

Integration

This topic contains the following sections:

- Integrate the Cisco Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC), on page 1
- Integrate with Cisco SecureX and Cisco Threat Response, on page 16
- Integrate Cisco Secure Web Appliance with Cisco Umbrella, on page 24

Integrate the Cisco Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC)

This topic contains the following sections:

- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 1
- ISE/ISE-PIC Certificates, on page 3
- Fallback Authentication, on page 5
- Tasks for Integrating the ISE/ISE-PIC Service, on page 5
- Configure ISE-SXP Integration, on page 12
- VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations, on page 15
- Troubleshooting Identity Services Engine Problems, on page 15

Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service

Cisco's Identity Services Engine (ISE), and Passive Identity Connector (ISE-PIC) are applications that run on separate servers in your network to provide enhanced identity management. The Secure Web Appliance can access user-identity information from an ISE or ISE-PIC server. When either ISE, or ISE-PIC is configured, information is retrieved (user names and associated Secure Group Tags from ISE, user names and Active Directory groups from ISE-PIC) for appropriately configured Identification Profiles, to allow transparent user identification in policies configured to use those profiles.

- You can construct access policies using Secure Group Tags and Active Directory groups.
- For users that fail transparent identification with ISE/ISE-PIC, you can configure fallback authentication with Active Directory based realms. See Fallback Authentication, on page 5.
- You can configure authentication of users in Virtual Desktop Environments (Citrix, Microsoft shared/remote desktop services etc.). See VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations, on page 15.



Note

- The ISE/ISE-PIC service is not available in Connector mode.
- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- The ISE configuration page in the Secure Web Appliance's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are similar and the any details specific for ISE-PIC configurations have been mentioned where applicable.

For more information on Secure Web Appliance ISE version support matrix, see ISE Compatibility Matrix Information.

Table 1: Secure Web Appliance -ISE Scale Support Matrix

Models	Session Scale Without AD Group Enabled	Session Scale With AD Group Enabled	
-	Maximum Supported Active Sessions	Maximum Supported Active Sessions	Maximum Supported End Points (AD group entries for each user, and end point in ISE database.)
S680*,S690,S695	200K	125K	400K
S380*,S390,S600V	150K	50K	150K
S190,S195,S300V	50K	50K	75K
S100V	50K	40K	50K



Note *S190, S390, and S690 models are not supported.

Related Topics

- About pxGrid, on page 3
- About the ISE/ISE-PIC Server Deployment and Failover, on page 3

About pxGrid

Cisco's Platform Exchange Grid (pxGrid) enables collaboration between components of the network infrastructure, including security-monitoring and network-detection systems, identity and access management platforms, and so on. These components can use pxGrid to exchange information via a publish/subscribe method.

There are essentially three pxGrid components: the pxGrid publisher, the pxGrid client, and the pxGrid controller.

- pxGrid publisher – Provides information for the pxGrid client(s).
- pxGrid client – Any system, such as the Secure Web Appliance, that subscribes to published information; in this case, Security Group Tag (SGT), Active Directory groups, user-group, and profiling information.
- pxGrid controller – In this case, the ISE/ISE-PIC pxGrid node that controls the client registration/management and topic/subscription processes.

Trusted certificates are required for each component, and these must be installed on each host platform.

About the ISE/ISE-PIC Server Deployment and Failover

A single ISE/ISE-PIC node set-up is called a standalone deployment, and this single node runs the Administration, and Policy Service. To support failover and to improve performance, you must set up multiple ISE/ISE-PIC nodes in a distributed deployment. The minimum required distributed ISE/ISE-PIC configuration to support ISE/ISE-PIC failover on your Secure Web Appliance is:

- Two pxGrid nodes
- Two Administration nodes
- One Policy Service node

This configuration is referred to in the *Cisco Identity Services Engine Hardware Installation Guide* as a 'Medium-Sized Network Deployment'. Refer to the network deployments section in that installation guide for additional information.

Related Topics

- ISE/ISE-PIC Certificates, on page 3
- Tasks for Integrating the ISE/ISE-PIC Service, on page 5
- Connect to the ISE/ISE-PIC Services, on page 7
- Troubleshooting Identity Services Engine Problems, on page 15

ISE/ISE-PIC Certificates



Note This section describes the certificates necessary for an ISE/ISE-PIC connection. Tasks for Integrating the ISE/ISE-PIC Service, on page 5 provides detailed information about these certificates. Certificate Management, provides general certificate-management information for AsyncOS.

A set of two certificates is required for mutual authentication and secure communication between the Secure Web Appliance and each ISE/ISE-PIC server:

- **Web Appliance Client Certificate** – Used by the ISE/ISE-PIC server to authenticate the Secure Web Appliance.
- **ISE pxGrid Certificate** – Used by the Secure Web Appliance to authenticate an ISE/ISE-PIC server on port 5222 for Secure Web Appliance-ISE/ISE-PIC data subscription (on-going publish/subscribe queries to the ISE/ISE-PIC server).

These two certificates can be Certificate Authority (CA)-signed or self-signed. AsyncOS provides the option to generate a self-signed Web Appliance Client Certificate, or a Certificate Signing Request (CSR) instead, if a CA-signed certificate is needed. Similarly, the ISE/ISE-PIC server provides the option to generate self-signed ISE/ISE-PIC pxGrid certificates, or CSRs instead if CA-signed certificates are needed.

Related Topics

- Using Self-signed Certificates, on page 4
- Using CA-signed Certificates, on page 4
- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 1
- Tasks for Integrating the ISE/ISE-PIC Service, on page 5
- Connect to the ISE/ISE-PIC Services, on page 7

Using Self-signed Certificates

When self-signed certificates are used on the ISE/ISE-PIC server, the ISE/ISE-PIC pxGrid certificate developed on the ISE/ISE-PIC server, as well as the Web Appliance Client Certificate developed on the Secure Web Appliance must be added to the Trusted Certificates store on the ISE/ISE-PIC server (On **ISE** - Administration > Certificates > Trusted Certificates > Import; on **ISE-PIC** - Certificates > Trusted Certificates > Import).



Caution We do not recommend using self-signed certificates for authentication as it is not as secured as other authentication methods. Also, a self-signed certificate does not support revocation policy.

Using CA-signed Certificates

In the case of CA-signed certificates:

- On the ISE/ISE-PIC server, ensure the appropriate CA root certificate for the Web Appliance Client Certificate is present in the Trusted Certificates store (Administration > Certificates > Trusted Certificates).
- On the Secure Web Appliance, ensure the appropriate CA root certificates are present in the Trusted Certificates list (Network > Certificate Management > Manage Trusted Root Certificates).
- On the Identity Services Engine page (Network > Identity Services Engine), be sure to upload the CA root certificate for the ISE/ISE-PIC pxGrid certificate.

Fallback Authentication

For user information not available in ISE/ISE-PIC, you can configure a fallback authentication. Ensure you have the following for successful fallback authentication.

- Identification profile configured with a fallback option of Active Directory based realm.
- Access policy with the correct Identification profile which contains the fallback option.

Tasks for Integrating the ISE/ISE-PIC Service

Note

- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- To continue using existing access policies with ISE-PIC, you must edit the respective identification profiles to use ISE-PIC and identify users transparently. This applies to identification profiles using CDA. If you are migrating from CDA identification, to ISE-PIC based identification, you must edit the respective identification profiles.

