SaaS Access Control

This chapter contains the following sections:

Overview of SaaS Access Control

The Web Security appliance uses the Security Assertion Markup Language (SAML) to authorize access to SaaS applications. It works with SaaS applications that are strictly compliant with SAML version 2.0.

Cisco SaaS Access Control allows you to:

- Control which users can access SaaS applications and from where.
- Quickly disable access to all SaaS applications when users are no longer employed by the organization.
- Reduce the risk of phishing attacks that ask users to enter their SaaS user credentials.
- Choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and pass phrase.

SaaS Access Control only works with SaaS applications that require an authentication mechanism that is supported by the Web Security appliance. Currently, the Web Proxy uses the "PasswordProtectedTransport" authentication mechanism.

To enable SaaS Access Control, you must configure settings on both the Web Security appliance and the SaaS application:

Procedure

	Command or Action	Purpose
Step 1	Configure the Web Security appliance as an identity provider.	Configuring the Appliance as an Identity Provider, on page 2
Step 2	Create an authentication policy for the SaaS application.	Creating SaaS Application Authentication Policies, on page 4

	Command or Action	Purpose
Step 3	Configure the SaaS application for single sign-on.	Configuring End-user Access to the Single Sign-on URL, on page 6
Step 4	(Optional) Configue multiple Web Security appliances.	Using SaaS Access Control and Multiple Appliances, on page 3

Configuring the Appliance as an Identity Provider

When you configure the Web Security appliance as an identity provider, the settings you define apply to all SaaS applications it communicates with. The Web Security appliance uses a certificate and key to sign each SAML assertion it creates.

Before you begin

- (Optional) Locate a certificate (PEM format) and key for signing SAML assertions.
- Upload the certificate to each SaaS application.

Step 1 Choose **Network > Identity Provider for SaaS**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable SaaS Single Sign-on Service**.

Step 4 Enter a virtual domain name in the **Identity Provider Domain Name** field.

Step 5 Enter a unique text identifier in the **Identity Provider Entity ID** field (a URI formatted string is recommended).

Step 6 Either upload or generate a certificate and key:

Method	Additional Steps
Upload a certificate and key	1. Select **Use Uploaded Certificate and Key**. 2. In the **Certificate** field, click Browse; locate the file to upload. **Note** The Web Proxy uses the first certificate or key in the file. The certificate file must be in PEM format. DER format is not supported. 3. In the **Key** field, click Browse; locate the file to upload. If the key is encrypted, select **Key is Encrypted**. **Note** The key length must be 512, 1024, or 2048 bits. The private key file must be in PEM format. DER format is not supported. 4. Click **Upload Files**. 5. Click **Download Certificate** to download a copy of the certificate for transfer to the SaaS applications with which the Web Security appliance will communicate.

Method	Additional Steps

Generate a certificate and key	1. Select **Use Generated Certificate and Key**.
	2. Click **Generate New Certificate and Key**.
	  1. In the Generate Certificate and Key dialog box, enter the information to display in the signing certificate.
	  Note You can enter any ASCII character except the forward slash (/) in the Common Name field.
	  2. Click **Generate**.
	3. Click **Download Certificate** to transfer the certificate to the SaaS applications with which the Web Security appliance will communicate.
	4. (Optional) To use a signed certificate, click the **Download Certificate Signing Request** (DCSR) link to submit a request to a certificate authority (CA). After you receive a signed certificate from the CA, click **Browse** and navigate to the signed certificate location. Click **Upload File**. (bug 37984)

Note If the appliance has both an uploaded certificate and key pair and a generated certificate and key pair, it only uses the certificate and key pair currently selected in the Signing Certificate section.

Step 7 Make note of the settings when you configure the appliance as an identity provider. Some of these settings must be used when configuring the SaaS application for single sign-on.

Step 8 Submit and Commit Changes.

What to do next

After specifying the certificate and key to use for signing SAML assertions, upload the certificate to each SaaS application.

Related Topics

- Configuring End-user Access to the Single Sign-on URL, on page 6

Using SaaS Access Control and Multiple Appliances

Before you begin

Configuring the Appliance as an Identity Provider, on page 2

Step 1 Configure the same Identity Provider Domain Name for each Web Security appliance.

Step 2 Configure the same Identity Provider Entity ID for each Web Security appliance.

Step 3 Upload the same certificate and private key to each appliance on the **Network > Identity Provider for SaaS** page.

Step 4 Upload this certificate to each SaaS application you configure.

Creating SaaS Application Authentication Policies

Before you begin

- Create associated identities.
- Configure Identity Provider, see Configuring the Appliance as an Identity Provider, on page 2.
- Provide an Identity Provider Signing Certificate and Key: Network > Identity Provider for SaaS > Enable and Edit Settings.
- Create an Authentication Realm, Authentication Realms.

