

System Settings

This topic contains the following sections:

- Perform System Administration Tasks, on page 1
- Connect the Appliance to a Cisco Cloud Web Security Proxy, on page 70
- Intercepting Web Requests, on page 77

Perform System Administration Tasks

This topic contains the following sections:

- Overview of System Administration, on page 2
- Saving, Loading, and Resetting the Appliance Configuration, on page 2
- Cisco Secure Web Appliance Licensing, on page 5
- Virtual Appliance License, on page 24
- Enabling Remote Power Cycling , on page 25
- Administering User Accounts, on page 26
- Defining User Preferences, on page 31
- Configuring Administrator Settings, on page 31
- User Network Access, on page 33
- Resetting the Administrator Passphrase, on page 34
- Configuring the Return Address for Generated Messages, on page 34
- Managing Alerts, on page 35
- FIPS Compliance, on page 44
- System Date and Time Management, on page 46
- SSL Configuration , on page 47
- Certificate Management, on page 49
- AsyncOS for Web Upgrades and Updates, on page 53

- Reverting to a Previous Version of AsyncOS for Web, on page 60
- Monitoring System Health and Status Using SNMP, on page 62
- Web Traffic Tap, on page 66
- Configuring HTTP 2.0 Protocol, on page 69

Overview of System Administration

The S-Series appliance provides a variety of tools for managing the system. Functionality on System Administration tab helps you manage the following tasks:

- Appliance configuration
- Feature keys
- Adding, editing, and removing user accounts
- AsyncOS software upgrades and updates
- System time

Saving, Loading, and Resetting the Appliance Configuration

All configuration settings within the Secure Web Appliance are managed using a single XML configuration file.

- Viewing and Printing the Appliance Configuration, on page 2
- Saving the Appliance Configuration File, on page 2
- Loading the Appliance Configuration File, on page 3
- Resetting the Appliance Configuration to Factory Defaults , on page 4

Viewing and Printing the Appliance Configuration

Procedure

Step 1 Choose **System Administration > Configuration Summary.**

Step 2 View or print the Configuration Summary page as required.

Saving the Appliance Configuration File

Procedure

Step 1 Choose **System Administration > Configuration File**.

Step 2 Complete the Configuration File options.

Option	Description
Specify a file-handling option	Choose how the generated configuration file is handled: • Download file to local computer to view or save. • **Save file to this appliance** (wsa_example.com). • **Email file to:** – provide one or more email addresses.
Specify a passphrase-handling option	• **Mask passphrases in the Configuration Files** – The original passphrases are replaced with "*****" in the exported or saved file. Please note that configuration files with masked passphrases cannot be loaded directly back into AsyncOS for Web. • **Encrypt passphrases in the Configuration Files** – If FIPS mode is enabled, this option is available. See Enabling or Disabling FIPS Mode , on page 45 for information about enabling FIPS mode.
Select a file-naming option	Choose how the configuration file is named: • **Use system-generated file name** • **Use user-defined file name**

Step 3 Click **Submit**.

Loading the Appliance Configuration File

Caution Loading configuration will permanently remove all of your current configuration settings. It is strongly recommended that you save your configuration before performing these actions.

We do not recommend loading configurations from a previous release into the latest version. You can retain the configuration settings by upgrading the paths.

Configuration files loaded with manual changes may result in performance and functional issues.

Note If a compatible configuration file is based on an older version of the set of URL categories than the version currently installed on the appliance, policies and identities in the configuration file may be modified automatically.

Note If you encounter a certificate validation error when loading the configuration file, upload the rootCA of the certificate to the trusted root directory of the Secure Web Appliance and then load the configuration file again. To know how to upload the rootCA, see Certificate Management, on page 49.

Procedure

Step 1 Choose **System Administration > Configuration File**.

Step 2 Choose Load Configuration options and a file to load. Note:

Note

- Files with masked passphrases cannot be loaded.
- Files must have the following header:

  ```
  <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
  ```

  and a correctly formatted config section:

  `<config>` ... *your configuration information in valid XML* `</config>`

Step 3 Click **Load**.

Step 4 Read the warning displayed. If you understand the consequences of proceeding, click **Continue**.

Resetting the Appliance Configuration to Factory Defaults

You can choose whether or not to retain existing network settings when you reset the appliance configuration.

This action does not require a commit.

Before you begin

Save your configuration to a location off the appliance.

Procedure

Step 1 Choose **System Administration > Configuration File**.

Step 2 Scroll down to view the **Reset Configuration** section.

Step 3 Read the information on the page and select options.

Step 4 Click **Reset**.

Saving Configuration File Backup

The configuration file backup feature records the appliance configuration on every commit and sends the previous configuration file before the current one to a remotely located backup server through FTP or SCP.

Procedure

Step 1 Choose **System Administration > Configuration File**

Step 2 Select the **Enable Config Backup** check box.

Step 3 Choose **Yes** to include the passphrase in the configuration file. Alternatively, choose **No** to exclude the passphrase in the configuration file.

Step 4 Choose the retrieval method. The available options are:

- FTP on Remote Server - Enter the FTP hostname, directory, username, and passphrase.
- SCP on Remote Server- Enter the SCP hostname, port number, directory, and username.
- Host Key Checking- The SSH automatically maintains and checks a database of identifications for all hosts with which it has been used. Host keys are stored in the user's home directory in the directory */.ssh/known_hosts*.

  If you select **SCP on Remote Server** and then select **Enable Host Key Checking**, you will have the following options:

  - Automatic- The host key will be set automatically by Secure Web Appliance.
  - Manual- User can enter the host key manually.

  Upon submitting the changes, Secure Web Appliance provides SSH key(s) to be added to authorized keys file on remote host, so that configuration files can be uploaded from Secure Web Appliance to the remote host. As a result, SSH maintains and checks a database containing identification information for all hosts it has ever connected to. Host keys are stored in the user's home directory in the directory */.ssh/known_hosts*.

Step 5 Click **Submit**.

You can also enable the configuration file backup feature by using the CLI command `configbackup`

Cisco Secure Web Appliance Licensing

- Working with Feature Keys, on page 5
- Smart Software Licensing, on page 6

Working with Feature Keys

Feature keys enable specific functionality on your system.Keys are specific to the serial number of your appliance (you cannot re-use a key from one system on another system).

- Displaying and Updating Feature Keys, on page 5
- Changing Feature Key Update Settings , on page 6

Displaying and Updating Feature Keys

Procedure

Step 1 Choose **System Administration > Feature Keys**.

Step 2 To refresh the list of pending keys, click **Check for New Keys** to refresh the list of pending keys.

Step 3 To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. If the feature key is valid, the feature key is added to the display.

Step 4 To activate a new feature key from the Pending Activation list, mark its "Select" checkbox and click **Activate Selected Keys**.

You can configure your appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list will always be empty. You can tell AsyncOS to look for new keys at any time by clicking the **Check for New Keys** button, even if you have disabled the automatic checking via the Feature Key Settings page.

Changing Feature Key Update Settings

The Feature Key Settings page is used to control whether your appliance checks for and downloads new feature keys, and whether or not those keys are automatically activated.

Procedure

Step 1 Choose **System Administration > Feature Key Settings**.

Step 2 Click **Edit Settings**.

Step 3 Change the Feature Key Settings as required.

Option	Description
Automatic Serving of Feature Keys	Options to automatically check and download feature keys and to automatically activate downloaded feature keys. Automatic checks are normally performed once a month but this changes to once a day when a feature key is to expire in less than 10 days and once a day after key expiration, for up to one month. After a month, the expired key is no longer included in the list of expiring/expired keys.

Step 4 Submit and commit your changes.

Smart Software Licensing

- Overview, on page 7
- Enabling Smart Software Licensing , on page 8
- Registering the Appliance with Cisco Smart Software Manager , on page 9
- Requesting for Licenses, on page 12
- Deregistering the Appliance from Smart Cisco Software Manager, on page 13
- Reregistering the Appliance with Smart Cisco Software Manager, on page 13
- Changing Transport Settings, on page 13
- Renewing Authorization and Certificate, on page 14

- Updating Smart Agent, on page 14
- Alerts, on page 14
- Command Line Interface, on page 15

Overview

Smart Software Licensing enables you to manage and monitor Cisco Secure Web Appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM) which is the centralized database that maintains the licensing details about all the Cisco products that you purchase and use. With Smart Licensing, you can register with a single token rather than registering them individually on the website using Product Authorization Keys (PAKs).

Once you register the appliance, you can track your appliance licenses and monitor license usage through the CSSM portal. The Smart Agent installed on the appliance connects the appliance with CSSM and passes the license usage information to the CSSM to track the consumption.

See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Cisco Smart Software Manager.

Note AsyncOS version 15.0 is the last release to support the Classic license. The next releases will only support Smart Licenses.

Before you begin

- Make sure that your appliance has internet connectivity.
- Contact Cisco sales team to create a smart account in Cisco Smart Software Manager portal (https://software.cisco.com/#module/SmartLicensing) or install a Cisco Smart Software Manager Satellite on your network.

  See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know more about Cisco Smart Software Manager user account creation or installing a Smart Software Manager On-Prem.

  For users who do not want to directly send the license usage information to the internet, the Smart Software Manager Satellite can be installed on the premises, and it provides a subset of CSSM functionality. Once you download and deploy the satellite application, you can manage licenses locally and securely without sending data to CSSM using the internet. The CSSM Satellite periodically transmits the information to the cloud.

Note If you want to use Smart Software Manager Satellite, use Smart Software Manager Satellite Enhanced Edition 6.1.0.

- The existing users of classic licenses (traditional) should migrate their classic licenses to smart licenses.

  See https://video.cisco.com/detail/video/6330894176112?autoStart=true&q=convert-classic-licenses-to-smart-licenses.

- The system clock of the appliance must be in sync with that of the CSSM. Any deviation in the system clock of the appliance with that of the CSSM, will result in failure of smart licensing operations.

Note If you have internet connectivity and want to connect to the CSSM through a proxy, you must use the same proxy that is configured for the appliance using **System Administration-> Upgrade and Update Settings**

Note For virtual users, every time you receive a new PAK file (new or renewal), generate the license file and load the file on the appliance. After loading the file, you must convert the PAK to Smart Licensing. In Smart Licensing mode, the feature keys section in the license file will be ignored while loading the file and only the certificate information will be used.

Note The appliance will move from the Smart Licensing mode to Classic Licensing mode when you revert the appliance to a previous veriosn of AsyncOS. You must enable Smart Licensing manually and request for required licences.

You must perform the following procedures to activate Smart Software Licensing for your appliance:

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing , on page 8
Step 2	Register the appliance with Cisco Smart Software Manager	Registering the Appliance with Cisco Smart Software Manager , on page 9
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 12

Enabling Smart Software Licensing

Procedure

Step 1 Choose **System Administration > Smart Software Licensing**.

Step 2 Click **Enable Smart Software Licensing**.

To know about Smart Software Licensing, click on the **Learn More about Smart Software Licensing** link.

Step 3 Click **OK** after reading the information about Smart Software Licensing.

Step 4 Commit your changes.

What to do next

After you enable Smart Software Licensing, all the features in the Classic Licensing mode will be automatically available in the Smart Licensing mode. If you are an existing user in Classic Licensing mode, you have 90-days evaluation period to use the Smart Software Licensing feature without registering your appliance with the CSSM.

You will get notifications on regular intervals (90th, 60th, 30th, 15th, 5th, and last day) prior to the expiry and also upon expiry of the evaluation period. You can register your appliance with the CSSM during or after the evaluation period.



Note

- New Virtual Appliance users with no active licenses in Classic Licensing mode will not have the evaluation period even if they enable the Smart Software Licensing feature. Only the existing Virtual Appliance users with active licenses in Classic Licensing mode will have evaluation period. If new Virtual Appliance users want to evaluate the smart licensing feature, contact Cisco Sales team to add the evaluation license to the smart account. The evaluation licenses are used for evaluation purpose after registration.
- After you enable the Smart Licensing feature on your appliance, you will not be able to roll back from Smart Licensing to Classic Licensing mode.
- The following features are restarted when you enable the Smart Licensing feature:
  - Secure Web Appliance Web Reputation Filters
  - Secure Web Appliance Anti-Virus Sophos
  - Secure Web Appliance Anti-Virus Webroot
  - Secure Web Appliance Web Proxy and DVS Engine
- In AsyncOS version 15.0, Smart Licensing can be enabled for new Secure Web Appliance virtual deployments. Even though Classic licensing is not mandatory. For more information, refer to the pre-requisites available under the Overview of Smart Licencing section.

Registering the Appliance with Cisco Smart Software Manager

You must enable the Smart Software Licensing feature under System Administration menu in order to register your appliance with the Cisco Smart Software Manager (CSSM).



Note

- You cannot register multiple appliances in a single instance. You should register appliances one by one.
- The initial registration is valid for one year. Renewal of registration is performed automatically every six months, if the appliance has connectivity to the CSSM.

Procedure

Step 1 Choose **System Administration** > **Smart Software Licensing**.

Step 2 Select the **Smart License Registration** option.

Step 3 Click **Confirm**.

Step 4 Click **Edit**, if you want to change the Transport Settings. The available options are:

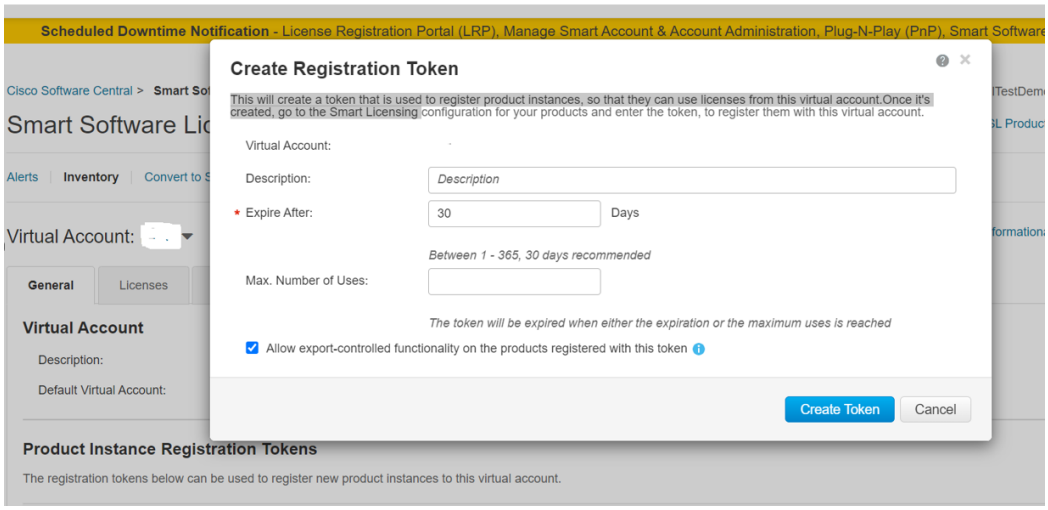
- **Direct**: Connects the appliance directly to the Cisco Smart Software Manager through HTTPs. This option is selected by default.
- **Transport Gateway**: Connects the appliance to the Cisco Smart Software Manager through a Transport Gateway or Smart Software Manager Satellite. When you choose this option, you must enter the URL of the Transport Gateway or the Smart Software Manager Satellite and click OK. This option supports HTTP and HTTPS. In FIPS mode, Transport Gateway supports only HTTPS.