Note

- Reconfigure the ISE on the Secure Web Appliance, if you are upgrading from AsyncOS 11.5 or earlier versions to AsyncOS 11.7 or later versions.
- The certificate must be generated through the ISE/ISE-PIC device and the generated certificate must be uploaded to the Secure Web Appliance.

Step	Task	Links to Topics and Procedures
1	Generate certificate through ISE/ISE-PIC device	Generating Certificate through ISE/ISE-PIC, on page 6
2	Configure the ISE/ISE-PIC for Secure Web Appliance access.	Configuring ISE/ISE-PIC server for Secure Web Appliance Access, on page 6
3	Configure and enable ISE/ISE-PIC Services in the Secure Web Appliance.	Connect to the ISE/ISE-PIC Services, on page 7
4	If the Secure Web Appliance Client Certificate is self-signed, import it to ISE/ISE-PIC.	Import the Self-signed Secure Web Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment, on page 9 Import the Self-signed Secure Web Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment, on page 10
5	If required, configure logging in the Secure Web Appliance.	Configuring logging for ISE/ISE-PIC, on page 11

Step	Task	Links to Topics and Procedures
6	Acquire ISE/ISE-PIC ERS server details.	Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 12

Related Topics

- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 1
- ISE/ISE-PIC Certificates, on page 3
- Troubleshooting Identity Services Engine Problems, on page 15

Generating Certificate through ISE/ISE-PIC

Note The certificate that is generated through the ISE/ISE-PIC device must be in the PKCS12 format.

- **ISE/ISE-PIC:**

Procedure

Step 1 Choose **Work Centres** > **PassiveID** > **Subscribers** > **Certificates**.

Step 2 Choose **PKCS 12 format** from the **Certificate Download Format** drop-down list. Enter other appropriate information on the **Certificates** tab and generate a pxGrid certificate.

Step 3 Extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file using the `openssl` command:

- **Root CA:** openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Web Appliance Client Certificate:** openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Web Appliance Client Key:** openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

Note
Use the same certificate password that you have entered on the ISE web interface while performing step 2.

Note
Follow the same steps to generate the secondary Root CA, Web Appliance Client Certificate, and Web Appliance Client Key through the secondary/failover ISE server.

Configuring ISE/ISE-PIC server for Secure Web Appliance Access

- **ISE**

- Each ISE server must be configured to allow identity topic subscribers (such as Secure Web Appliance) to obtain session context in real-time.
  1. Choose **Administration** > **pxGrid Services** > **Settings** > **pxGrid Settings**.
  2. Ensure **Automatically approve new certificate-based accounts** is checked.

  Delete any old Secure Web Appliances configured that do not take part in any authentication with ISE/ISE-PIC.

  Ensure the ISE server footer is green, and says **Connected to pxGrid**.

- **ISE-PIC**
  - Each ISE-PIC server must be configured to allow identity topic subscribers (such as Secure Web Appliance) to obtain session context in real-time.
    1. Choose **Subscribers** > **Settings**.
    2. Ensure **Automatically approve new certificate-based accounts** is checked.

    Delete any old Secure Web Appliances configured that do not take part in any authentication with ISE/ISE-PIC.

    Ensure the ISE server footer is green, and says **Connected to pxGrid**.

Refer to Cisco *Identity Services Engine* documentation for more information.

Connect to the ISE/ISE-PIC Services

Note If the ISE Admin, pxGrid, and MNT certificates are signed by your Root CA certificate, then upload the Root CA certificate itself to the ISE pxGrid Node Certificate fields on the appliance (**Network** > **Identity Services Engine**).

Before you begin

- Be sure each ISE/ISE-PIC server is configured appropriately for Secure Web Appliance access; see Tasks for Integrating the ISE/ISE-PIC Service, on page 5.
- Obtain valid ISE/ISE-PIC-related certificates and keys. See Generating Certificate through ISE/ISE-PIC, on page 6for related information.
- Import the obtained RootCA.pem to the Secure Web Appliance (**Network** > **CertificateManagement** > **TrustedRootCertificate** > **Client on ManageTrustedRootCertificate**). To extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file, see Generating Certificate through ISE/ISE-PIC, on page 6.

Note Follow the same procedure for RootCA.pem extracted from secondary XXXX.pk12 file (if secondary/failover ISE Sever is available).

- The ISE configuration page in the Secure Web Appliance's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are identical, and any details specific to ISE-PIC configurations have been mentioned where applicable.
- Enable ERS if you are building access policies using Active Directory groups provided by ISE/ISE-PIC.
- As part of AsyncOS 15.0 release, OpenSSL version 1.1.1, and the library no longer accepts IP-based certificates.You should use only the Hostname in the SWA ISE Configuration to ensure that the **Start Test** succeeds and ISE functions as expected.

Procedure

Step 1 Choose **Network > Identification Service Engine**.

Step 2 Click **Edit Settings**.

If you are configuring ISE/ISE-PIC for the first time, click **Enable and Edit Settings**.

Step 3 Check **Enable ISE Service**.

Step 4 Identify the **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Primary ISE pxGrid Node Tab** on the Secure Web Appliance.

a) Provide an **ISE pxGrid Node Certificate** for Secure Web Appliance-ISE/ISE-PIC data subscription (on-going queries to the ISE/ISE-PIC server).

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the primary ISE server as Root CA (i.e. RootCA.pem); see ,Generating Certificate through ISE/ISE-PIC, on page 6 and then click **Upload File**. See Uploading a Certificate and Key for additional information.

Step 5 If you are using a second ISE/ISE-PIC server for failover, identify its **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Secondary ISE pxGrid Node** tab on the Secure Web Appliance using its host name or IPv4 address.

a) Provide the secondary **ISE pxGrid Node Certificate**.

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the secondary ISE server as Root CA (i.e. **RootCA.pem**); see Generating Certificate through ISE/ISE-PIC, on page 6, and then click **Upload File** .See Uploading a Certificate and Key for additional information.

Note
During failover from primary to secondary ISE servers, any user not in the existing ISE SGT cache will be required to authenticate, or will be assigned Guest authorization, depending on your Secure Web Appliance configuration. After ISE failover is complete, normal ISE authentication resumes.

Step 6 Provide a **Web Appliance Client Certificate** for Secure Web Appliance-ISE/ISE-PIC server mutual authentication:

- **Use Uploaded Certificate and Key**

  For both the certificate and the key, click Choose and browse to the respective file.

  Note
  Select and upload publicCert.pem and privateKey.pem generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 6.

If the **Key is Encrypted**, check this box.

Click **Upload Files**. (See Uploading a Certificate and Key for additional information about this option.)

Step 7 Enable the ISE SGT eXchange Protocol (SXP) service.

For information on enabling Secure Web Appliance to retrieve SXP binding topics from ISE services, see Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 13.

Step 8 Enable the ISE External Restful Service (ERS).

- Enter the username and password of the ERS administrator. SeeAcquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 12.
- If ERS is available on the same ISE/ISE-PIC pxGrid nodes, check the **Server name same as ISE pxGrid Node** check box. Otherwise, enter the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

Step 9 Click **Start Test** to test the connection with the ISE/ISE-PIC pxGrid node(s).

Step 10 Click **Submit**.

What to do next

- Classifying Users and Client Software
- Create Policies to Control Internet Requests

Related Information

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html , particularly “How To Integrate Cisco Secure Web Appliance using ISE/ISE-PIC and TrustSec through pxGrid..”