Step 1 Choose **Web Security Manager > SaaS Policies.**

Step 2 Click **Add Application**.

Step 3 Configure the settings:

Property	Description
Application Name	Enter a name to identify the SaaS application for this policy; each application name must be unique. The Web Security appliance uses the application name to generate a single sign-on URL.
Description	(Optional) Enter a description for this SaaS policy.
Metadata for Service Provider	Configure the metadata that describes the service provider referenced in this policy. You can either describe the service provider properties manually or upload a metadata file provided by the SaaS application. The Web Security appliance uses the metadata to determine how to communicate with the SaaS application (service provider) using SAML. Contact the SaaS application to learn the correct settings to configure the metadata. **Configure Keys Manually** – If you select this option, provide the following: • **Service Provider Entity ID**. Enter the text (typically in URI format) the SaaS application uses to identify itself as a service provider. • **Name ID Format**. Choose from the drop-down list the format the appliance should use to identify users in the SAML assertion it sends to service providers. The value you enter here must match the corresponding setting configured on the SaaS application. • **Assertion Consumer Service URL**. Enter the URL to which the Web Security appliance is to send the SAML assertion it creates. Read the SaaS application documentation to determine the correct URL to use (also known as the login URL). **Import File from Hard Disk** – If you select this option, click Browse, locate the file, and then click **Import**. **Note** This metadata file is an XML document, following the SAML standard, that describes a service provider instance. Not all SaaS applications use metadata files, but for those that do, contact the SaaS application provider for the file.

Property	Description
User Identification / Authentication for SaaS SSO	Specify how users are identified/authenticated for SaaS single sign-on: • Always prompt users for their local authentication credentials. • Prompt users for their local authentication credentials if the Web Proxy obtained their user names transparently. • Automatically sign in SaaS users using their local authentication credentials. Choose the authentication realm or sequence the Web Proxy should use to authenticate users accessing this SaaS application. Users must be a member of the authentication realm or authentication sequence to successfully access the SaaS application. If an Identity Services Engine is used for authentication, and LDAP was selected, the realm will be used for the SAML user names and attribute mapping.
SAML User Name Mapping	Specify how the Web Proxy should represent user names to the service provider in the SAML assertion. You can pass the user names as they are used inside your network (**No mapping**), or you can change the internal user names into a different format using one of the following methods: • **LDAP query**. The user names sent to the service provider are based on one or more LDAP query attributes. Enter an expression containing LDAP attribute fields and optional custom text. You must enclose attribute names in angled brackets. You can include any number of attributes. For example, for the LDAP attributes "user" and "domain," you could enter <user>@<domain>.com. • **Fixed Rule Mapping**. The user names sent to the service provider are based on the internal user name with a fixed string added before or after the internal user name. Enter the fixed string in the **Expression Name** field, with %s either before or after the string to indicate its position in the internal user name.
SAML Attribute Mapping	(Optional) You can provide to the SaaS application additional information about the internal users from the LDAP authentication server if required by the SaaS application. Map each LDAP server attribute to a SAML attribute.
Authentication Context	Choose the authentication mechanism the Web Proxy uses to authenticate its internal users. **Note** The authentication context informs the service provider which authentication mechanism the identity provider used to authenticate the internal users. Some service providers require a particular authentication mechanism to allow users to access the SaaS application. If a service provider requires an authentication context that is not supported by an identity provider, users cannot access the service provider using single sign-on from the identity provider.

Step 4 Submit and Commit Changes.

What to do next

Set up the single sign-on settings on the SaaS application side, using the same parameters to configure the application.

Configuring End-user Access to the Single Sign-on URL

After you configure the Web Security appliance as an identity provider and create a SaaS Application Authentication Policy for the SaaS application, the appliance creates a single sign-on URL (SSO URL). The Web Security appliance uses the application name configured in the SaaS Application Authentication Policy to generate the single sign-on URL; the SSO URL format is:

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

Step 1 Obtain the single sign-on URL from the **Web Security Manager > SaaS Policies** page.

Step 2 Make the URL available to end-users depending on which flow type.

Step 3 If you choose Identity provider initiated flow, the appliance redirects users to the SaaS application.

Step 4 If you choose Service Provider initiated flows, you must configure this URL in the SaaS application.

- Always prompt SaaS users for proxy authentication. After entering valid credentials, users are logged into the SaaS application.
- Transparently sign in SaaS users. Users are logged into the SaaS application automatically.

Note To achieve single sign-on behavior using explicit forward requests for all authenticated users when the appliance is deployed in transparent mode, select "**Apply same surrogate settings to explicit forward requests**" when you configure the Identity group.