  See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Transport Gateway.

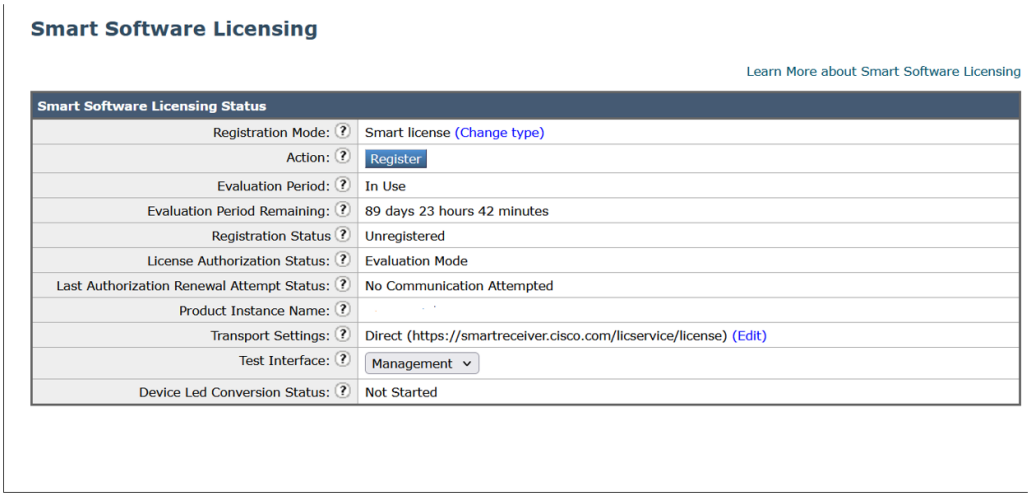
Step 5 (Optional) **Test Interface**: Choose Management or Data interface while registering the appliance for the smart licensing feature. This is applicable only when you enable split routing and register for smart licensing.

Note
If split routing is not enabled, only Management interface option is available in the **Test Interface** drop-down list.

Step 6 Access the Cisco Smart Software Manager portal (https://software.cisco.com/#module/SmartLicensing) using your login credentials. Navigate to the Virtual Account page of the portal and access the General tab to generate a new token. Copy the Product Instance Registration Token for your appliance. See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_ Deployment_Guide.html to know about Product Instance Registration Token creation.

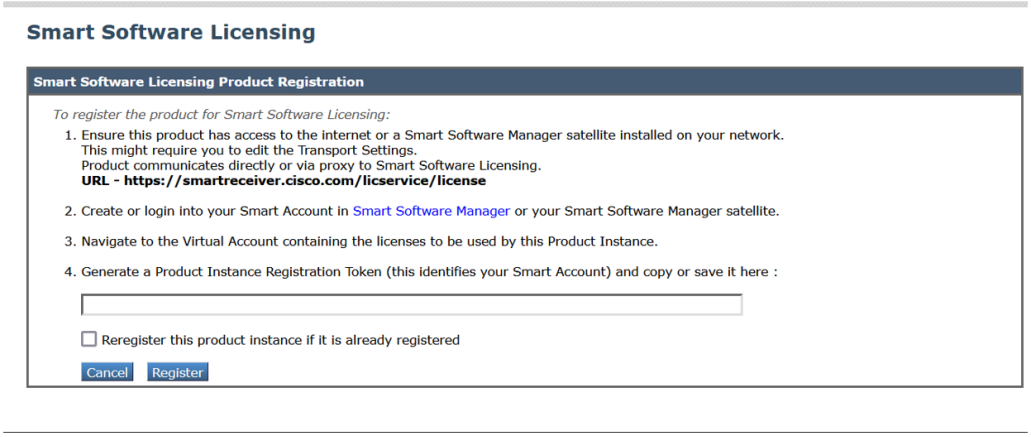


Step 7 Switch back to your appliance and click **Register**.



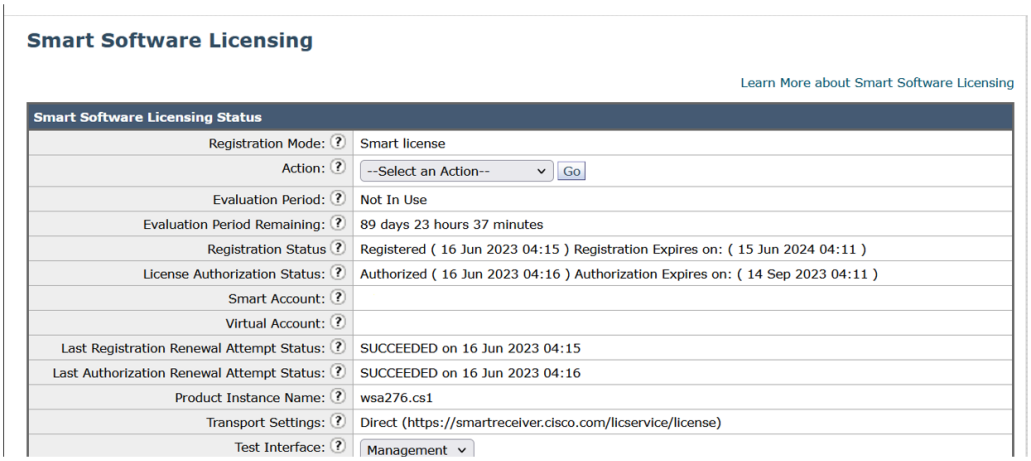
Step 8 Paste the **Product Instance Registration Token** in the textbox.

On the Smart Software Licensing page, you can select the **Reregister this product instance if it is already registered** check box to reregister your appliance.



What to do next

The product registration process takes a few minutes and you can view the registration status on the Smart Software Licensing page.



Requesting for Licenses

Once you complete the registration process successfully, you must request for licenses for the appliance's features as required.

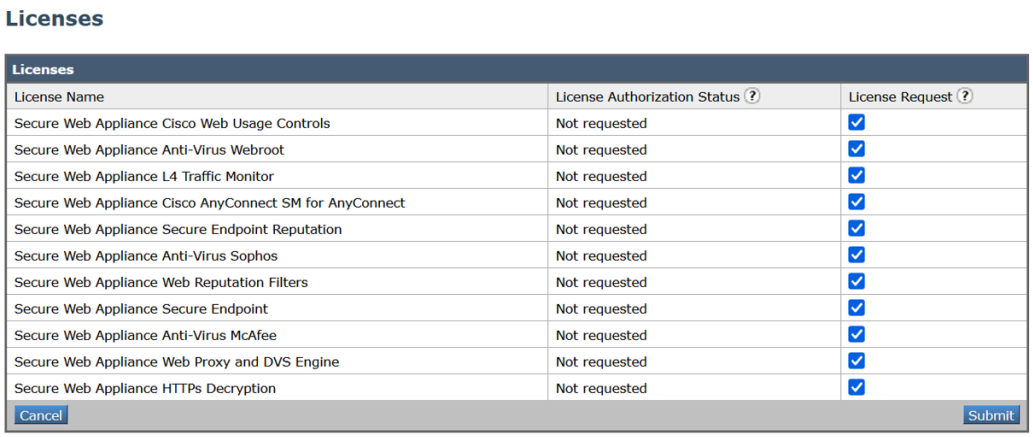
Procedure

Step 1 Choose **System Administration > Licenses**.

Step 2 Click **Edit Settings**.

Step 3 Check the checkboxes under the License Request/Release column corresponding to the licenses you want to request for.

Step 4 Click **Submit**.



What to do next

When the licenses are overused or expired, they will go into out of compliance (OOC) mode and 30-days grace period is provided to each license. You will get notifications on regular intervals (30th, 15th, 5th, and last day) prior to the expiry and also upon the expiry of the OOC grace period.

After the expiry of the OOC grace period, you cannot use the licenses and the features will be unavailable. To access the features again, you must update the licenses on the CSSM portal and renew the authorization.

Releasing Licenses

Procedure

Step 1 Choose **System Administration** > **Licenses**.
Step 2 Click **Edit Settings**.
Step 3 Uncheck the checkboxes under the License Request column corresponding to the licenses you want to release.
Step 4 Click **Submit**.

Deregistering the Appliance from Smart Cisco Software Manager

Procedure

Step 1 Choose **System Administration** > **Smart Software Licensing**.
Step 2 From the **Action** drop-down list, choose **Deregister** and click **Go**.
Step 3 Click **Submit**.

Reregistering the Appliance with Smart Cisco Software Manager

Procedure

Step 1 Choose **System Administration** > **Smart Software Licensing**.
Step 2 From the **Action** drop-down list, choose **Reregister** and click **Go**.

What to do next

See Registering the Appliance with Cisco Smart Software Manager , on page 9 to know about registration process.

You can reregister the appliance after you reset the appliance configurations during unavoidable scenarios.

Changing Transport Settings

You can change the transport settings only before registering the appliance with CSSM.

Note You can change the transport settings only when the smart licensing feature is enabled.If you have already registered your appliance, you must deregister the appliance to change the transport settings. After changing the transport settings, you must register the appliance again.

See Registering the Appliance with Cisco Smart Software Manager , on page 9 to know how to change the transport settings.

Renewing Authorization and Certificate

After you register your appliance with the Smart Cisco Software Manager, you can renew the certificate.

Note You can renew authorization only after the successful registration of the appliance.

Procedure

Step 1 Choose **System Administration > Smart Software Licensing**.

Step 2 From the **Action** drop-down list, choose the appropriate option:

- **Renew Authorization Now**
- **Renew Certificates Now**

Step 3 Click **Go**.

What to do next

Updating Smart Agent

To update the Smart Agent version installed on your appliance, perform the following steps:

Procedure

Step 1 Choose **System Administration > Smart Software Licensing**.

Step 2 In the **Smart Agent Update Status** section, click **Update Now** and follow the process.

Note
If you try to save any configuration changes using the CLI command `saveconfig` or through the web interface using **System Administration > Configuration Summary**, then Smart Licensing related configuration will not be saved.

Alerts

You will receive notifications on the following scenarios:

- Smart Software Licensing successfully enabled
- Smart Software Licensing enabling failed
- Beginning of the evaluation period

- Expiry of evaluation period (on regular intervals during evaluation period and upon expiry)
- Successfully registered
- Registration failed
- Successfully authorized
- Authorization failed
- Successfully deregistered
- Deregistration failed
- Successfully renewed Id certificate
- Renewal of Id certificate failed
- Expiry of authorization
- Expiry of Id certificate
- Expiry of out of compliance grace period (on regular intervals during out of compliance grace period and upon expiry).
- First instance of the expiry of a feature

Command Line Interface

- license_smart, on page 15
- show_license, on page 19
- cloudserviceconfig

license_smart

- Description, on page 15
- Usage, on page 16
- Example: Configuring Port for Smart Agent Service, on page 16
- Example: Enabling Smart Licensing, on page 16
- Example: Registering the Appliance with the Smart Software Manager , on page 16
- Example: Status of Smart Licensing , on page 17
- Example: Status Summary of Smart Licensing , on page 17
- Example: Setting the Smart Transport URL, on page 17
- Example: Requesting Licenses, on page 18
- Example: Releasing Licenses, on page 18

Description

Configure smart software licensing feature.

Usage

Commit: This command requires a 'commit'.

Batch Command: This command supports a batch format. For details, see the inline help by typing the command: `help license_smart`.

Example: Configuring Port for Smart Agent Service

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

Example: Enabling Smart Licensing

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
 [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

Example: Registering the Appliance with the Smart Software Manager

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
```

```
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

Example: Status of Smart Licensing

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Example: Status Summary of Smart Licensing

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Web Security Appliance Cisco                 Eval
Web Usage Controls
Web Security Appliance Anti-Virus Webroot    Eval
Web Security Appliance Anti-Virus Sophos     Eval
```

Example: Setting the Smart Transport URL

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
```

```
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
 satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.
```

Example: Requesting Licenses



Note Users of virtual appliance must register their appliance to request for or release the licenses.

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Web Security Appliance Anti-Virus Sophos      Not Requested
2. Web Security Appliance                        Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

Example: Releasing Licenses

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Web Security Appliance Cisco                Eval
   Web Usage Controls
2. Web Security Appliance                      Eval
   Anti-Virus Webroot
3. Web Security Appliance                      Eval
   L4 Traffic Monitor
4. Web Security Appliance Cisco                Eval
   AnyConnect SM for AnyConnect
5. Web Security Appliance Advanced             Eval
```

```
   Malware Protection Reputation
6. Web Security Appliance                  Eval
   Anti-Virus Sophos
7. Web Security Appliance                  Eval
   Web Reputation Filters
8. Web Security Appliance Advanced         Eval
   Malware Protection
```

show_license

- Description, on page 19
- Example: Status of Smart Licensing, on page 19
- Example: Status Summary of Smart Licensing, on page 19

Description

Show Smart Licensing status and summary of status.

Example: Status of Smart Licensing

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Example: Status Summary of Smart Licensing

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Web Security Appliance Cisco         Eval
Web Usage Controls
Web Security Appliance               Eval
Anti-Virus Webroot
Web Security Appliance               Eval
Anti-Virus Sophos
```

cloudserviceconfig

- Description
- Usage
- Example: Enabling Cisco Cloud Services on Secure Web Appliance
- Example: Disabling Cisco Cloud Services on Secure Web Appliance

- Example: Registering Secure Web Appliance with Cisco Cloud Services Portal
- Example: Automatically Registering Secure Web Appliance with Cisco Cloud Services Portal
- Example: Deregistering Secure Web Appliance from Cisco Cloud Services Portal
- Example: Choosing Cisco Secure Cloud Server to connect Secure Web Appliance to Cisco Cloud Services Portal
- Example: Download a Certificate and Key
- Example: Client Certificate updateconfig

Description

The **cloudserviceconfig** command is used to:

- Enable the Cisco Cloud Services portal on Secure Web Appliance.
- Disable the Cisco Cloud Services portal on Secure Web Appliance.
- Register your Secure Web Appliance with the Cisco Cloud Services portal.
- Automatically register your Secure Web Appliance with the Cisco Cloud Services portal.
- Deregister your Secure Web Appliance from the Cisco Cloud Services portal.
- Choose the Cisco Secure Cloud server to connect Secure Web Appliance to the Cisco Cloud Services portal.
- Download the Cisco Cloud Services Certificate and key from the Cisco Talos Intelligence Services portal.
- Uploading the Client Certificate and the key.

Note This command is applicable only in Smart Licensing mode.