Import the Self-signed Secure Web Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment

The basic steps are:

- **ISE Admin Node**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE
  - Trust for client authentication and syslog
  - Trust for authentication of Cisco services
- **ISE-PIC Admin Node**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:

- Trust for Authentication within ISE
- Trust for client authentication and syslog
- Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

Import the Self-signed Secure Web Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment

The basic steps are:

- **ISE Admin Node:**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE
  - Trust for client authentication and syslog
  - Trust for authentication of Cisco services
- **ISE-PIC Admin Node:**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:
    - Trust for Authentication within ISE
    - Trust for client authentication and syslog
    - Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

Note In Distributed ISE Deployment, the Secure Web Appliance communicates with MNT, PAN, and PxGrid nodes. In this case, the certificates or the issuer for all of the certificates, must be available in the 'Extracted Root certificate' i.e. in the RootCA which is generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 6.

Procedure

Step 1 Follow the steps in the Generating Certificate through ISE/ISE-PIC, on page 6 to generate RootCA, Web Appliance Client Certificate, and Web Appliance Client Key.

Step 2 On **ISE/ISE-PIC Admin Node**, export the self-signed certificates manually through **ISE/ISE-PIC** > **Administration** > **System** > **Certificates** > **System Certificates**

a. Select a certificate which is having 'Used by' one of these:[pxGrid, EAP Authentication, Admin, Portal, RADIUS DTLS].

b. Click **Export** and save the generated .pem file.

Repeat the above steps for all ISE/ISE-PIC distributed nodes.

Step 3 Append the downloaded certificate-files in RootCA.pem manually using `openssl` commands. To generate and extract certificate-files in RootCA.pem through the ISE/ISE-PIC device, see Generating Certificate through ISE/ISE-PIC, on page 6.

a. Execute the following command on the downloaded certificate:

```
Example:

openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

Example (output):

Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

b. Modify the content as follows:

```
Example:
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

c. Add the following line in the RootCA.pem:

```
Bag Attributes: <Empty Attributes>
```

