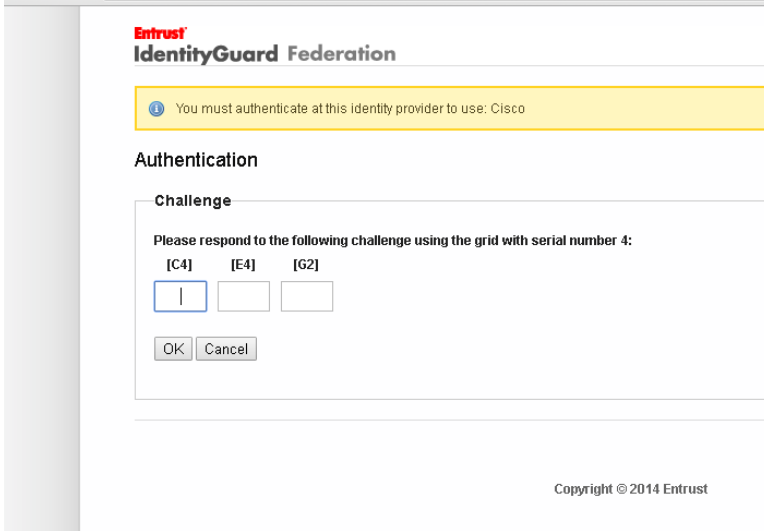
* Password:

Group:

Note: Cookies must be enabled in your browser for this site to work.

Copyright © 2014 Entrust

4. In the **User Name** field, enter the Entrust IdentityGuard server username.
5. In the **Password** field, enter the Entrust IdentityGuard server user password.
6. The **Group** field is optional. The Entrust IdentityGuard user belongs to the group.
7. Click **Login**. You brought to the Entrust IdentityGuard second-factor authentication page.



You must authenticate at this identity provider to use: Cisco

Authentication

Challenge

Please respond to the following challenge using the grid with serial number 4:

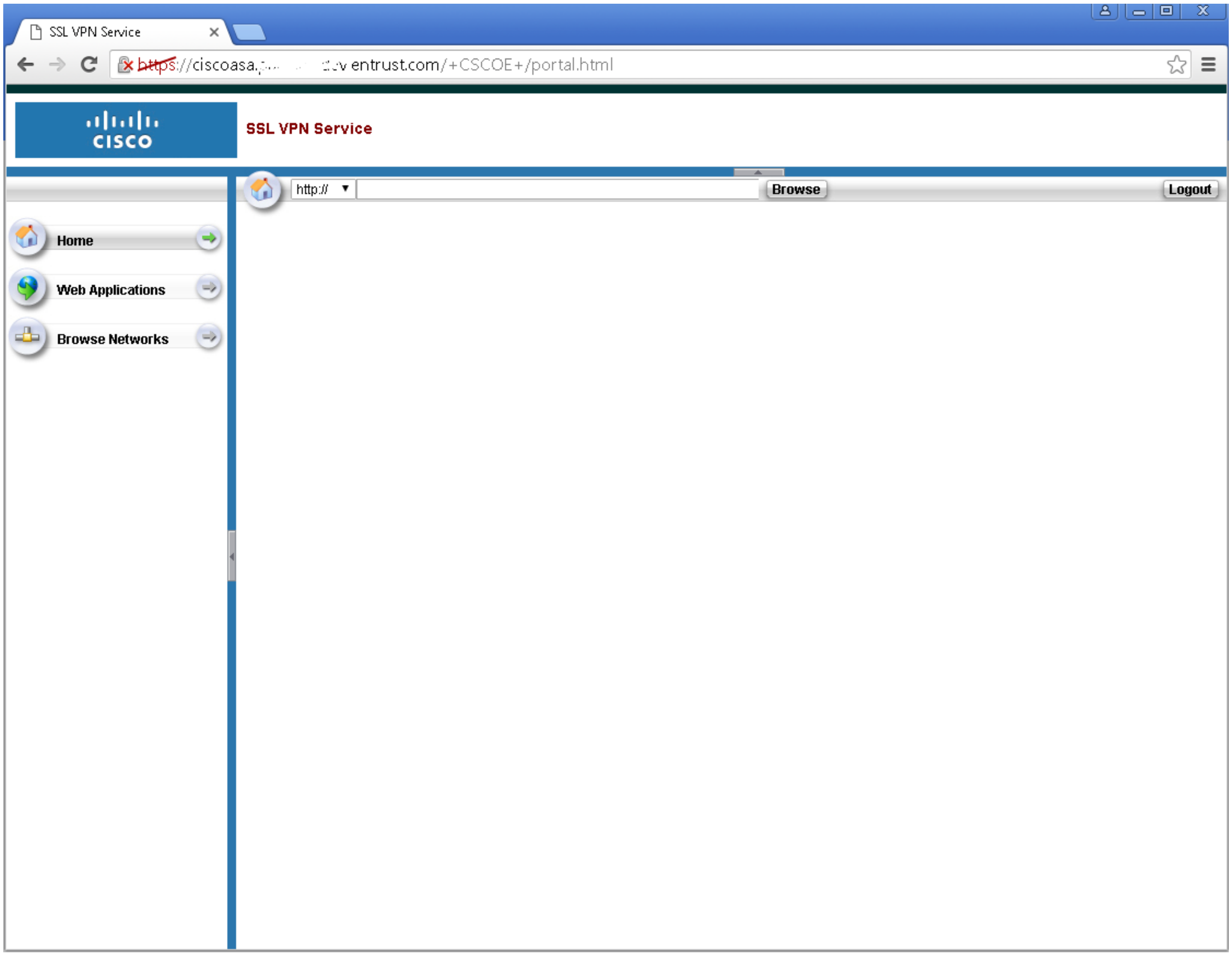
[C4] [E4] [G2]

Copyright © 2014 Entrust

8. In the **Challenge** field, enter the Grid response.

**Note:** The challenge depends on the type of second factor authentication you have configured in Entrust IdentityGuard Federation Server.

**9.** Click **OK**. You are brought to the **Cisco User Portal** page.



# Testing IDP-initiated logout

A Cisco user can initiate a logout from the Federation Module.

## To test IDP-initiated logout

1. Perform an IDP-initiated login (see the section, " Testing IDP-initiated login"). You are logged in at Cisco and the IDP.
2. At the IDP (Federation Module), log out using the SAML logout link. You are logged out of the IDP
3. Go back to Cisco. You should still be logged in. This is the expected behavior with this integration.
4. Logout of Cisco.

# Testing SP-initiated logout

### To test SP-initiated logout

1. Perform an SP-initiated login (see the section, "Testing SP-initiated login"). You are logged in at Cisco and the SP.
2. At the SP (Cisco), logout. You are logged out of Cisco.
3. Go back to the Federation Module Home page. You should also be logged out. This is the expected behavior with this integration.

# Testing Cisco using a PVN with your second-factor authentication response

When using tokens with a PVN, see the information about using a token in the *Entrust IdentityGuard Administration Guide*. When using the Radius proxy, PVNs are specified as part of the token or grid response.

For example, if your PVN is 1234, and the token response is 94167505, the combined Radius password is entered as: 123494167505 (PVN first, followed by token response). The PVN and grid response are combined similarly.

For details of how to enable "Separate Challenge for PVN update" and other related information, see the *Entrust IdentityGuard Administration Guide*.

# Known issues

There are no known issues with this integration.