Usage

- **Commit**: This command does not require a 'commit.
- **Batch Command**: This command supports a batch format.

Example: Enabling Cisco Cloud Services on Secure Web Appliance

In the following example, you can use the `cloudserviceconfig` > `enable` sub command to enable Cisco Cloud Services on Secure Web Appliance

```
example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
```

```
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMTexample.com >
```

Example: Disabling Cisco Cloud Services on Secure Web Appliance

In the following example, you can use the `cloudserviceconfig > disable` sub command to disable Cisco Cloud Services on Secure Web Appliance.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
example.com >
```

Example: Registering Secure Web Appliance with Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > register` sub command to register the Secure Web Appliance with the Cisco Cloud Services portal.



Note You can only use this sub command if Smart Software licensing is not enabled, and Secure Web Appliance is not registered with Cisco Smart Software Manager

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> register

Enter a registration token key to register your appliance
[]> c51fa32bd9a31227eaab50dea873062c

Registering
The Web Security appliance is successfully registered with the Cisco Cloud Service portal.
example.com >
```

Example: Automatically Registering Secure Web Appliance with Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > autoregister` command to register the Secure Web Appliance with the Cisco cloud Service Portal.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically
using SL Payload.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> autoregister

The Web Security appliance successfully auto-registered with the Cisco Cloud Service portal.
```

Example: Deregistering Secure Web Appliance from Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > deregister` sub command to deregister the Secure Web Appliance from the Cisco Cloud Services portal.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> y

The Web Security appliance successfully deregistered from the Cisco Cloud Service portal.
example.com >
```

Example: Choosing Cisco Secure Cloud Server to connect Secure Web Appliance to Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > settrs` sub command to choose the required Cisco Secure Cloud Server to connect the Secure Web Appliance to the Cisco Cloud Services portal.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

Example: Downloading Cisco Cloud Services Certificate and Key from Cisco Talos Intelligence Services Portal

In the following example, you can use the `cloudserviceconfig` > `fetchcertificate` sub command to download the Cisco Cloud Services certificate and key from the Cisco Talos Intelligence Services portal..

Note You can only use this sub command when the existing Cisco Cloud Services certificate is expired and if you have registered the Secure Web Appliance with Cisco Smart Software Manager.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:


Choose the operation you want to perform:
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> fetchcertificate

Successfully downloaded the Cisco Talos certificate and key
example.com >
```

Example: Client Certificate updateconfig

In the following example, you can use the `Updateconfig` > `clientcertificate` sub command to upload the certificate and the key.

```
example.com > updateconfig

Service (images):                Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters           Cisco Servers
Support Request updates          Cisco Servers
Timezone rules                   Cisco Servers
How-Tos Updates                  Cisco Servers
HTTPS Proxy Certificate Lists    Cisco Servers
Cisco AsyncOS upgrades           Cisco Servers
Smart License Agent Updates      Cisco Servers

Service (list):                  Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters           Cisco Servers
Support Request updates          Cisco Servers
Timezone rules                   Cisco Servers
How-Tos Updates                  Cisco Servers
HTTPS Proxy Certificate Lists    Cisco Servers
Cisco AsyncOS upgrades           Cisco Servers
Smart License Agent Updates      Cisco Servers

Update interval for Web Reputation and Categorization: 5m
Update interval for all other services: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
    The following services will use this routing table:
    - Web Reputation Filters
    - Support Request updates
    - Timezone rules
    - How-Tos Updates
    - HTTPS Proxy Certificate Lists
    - Cisco AsyncOS upgrades
    - Smart License Agent Updates
```

```
Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> clientcertificate

Current Cisco certificate is valid for 179 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> y

Paste the certificate.
Press CTRL-D on a blank line when done.
^D
```

Paste your certificate and private key details. Certificate and key are stored successfully.

Smart Software Licensing Key Points for AsyncOS 14.0 and later

- When smart software licensing is enabled and registered, Cisco Cloud Service will be enabled and registered automatically.
- If the Cisco Cloud Services certificate is expired, you can now download a new certificate from the Cisco Talos Intelligence Services portal using the `cloudserviceconfig` > `fetchcertificate` sub command in the CLI.
- You cannot perform Cisco Cloud Service auto registration when smart license is in evaluation mode.

Virtual Appliance License

The Cisco Web Security Virtual appliance requires an additional license to run the virtual appliance on a host.

For more information about virtual appliance licensing, see the *Cisco Content Security Virtual Appliance Installation Guide* , available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Note You cannot open a Technical Support tunnel before installing the virtual appliance license.

After the license expires, the appliance will continue to serve as a web proxy without security services for180 days. Security service updates do not occur during this period.

You can configure the appliance so you receive alerts about license expiration.

Related Topics

- Managing Alerts, on page 35

Installing a Virtual Appliance License

See the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Enabling Remote Power Cycling

Before you begin

- Cable the dedicated Remote Power Cycle (RPC) port directly to a secure network. For information, see the hardware guide for your appliance model. For the location of this document, see Documentation Set.
- Ensure that the appliance is accessible remotely; for example, open any necessary ports through the firewall.
- This feature requires a unique IPv4 address for the dedicated Remote Power Cycle interface. This interface is configurable only via the procedure described in this section; it cannot be configured using the ipconfig command.
- In order to cycle appliance power, you will need a third-party tool that can manage devices that support the Intelligent Platform Management Interface (IPMI) version 2.0. Ensure that you are prepared to use such a tool.
- For more information about accessing the command-line interface, see Command Line Interface

After you configure RPC and commit the changes, wait for 10 to 15 minutes before sending the calls to RPC. Secure Web Appliance initializes the RCP services during this wait time.

The ability to remotely reset the power for the appliance chassis is available on x80, x90, and x95 series hardware.

If you want to be able to remotely reset appliance power, you must enable and configure this functionality in advance, using the procedure described in this section.

Procedure

Step 1 Use SSH or the serial console port to access the command-line interface.

Step 2 Sign in using an account with Administrator access.

Step 3 Enter the following commands:

```
remotepower

setup
```

Step 4 Follow the prompts to specify the following:

- The dedicated IP address for this feature, plus netmask and gateway.
- The username and passphrase required to execute the power-cycle command.

  These credentials are independent of other credentials used to access your appliance.

Step 5 Enter `commit` to save your changes.

Step 6 Test your configuration to be sure that you can remotely manage appliance power.

Step 7 Ensure that the credentials that you entered will be available to you in the indefinite future. For example, store this information in a safe place and ensure that administrators who may need to perform this task have access to the required credentials.

What to do next

Related Topics

- Hardware Appliances: Remotely Resetting Appliance Power

Administering User Accounts

The following types of users can log into the appliance to manage it:

- **Local users.** You can define users locally on the appliance itself.
- **Users defined in an external system.** You can configure the appliance to connect to an external LDAP or RADIUS server to authenticate users logging into the appliance.

Note Any user you define can log into the appliance using any method, such as logging into the web interface or using SSH.

Related Topics

- Managing Local User Accounts, on page 26
- RADIUS User Authentication, on page 29
- Configuring External Authentication through an LDAP Server

Managing Local User Accounts

You can define any number of users locally on the Secure Web Appliance.

The default system admin account has all administrative privileges. You can change the admin account passphrase, but you cannot edit or delete this account.

Note If you have lost the admin user passphrase, contact your Cisco support provider. For more details, see Reset Your Administrator Password and Unlock the Administrator User Account.

Adding Local User Accounts

Before you begin

Define the passphrase requirements that all user accounts must follow. See Setting Passphrase Requirements for Administrative Users , on page 31.

Procedure

Step 1 Choose **System Administration > Users.**

Step 2 Click **Add User**

Step 3 Enter a username, noting the following rules:

- Usernames can contain lowercase letters, numbers, and the dash (-) character, but cannot begin with a dash.
- Usernames cannot greater than 16 characters.
- Usernames cannot be special names that are reserved by the system, such as “operator” or “root.”
- If you also use external authentication, usernames should not duplicate externally-authenticated usernames.

Step 4 Enter a full name for the user.

Step 5 Select a user type.

User Type	Description
Administrator	Allows full access to all system configuration settings. However, the `upgradecheck` and `upgradeinstall` CLI commands can be issued only from the system defined “admin” account.
Operator	Restricts users from creating, editing, or removing user accounts. The operators group also restricts the use of the following CLI commands: • `resetconfig` • `upgradecheck` • `upgradeinstall` The operators group restricts the use of System Setup Wizard as well.
Read-Only Operator	User accounts with this role: • Can view configuration information. • Can make and submit changes to see how to configure a feature, but they cannot commit them. • Cannot make any other changes to the appliance, such as clearing the cache or saving files. • Cannot access the file system, FTP, or SCP.
Guest	The guests group users can only view system status information, including reporting and tracking.

Step 6 Enter or generate a passphrase.

Step 7 Submit and commit your changes.

Deleting User Accounts

Procedure

Step 1 Choose **System Administration > Users**.

Step 2 Click the trash can icon corresponding to the listed user name and confirm when prompted.

Step 3 Submit and commit your changes.

Editing User Accounts

Procedure

Step 1 Choose **System Administration > Users**.

Step 2 Click the user name.

Step 3 Make changes to the user on the Edit User page as required.

Step 4 Submit and commit your changes.

Changing Passphrases

To change the passphrase of the account currently logged in, select **Options > Change Passphrase** from the top right-hand side of the window.

For other accounts, edit the account and change the passphrase in the Local User Settings page.

Related Topics

- Editing User Accounts, on page 28
- Setting Passphrase Requirements for Administrative Users , on page 31

Configuring Restrictive User Account and Passphrase Settings

You can define user account and passphrase restrictions to enforce organizational passphrase policies. The user account and passphrase restrictions apply to local users defined on the Cisco appliance. You can configure the following settings:

- **User account locking.**You can define how many failed login attempts cause the user to be locked out of the account. You can set the number of user login attempts from 1 to 60. The default value is 5.
- **Passphrase lifetime rules.**You can define how long a passphrase can exist before the user is required to change the passphrase after logging in.
- **Passphrase rules.**You can define what kinds of passphrases users can choose, such as which characters are optional or mandatory.

Note From AsyncOS version 14.0 onwards, the passphrase rules are enabled by default except for **Reject 3 or more repetitive or sequential characters in passphrases** and **List of words to disallow in passphrases** rules.

- **Passphrase strength.** You can display a passphrase-strength indicator when an administrative user enters a new passphrase.

  For more information, see Setting Passphrase Requirements for Administrative Users.

You define user account and passphrase restrictions on the System Administration > Users page in the Local User Account & Passphrase Settings section.

RADIUS User Authentication

The Secure Web Appliance can use a RADIUS directory service to authenticate users that log in to the appliance using HTTP, HTTPS, SSH, and FTP. You can configure the appliance to contact multiple external servers for authentication, using either PAP or CHAP authentication. You can map groups of external users to different Secure Web Appliance user role types.

Sequence of Events For Radius Authentication

When external authentication is enabled and a user logs into the Secure Web Appliance, the appliance:

1. Determines if the user is the system-defined “admin” account.
2. If not, checks the first configured external server to determine if the user is defined there.
3. If the appliance cannot connect to the first external server, it checks the next external server in the list.
4. If the appliance cannot connect to any external server, it tries to authenticate the user as a local user defined on the Secure Web Appliance.
5. If the user does not exist on any external server or on the appliance, or if the user enters the wrong passphrase, access to the appliance is denied.

Enabling External Authentication Using RADIUS

Procedure

Step 1 On the **System Administration > Users** page, click **Enable External Authentication**.

Step 2 Choose **RADIUS** as the Authentication Type.

Step 3 Enter the host name, port number, and Shared Secret passphrase for the RADIUS server. Default port is `1812`.

Step 4 Enter the number of seconds the appliance is to wait for a response from the server before timing out.

Step 5 Choose the authentication protocol used by the RADIUS server.

Step 6 (Optional) Click **Add Row** to add another RADIUS server. Repeat **Steps 1 – 5** for each RADIUS server.

Note
You can add up to ten RADIUS servers.

Step 7 In the **External Authentication Cache Timeout** field, enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to re-authenticate. Default is zero.

Note
If the RADIUS server uses one-time passphrases, for example passphrases created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.

Step 8 Configure Group Mapping—Select whether to map all externally authenticated users to the Administrator role or to different appliance-user role types.

Setting	Description
Map externally authenticated users to multiple local roles.	Enter a group name as defined in the RADIUS CLASS attribute, and choose an appliance Role type. You can add more role mappings by clicking Add Row. AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements: • three-character minimum • 253-character maximum • no colons, commas, or newline characters • one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.) For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role. These are the appliance roles ordered from most restrictive to least restrictive: • Administrator • Operator • Read-Only Operator • Guest
Map all externally authenticated users to the Administrator role.	AsyncOS assigns all RADIUS users to the Administrator role.

Step 9 Submit and commit your changes.

What to do next

Related Topics

- External Authentication
- Adding Local User Accounts, on page 26.

Defining User Preferences

Preference settings, such as reporting display formats, are stored for each user and are the same regardless from which client machine the user logs into the appliance.

Procedure

Step 1 Choose **Options > Preferences**.

Step 2 On the User Preferences page, click **Edit Preferences**.

Step 3 Configure the preference settings as required.

Preference Setting	Description
Language Display	The language AsyncOS for Web uses in the web interface and CLI.
Landing Page	The page that displays when the user logs into the appliance.
Reporting Time Range Displayed (default)	The default time range that displays for reports on the Reporting tab.
Number of Reporting Rows Displayed	The number of rows of data shown for each report by default.

Step 4 Submit and commit your changes.

Configuring Administrator Settings

Setting Passphrase Requirements for Administrative Users

To set passphrase requirements for locally-defined administrative users of the appliance:

Procedure

Step 1 Select **System Administration > Users**.

Step 2 In the **Passphrase Settings** section, click **Edit Settings**.

Step 3 Choose options:

Option	Description
List of words to disallow in passphrases	Create a .txt file with each forbidden word on a separate line, then select the file to upload it. Subsequent uploads overwrite previous uploads.

Option	Description
Passphrase Strength	You can display a passphrase-strength indicator when an administrative user enters a new passphrase. This setting does not enforce creation of strong passphrases, it merely shows how easy it is to guess the entered passphrase. Select the roles for which you wish to display the indicator. Then, for each selected role, enter a number greater than zero. A larger number means that a passphrase that registers as strong is more difficult to achieve. This setting has no maximum value, but a very high number makes it effectively impossible to enter a passphrase that evaluates as "good." Experiment to see what number best meets your requirements. Passphrase strength is measured on a logarithmic scale. Evaluation is based on the U.S. National Institute of Standards and Technology rules of entropy as defined in NIST SP 800-63, Troubleshooting topic. Generally, stronger passphrases: • Are longer • Include upper case, lower case, numeric, and special characters • Do not include words in any dictionary in any language. To enforce passphrases with these characteristics, use the other settings on this page.

Step 4 Submit and commit your changes.

Additional Security Settings for Accessing the Appliance

You can use the CLI command `adminaccessconfig` to configure the Secure Web Appliance to have stricter access requirements for administrators logging into the appliance.

Command	Description
`adminaccessconfig > banner`	Configures the appliance to display any text you specify when an administrator tries to log in. The custom log-in banner appears when an administrator accesses the appliance through any interface; for example, via the Web UI, CLI, or FTP. You can load the custom text either by pasting it into the CLI prompt, or by copying it from a text file located on the Secure Web Appliance. To upload the text from a file, you must first transfer the file to the configuration directory on the appliance using FTP.
`adminaccessconfig > welcome`	This is a post-log-in banner, displayed after successful administrator log-in. This text is added to the appliance configuration by the same means as the log-in `adminaccessconfig > banner` text.

Command	Description
`adminaccessconfig > ipaccess`	Controls from which IP addresses administrators access the Secure Web Appliance. Administrators can access the appliance from any machine, or from machines with an IP address from a list you specify. When restricting access to an allow list, you can specify IP addresses, subnets, or CIDR addresses. By default, when you list the addresses that can access the appliance, the IP address of your current machine is listed as the first address in the allow list. You cannot delete the IP address of your current machine from the allow list. This information also can be provided using the Web UI; see User Network Access, on page 33.
`adminaccessconfig > csrf`	Enable/disable Web UI cross-site request forgery protection, used to identify and protect against malicious or spoofed requests. For best security, it is recommended that CSRF protection be enabled.
`adminaccessconfig > hostheader`	Configure use of host header in HTTP requests. By default, the Web UI responds with the host header sent by the Web client in an HTTP request. For increased security, you can configure the Web UI to respond with only the appliance-specific host name; that is, the appliance's configured name (for example, `wsa_04.local`).
`adminaccessconfig > timeout`	Provide an inactivity time-out interval; that is, the number of minutes users can be inactive before being logged out. This value can be between five and 1440 minutes (24 hours); the default value is 30 minutes. This information also can be provided using the Web UI; see User Network Access, on page 33.
`adminaccessconfig > how-tos`	Enable walkthroughs that assist you in accomplishing specific configuration tasks.
`adminaccessconfig > strictssl`	Configures the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption). When you configure the appliance to require stronger SSL ciphers, the change only applies to administrators accessing the appliance using HTTPS to manage the appliance. It does not apply to other network traffic connected to the Web Proxy using HTTPS.
`adminaccessconfig > loginhistory`	Configure the number of days for which the login history is retained.
`adminaccessconfig > maxsessions`	Configure the maximum number of concurrent login sessions (CLI and web interface).

User Network Access

You can specify how long a user can be logged into the appliance before AsyncOS logs the user out due to inactivity. You also can specify the type of user connections allowed.

The session timeout applies to all users, including administrators, logged into either the Web UI or the CLI. When AsyncOS logs a user out, the user is redirected to the appliance log-in page.



Note You also can use the CLI `adminaccessconfig` > `timeout` to set this time-out value.

Procedure

Step 1 Choose **System Administration** > **Network Access**.

Step 2 Click **Edit Settings**.

Step 3 In the **Session Inactivity Timeout** field, enter the number of minutes users can be inactive before being logged out.

You can define a time-out interval between five and 1440 minutes (24 hours); the default value is 30 minutes.

Step 4 In the **User Access** section, you control users' system access: choose either **Allow Any Connection** or **Only Allow Specific Connections**.

If you choose **Only Allow Specific Connections**, define the specific connections as IP addresses, IP ranges, or CIDR ranges. Along with the client IP address, the appliance IP address is automatically added in the **User Access** section.

Step 5 Submit and commit your changes.

Resetting the Administrator Passphrase

Before you begin

- If you do not know the passphrase for the admin account, contact your customer support provider to reset the passphrase.
- Understand that changes to the passphrase take effect immediately and do not require you to commit the change.

Any administrator-level user can change the passphrase for the "admin" user.

Procedure

Step 1 Select **Management Appliance** > **System Administration** > **Users**.

Step 2 Click the **admin** link in the Users list.

Step 3 Select **Change the passphrase**.

Step 4 Generate or enter the new passphrase.

Configuring the Return Address for Generated Messages

You can configure the return address for mail generated by AsyncOS for reports.

Procedure

Step 1 Choose **System Administration** > **Return Addresses**.

Step 2 Click **Edit Settings**.

Step 3 Enter the display name, user name, and domain name.

Step 4 Submit and commit your changes.

Managing Alerts

Alerts are email notifications containing information about events occurring on the Cisco Secure Web Appliance. These events can be of varying levels of importance (or severity) from minor (Informational) to major (Critical) and pertain generally to a specific component or feature on the appliance.



Note To receive alerts and email notifications, you must configure the SMTP relay host that the appliance uses to send the email messages.

Alert Classifications and Severities

The information contained in an alert is determined by an alert classification and a severity. You can specify which alert classifications, at which severity, are sent to any alert recipient.

Alert Classifications

AsyncOS sends the following types of alert:

- System
- Hardware
- Updater
- Web Proxy
- Anti-Malware
- AMP
- L4 Traffic Monitor
- External URL Categories
- Policy Expiration

Alert Severities

Alerts can be sent for the following severities:

- **Critical**: Requires immediate attention.

- **Warning**: Problem or error requiring further monitoring and potentially immediate attention.
- **Information**: Information generated in the routine functioning of this device.

Managing Alert Recipients



Note If you enabled AutoSupport during System Setup, the email address you specified will receive alerts for all severities and classes by default. You can change this configuration at any time.

Adding and Editing Alert Recipients

Procedure

Step 1 Choose **System Administration** > **Alerts**.
Step 2 Click on a recipient in the Alert Recipients list to edit it, or click **Add Recipient** to add a new recipient.
Step 3 Add or edit the recipient's email address. You can enter multiple addresses, separated by commas.
Step 4 Select which alert severities to receive for each alert type.
Step 5 Submit and commit your changes.

Deleting Alert Recipients

Procedure

Step 1 Choose **System Administration** > **Alerts**.
Step 2 Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing and confirm.
Step 3 Commit your changes.

Configuring Alert Settings

Alert settings are global settings, meaning that they affect how all of the alerts behave.

Procedure

Step 1 Choose **System Administration** > **Alerts**.
Step 2 Click **Edit Settings**.
Step 3 Configure the alert settings as required.

Option	Description
From Address to Use When Sending Alerts	The RFC 2822 compliant “Header From:” address to use when sending alerts. An option is provided to automatically generate an address based on the system hostname (“alert@<hostname>”)
Wait Before Sending a Duplicate Alert	Specifies the time interval for duplicate alerts. There are two settings: **Initial Number of Seconds to Wait Before Sending a Duplicate Alert**. If you set this value to 0, duplicate alert summaries are not sent and instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5 second wait would have alerts sent at 5 seconds, 15, seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, etc. **Maximum Number of Seconds to Wait Before Sending a Duplicate Alert**. You can set a cap on the number of seconds to wait between intervals via the maximum number of seconds to wait before sending a duplicate alert field. For example, if you set the initial value to 5 seconds, and the maximum value to 60 seconds, alerts would be sent at 5 seconds, 15 seconds, 35 seconds, 60 seconds, 120 seconds, etc

Note