d. Add Subject and Issuer from step (2) in RootCA.pem along with step (3).

```
Example:
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

e. Copy the whole content of the downloaded certificate file and paste them at the end of the RootCA after step (4) data.

Repeat steps (1) to (5) for all Distributed ISE/ISE-PIC node downloaded certificates and save the modified RootCA certificate.

Step 4 Upload the modified RootCA.pem in the ISE configuration page of the Secure Web Appliance. See Connect to the ISE/ISE-PIC Services, on page 7.

Configuring logging for ISE/ISE-PIC

- Add the custom field %m to the Access Logs to log the Authentication mechanism—Customizing Access Logs.
- Verify that the ISE/ISE-PIC Service Log was created; if it was not, create it—Adding and Editing Log Subscriptions.
- Define Identification Profiles that access ISE/ISE-PIC for user identification and authentication—Classifying Users and Client Software, on page 117.

- Configure access policies that utilize ISE/ISE-PIC identification to define criteria and actions for user requests—Policy Configuration, on page 191.

Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC

- Enable the Cisco ISE REST API in ISE/ISE-PIC (the APIs use HTTPS port 9060).

Note You must enable ISE External Restful Service (ERS) on the Secure Web Appliance (Network > Identity Services Engine) to configure security policies based on groups. This is applicable to 11.7 and later versions.

  - **ISE**
    - Choose **Administration** > **Settings** > **ERS Settings** > **ERS settings for primary admin node** > **Enable ERS**.

      Enable **ERS for Read for All Other Nodes** if there are any secondary nodes.
  - **ISE-PIC**
    - Choose **Settings** > **ERS Settings** > **Enable ERS**.

- Ensure you have created an ISE administrator with the correct External RESTful Services group. The External RESTful Services Admin group has full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests. The External RESTful Services Operator has Read Only access (GET request only).
  - **ISE**
    - Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users**.
  - **ISE-PIC**
    - Choose **Administration** > **Admin Access** > **Admin Users**.

If the ERS service is available on separate servers, and not on the ISE/ISE-PIC pxGrid nodes, you will need the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

Refer to Cisco *Identity Services Engine* documentation for more information.

Configure ISE-SXP Integration

This section includes the following topics:

- About ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 13
- Guidelines and Limitations, on page 13
- Prerequisites, on page 13
- Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 13

• Verifying the ISE-SXP Protocol Configuration, on page 14

About ISE-SXP Protocol for SGT-to-IP Address Mapping

SGT Exchange Protocol (SXP) is a protocol developed to propagate the IP-SGT bindings across network devices. A Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network.

You can integrate Cisco Identity Services Engine (ISE) deployment with Cisco Secure Web Appliance for passive authentication. Secure Web Appliance can subscribe to SXP mappings from ISE. ISE uses SXP to propagate the SGT-to-IP address mapping database to managed devices. When you configure Secure Web Appliance to use the ISE server, you enable the option to listen to the SXP topic from ISE. This causes Secure Web Appliance to learn about the SGTs and IP address mappings directly from ISE.

Secure Web Appliance generates a dummy user authentication IP addresses, which include the ISE cluster IP address along with the IP address of the client. Therefore, multiple client IP addresses can be authenticated on the cluster IP address.

Guidelines and Limitations

ISE-SXP protocol for SGT-to-IP address mapping has the following guidelines and limitations:

- IPv6 enabled endpoints are not support in Secure Web Appliance Release 14.5.
- In Secure Web Appliance Release 14.5, usernames and group mapping are not available in the SGT-to-IP address mappings. Therefore, the administrator cannot create policies based on ISE users and groups in Secure Web Appliance. However, it can be created with SGTs.
- To schedule the restart timestamp for the bulk download process, you must configure time in the HH::MM format within 24 hours to restart the ised process.



Note It is recommended that you configure the time when the user authentication process is indicated to be less in the day. For example, at 00:00 hour.

Prerequisites

ISE-SXP protocol for SGT-to-IP address mapping has the following prerequisite:

- Requires a trusted root certificate. To add a trusted root certificate, see Managing Trusted Root Certificates.

Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping

All mappings that are defined in ISE, including the SGT-to-IP address mappings can be published through SXP. You can retrieve the ISE-SXP information using the following mechanisms:

- Bulk download—After a ised process restart, Secure Web Appliance sends the bulk download request to the ISE aggregator node in order to get information for all ISE-SXP entries that are available on the aggregator node. You can schedule the restart timestamp using AsyncOS Command Line Interface (CLI).
- Incremental update— Secure Web Appliance subscribes over a websocket to get incremental update messages. There are two types of messages:
  - Create—for all newly created entries

- Delete—for all SXP updated entries

Note Secure Web Appliance receives two messages (Delete followed by Create) for each entry that is updated.

You are allowed to schedule restart.

Procedure

Step 1 Navigate to **Network** > **Identification Service Engine**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable ISE Service**.

Step 4 Check **Enable** to enable Secure Web Appliance to retrieve SXP binding topics from ISE services.

By default, the ISE SGT eXchange Protocol (SXP) service is disabled.

Step 5 Click **Start Test** to test the connection.

Note
The SXP information is displayed only if the ISE-SGT eXchange Protocol (SXP) service has been enabled.

Step 6 Click **Submit**.

Verifying the ISE-SXP Protocol Configuration

You can verify the ISE-SXP protocol configuration using any one of the following methods:

- Click **Start Test** in the Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 13 and verify the displayed information.
- Use the **STATISTICS** command under the **ISEDATA** command in the AsyncOS Command Line Interface (CLI).

When you use the **STATISTICS** command, the following information appears:

- ERS Hostname
- ERS Time of Connection
- Session Bulk Download
- Group Bulk Download
- SGT Bulk Download
- SXP Bulk Download
- Session Update

- Group Update
- SXP Update
- Memory Allocation
- Memory Deallocation
- Total Session Count

The user name is generated in the following format:

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

For example: isesxp_10.10.2.68_sgt18_10.10.10.10

VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations

You can configure transparent identification with ISE/ISE-PIC for users on VDI environments based on the source ports used.

You must install the Cisco Terminal Services (TS) Agent, on the VDI servers. The Cisco TS agent provides the identity information to ISE/ISE-PIC. The identity information includes domain, user name, and the port ranges used by each user.

- Download the Cisco TS agent from the support site https://www.cisco.com/c/en/us/support/index.html.
- See the Cisco Terminal Services (TS) Agent Guide https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html for more information.
- Configure the ISE/ISE-PIC API provider to work with a Cisco TS agent. See the Cisco TS agent documentation for information about sending API calls.

Note

- Fallback authentication for VDI environment users is not supported.
- Ensure the number of maximum remote desktop sessions are the same in the Cisco Terminal Services agent and Microsoft server settings. This prevents incorrect session information from being sent to the Secure Web Appliance from ISE, and avoids false authentication for new sessions.

Troubleshooting Identity Services Engine Problems

- Identity Services Engine Problems
  - Tools for Troubleshooting ISE Issues
  - ISE Server Connection Issues
  - ISE-related Critical Log Messages

Integrate with Cisco SecureX and Cisco Threat Response

This topic contains the following sections:

- Integrating Your Appliance with Cisco SecureX and Cisco Threat Response, on page 16
- How to Integrate Your Appliance with Cisco SecureX and Cisco Threat Response, on page 17
- Enabling Cisco Cloud Services Portal on Secure Web Appliance, on page 19
- Registering Secure Web Appliance with Cisco Cloud Services Portal, on page 20
- Performing Threat Analysis using Cisco SecureXRibbon, on page 20

Integrating Your Appliance with Cisco SecureX and Cisco Threat Response

Cisco SecureX is a security platform embedded with every Cisco security product. It is cloud-native with no new technology to deploy. Cisco SecureX simplifies the demands of threat protection by providing a platform that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. By connecting technology in an integrated platform, Cisco SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. Cisco SecureX enables you to expand your capabilities by connecting your security infrastructure.

Integrating the Appliance with Cisco SecureX and Cisco Threat Response contains the following sections:

- How to Integrate Your Appliance with Cisco SecureX and Cisco Threat Response, on page 17
- Performing Threat Analysis using Cisco SecureXRibbon, on page 20

You can integrate your appliance with Cisco SecureX and Cisco Threat Response, and perform the following actions in Cisco SecureX and Cisco Threat Response:

- View and send the web data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in the web reports and tracking.
- Block compromised URL or web traffic.
- Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
- Document the threats to save the investigation and enable collaboration of information among other devices.
- Block malicious domains, track suspicious observances, initiate an approval workflow or to create an IT ticket to update web policy.

You can access Cisco SecureX and Cisco Threat Response using the following URLs:

https://securex.us.security.cisco.com/login

The Cisco Secure Web Appliance provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secure important information in transit with end-to-end encryption. For more information on observables that can be enriched by the Secure Web Appliance module,

go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX and click **Learn More**.

When you integrate Secure Web Appliance with SecureX, it validates Secure Web Appliance's web tracking data. The transaction timeout (60 seconds) occurs due to the processing delay on Secure Web Appliance resulting an integration failure. Reduce the integration time limit from the default 30 days to 1 or 2 days for a successful integration. However, this reduction will impact the monitoring effectiveness on Secure Web Appliance.

How to Integrate Your Appliance with Cisco SecureX and Cisco Threat Response

Table 2: How to Integrate Your Appliance with Cisco SecureX and Cisco Threat Response

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 17
Step 2	On your Secure Web Appliance, enable the Cisco SecureX or Cisco Threat Response integration.	Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Secure Web Appliance, on page 18
Step 3	On Cisco SecureX, add your appliance as a device, register it, and generate a registration token.	For more information, go to https://securex.us.security.cisco.com/help/settings-devices
Step 4	On your Secure Web Appliance, complete the Cisco SecureX or Cisco Threat Response registration.	Registering Cisco SecureX or Cisco Threat Response on Cisco Secure Web Appliance, on page 18
Step 5	Confirm whether the registration was successful.	Confirm Whether the Registration was Successful, on page 19
Step 6	On Cisco SecureX, add Web Secirity Appliance Module.	For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the required Secure Web Appliance module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Prerequisites

Note If you already have a Cisco Threat Response user account, you do not need to create a Cisco SecureX user account. You can log in to Cisco SecureX using your Cisco Threat Response user account credentials.

- Make sure that you create a user account in Cisco SecureX with admin access rights. To create a new user account, go to **Cisco SecureX login** page using the URL https://securex.us.security.cisco.com/login and click **Create a SecureX Sign-on Account** in the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.

- (Only if you are not using a proxy server.) Make sure that you open HTTPS (In and Out) 443 port on the firewall for the following FQDNs to register your appliance with Cisco SecureX or Cisco Threat Response:
  - api-sse.cisco.com (applicable for NAM users only)
  - api.eu.sse.itd.cisco.com (applicable for European Union (EU) users only)
  - api.apj.sse.itd.cisco.com (applicable for APJC users only)
  - est.sco.cisco.com (applicable for APJC, EU, and NAM users)

Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Secure Web Appliance

Procedure

Step 1 Log in to your appliance.

Step 2 Select **Network** > **Cloud Service Settings**.

Step 3 Click **Edit Settings**.

Step 4 Check the **Enable** check box.

Step 5 Choose the required Cisco SecureX or Cisco Threat Response server to connect your appliance to Cisco SecureX or Cisco Threat Response.

Step 6 Submit and commit your changes.

Step 7 Wait for few minutes, and check whether the **Register** button appears on your appliance.

What to do next

Register your appliance on Cisco SecureX or Cisco Threat Response. For more information, go tohttps://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Registering Cisco SecureX or Cisco Threat Response on Cisco Secure Web Appliance

Procedure

Step 1 Go to **Network** > **Cloud Service Settings**.

Step 2 In **Cloud Services Settings**, enter the registration token, and click **Register**.



Note To register Cisco SecureX or Cisco Threat Response using the CLI, use the `cloudserviceconfig` command.

What to do next

Confirm Whether the Registration was Successful, on page 19

Confirm Whether the Registration was Successful

- On security services exchange, confirm successful registration by reviewing the status in security services exchange.
- On Cisco SecureX, navigate to the **Devices** page and view the Secure Web Appliance that has been registered with Security Services Exchange.

Note If you want to switch to another Cisco SecureX or Cisco Threat Response server (for example, 'Europe - api.eu.sse.itd.cisco.com'), you must first deregister your appliance from Cisco SecureX or Cisco Threat Response and follow steps mentioned in How to Integrate Your Appliance with Cisco SecureX and Cisco Threat Response, on page 17.

After you have integrated your appliance with Cisco SecureX or Cisco Threat Response, you do not need to integrate your Cisco Security Management appliance with Cisco SecureX or Cisco Threat Response.

After successful registration of your appliance on Security Services Excange, add the Secure Web Appliance Web module on Cisco SecureX. For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Enabling Cisco Cloud Services Portal on Secure Web Appliance

Procedure

Step 1 Log in to your Secure Web Appliance.

Step 2 Select **Network** > **Cloud Service Settings**.

Step 3 Click **Enable**.

Step 4 Check the **Enable Cisco Cloud Services** check box.

Step 5 Choose the required Cisco Secure server to connect your Secure Web Appliance to the Cisco Cloud Services portal.

Step 6 Submit and commit your changes.

Step 7 Wait for few minutes, and check whether the **Register** button appears on the **Cloud Services Settings** page.

Note To enable Cisco Cloud Services portal using the CLI, use the `cloudserviceconfig` command.

What to do next

Register your Secure Web Appliance with the Cisco Cloud Services portal. For more information, go to https://securex.us.security.cisco.com/settings/modules/available, navigate to the module to integrate with Cisco SecureX, click **Add New Module**, and see the instructions on the page.

Registering Secure Web Appliance with Cisco Cloud Services Portal

Procedure

Step 1 Go to **Network** > **Cloud Service Settings**.

Step 2 Enter the registration token under Cloud Services Settings and click **Register**.



Note To register your Secure Web Appliance with or the Cisco Cloud Services portal using the CLI, use the `cloudserviceconfig` command.

You cannot disable or deregister Cisco Cloud Services if smart licensing is registered on your appliance.

Performing Threat Analysis using Cisco SecureXRibbon



Note When you downgrade from AsyncOS 14.0 or earlier versions, **Casebook** will be part of the Cisco SecureX Ribbon.

Cisco SecureX supports a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These distributed capabilities are presented in the form of applications (apps) and tools in the Cisco SecureX Ribbon.

This topic contains the following sections:

- Accessing the Cisco SecureX Ribbon, on page 21
- Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu, on page 22

You will find the Cisco SecureX Ribbon at the bottom pane of the page, and it persists as you move between the dashboard and other security products in your environment. Cisco SecureX Ribbon consists of the following icons and elements:

- Expand/Collapse Ribbon
- Home
- Casebook App
- Incidents App

- Orbital App
- Enrichment Search Box
- Find Observables
- Settings

For more information on Cisco SecureX Ribbon, see https://securex.us.security.cisco.com/help/ribbon.