From AsyncOS 12.0, Cisco AutoSupport option is removed from the alert settings. You can only enable or disable AutoSupport fuctionality using the **alertconfig** CLI.

Step 4 Submit and commit your changes.

Alert Listing

The following sections list alerts by classification. The table in each section includes the alert name (internally used descriptor), actual text of the alert, description, severity (critical, information, or warning) and the parameters (if any) included in the text of the message.

Hardware Alerts

The following table contains a list of the various hardware alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A RAID-event has occurred: $error	Warning	**$error:** Text of the RAID error.

System Alerts

The following table contains a list of the various system alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
Startup script $name exited with error: $message	Critical.	**$name:** Name of the script. **$message:** Error message text.
System halt failed: $exit_status: $output',	Critical.	**$exit_status:** Exit code of the command. **$output:** Output from the command.
System reboot failed: $exit_status: $output	Critical.	**$exit_status:** Exit code of the command. **$output:** Output from the command.
Process $name listed $dependency as a dependency, but it does not exist.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Process $name listed itself as a dependency.	Critical.	**$name:** Name of the process.
Process $name listed $dependency as a dependency multiple times.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Dependency cycle detected: $cycle.	Critical.	**$cycle:** The list of process names involved in the cycle.
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	Warning.	**$error:** The error message associated with the exception.
There is an error with “$name”.	Critical.	**$name:** Name of the process that generated a core file.
An application fault occurred: “$error”	Critical.	**$error:** Text of the error, typically a traceback.

Message	Alert Severity	Parameters
Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts. User $username is locked after X consecutive login failures. Last login attempt was from $ip.	Information.	**$appliance**: Identifier of the specific Secure Web Appliance. **$username**: Identifier of the specific user account. **$ip**: - IP address from which the login attempt occurred.
Tech support: Service tunnel has been enabled, port $port	Information.	**$port:** Port number used for the service tunnel.
Tech support: Service tunnel has been disabled.	Information.	Not applicable.
• The host at $ip has been added to the blocked list because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh allowed list. • The host at $ip has been removed from the blocked list.	Warning.	**$ip** - IP address from which a login attempt occurred. **Description:** IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blocked list if more than 10 failed attempts occur within two minutes. When a user logs in successfully from the same IP address, that IP address is added to the allowed list. Addresses on the allowed list are allowed access even if they are also on the blocked list. Entries are automatically removed from the blocked list after about a day.

Note System alerts include Feature Key Alerts, Logging Alerts, and Reporting Alerts. You will receive these alerts after configuring them as part of the system alerts.

Feature Key Alerts

The following table contains a list of the various feature key alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A "$feature" key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information.	**$feature:** Name of the feature.

Message	Alert Severity	Parameters
Your "$feature" evaluation key has expired. Please contact your authorized sales representative.	Warning.	**$feature:** Name of the feature.
Your "$feature" evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	Warning.	**$feature:** Name of the feature. **$days:** The number of days that will pass before the feature key will expire.

Logging Alerts

The following table contains a list of the various logging alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
$error.	Information.	**$error:** The traceback string of the error.
Log Error: Subscription $name: Log partition is full.	Critical.	**$name:** Log subscription name.
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$reason:** Text describing the connect error
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$reason:** Text describing what went wrong.
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$port:** Port number on the remote host. **$reason:** Text describing what went wrong.
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server. **$error:** Text of the error message.

Message	Alert Severity	Parameters
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server. **$error:** Text of the error message.
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	Critical.	**$name:** Log subscription name. **$timeout:** Timeout in seconds. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server.
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server.
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	Information.	**$name:** Log subscription name. **$max_num_files:** Maximum number of files allowed per log subscription. **$files_removed:** List of files that were removed.

Reporting Alerts

The following table contains a list of the various reporting alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	Critical.	Not applicable.
The reporting system is now able to handle new data.	Information.	Not applicable.
A failure occurred while building periodic report '$report_title'. This subscription should be examined and deleted if its configuration details are no longer valid.	Critical.	**$report_title:** Title of the report.

Message	Alert Severity	Parameters
A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	Critical.	**$report_title:** Title of the report.
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning.	**$threshold:** Threshold value.
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent.	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file.
Counter group "$counter_group" does not exist.	Critical.	**$counter_group:** Name of the counter_group.
PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent.	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file.
PERIODIC REPORTS: Errors were encountered while processing the domain specification file '$file_name' for the periodic report '$report_title'. Any line which has any reported problem had no report sent. $error_text	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file. **$error_text:** List of errors encountered.
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning.	**$threshold:** Threshold value.

Message	Alert Severity	Parameters
The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	Critical.	**$err_msg:** Error message text.

Updater Alerts

The following table contains a list of the various updater alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning.	**$app:** Secure Web Appliance security service name. **$attempts:** Number of attempts tried.
The updater has been unable to communicate with the update server for at least $threshold.	Warning.	**$threshold:** Threshold value time.
Unknown error occurred: $traceback.	Critical.	**$traceback:** Traceback information.
Certificate Revoke: OCSP validation failed for the UPDATER Server Certificate ($host:$port). Ensure the certificate is valid.	Critical	**$host:** The hostname of the UPDATER Server. **$port:** The port of the UPDATER Server.

Anti-Malware Alerts

For information about alerts related to Secure Endpoint, see Ensuring That You Receive Alerts About Secure Endpoint Issues.

Policy Expiration Alerts

The following table contains a list of the various Policy Expiration alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
'$PolicyType': '$GroupName' has been disbaled due to expiry configuration.	Information	**$PolicyType:** Access policy / decryption policy based on the web policy type. **$GroupName:**Policy group name.

Message	Alert Severity	Parameters
'$PolicyType' : '$GroupName' will expire in days : 3.	Information	**$PolicyType:** Access policy / decryption policy based on the web policy type. **$GroupName:** Policy group name.

FIPS Compliance

Federal Information Processing Standards (FIPS) specify requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. FIPS help ensure compliance with federal security and data privacy requirements. FIPS, developed by the National Institute for Standards and Technology (NIST), are for use when no voluntary standards exist to meet federal requirements.

The Secure Web Appliance achieves FIPS 140-2 compliance in FIPS mode using Cisco Common Cryptographic Module (C3M). By default, FIPS mode is disabled.

Note **From the AsyncOS 15.0 release onwards, the Federal Information Processing Standards (FIPS) mode is not supported.**

Related Topics

- FIPS Mode Problems

FIPS Certificate Requirements

FIPS mode requires that all enabled encryption services on the Secure Web Appliance use a FIPS-compliant certificate. This applies to the following encryption services:

- HTTPS Proxy
- Authentication
- Identity Provider for SaaS
- Appliance Management HTTPS Service
- Secure ICAP External DLP Configuration
- Identity Services Engine
- SSL Configuration
- SSH Configuration

Note The Appliance Management HTTPS Service must be configured with a FIPS Complaint certificate before FIPS mode can be enabled. The other encryption services need not be enabled.

A FIPS-compliant certificate must meet these requirements:

Certificate	Algorithm	Signature Algorithm	Notes
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	Cisco recommends a bit key size of 1024 for best decryption performance and sufficient security. A larger bit size will increase security, but impact decryption performance.

FIPS Certificate Validation

When you enable FIPS mode, the appliance performs the following certificate checks:

- All certificates uploaded to the Secure Web Appliance, whether by means of the UI or the `certconfig` CLI command, are validated to comply strictly with CC standards. Any certificate without a proper trust path in the Secure Web Appliance's trust store cannot be uploaded.
- Certificate Signature with a trusted path validation; Certificate/Public Key tampering with `basicConstrains` and `CAFlag` set validated for all signer certificates.
- OCSP validation is available to validate a certificate against a revocation list. This is configurable using the `certconfig` CLI command.

Note A new subcommand `OCSPVALIDATION_FOR_SERVER_CERT` is added under the main CLI command `certconfig`. Using the new subcommand you can enable the OCSP validation for LDAP and Updater server certificates. If the certificate validation is enabled, you will receive an alert if the certificates involved in communication are revoked.

See also Strict Certificate Validation, on page 49.

Enabling or Disabling FIPS Mode

Before you begin

- Make a back-up copy of the appliance configuration; see Saving the Appliance Configuration File, on page 2
- Ensure the certificates to be used in FIPS mode use FIPS 140-2 approved public key algorithms (see FIPS Certificate Requirements, on page 44).

Note

- Changing the FIPS mode initiates a reboot of the appliance.
- When you disable FIPS mode, the SSL and SSH settings—which were automatically made FIPS-compliant when FIPS mode was enabled—are not reset to their default values. You must explicitly change these settings if you wish to allow a client using weaker SSH/SSL settings to connect. See SSL Configuration , on page 47 for additional information.

Procedure

Step 1 Choose **System Administration > FIPS Mode**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable FIPS Compliance** to enable FIPS compliance.

When you check Enable FIPS Compliance, the **Enable encryption of Critical Sensitive Parameters (CSP)** check box is enabled.

Step 4 Check **Enable encryption of Critical Sensitive Parameters (CSP)** to enable encryption of configuration data such as passwords, authentication information, certificates, shared keys, and so on.

Step 5 Click **Submit**.

Step 6 Click **Continue** to allow the appliance to reboot.

System Date and Time Management

- Setting the Time Zone, on page 46
- Synchronizing the System Clock with an NTP Server , on page 46

Setting the Time Zone

Procedure

Step 1 Choose **System Administration > Time Zone**.

Step 2 Click **Edit Settings**.

Step 3 Select your region, country, and time zone or select the GMT offset.

Step 4 Submit and commit the changes.

Synchronizing the System Clock with an NTP Server

Cisco recommends that you set your Secure Web Appliance to track the current date and time by querying a Network Time Protocol (NTP) server, not by manually setting the time on the appliance. This is especially true if your appliance integrates with other devices. All integrated devices should use the same NTP server.

Procedure

Step 1 Choose **System Administration > Time Settings**.

Step 2 Click **Edit Settings**.

Step 3 Select **Use Network Time Protocol** as the Time Keeping Method.

Step 4 Enter the fully qualified hostname or IP address of the NTP server, clicking **Add Row** as needed to add servers.

Step 5 (Optional) Choose the routing table associated with an appliance network interface type, either Management or Data, to use for NTP queries. This is the IP address from which NTP queries should originate.

Note
This option is only editable if the appliance is using split routing for data and management traffic.

Step 6 Submit and commit your changes.

SSL Configuration

For enhanced security, you can enable and disable SSL v3 and various versions of TLS for several services. Disabling SSL v3 for all services is recommended for best security. By default, all versions of TLS are enabled, and SSL is disabled.

Note You also can use the `sslconfig` CLI command to enable or disable these features. See Secure Web Appliance CLI Commands.

Note Restart the application when you modify or change the SSL configuration that results in disabling the TLS ciphers.

Procedure

Step 1 Choose **System Administration > SSL Configuration**.

Step 2 Click **Edit Settings**.

Step 3 Check the corresponding boxes to enable SSL v3 and TLS v1.x for these services:

- **Appliance Management Web User Interface** – Changing this setting will disconnect all active user connections.

  Note
  - For protocol versions, TLSv1.2 is enabled by default. You can now select TLSv1.3 by checking the TLSv1.3 checkbox or using the `sslconfig` command. Fore more details on the command, see Secure Web Appliance CLI Commands. If you are selecting TLSv1.3 as the protocol versions, it is mandatory to provide ciphers to use it.

- **Proxy Services** – Includes HTTPS Proxy and Credential Encryption for Secure Client. This section also includes:
  - **Cipher(s) to Use** – You can enter additional cipher suites to be used with Proxy Services communications. Use colons (:) to separate the suites. To prevent use of a particular cipher, add an exclamation point (!) to the front of that string. For example, `!EXP-DHE-RSA-DES-CBC-SHA`.

    Be sure to enter only suites appropriate to the TLS/SSL versions you have checked. Refer to https://www.openssl.org/docs/manmaster/man1/ciphers.html for additional information, and cipher lists.

    The appliance supports TLSv1.3 version. Cipher `TLS_AES_256_GCM_SHA384` is added to the default cipher list. By default, TLSv1.3 is enabled on the appliance.

In AsyncOS version 14.0, ciphers `TLS_AES_128_GCM_SHA256` and `TLS_CHACHA20_POLY1305_SHA256` are added to the default cipher list.

The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH`.

The default cipher for AsyncOS versions 9.1 - 11.8 is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

In this case, the default cipher may change based on your ECDHE cipher selections.

The default cipher for AsyncOS versions 12.0 and later is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

Note
Update the default cipher suite while upgrading to a newer AsyncOS version. The ciphers suites are not automatically updated. When you upgrade from an earlier version to AsyncOS 12.0 and later, Cisco recommends updating the cipher suite to:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

- **Disable TLS Compression (Recommended)** – You can check this box to disable TLS compression; this is recommended for best security.

- **Secure LDAP Services** – Includes Authentication, External Authentication and Secure Mobility.
- **Secure ICAP Services (External DLP)** – Select the protocol(s) used to secure ICAP communications between the appliance and external DLP (data loss prevention) servers. See Configuring External DLP Servers for more information.
- **Update Service** – Select the protocol(s) used for communications between the appliance and available update servers. See AsyncOS for Web Upgrades and Updates, on page 53 for more information about update services.

Note
Cisco's Update servers do not support SSL v3, therefore TLS 1.0 or above must be enabled for the Cisco Update service. However, SSL v3 can still be used with a local update server, if it is so configured—you must determine which versions of SSL/TLS are supported on that server.

Step 4 Click **Submit**.

Certificate Management

The appliance uses digital certificates to establish, confirm and secure a variety of connections. The Certificate Management page lets you view and update current certificate lists, manage trusted root certificates, and view blocked certificates.

Note The Certificate Management page takes a long time to load and results in a timed-out error when the appliance is not connected to the internet. In addition, the "Failed to fetch manifest" network error is displayed in the Certificate Updates list after loading the certificate.

Related Topics

- About Certificates and Keys, on page 49
- Certificate Updates, on page 50
- Managing Trusted Root Certificates, on page 50
- Viewing Blocked Certificates, on page 51

Strict Certificate Validation

With the release of the FIPS-mode updates in AsyncOS 10.5, all presented certificates are validated strictly to comply with Common Criteria (CC) standards before uploading, and OCSP validation is available to validate certificates against a revocation list.

You must ensure that proper, valid certificates are uploaded to the Secure Web Appliance, and that valid, secure certificates are configured on all related servers to facilitate smooth SSL handshakes with those servers.

Strict certificate validation is applied for the following certificate uploads:

- HTTPS Proxy (Security Services > HTTPS Proxy)
- File Analysis Server (Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority)
- Trusted Root Certificates (Network > Certificate Management)
- Global Authentication Settings (Network > Authentication > Global Authentication Settings)
- Identity Provider for SaaS (Network > Identity Provider for SaaS)
- Identity Services Engine (Network > Identity Services Engine)
- External DLP Servers (Network > External DLP Servers)
- LDAP & Secure LDAP (Network > Authentication > Realm)

See also FIPS Compliance, on page 44.

About Certificates and Keys

When a browser prompts its user to authenticate, the browser sends the authentication credentials to the Web Proxy using a secure HTTPS connection. By default, the Secure Web Appliance uses the “Cisco Web Security Appliance Demo Certificate” that comes with it to create an HTTPS connection with the client. Most browsers

will warn users that the certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a certificate and key pair that your applications recognize automatically.

Related Topics

- Uploading or Generating a Certificate and Key, on page 51
- Certificate Signing Requests, on page 52
- Intermediate Certificates, on page 52

Managing Trusted Root Certificates

The Secure Web Appliance ships with and maintains a list of trusted root certificates. Web sites with trusted certificates do not require decryption.

You can manage the trusted certificate list, adding certificates to it and functionally removing certificates from it. While the Secure Web Appliance does not delete certificates from the primary list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

To add, override or download a trusted root certificate:

Procedure

Step 1 Choose **Network** > **Certificate Management**.