Accessing the Cisco SecureX Ribbon

Before you begin

Make sure that you meet all the prerequisites that are mentioned in Prerequisites, on page 17.

Note Suppose you have already configured **Casebook** for AsyncOS earlier versions. You need to create a new **Client ID** and **Client Secret** in Cisco SecureX API client with additional scopes, as mentioned in the following procedure.

You can drag the Cisco SecureX Ribbon, positioned at the bottom pane of the page, from right using  button.

Procedure

Step 1 Log in to the new web interface of your appliance. For more information, see Understanding the Web Reporting Pages on the New Web Interface.

Step 2 Click the Cisco SecureX Ribbon.

Step 3 Create a **Client ID** and **Client Secret** in **SecureX API Clients**. For more information to generate API Client credentials, see Creating an API Client.

While creating a client ID and client password, make sure that you choose the following scopes:

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon

- telemetry:write
- users:read
- orbital (if you have access)

Step 4 Enter the client ID and client password obtained in step 3 in the **Login to use SecureX Ribbon** dialog box in your appliance.

Step 5 Select the required Cisco SecureX server in the **Login to use SecureX Ribbon** dialog box.

Step 6 Click **Authenticate**.

Note
If you want to edit the client ID, client password, and Cisco SecureX server, right-click on the Cisco SecureX Ribbon, and add the details.

What to do next

Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu, on page 22

Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu

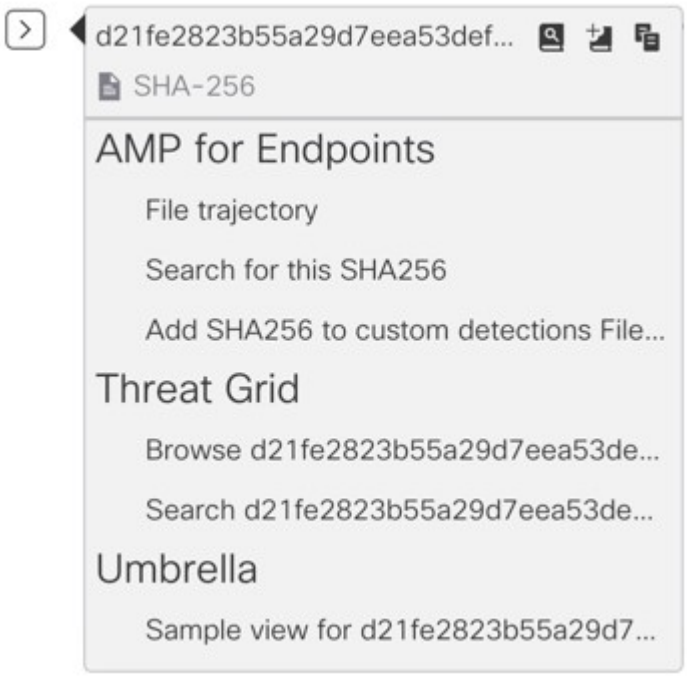
Before you begin

Make sure that you obtain the client ID and client password to access the Cisco SecureX Ribbon and pivot menu widgets on your appliance. For more information, see Accessing the Cisco SecureX Ribbon, on page 21.

Procedure

Step 1 Log in to the new web interface of your appliance. For more information, see Understanding the Web Reporting Pages on the New Web Interface.

Step 2 Navigate to the **Web Reporting** page, click the pivot menu  button next to the required observable (for example, bit.ly).



Perform the following:

- Click button to add an observable to active case.
- Click button to add the observable to new case.

Note

Use the pivot menu button to pivot an observable to other devices registered on the portal (for example, AMP for Endpoints) to investigate for threat analysis.

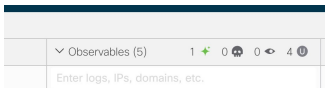
Step 3 Hover over icon and click button to open the **Casebook**. Check whether the observable is added to a new or an existing case.

Step 4 (Optional) Click button to add a title, description, or notes to the **Casebook**.

Note You can search for observables for threat analysis in two different ways:

- Click the **Enrichment** search box from the Cisco SecureX Ribbon and search for the observables.

- Click the **Casebook** icon inside the Cisco SecureX Ribbon and search for the observables in the search field.



For more information on Cisco SecureX Ribbon, see https://securex.us.security.cisco.com/help/ribbon.

Integrate Cisco Secure Web Appliance with Cisco Umbrella

This topic contains the following sections:

- About Secure Web Appliance (SWA) and Umbrella, on page 24
- Guidelines for the Integration, on page 24
- End-to-End Procedure, on page 25
- How to Integrate Secure Web Appliance with Umbrella, on page 25
- Configure Web Policies and Destination Lists, on page 28
- Configure AD Users or AD Groups, on page 31
- Configure Microsoft 365 Compatibility, on page 31
- Policy Conflict Management and Policy Ordering, on page 31
- Block Page Management, on page 32
- Cisco Umbrella Seamless ID, on page 32

About Secure Web Appliance (SWA) and Umbrella

Umbrella is Cisco's cloud-based Secure Internet Gateway (SIG) platform that provides you with multiple levels of defense against internet-based threats. Umbrella integrates secure web gateway, firewall, DNS-layer security, and cloud access security broker (CASB) functionality to protect your systems against threats.

The integration of Umbrella and Secure Web Appliance facilitates deployment of common web policies from Umbrella to Secure Web Appliance. You can configure policies through Umbrella dashboard and view logs.

When you configure the common web policies in the Umbrella Dashboard, the policies are pushed to Secure Web Appliance. The reporting data of those configured web policies are sent back to Umbrella and avialable on Umbrella Dashboard. Reporting data includes information such as URLs browsed, their IP addresses, and whether the URL was permitted or blocked.

You can access Umbrella using the following URL:

https://login.umbrella.com/umbrella

For more information, see Umbrella Integration with Secure Web Appliance

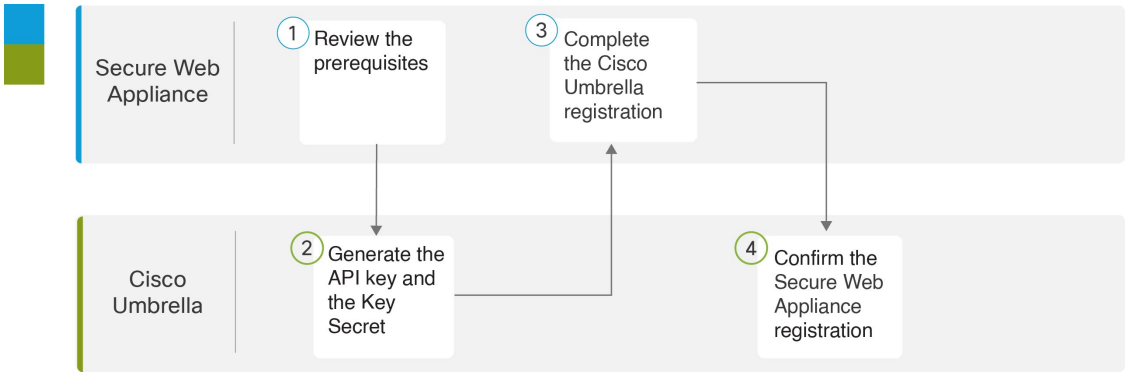
Guidelines for the Integration

- For a successful registration of the device with Umbrella, acquire the API Key and key Secret with Valid scopes from Umbrella Organization.

- For a successful translation of web policies, update certificate bundle and categories to the latest categories in Secure Web Appliance.

End-to-End Procedure

The following flowchart illustrates the workflow for integrating Secure Web Appliance with Umbrella.



How to Integrate Secure Web Appliance with Umbrella

Table 3: How to Integrate Secure Web Appliance with Umbrella

	Do This	More Info
Step 1	On Secure Web Appliance, review the prerequisites.	Prerequisites, on page 25
Step 2	On Umbrella, generate the API Key and the Key Secret.	Generate API Keys and Key Secret
Step 3	On Secure Web Appliance, complete the Cisco registration.	Register Cisco Secure Web Appliance with Cisco Umbrella
Step 4	On Umbrella, confirm the Secure Web Appliance registration.	Confirm whether the registration was successful

Prerequisites

Perform the following in Secure Web Appliance:

- For a successful connection to Umbrella, update the Cert bundle (Cisco Trusted Root Certificate Bundle: 2.2).
- To configure the translated policy from Umbrella successfully, update the Content Categories (107).
- Manually enable the HTTPS Proxy in Secure Web Appliance, if HTTPS inspection is enabled in the ruleset of Umbrella.
- For successful translation of the application settings selected in Umbrella rules, in Secure Web Appliance navigate to **Security Services** > **Acceptable Use Controls** and enable **Application Discovery and Control (ADC)** .

- If AD is integrated in Umbrella, configure the Active Directory (AD) realm in Secure Web Appliance. We recommend to have a healthy AD Connector and Domain Controller.
- To upgrade to AsyncOS version 15.1, you must activate Smart Licensing.
- Ensure that the internal network is associated with the public network or that Active Directory is integrated with Umbrella.

In Umbrella:

Generate the **API Key** and **Key Secret** using **Key Scopes** from Umbrella. For instructions on generating the keys, see Cisco Umbrella SIG User Guide.



Note

- While generating the **API Key** and **Key Secret** (**Admin** > **API Keys**), for a specific organization ensure you select **Key Scope** as *Auth* (Read Only) and **Registered Appliances** as *Deployments/Registered Appliances* (Read or Write).
- You can view the **Registered Appliance** page only with a valid subscription.

You can now configure and manage Secure Web Appliance policies from Umbrella.

Register Cisco Secure Web Appliance with Cisco Umbrella

Procedure

Step 1 Log in to Secure Web Appliance.

Step 2 Select **Network** > **Umbrella Settings**.

Step 3 Click **Edit Settings**.

Step 4 In **Umbrella Settings**, enter the **API Key**, **API Secret**, and click **Register**.

Once the Secure Web Appliance is registered, a successful message appears.

Note
If the internet is not accessible via the M1 interface, access to the public domain—api.umbrella.com will be blocked and the registration with Umbrella will also fail.

Step 5 To initiate the connection between Secure Web Appliance and Umbrella, you must enable the hybrid policy. To enable, check the **Hybrid Policy** check box.

Step 6 To send Umbrella configured web policies reporting data from Secure Web Appliance to Umbrella reporting dashboard, check the **Hybrid Reporting** check box. The Umbrella dashboard filters Secure Web Appliance reporting data based on the IP address of external clients.

Note
Disabling Hybrid Policy also disables Hybrid Reporting.

Step 7 Select **Management** or **Data** from **Source Interface** dropdown list. Secure Web Appliance displays the **Data** interface only if **Data Port** is configured as an interface.

Step 8 Submit and commit your changes.

What to do next

Confirm whether the Registration was Successful, on page 27

Note

- When the **Hybrid Policy** checkbox is enabled, policies are translated and pushed from Umbrella to Secure Web Appliance. The user can be notified via email when a policy push fails. This can be configured as a **System** alert under **System Administration** > **Alerts**.
- By enabling Hybrid Reporting, only the Secure Web Appliance reporting data of Umbrella configured policies will be sent to Umbrella Reporting. The user can be notified via email when reporting data is not sent by Secure Web Appliance. This can be configured as a **System** alert under **System Administration** > **Alerts**.

Confirm whether the Registration was Successful

On Umbrella, navigate to the **Deployments** > **Core Identities** > **Registered Appliances** page and view the Secure Web Appliance devices that are registered with Umbrella.

Note

- The status of the registered Secure Web Appliance will be Active, only if you have selected the **Hybrid Policy** check box in the Secure Web Appliance **Umbrella Settings** page. Otherwise, the Secure Web Appliance device status is Offline.
- If you have selected the **Hybrid Policy** and **Hybrid Reporting** check box in the Secure Web Appliance **Umbrella Settings** page, the Hybrid Reporting status in Umbrella will be **Active**.
- If the Status of Policy Sync is **Failed**, an error message appears when you hover over the status.
- If the Policy Sync status is **Success** with a warning icon, the following warning message appears when you hover over the status: ***If a few users/groups have been selected in rules/rulesets from AD Connectors or Domain Controllers which are not in a healthy state, navigate to Deployments > Configuration > Sites and Active Directory to see the error details and fix it.***AD Details and selected users/group information will are also available in the warning message.

The **Policy Push** option available on the Registered Appliances page of the Umbrella UI allows you to push configured web policies to selected Secure Web Appliances.

Deregister Cisco Secure Web Appliance from Cisco Umbrella

Procedure

Step 1 Log in to Secure Web Appliance.

Step 2 Select **Network** > **Umbrella Settings**.

Step 3 Click **Edit Settings**.

Step 4 Check the **Hybrid Policy** and **Hybrid Reporting** checkboxes to disable them.

Step 5 Commit your changes.

Step 6 Enter the **API Key**, **API Secret**, and click **Deregister**.

You will be prompted to keep or delete Umbrella pushed policies. If you select Yes, Umbrella pushed policies are removed from Secure Web Appliance after the changes are committed.

View Umbrella Reporting Dashboard

Secure Web Appliance sends Umbrella configured policies reporting data to Umbrella Dashboard. To view this reporting data on Umbrella, navigate to **Reporting** > **Activity Search** and select the **Identity Type** as **Secure Web Appliance**.

Configure Web Policies and Destination Lists

After successful integration, the web policies get translated and pushed from Umbrella to Secure Web Appliance.

If you have enabled Hybrid Reporting while integrating, Secure Web Appliance sends reporting data generated based on Umbrella policies to the Umbrella reporting dashboard.

The following profiles and policies are translated to Secure Web Appliance:

- Configure Identification Profiles, on page 28
- Configure Custom and External URL Categories, on page 29
- Configure Access Policies, on page 29
- Configure Decryption Policies, on page 29
- Configure Application in Access Policies, on page 30

Configure Identification Profiles

There will be only one global identification profile with Authenticate option (if AD is integrated in Umbrella) or with Exempt from Authentication option (if AD is not integrated in Umbrella).

To create a ruleset identity in Umbrella, navigate to **Web Policy**, select **Networks** or **AD Users** or **AD Groups** as Ruleset Identities. For more information, see https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy#setup.

Note Ensure that the network identity has an internal network that is associated with it.

You can create an internal network in Umbrella (**Deployments** > **Configuration** > **Internal Networks**) and associate it with a public network. Internal networks are translated as subnets in access policy and decryption policy in Secure Web Appliance.

Configure Custom and External URL Categories

The Destination lists on Umbrella are translated as Custom and External URL Categories in Secure Web Appliance (**Web Security Manager** > **Custom and External URL Categories**).

Create a destination list on Umbrella (**Policy** > **Policy Components** > **Destination Lists**) and associate it with a web policy. For more information, see https://docs.umbrella.com/umbrella-user-guide/docs/add-a-destination-list.

Configure Access Policies

Web Policy (rules) of Umbrella is translated as Access Policies in Secure Web Appliance.

Create a rule in Umbrella with public network (for which an internal network is associated), internal network, AD Users, and AD Groups configured as rule identities. Configure destinations with **Content Categories** or **Destination Lists**.

For more information, see https://docs.umbrella.com/umbrella-user-guide/docs/add-rules-to-a-ruleset#procedure.

You can now view the translated rules in Secure Web Appliance (**Web Security Manager** > **Access Policies** > **URL Filtering**).

For an access policy, you can view the selected **Content Categories** from **Umbrella Rules** under **URL Filtering** > **Predefined URL Category Filtering** and **Destination lists** under **URL Filtering** > **Custom and External URL Category Filtering**.

Based on the identities selected in the Ruleset, an additional access policy is created to monitor all destinations.



Note

- Based on the identities selection for translation, one-to-one mapping or one-to-many mapping from Umbrella rules to Secure Web Appliance access policy is created.
- An extra access policy to monitor all the destinations will be created based on the identities selected in the Ruleset.

Configure Decryption Policies

The **HTTPS Inspection** policies in Umbrella are translated as **Decryption policies** in Secure Web Appliance so that it can be used along with identities.



Note You can configure Decryption policies from Umbrella only if **HTTPS Proxy** is enabled in Secure Web Appliance.

Enable the HTTPS Inspection in Umbrella (**Policies** > **Management** > **Web Policy** > **Ruleset Settings** > **HTTPS Inspection Settings**).

If you select **None** in the **Selective Decrpytion List**, all the pre-defined content categories will be decrypted. Choose a selective decryption list from the drop-down to bypass the HTTPS inspection.

The translated Content Categories from the **Selective Decryption List** of Umbrella is displayed under **URL Filtering** > **Predefined URL Category Filtering** and Domains from the **Selective Decrpytion List** of

Umbrella is displayed under **URL Filtering** > **Custom and External URL Category Filtering** for a decryption policy.

The HTTPS Inspection configuration in Umbrella is translated to Secure Web Appliance as follows:

- If enabled, the **Domains** and the **Content Categories** from the **Selective Decryption List**, will be set to *Passthrough* in Secure Web Appliance and the remaining categories to *Decrypt*.
- If disabled, the **Decryption Policies** are displayed with all Predefined URL Category Filtering as *Monitor* in Secure Web Appliance.
- If **Display Block Page Over HTTPS** is selected, the **Decryption Policies** is displayed with all Predefined URL Category Filtering as *Monitor* in the Secure Web Appliance.

For more information, see Add a Ruleset to the WebPolicy.



Note

- Translation of **Applications** in **Selective Decryption List** from Umbrella as **Decryption Policies** in Secure Web Appliance is not supported.
- An additional decryption policy will be created when AD Users or AD Groups are selected along with network in ruleset identities.
- Default action of decryption Policies translated from Umbrella will be to set to *Decrypt*.
- The WBRS is disabled in Secure Web Appliance for the **Decryption Policies** that are translated from Umbrella.

Configure Application in Access Policies

The **Application Settings** also known as CASI in Umbrella are translated as **ADC Applications** in the access policies of Secure Web Appliance.

You can select application categories or specific applications in the Umbrella Rules, and the same rule action is applied to Access policy's applications in the Secure Web Appliance. Applications that are not selected in the Rules inherit global settings.

Custom URL categories consisting of domains for selected applications are created and pushed to the Secure Web Appliance. You can view this by navigating to **URL Filtering** > **Custom and External URL Category Filtering** and selecting the **Action** as **Monitor** in the URL Filtering section of the Access Policy.

For more information, see Manage Application Settings on Umbrella.