Step 2 Click **Manage Trusted Root Certificates** on the Certificate Management page.

Step 3 To add a custom trusted root certificate with a signing authority not on the Cisco-recognized list:

Click **Import** and then browse to, select, and **Submit** the certificate file.

Step 4 To override the trust for one or more Cisco-recognized certificates:

a) Check the **Override Trust** checkbox for each entry you wish to override.
b) Click **Submit**.

Step 5 To download a copy of a particular certificate:

a) Click the name of the certificate in the Cisco Trusted Root Certificate List to expand that entry.
b) Click **Download Certificate**.

Certificate Updates

The Updates section lists version and last-updated information for the Cisco trusted-root-certificate and blocked list bundles on the appliance. These bundles are updated periodically.

Procedure

Click **Update Now** on the Certificate Management page to update all bundles for which updates are available.

Viewing Blocked Certificates

To view a list of certificates which Cisco has determined to be invalid, and has blocked:

Procedure

Click **View Blocked Certificates**.

Uploading or Generating a Certificate and Key

Certain AsyncOS features require a certificate and key to establish, confirm or secure a connection Identity Services Engine (ISE) and . You can either upload an existing certificate and key, or you can generate one when you configure the feature.

Uploading a Certificate and Key

A certificate you upload to the appliance must meet the following requirements:

- It must use the X.509 standard.
- It must include a matching private key in PEM format. DER format is not supported.

Procedure

Step 1 Select **Use Uploaded Certificate and Key**.

Step 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.

Step 3 In the **Key** field, click Browse; locate the file to upload.

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.

Step 4 If the key is encrypted, select **Key is Encrypted**.

Step 5 Click **Upload Files**.

Generating a Certificate and Key

Procedure

Step 1 Select **Use Generated Certificate and Key**.

Step 2 Click **Generate New Certificate and Key**.

a) In the Generate Certificate and Key dialog box, enter the necessary generation information.

Note
You can enter any ASCII character except the forward slash (/) in the Common Name field.

b) Click **Generate** in the Generate Certificate and Key dialog box.

When generation is complete, the certificate information is displayed in the Certificate section, along with two links: **Download Certificate** and **Download Certificate Signing Request**. In addition, there is a Signed Certificate option that is used to upload the signed certificate when you receive it from the Certificate Authority (CA).

Step 3 Click **Download Certificate** to download the new certificate for upload to the appliance.

Step 4 Click **Download Certificate Signing Request** to download the new certificate file for transmission to a Certificate Authority (CA) for signing. See Certificate Signing Requests, on page 52 for more information about this process.

a) When the CA returns the signed certificate, click Browse in the Signed Certificate portion of the Certificate field to locate the signed-certificate file, and then click Upload File to upload it to the appliance.

b) Ensure the CA's root certificate is present in the appliance's list of trusted root certificates. If it is not, add it. See Managing Trusted Root Certificates, on page 50 for more information.

Certificate Signing Requests

The Secure Web Appliance cannot generate Certificate Signing Requests (CSR) for certificates uploaded to the appliance. Therefore, to have a certificate created for the appliance, you must issue the signing request from another system. Save the PEM-formatted key from this system because you will need to install it on the appliance later.

You can use any UNIX machine with a recent version of OpenSSL installed. Be sure to put the appliance hostname in the CSR. Use the guidelines at the following location for information on generating a CSR using OpenSSL:

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

Once the CSR has been generated, submit it to a certificate authority (CA). The CA will return the certificate in PEM format.

If you are acquiring a certificate for the first time, search the Internet for "certificate authority services SSL server certificates," and choose the service that best meets the needs of your organization. Follow the service's instructions for obtaining an SSL certificate.



Note You can also generate and sign your own certificate. Tools for doing this are included with OpenSSL, free software from `http://www.openssl.org` .

Intermediate Certificates

In addition to root certificate authority (CA) certificate verification, AsyncOS supports the use of intermediate certificate verification. Intermediate certificates are certificates issued by a trusted root CA which are then used to create additional certificates. This creates a chained line of trust. For example, a certificate may be issued by example.com who, in turn, is granted the rights to issue certificates by a trusted root CA. The certificate issued by example.com must be validated against example.com's private key as well as the trusted root CA's private key.

Servers send a “certificate chain” in an SSL handshake in order for clients (for example, browsers and in this case the Secure Web Appliance, which is a HTTPS proxy) to authenticate the server. Normally, the server certificate is signed by an intermediate certificate which in turn is signed by a trusted root certificate, and during the handshake, the server certificate and the entire certificate chain are presented to the client. As the root certificate is typically present in the Trusted Certificate store of the Secure Web Appliance, verification of the certificate chain is successful.

However, sometimes when the end-point entity certificate is changed on the server, necessary updates for the new chain are not performed. As a result, going forward the server presents only the server certificate during the SSL handshake and the Secure Web Appliance proxy is unable to verify the certificate chain since the intermediate certificate is missing.

Previously, the solution was manual intervention by the Secure Web Appliance administrator, who would upload the necessary intermediate certificate to the Trusted Certificate store. Now you can use the CLI command `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` to enable “intermediate certificate discovery,” a process the Secure Web Appliance uses in an attempt to eliminate the manual step in these situations.

Intermediate certificate discovery uses a method called “AIA chasing”: when presented with an untrusted certificate, the Secure Web Appliance examines it for an extension named “Authority Information Access.” This extension includes an optional CA Issuers URI field, which can be queried for the Issuer Certificate used to sign the server certificate in question. If it is available, the Secure Web Appliance fetches the issuer’s certificate recursively until the root CA certificate is obtained, and then tries to verify the chain again.

AsyncOS for Web Upgrades and Updates

Cisco periodically releases upgrades (new software versions) and updates (changes to current software versions) for AsyncOS for Web and its components.

Best Practices For Upgrading AsyncOS for Web

- Before you start the upgrade, save the XML configuration file off the Secure Web Appliance from the **System Administration > Configuration File** page or by using the saveconfig command.
- Save other files stored on the appliance, such as PAC files or customized end-user notification pages.
- When upgrading, do not pause for long amounts of time at the various prompts. If the TCP session times out during the download, the upgrade may fail.
- After the upgrade completes, save the configuration information to an XML file.

Related Topics

- Saving, Loading, and Resetting the Appliance Configuration, on page 2

Upgrading and Updating AsyncOS and Security Service Components

Downloading and Installing an Upgrade

Before you begin

Save the appliance configuration file (see Saving, Loading, and Resetting the Appliance Configuration, on page 2).

Note When downloading and upgrading AsyncOS in a single operation from a local server instead of from a Cisco server, the upgrade installs immediately while downloading. A banner is displayed for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you can type Control-C to exit the upgrade process before downloading starts.

Note While performing an upgrade, if the secure authentication certificate is not FIPs-complaint, it will be replaced with the default certificate of the latest path to which your appliance is upgraded to. This happens only when the customer has used the default certificate before the upgrade.

You can download and install in a single operation, or download in the background and install later.

Upgrade fails if any configuration value stored in varstore files have non-ASCII characters.

Procedure

Step 1 Choose **System Administration** > **System Upgrade**.

Step 2 Click **Upgrade Options**.

Select upgrade options and an upgrade image:

Setting	Description
Choose an upgrade option	• **Download and install** – Download and install the upgrade in a single operation. If you have already downloaded an installer, you will be prompted to overwrite the existing download. • **Download only** – Download an upgrade installer, but do not install. If you have already downloaded an installer, you will be prompted to overwrite the existing download. The installer downloads in the background without interrupting service. An **Install** button is displayed when the download is complete; click to install a previously downloaded upgrade.
	Select an upgrade image to be downloaded, or downloaded and installed, from the **List of available upgrade images files at upgrade server**.

Setting	Description
Upgrade Preparation	• To save a back-up copy of the current configuration to the `configuration` directory on the appliance, check **Save the current configuration to the configuration directory before upgrading**. • If the **Save current configuration** option is checked, you can check **Mask passwords in the configuration file** to have all current-configuration passwords masked in the back-up copy. However, you cannot load a configuration file with masked passwords using the **Load Configuration** command, nor with the CLI `loadconfig` command. If FIPS mode is enabled, you can select **Encrypt passphrases in the Configuration Files**. These files can be reloaded. • If the **Save current configuration** option is checked, you can enter one or more email addresses into the **Email file to** field; a copy of the back-up configuration file is mailed to each address. Separate multiple addresses with commas.

Step 3 Click **Proceed**.

If you are installing:

a) Be prepared to respond to prompts during the process.
b) At the completion prompt, click **Reboot Now**.
c) After about 10 minutes, access the appliance again and log in.

If you feel you need to power-cycle the appliance to troubleshoot an upgrade issue, do not do so until at least 20 minutes have passed since you rebooted.

Viewing Status of, Canceling, or Deleting a Background Download

Procedure

Step 1 Choose **System Administration** > **System Upgrade**.

Step 2 Click **Upgrade Options**.

Step 3 Choose an option:

To	Do This
View download status	Look in the middle of the page. If there is no download in progress and no completed download waiting to be installed, you will not see download status information.
Cancel a download	Click the **Cancel Download** button in the middle of the page. This option appears only while a download is in progress.
Delete a downloaded installer	Click the **Delete File** button in the middle of the page. This option appears only if an installer has been downloaded.

Step 4 (Optional) View the Upgrade Logs.

What to do next

Related Topics

- Local And Remote Update Servers, on page 57

Automatic and Manual Update and Upgrade Queries

AsyncOS periodically queries the update servers for new updates to all security service components, but not for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades. You can also manually prompt AsyncOS to query for available security service updates. For more information, see Reverting to a Previous Version of AsyncOS for Web, on page 60.

When AsyncOS queries an update server for an update or upgrade, it performs the following steps:

1. Contacts the update server.

   Cisco allows the following sources for update servers:

   - **Cisco update servers.** For more information, see Updating and Upgrading from the Cisco Update Servers, on page 57.
   - **Local server.** For more information, see Upgrading from a Local Server, on page 58.
2. Receives an XML file that lists the available updates or AsyncOS upgrade versions. This XML file is known as the "manifest."
3. Downloads the update or upgrade image files.

Manually Updating Security Service Components

By default, each security service component periodically receives updates to its database tables from the Cisco update servers. However, you can manually update the database tables.

Note Some updates are available on demand from the GUI pages related to the feature.

Tip View a record of update activity in the updater log file. Subscribe to the updater log file on the **System Administration** > **Log Subscriptions** page.

Note Updates that are in-progress cannot be interrupted. All in-progress updates must complete before new changes can be applied.

Procedure

Step 1 Choose **System Administration > Upgrade and Update Settings**.

Step 2 Click **Edit Update Settings**.

Step 3 Specify the location of the update files.

Step 4 Initiate the update using the Update Now function key on the component page located on the Security Services tab. For example, Security Services > Web Reputation Filters page.

The CLI and the Web application interface may be sluggish or unavailable during the update process.

Local And Remote Update Servers

By default, AsyncOS contacts the Cisco update servers for both update and upgrade images and the manifest XML file. However, you can choose from where to download the upgrade and update images and the manifest file. Using a local update server for the images or manifest file for any of the following reasons:

- **You have multiple appliances to upgrade simultaneously.** You can download the upgrade image to a web server inside your network and serve it to all appliances in your network.
- **Your firewall settings require static IP addresses for the Cisco update servers.** The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades. For more information, see Configuring a Static Address for the Cisco Update Servers, on page 57.

Note Local update servers do not automatically receive security service updates, only AsyncOS upgrades. After using a local update server for upgrading AsyncOS, change the update and upgrade settings back to use the Cisco update servers so the security services update automatically again.

Updating and Upgrading from the Cisco Update Servers

A Secure Web Appliance can connect directly to Cisco update servers and download upgrade images and security service updates. Each appliance downloads the updates and upgrade images separately.

Configuring a Static Address for the Cisco Update Servers

The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades.

Procedure

Step 1 Contact Cisco Customer Support to obtain the static URL address.

Step 2 Navigate to the **System Administration** > **Upgrade and Update Settings** page, and click **Edit Update Settings**.

Step 3 On the Edit Update Settings page, in the “Update Servers (images)” section, choose **Local Update Servers** and enter the static URL address received in step 1.

Step 4 Verify that Cisco Update Servers is selected for the "Update Servers (list)" section.

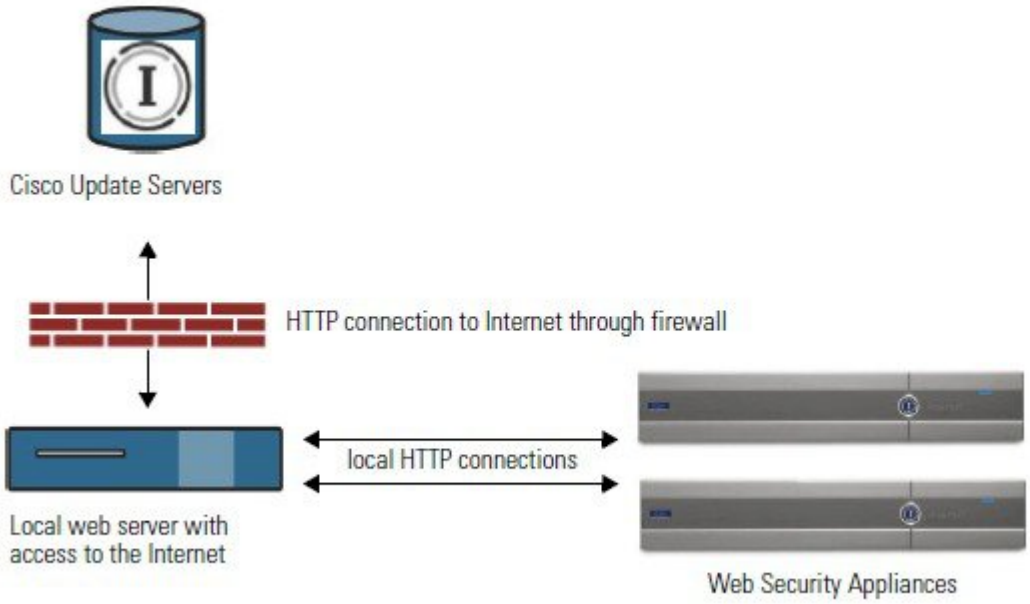
Step 5 Submit and commit your changes.

Upgrading from a Local Server

The Secure Web Appliance can download AsyncOS upgrades from a server within your network instead of obtaining upgrades directly from the Cisco update servers. When you use this feature, you download the upgrade image from Cisco once only, and then serve it to all Secure Web Appliances in your network.

The following figure shows how Secure Web Appliances download upgrade images from local servers.

Figure 1: Upgrading from a Local Server



Hardware and Software Requirements for Local Upgrade Servers

For *downloading* AsyncOS upgrade files, you must have a system in your internal network that has a web browser and Internet access to the Cisco update servers.

Note If you need to configure a firewall setting to allow HTTP access to this address, you must configure it using the DNS name and not a specific IP address.

For *hosting* AsyncOS upgrade files, a server on the internal network must have a web server, such as Microsoft IIS (Internet Information Services) or the Apache open source server, which has the following features:

- Supports the display of directory or filenames in excess of 24 characters.
- Has directory browsing enabled.
- Is configured for anonymous (no authentication) or Basic ("simple") authentication.

- Contains at least 350MB of free disk space for each AsyncOS upgrade image.

Configuring Upgrades from a Local Server



Note Cisco recommends changing the update and upgrade settings to use the Cisco update servers (using dynamic or static addresses) after the upgrade is complete to ensure the security service components continue to update automatically.

Procedure

Step 1 Configure a local server to retrieve and serve the upgrade files.

Step 2 Download the upgrade zip file.

Using a browser on the local server, go to http://updates.ironport.com/fetch_manifest.html to download a zip file of an upgrade image. To download the image, enter your serial number (for a physical appliance) or VLN (for a virtual appliance) and the version number of the appliance. You will then be presented with a list of available upgrades. Click on the upgrade version that you want to download.

Step 3 Unzip the zip file in the root directory on the local server while keeping the directory structure intact.

Step 4 Configure the appliance to use the local server using the **System Administration > Upgrade and Update Settings** page or the updateconfig command.

Step 5 On the **System Administration > System Upgrade** page, click **Available Upgrades** or run the upgrade command.

Differences Between Local and Remote Upgrading Methods

The following differences apply when upgrading AsyncOS from a local server rather than from a Cisco update server:

- The upgrading installs immediately *while downloading* .
- A banner displays for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you have the option to type Control+C to exit the upgrade process before downloading starts.

Configuring Upgrade and Service Update Settings

You can configure how the Secure Web Appliance downloads security services updates and AsyncOS for Web upgrades. For example, you can choose which network interface to use when downloading the files, configure the update interval or disable automatic updates.

Procedure

Step 1 Choose **System Administration > Upgrade and Update Settings**.

Step 2 Click **Edit Update Settings**.

Step 3 Configure the settings, referencing the following information:

Setting	Description
Automatic Updates	Choose whether to enable automatic updates of the security components. If you choose automatic updates, enter the time interval. The default is enabled and the update interval is 5 minutes.
Upgrade Notifications	Choose whether to display a notification at the top of the Web Interface when a new upgrade to AsyncOS is available. The appliance only displays this notification for administrators. For more information, see AsyncOS for Web Upgrades and Updates, on page 53.
Update Servers (list)	Whether to download the list of available upgrades and updates (the manifest XML file) from the Cisco update servers or a local web server. When you choose a local update server, enter the full path to the manifest XML file for the list including the file name and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and passphrase.