When these rules are translated to Secure Web Appliance, you can view them by navigating to **Web Security Manager** > **Access Policies** > **Applications**.

Important! For successful translation of the applications rules with selected applications from Umbrella to Secure Web Appliance, you must enable **Application Discovery and Control (ADC)**.

For more information, see Enabling the AVC or ADC Engine.



Note The Application policies in Umbrella are not translated as Decryption policies in Secure Web Appliance.

Configure AD Users or AD Groups

The AD Users or AD Groups in Umbrella web policies should be configured in Secure Web Appliance policies as **Selected Groups and Users** in **Policy Member Definition** section.

In Umbrella, when AD is integrated (**Deployments** > **Configuration** > **Sites and Active Directory**), only one global identification profile will be created with the Realms as *All Realms*; Schema as *Use Kerberos or NTLMSSP or Basic*; Authentication Surrogates as *IP Address*. The **Apply same surrogate settings to explicit forward requests** check box will be enabled in the Secure Web Appliance when the **Web Proxy Mode** is **Transparent** under **Security Services** > **Proxy Settings** > **Web Proxy Settings** > **Basic Settings** > **Proxy Mode**.



Note The active directories which are integrated in Umbrella should be configured manually on the Secure Web Appliance and must be reachable.

In Umbrella (**Policies** > **Management** > **Web Policy** > **Ruleset Identities**), select **AD Users** or **AD Groups** from the integrated AD of Umbrella. The selected **AD Users** or **AD Groups** in the ruleset identities should be mapped to the membership section (**Web Security Manager** > **Decryption Policies** > **Policy Member Definition**) of the decryption policy in Secure Web Appliance.

In Umbrella (**Policies** > **Management** > **Web Policy** > **Ruleset** > **Rules**), create a rule with the identity selected as **AD Users** or **AD Groups** with the rule action and the destination selected. The selected **AD Users** or **AD Groups** in the rules are mapped to the membership section (**Web Security Manager** > **Access Policies** > **Policy Member Definition**) of the access policy in Secure Web Appliance.

An additional policy will be created with the selected **AD Users** or **AD Groups** of ruleset identities to allow all the predefined content categories.

Configure Microsoft 365 Compatibility

You can translate **Microsoft 365 Compatibility** configuration from Umbrella to Secure Web Appliance **Custom and External URL Categories**.

In Umbrella, if **Microsoft 365 Compatibility** is enabled (**Policies** > **Management** > **Web Policy** > **Global Settings**), **Custom and External URL Categories** in Secure Web Appliance will be created with the **Category Type** as *External Live Feed Category* and with **Feed File Location** as *Office 365 Web Service*. This category will be selected for the decryption policies configured from Umbrella under **URL Filtering** section of Secure Web Appliance with **Action** as *Passthrough*.



Note Decryption policies will be configured only if **HTTPS Proxy** is enabled in Secure Web Appliance.

Policy Conflict Management and Policy Ordering

You cannot edit or delete Umbrella managed profiles or policies like identification profiles, access policies, decryption policies, and custom and external url categories configured from Umbrella to Secure Web Appliance. You cannot create profiles or policies with names that are prefixed with 'umbrella<space>', example, umbrella abc.

Note

- You cannot clone an Umbrella policy that is configured in Secure Web Appliance.
- You cannot change the order of policies that are translated from Umbrella in Secure Web Appliance.
- You can edit or delete policies that are pushed from Umbrella after disabling the hybrid policy option under **Network** > **Umbrella Settings** in Secure Web Appliance.
- You can edit and delete policies pushed from Umbrella using REST APIs.

The sequence of the policy rules in Umbrella are retained during policy translation to Secure Web Appliance. Thus, the Secure Web Appliance admin-configured policies or profiles will take precedence over policies that are translated from Umbrella.

Block Page Management

You can now translate Umbrella's **Block Page** settings (**Policies** > **Management** > **Policy Components** > **Block Page Appearance**) that is associated with the first ruleset to **End-User Notification** page (**Security Services** > **End-User Notification**) in Secure Web Appliance.

In Umbrella, to translate the Umbrella **Block Page** settings, configure the block page, and select the block page under the first ruleset (**Policies** > **Web Policy**).

Note Changes in the selected **Block Page** of the first ruleset will be pushed to the Secure Web Appliance every three hours.

For more information, see https://docs.umbrella.com/umbrella-user-guide/docs/create-a-custom-block-page.

Cisco Umbrella Seamless ID

The Cisco Umbrella Seamless ID feature enables the appliance to pass the user identification information to the Cisco Umbrella Secure Web Gateway (SWG) after successful authentication. The Cisco Umbrella SWG checks the user information in the Active Directory based on the authenticated identification information received from the Secure Web Appliance. The Cisco Umbrella SWG considers the user as authenticated and provides access to the user based on the defined security policies.

The Secure Web Appliance passes the user identification information to the Cisco Umbrella SWG using the HTTP headers; X-USWG-PKH, X-USWG-SK, and X-USWG-Data.

Note

- The Cisco Umbrella Seamless ID headers overwrite the headers with the same names on the Secure Web Appliance, if any.
- The Cisco Umbrella Seamless ID feature supports authentication scheme with Active Directory only. This feature does not support LDAP, Cisco Identity Services Engine (ISE), and Cisco Context Directory Agent (CDA).
- The Cisco Umbrella SWG does not support FTP and SOCKS traffic.

Table 4: HTTPs Traffic Behavior

Deployment Mode	Surrogate	Decrypt for Authentication	Secure Web Appliance Authentication	Cisco Umbrella Seamless ID Sharing
Explicit	IP surrogate	Yes/No	Yes	Yes
Transparent	IP surrogate	Yes	Yes	Yes
Transparent	IP surrogate	No	Skips authentication	No
Explicit	Cookie, without credential encryption	Yes/No	Yes	Yes
Explicit	Cookie, with credential encryption	Yes/No	Yes	No
Transparent	Cookie with/without credential encryption	Yes/No	Skips authentication	No

Note The Secure Web Appliance retrieves the UPN value for the authenticated user from the active directory and allows the Cisco Umbrella Seamless ID to apply the correct web policies for the users. For this functionality to work, you must assign all the active directory users with default or customized UPN values.

This section contains the following topics:

- Configuring Cisco Umbrella Seamless ID
- Configuring Routing Destination for Cisco Umbrella SWG

Configuring Cisco Umbrella Seamless ID

Before you begin

- Upload the root or custom Umbrella certificate to the appliance manually through **Network** > **Certificate Management** > **Manage Trusted Root Certificates**. See Certificate Management.
- Ensure you have configured identification profiles for authentication.
- Define routing policies with configured identification profiles.

Procedure

Step 1 Choose **Web Security Manager** > **Cisco Umbrella Seamless ID** .

Step 2 Click **Edit Settings**.

Step 3 Enter the Cisco Umbrella SWG hostname or IP address.

Step 4 Enter the port numbers of the SWG for HTTP and HTTPS traffic.

You can enter a maximum of six port numbers.

Step 5 (Optional) Click **Connectivity Test** to ensure the successful connectivity of the Cisco Umbrella SWG over ports and validation of certificates.

Step 6 Enter the unique customer organization ID of Cisco Umbrella SWG.

Step 7 Submit and commit.

Configuring Routing Destination for Cisco Umbrella SWG

To create a new routing policy, see Adding Routing Destination and IP Spoofing Profile to Routing Policy

.

Procedure

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

Step 2 On the **Routing Policies** page, click the link under **Routing Destination** column for the routing policy that you want to configure the Cisco Umbrella Seamless ID with the required port.

Step 3 Select the appropriate Cisco Umbrella Seamless ID with port as the Upstream Proxy Group for the policy. The Upstream Proxy Group drop-down list displays all the Cisco Umbrella Seamless ID with ports that you have configured through the **Cisco Umbrella Seamless ID** page (**Web Security Manager** > **Cisco Umbrella Seamless ID**).

Note
If you remove a **Cisco Umbrella Seamless ID** with port number (**Web Security Manager** > **Cisco Umbrella Seamless ID**) which is already linked to a routing policy, then the routing destination is automatically changed to 'Direct Connection'.

Step 4 Submit and commit your changes.