Update Servers (images)	Whether to download upgrade and update images from the Cisco update servers or a local web server. When you choose a local update server, enter the base URL and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and passphrase.
Routing Table	Choose which network interface's routing table to use when contacting the update servers.
Proxy Server (optional)	If an upstream proxy server exists and requires authentication, enter the server information and user name and passphrase here.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Local And Remote Update Servers, on page 57
- Automatic and Manual Update and Upgrade Queries, on page 56
- Upgrading and Updating AsyncOS and Security Service Components, on page 53

Reverting to a Previous Version of AsyncOS for Web

AsyncOS for Web supports the ability to revert the AsyncOS for Web operating system to a previous qualified build for emergency uses.

Note You cannot revert to a version of AsyncOS for Web earlier than version 7.5.

Reverting AsyncOS on Virtual Appliances Impacts the License

If you revert to AsyncOS 8.0, there is no 180-day grace period during which the appliance processes web transactions without security features. License expiration dates are unaffected.

Configuration File Use in the Revert Process

Effective in version 7.5, when you upgrade to a later version, the upgrade process automatically saves the current system configuration to a file on the Secure Web Appliance. (However, Cisco recommends manually saving the configuration file to a local machine as a backup.) This allows AsyncOS for Web to load the configuration file associated with the earlier release after reverting to the earlier version. However, when it performs a reversion, it uses the current network settings for the management interface.

Reverting AsyncOS for an Appliance Managed by the SMA

You can revert AsyncOS for Web from the Secure Web Appliance. However, if the Secure Web Appliance is managed by a Security Management appliance, consider the following rules and guidelines:

- When Centralized Reporting is enabled on the Secure Web Appliance, AsyncOS for Web finishes transferring the reporting data to the Security Management appliance before it starts the reversion. If the files take longer than 40 seconds to transfer to the Security Management appliance, AsyncOS for Web prompts you to continue waiting to transfer the files, or continue the reversion without transferring all files.
- You must associate the Secure Web Appliance with the appropriate Primary Configuration after reverting. Otherwise, pushing a configuration from the Security Management appliance to the Secure Web Appliance might fail.

Reverting AsyncOS for Web to a Previous Version

Caution Reverting the operating system on a Secure Web Appliance is a very destructive action and destroys all configuration logs and databases. Reversion also disrupts web traffic handling until the appliance is reconfigured. Depending on the initial Secure Web Appliance configuration, this action may destroy network configuration. If this happens, you will need physical local access to the appliance after performing the reversion.

Caution Smart Licensing configuration cannot be preserved if the operating system on a Secure Web Appliance is reverted to the previous version with Smart Licensing enabled. When you have successfully reverted to previous AsyncOS version, you should enable Smart Licensing and register it with the CSSM portal. If the **Specific/Permanent License Reservation** option was selected when Smart Software Licensing was activated, it is recommended to release the licenses used by the appliance before reverting the operation and de-register the appliance from CSSM portal. You can contact Cisco support for assistance if the licenses were not released or the appliance was not de-registered before the revert operation.

Note If updates to the set of URL categories are available, they will be applied after AsyncOS reversion.

Before you begin

- Contact Cisco Quality Assurance to confirm that you can perform the intended reversion. (BS: this is a summary of the Available Versions section in the original topic. Have asked if this is correct.)
- Back up the following information from the Secure Web Appliance to a separate machine:
  - System configuration file (with passphrases unmasked).
  - Log files you want to preserve.
  - Reports you want to preserve.
  - Customized end-user notification pages stored on the appliance.
  - PAC files stored on the appliance.

Procedure

Step 1 Log into the CLI of the appliance you want to revert.

Note
When you run the `revert` command in the next step, several warning prompts are issued. After these warning prompts are accepted, the revert action takes place immediately. Therefore, do not begin the reversion process until after you have completed the pre-reversion steps.

Step 2 Enter the `revert` command.

Step 3 Confirm twice that you want to continue with the reversion.

Step 4 Choose one of the available versions to revert to.

The appliance reboots twice.

Note
The reversion process is time-consuming. It may take fifteen to twenty minutes before reversion is complete and console access to the appliance is available again.

The appliance should now run using the selected AsyncOS for Web version. You can access the web interface from a web browser.

Monitoring System Health and Status Using SNMP

The AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). (For more information about SNMP, see RFCs 1065, 1066, and 1067.)

Please note:

- SNMP is **off** by default.
- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3. For more information on SNMPv3, see RFCs 2571-2575.

- Message authentication and encryption are mandatory when enabling SNMPv3. Passphrases for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5. The snmpconfig command “remembers” your passphrases the next time you run the command.
- The SNMPv3 username is: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.
- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a host name, but if you do, traps will only work if DNS is working.)

MIB Files

MIB files are available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Use the latest version of each MIB file.

There are multiple MIB files:

- asyncoswebsecurityappliance-mib.txt — an SNMPv2 compatible description of the Enterprise MIB for Secure Web Appliances.
- ASYNCOS-MAIL-MIB.txt — an SNMPv2 compatible description of the Enterprise MIB for Email Security appliances.
- IRONPORT-SMI.txt — This “Structure of Management Information” file defines the role of the asyncoswebsecurityappliance-mib.

This release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907.

See https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html to know about monitoring CPU usage on the appliance using SNMP.

Enabling and Configuring SNMP Monitoring

To configure SNMP to gather system status information for the appliance, use the snmpconfig command in the command-line interface (CLI). After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests.

When you use SNMP monitoring, keep the following points in mind:

- These version 3 requests must include a matching passphrase.
- By default, version 1 and 2 requests are rejected.
- If enabled, version 1 and 2 requests must have a matching community string.

Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report information such as temperature, fan speed, and power supply status.

To determine the hardware-related objects available for monitoring (for example, the number of fans or the operating temperature range), see the hardware guide for your appliance model.

Related Topics

- Documentation Set

SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the Cisco Secure Web Appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it to the host running the SNMP management console software.

You can configure SNMP traps (enable or disable specific traps) when you enable SNMP for an interface.

To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.

Related Topics

- About the connectivityFailure SNMP Trap , on page 64

About the connectivityFailure SNMP Trap

The connectivityFailure trap is intended to monitor your appliance's connection to the internet. It does this by attempting to connect and send an HTTP GET request to a single external server every 5 to 7 seconds. By default, the monitored URL is `downloads.ironport.com` on port 80.

To change the monitored URL or port, run the `snmpconfig` command and enable the connecivityFailure trap, even if it is already enabled. You will see a prompt to change the URL.

Tip To simulate connectivityFailure traps, you can use the `dnsconfig` CLI command to enter a non-working DNS server. Lookups for downloads.ironport.com will fail, and traps will be sent every 5-7 seconds. Be sure to change the DNS server back to a working server after completing your test.

CLI Example: snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>
```

```
Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y
```

```
Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

Web Traffic Tap

Before You Begin: Enabling Web Traffic Tap feature will result in reduced transaction handling capacity (requests per second) for the appliance as appliance will need additional CPU cycles and memory to copy the messages to the tap interface.



Note For reducing the performance impact due to Web Traffic Tap feature, reduce the amount of traffic that gets tapped by setting appropriate Web Traffic Tap policies.

This feature is not supported on Amazon Web Services (AWS)

Web Traffic Tap feature allows you to tap the HTTP and HTTPS web traffic that passes through the appliance and copy it to a Secure Web Appliance interface in-line with the real time data traffic. You can select the Secure Web Appliance interface to which the tapped traffic data is sent. If the tapped traffic includes HTTPS data, the appliance decrypts them based on the decryption policies before sending them to the tap interface. See Decryption Policies.

The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN.

Note The traffic mirrored on the tap interface is broadcast over Ethernet layer and not IP routable. Therefore a dedicated VLAN is required if connected to a L2 switch.

This feature also enables you to set Web Traffic Tap policies. Based on these customer defined policy filters, the appliance mirrors the web traffic that is available for the external security device. Web Traffic Tap feature provides visibility to the HTTPS traffic.

The term tapping refers to the reconstruction of complete TCP (Transmission Control Protocol) streams as if occurring between a directly connected client and server.

Virtual Secure Web Appliances support Web Traffic Tap feature.

Note The act of inspecting SSL traffic might be subject to corporate policy guidelines and/or national legislation. Cisco is not responsible for any legal obligations and it is your sole responsibility to ensure that your use of Web Traffic Tap feature on Secure Web Appliance is in accordance with any such legal or policy requirements.

You must perform the following procedures to tap the web traffic using the appliance:

1. Enable Web Traffic Tap feature
2. Configure Web Traffic Tap policies

Related Topics

- Enabling Web Traffic Tap, on page 67
- Configuring Web Traffic Tap Policies, on page 68

Enabling Web Traffic Tap

Before you begin

The Web Traffic Tap feature is disabled by default. You must enable the feature before you define the Web Traffic Tap policies using **Web Security Manager** > **Web Traffic Tap Policies**.

Note Decryption policies must be defined in order to tap HTTPS transactions. See Decryption Policies.

Procedure

Step 1 Choose **Network** > **Web Traffic Tap**.

Step 2 Click **Edit Settings**.

Step 3 In the Edit Web Traffic Tap page, check the **Enable** check box to enable Web Traffic Tap feature.

Note
To disable the Web Traffic Tap feature, uncheck the **Enable** check box. If you disable the Web Traffic Tap feature, you will not be able to view or edit the Web Traffic Tap policies. You must enable the feature again to view and edit the policies.

Step 4 From the Tap Interface drop-down list, choose the Secure Web Appliance interface to which the tapped traffic data is sent. The interface options are P1, P2, T1, and T2. See Connect the Appliance to know about interfaces.

Note
The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN. The tap interface chosen should be connected and its status should be active; if not, mirroring of tapped traffic will fail.

Step 5 Click **Submit** and commit your changes.

Configuring Web Traffic Tap Policies

Procedure

Step 1 Choose **Web Security Manager** > **Web Traffic Tap Policies**.

Step 2 Click **Add Policy**.

Follow the instructions in Creating a Policyto add a new Web Traffic Tap policy.

Note
A Global Traffic Tap policy with no tapping set is available by default on the Web Traffic Tap Policies page (**Web Security Manager** > **Web Traffic Tap Policies**).

Step 3 Expand the Advanced section of the Policy Member Definition area to add the following additional group membership criteria for Web Traffic Tap.

- Protocols - Choose either HTTP or HTTPS protocol or both of them to create Web Traffic Tap Policy.

  Note
  You must define matching decryption policy (**Web Security Manager** > **Decryption Policies**) in order to tap HTTPS traffic.

  Web Traffic Tap policies do not support Native FTP and SOCKS protocols.

- Subnets
- URL Categories – Set **Tap** or **No Tap** for the URL Filtering categories as required. To set traffic tap for uncategorized URLs, choose **Tap** from the Uncategorized URLs drop-down list and click **Submit**.

- User Agents

See Creating a Policy to know more about defining additional group membership criteria.

Note
The traffic that you want to tap must satisfy all the filter conditions that you have defined for the Web Traffic Tap policy.

You can also add URL categories from the URL Filtering table using **Web Security Manager** > **Web Traffic Tap Policies**.

Note
If you have already added the URL categories in the Advanced section, you will see only those URL categories listed in the URL Filtering table (**Web Security Manager** > **Web Traffic Tap Policies**).

See Policy Order to know about the Web Traffic Tap policy order.

Configuring HTTP 2.0 Protocol

The Cisco AsyncOS 14.0 version supports HTTP 2.0 for web request and response over TLS.

HTTP 2.0 for web request and response over TLS. HTTP 2.0 support requires TLS ALPN based negotiation which is available only from TLS 1.2 version onwards.

In this release, the HTTPS 2.0 is not supported for the following features:

- Web Traffic Tap
- External DLP
- Overall Bandwidth and Application Bandwidth

Note By default, the HTTP 2.0 feature is disabled and use the CLI command HTTP 2 to enable the feature.

The HTTP 2.0 feature supports:

- A maximum of 4096 concurrent sessions and 128 concurrent streams
- All HTTP protocol in ALPN and a maximum of seven protocols in advertised ALPN.
- A maximum header size of 16k.

Note CONNECT for explicit proxy in 2.0 also starts with HTTP1.1

A new CLI command `HTTP2` is introduced to enable or disable HTTP 2.0 configurations. See Secure Web Appliance CLI Commands.

You cannot enable or disable HTTP 2.0 and restrict domain for HTTP 2.0 through the appliance's web user interface. The configuration of HTTP 2.0 is not supported through Cisco Secure Email and Web Manager (Cisco Content Security Management Appliances).

- When URL fails in both HTTP 2 exception lists and passthrough URL Categories, HTTP 2 takes precedence over passthrough.
- ALPN logging is not consistent for Passthrough URL Categories.

Connect the Appliance to a Cisco Cloud Web Security Proxy

This topic contains the following sections:

- How to Configure and Use Features in Cloud Connector Mode , on page 70
- Deployment in Cloud Connector Mode , on page 70
- Configuring the Cloud Connector, on page 71
- Controlling Web Access Using Directory Groups in the Cloud, on page 74
- Bypassing the Cloud Proxy Server, on page 74
- Partial Support for FTP and HTTPS in Cloud Connector Mode , on page 74
- Preventing Loss of Secure Data, on page 75
- Viewing Group and User Names and IP Addresses , on page 75
- Subscribing to Cloud Connector Logs, on page 75
- Identification Profiles and Authentication with Cloud Web Security Connector , on page 76

How to Configure and Use Features in Cloud Connector Mode

Use of the features included in the Cloud Connector subset is the same as in standard mode, except as noted. See Comparison of Modes of Operation for additional information.

This topic links to locations within this documentation that provide information about some of the major features of the Secure Web Appliance that are common to both standard mode and Cloud Web Security Connector mode. With the exception of Cloud Connector configuration settings and information about sending directory groups to the cloud, relevant information is in other locations throughout this document.

This topic includes information about configuring the Cloud Web Security Connector that is not applicable in standard mode.

This document does not include information about the Cisco Cloud Web Security product. Cisco Cloud Web Security documentation is available from http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Deployment in Cloud Connector Mode

When you initially set up the appliance, you choose whether to deploy in Cloud Connector mode or standard mode. You can also run the System Setup Wizard on an appliance that is currently deployed in standard mode to redeploy it in Cloud Connector mode, if you have the required licensing. Running the System Setup Wizard overwrites your existing configurations and deletes all existing data.

Deployment of the appliance is the same in both standard and Cloud Security mode except that on-site web proxy services and Layer-4 Traffic Monitor services are not available in Cloud Web Security Connector mode.

You can deploy the Cloud Web Security Connector in either explicit forward mode or in transparent mode.

To modify Cloud Connector settings after initial setup, select **Network** > **Cloud Connector**.

Related Topics

- Connect, Install, and Configure

Configuring the Cloud Connector

Before you begin

See Enabling Access to the Web Interface on Virtual Appliances.

Procedure

Step 1 Access the Web Interface for the Secure Web Appliance:

Enter the IPv4 address of the Secure Web Appliance in an Internet browser.

The first time you run the System Setup Wizard, use the default IPv4 address:

`https://192.168.42.42:8443`

-or-

`http://192.168.42.42:8080`

where `192.168.42.42` is the default IPv4 address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for HTTPS.

Step 2 Select **System Administration** > **System Setup Wizard**.

Step 3 Accept the terms of the license agreement.

Step 4 Click **Begin Setup**.

Step 5 Configure system settings:

Setting	Description
Default System Hostname	The fully-qualified hostname for the Secure Web Appliance.
DNS Server(s)	The Internet root DNS servers for domain name service lookups. See also DNS Settings.
NTP Server	A server with which to synchronize the system clock. The default is time.ironport.com.
Time Zone	Sets the time zone on the appliance so that timestamps in message headers and log files are correct.

Step 6 Select **Cloud Web Security Connector** for the appliance mode.

Step 7 Configure Cloud Connector settings:

Setting	Description
Cloud Web Security Proxy Servers	The address of the Cloud Proxy Server (CPS), for example, proxy1743.scansafe.net.
Failure Handling	If AsyncOS fails to connect to a Cloud Web Security proxy, either **Connect directly** to the Internet or **Drop requests**.
Cloud Web Security Authorization Scheme	Method for authorizing transactions: • Secure Web Appliance public facing IPv4 address • Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal.

Step 8 Configure network interfaces and wiring:

Setting	Description
Ethernet Port	If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic.
IP Address	The IPv4 address to use to manage the Secure Web Appliance.
Network Mask	The network mask to use when managing the Secure Web Appliance on this network interface.
Hostname	The hostname to use when managing the Secure Web Appliance on this network interface.

Step 9 Configure routes for Management and Data traffic:

Setting	Description
Default Gateway	The default gateway IPv4 address to use for the traffic through the Management and/or Data interface.
Name	A name used to identify the static route.
Internal Network	The IPv4 address for this route's destination on the network.
Internal Gateway	The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Step 10 Configure transparent connection settings:

Note
By default, the Cloud Connector is deployed in transparent mode. which requires a connection to a Layer-4 switch or a version 2 WCCP router.

Setting	Description
Layer-4 Switch or No Device	• The Secure Web Appliance is connected to a layer 4 switch. or • You will deploy the Cloud Connector in explicit forward mode.
WCCP v2 Router	The Secure Web Appliance is connected to a version 2 WCCP capable router. Note: A passphrase can contain up to seven characters and is optional.

Step 11 Configure administrative settings:

Setting	Description
Administrator Passphrase	A passphrase to access the Secure Web Appliance. The passphrase must be six characters or more.
Email system alerts to	An email address to which the appliance sends alerts.
Send Email via SMTP Relay Host	(Optional) A hostname or address for an SMTP relay host that AsyncOS uses for sending system generated email messages. The default SMTP relay host is the mail servers listed in the MX record. The default port number is 25.
AutoSupport	The appliance can send system alerts and weekly status report to Cisco Customer Support.

Step 12 Review and install:

a) Review the installation.
b) Click **Previous** to go back and make changes.
c) Click **Install This Configuration** to continue with the information you provided.

What to do next

Related Topics

- Preventing Loss of Secure Data, on page 75
- Network Interfaces
- Configuring TCP/IP Traffic Routes
- Configuring Transparent Redirection
- Managing Alerts, on page 35
- Configuring an SMTP Relay Host

Controlling Web Access Using Directory Groups in the Cloud

You can use Cisco Cloud Web Security to control web access based on directory groups. When traffic to Cisco Cloud Web Security is being routed through a Secure Web Appliance in Cloud Connector mode, Cisco Cloud Web Security needs to receive the directory-group information with the transactions from the Cloud Connector so it can apply the group-based cloud policies.

Before you begin

Add an authentication realm to the Secure Web Appliance configuration.

Procedure

Step 1 Navigate to **Network** > **Cloud Connector**.

Step 2 In the **Cloud Policy Directory Groups** area, click **Edit Groups**.

Step 3 Select the User Groups and Machine Groups for which you have created Cloud Policies within Cisco Cloud Web Security.

Step 4 Click **Add**.

Step 5 Click **Done** and Commit your changes.

What to do next

Related information

- Authentication Realms

Bypassing the Cloud Proxy Server

Cloud routing policies allow you to route web traffic to either Cisco Cloud Web Security proxies or directly to the Internet based on these characteristics:

- **Identification Profile**
- Proxy Port
- Subnet
- URL Category
- User Agent

The process of creating cloud routing policies in Cloud Connector mode is identical to the process of creating routing policies using the standard mode.

Related Topics

- Creating a Policy

Partial Support for FTP and HTTPS in Cloud Connector Mode

The Secure Web Appliance in Cloud Connector mode does not fully support FTP or HTTPS.

FTP

FTP is not supported by the Cloud Connector. AsyncOS drops native FTP traffic when the appliance is configured for Cloud Connector.

FTP over HTTP is supported in Cloud Connector mode.

HTTPS

The Cloud Connector does not support decryption. It passes HTTPS traffic without decrypting.

Because the Cloud Connector does not support decryption, AsyncOS generally does not have access to information in the client headers of HTTPS traffic. Therefore, AsyncOS generally cannot enforce routing policies that rely on information in encrypted headers. This is always the case for transparent HTTPS transactions. For example, for transparent HTTPS transactions, AsyncOS does not have access to the port number in the HTTPS client header and therefore it cannot match a routing policy based on port number. In this case, AsyncOS uses the default routing policy.

There are two exceptions for explicit HTTPS transactions. AsyncOS has access to the following information for explicit HTTPS transactions:

- URL
- Destination port number

For explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

Preventing Loss of Secure Data

You can integrate the Cloud Connector with external Data Loss Prevention servers through **Network** > **External DLP Servers**.

Related Topics

- Prevent Loss of Sensitive Data

Viewing Group and User Names and IP Addresses

To view the configured group names, user names, and IP addresses, go to whoami.scansafe.net.

Subscribing to Cloud Connector Logs

The Cloud Connector Logs provides useful information for troubleshooting problems with the Cloud Connector, for example, authenticated users and groups, the Cloud header, and the authorization key.

Procedure

Step 1 Navigate to **System Administration** > **Log Subscriptions**.

Step 2 Select **Cloud Connector Logs** from the **Log Type** menu.

Step 3 Type a name in the **Log Name** field.

Step 4 Set the log level.

Step 5 Submit and Commit your changes.

What to do next

Related Topics

- Monitor System Activity Through Logs

Identification Profiles and Authentication with Cloud Web Security Connector

The Cloud Web Security Connector supports basic authentication and NTLM. You can also bypass authentication for certain destinations.

In Cloud Connector mode, using an Active Directory realm, you can identify transaction requests as originating from specific machines. The Machine ID service is not available in standard mode.

With two exceptions, Authentication works the same throughout the Secure Web Appliance, whether in standard configuration or Cloud Connector configuration. Exceptions:

- The Machine ID service is not available in standard mode.
- AsyncOS does not support Kerberos when the appliance is configured in Cloud Connector mode.



Note Identification Profiles based on User Agent or Destination URL are not supported for HTTPS traffic.

Related Topics

- Identifying Machines for Policy Application, on page 76
- Guest Access for Unauthenticated Users, on page 77
- Classify End-Users for Policy Application
- Overview of Acquire End-User Credentials

Identifying Machines for Policy Application

By enabling the Machine ID service, AsyncOS can apply policies based on the machine that made the transaction request rather than the authenticated user or IP address or some other identifier. AsyncOS uses NetBIOS to acquire the machine ID.



Note Be aware that the machine identity service is only available through Active Directory realms. If you do not have an Active Directory realm configured, this service is disabled.

Procedure

Step 1 Select **Network > Machine ID Service**.

Step 2 Click **Enable and Edit Settings**.

Step 3 Configure Machine Identification settings:

Setting	Description
Enable NetBIOS for Machine Identification	Select to enable the machine identification service.
Realm	The Active Directory realm to use to identify the machine that is initiating the transaction request.
Failure Handling	If AsyncOS cannot identify the machine, should it drop the transaction or continue with policy matching?

Step 4 Submit and Commit your changes.

Guest Access for Unauthenticated Users

If the Secure Web Appliance is configured to provide guest access for unauthenticated users, in Cloud Connector mode, AsyncOS assigns guest users to the group, __GUEST_GROUP__, and sends that information to Cisco Cloud Web Security. Use Identities to provide guest access to unauthenticated users. Use Cisco Cloud Web Security policies to control these guest users.

Related Topics

- Granting Guest Access After Failed Authentication

Intercepting Web Requests

This topic contains the following sections:

- Overview of Intercepting Web Requests, on page 78
- Tasks for Intercepting Web Requests, on page 78
- Best Practices for Intercepting Web Requests, on page 79
- Web Proxy Options for Intercepting Web Requests, on page 79
- Domain Map, on page 92
- Client Options for Redirecting Web Requests, on page 94
- Using PAC Files with Client Applications, on page 94
- FTP Proxy Services, on page 97

- SOCKS Proxy Services, on page 99
- Troubleshooting Intercepting Requests, on page 102

Overview of Intercepting Web Requests

The Secure Web Appliance intercepts requests that are forwarded to it by clients or other devices over the network.

The appliance works in conjunction with other network devices to intercept traffic. These may be ordinary switches, transparent redirection devices network taps,and other proxy servers or Secure Web Appliances.

Tasks for Intercepting Web Requests

Steps	Task	Links to Related Topics and Procedures
Step 1	Review best practices.	• Best Practices for Intercepting Web Requests, on page 79
Step 2	(Optional) Perform follow up networking tasks: • Connect and configure upstream proxies. • Configure network interface ports. • Configure transparent redirection devices. • Configure TCP/IP routes. • Configure VLANs.	• Upstream Proxies • Network Interfaces • Configuring Transparent Redirection • Configuring TCP/IP Traffic Routes • Increasing Interface Capacity Using VLANs
Step 3	(Optional) Perform follow up Web Proxy tasks: • Configure the web proxy to operate in either Forward or Transparent mode. • Decide if additional services are needed for the protocol types you want to intercept • Configure IP spoofing. • Manage the web proxy cache. • Use custom web request headers. • Bypass the proxy for some requests.	• Web Proxy Options for Intercepting Web Requests, on page 79 • Configuring Web Proxy Settings, on page 79 • Web Proxy Options for Intercepting Web Requests, on page 79 • Web Proxy Cache, on page 82 • Web Proxy IP Spoofing, on page 85 • Web Proxy Bypassing, on page 88
Step 4	Perform client tasks: • Decide how clients should redirect requests to the web proxy. • Configure clients and client resources.	• Client Options for Redirecting Web Requests, on page 94 • Using PAC Files with Client Applications, on page 94
Step 5	(Optional) Enable and Configure the FTP proxy.	• FTP Proxy Services, on page 97

Best Practices for Intercepting Web Requests

- Enable only the proxy services you require.
- Use the same forwarding and return method (either L2 or GRE) for all WCCP services defined in the Secure Web Appliance. This allows the proxy bypass list to work consistently.
- Ensure that users cannot access PAC files from outside the corporate network. This allows your mobile workers to use the web proxy when they are on the corporate network and to connect directly to web servers at other times.
- Allow a web proxy to accept X-Forwarded-For headers from trustworthy downstream proxies or load balancers only.
- Leave the web proxy in the default transparent mode, even if initially using only explicit forwarding. Transparent mode also accepts explicitly forwarded requests.

Web Proxy Options for Intercepting Web Requests

By itself, the Web Proxy can intercept web requests that use HTTP (including FTP over HTTP) and HTTPS. Additional proxy modules are available to enhance protocol management:

- **FTP Proxy.** The FTP Proxy allows the interception of native FTP traffic (rather than just FTP traffic that has been encoded within HTTP).
- **HTTPS Proxy.** The HTTPS proxy supports the decryption of HTTPS traffic and allows the web proxy to pass unencrypted HTTPS requests on to policies for content analysis.



Note When in transparent mode, the Web Proxy drops all transparently redirected HTTPS requests if the HTTPS proxy is not enabled. No log entries are created for dropped transparently redirected HTTPS requests.

- **SOCKS Proxy.** The SOCKS proxy allows the interception of SOCKS traffic.

Each of these additional proxies requires the Web Proxy in order to function.You cannot enable them if you disable the Web Proxy.



Note The Web proxy is enabled by default. All other proxies are disabled by default.

Related Topics

- FTP Proxy Services, on page 97
- SOCKS Proxy Services, on page 99

Configuring Web Proxy Settings

Before you begin

Enable the web proxy.

Procedure

Step 1 Choose **Security Services** > **Web Proxy**.

Step 2 Click **Edit Settings**.

Step 3 Configure the basic web proxy settings as required.

Property	Description
HTTP Ports to Proxy	The ports that the web Proxy will listen on for HTTP connections
Caching	Specifies whether to enable or disable Web Proxy caching. The web proxy caches data to increase performance.
Proxy Mode	• **Transparent** (Recommended) — Allow the web proxy to name the internet target. The web proxy can intercept both transparent and explicitly forwarded web requests in this mode. • **Forward** — Allow the client browser to name the internet target. Requires individual configuration of each web browser to use the web proxy. The web proxy can intercept only explicitly forwarded web requests in this mode.
IP Spoofing Connection Type	If you have selected the Proxy Mode as **Transparent**, choose one of the IP spoofing connection types: • **For Transparent Connections Only** - To configure IP Spoofing for transparent connections only. • **For All Connections** - To configure IP Spoofing for Transparent and Explicit connections. If you have selected the Proxy Mode as **Forward**, then the IP Spoofing Connection Type is always Explicit. **Note** The IP spoofing connection type that you choose is applicable for all protocols - native FTP, HTTP, and HTTPS. To add IP spoofing profiles in routing policies, see Adding Routing Destination and IP Spoofing Profile to Routing Policy

Step 4 Complete the advanced web proxy settings as required.

Property	Description
Persistent Connection Timeout	The maximum time in seconds the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected. • **Client side.** The timeout value for connections to clients. • **Server side.** The timeout value for connections to servers. If you increase these values connections will remain open longer and reduce the overhead used to open and close connections repeatedly. However, you also reduce the ability of the Web Proxy to open new connections if the maximum number of simultaneous persistent connections has been reached. After establishing a connection and performing an SSL handshake, if client requests are not sent to the proxy, the proxy waits for the persistent connection timeout, and then ceases its connection with the client. Cisco recommends keeping the default values.
In-Use Connection Timeout	The maximum time in seconds that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed. • **Client side.** The timeout value for connections to clients. • **Server side.** The timeout value for connections to servers.
Simultaneous Persistent Connections (Server Maximum Number)	The maximum number of connections (sockets) the Web Proxy keeps open with servers.
Maximum Connections Per Client	Restricts the number of concurrent connections initiated by the client to a configured value. When the number of connections exceed the configured limit, the connections are dropped, and an alert is sent to the administrator. **Note** By default, Maximum Connections Per Client is disabled. To configure the limit, check the **Maximum Connections Per Client** check box, and do the following: • **Connections**—Enter the number of permissible concurrent connections. • **Exempted Downstream Proxy or Load Balancer**—Enter the IP address of the downstream proxy, load balancer, or any other client IP address (you cannot configure the subnets or host names). The web proxy does not apply the restrictions of the concurrent connections on the IP addresses that are included in this exempted list.

Property	Description
Generate Headers	Generate and add headers that encode information about the request. • **X-Forwarded-For** headers encode the IP address of the client from which an HTTP request originated. **Note** • To turn header forwarding on or off, use the CLI `advancedproxyconfig` command, Miscellaneous option, "Do you want to pass HTTP X-Forwarded-For headers?" • Using an explicit forward upstream proxy to manage user authentication or access control with proxy authentication requires forwarding of these headers. • For transparent HTTPS requests, the appliance does not decrypt the XFF header. For explicit requests, the appliance uses the XFF header received in the CONNECT request, and does not decrypt the XFF inside the SSL tunnel, so identification of client IP Addresses using X-Forwarded-For is not applicable for HTTPS transparent requests. • **Request Side VIA** headers encode the proxies through which the request passed on its way from the client to the server. • **Response Side VIA** headers encode the proxies through which the request passed on its way from the server to the client.
Use Received Headers	Allows a Web proxy deployed as an upstream proxy to identify clients using X-Forwarded-For headers send by downstream proxies. The Web Proxy will not accept the IP address in a X-Forwarded-For header from a source that is not included in this list. If enabled, requires the IP address of a downstream proxy or load balancer (you cannot enter subnets or host names).
Range Request Forwarding	Use the **Enable Range Request Forwarding** check box to enable or disable forwarding of range requests. Refer to Managing Access to Web Applications for more information.

Step 5 Submit and commit your changes.

What to do next

- Web Proxy Cache, on page 82
- Configuring Transparent Redirection

Web Proxy Cache

The web proxy caches data to increase performance. AsyncOS includes defined caching modes that range from safe to aggressive, and also allows customized caching. You can also exclude specific URLs from being cached, either by removing them from the cache, or by configuring the cache to ignore them.

Clearing the Web Proxy Cache

Procedure

Step 1 Choose **Security Services** > **Web Proxy**.

Step 2 Click **Clear Cache** and confirm your action.

Removing URLs from the Web Proxy Cache

Procedure

Step 1 Access the CLI.

Step 2 Use the `webcache > evict` commands to access the required caching area:

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

Step 3 Enter the URL to be removed from the cache.

Note
If you do not include a protocol in the URL, `http://` will be prepended to it (e.g., `www.cisco.com` will become `http://www.cisco.com`)

Specifying Domains or URLs that the Web Proxy never Caches

Procedure

Step 1 Access the CLI.

Step 2 Use the `webcache -> ignore` commands to access the required submenus:

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

Step 3 Enter the address type you wish to manage: `DOMAINS` or `URLS`.

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

Step 4 Enter **add** to add new entries:

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

Step 5 Enter domains or URLs, one per line; for example:

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

You can include certain regular expression (regex) characters when specifying a domain or URLs. With the `DOMAINS` option, you can use a preceding dot character to exempt an entire domain and its subdomains from caching. For example, you can enter `.google.com` rather than simply `google.com` to exempt www.google.com, docs.google.com, and so on.

With the `URLS` option, you can use the full suite of regular-expression characters. See Regular Expressions for more information about using regular expressions.

Step 6 When you are finished entering values, press Enter until you are returned to the main command-line interface.

Step 7 Commit your changes.

Choosing The Web Proxy Cache Mode

Procedure

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> caching` commands to access the required submenus:

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

```
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

Step 3 Enter a number corresponding to the web proxy cache settings you require:

Entry	Mode	Description
1	Safe	The least caching and the most adherence to RFC #2616 compared to the other modes.
2	Optimized	Moderate caching and moderate adherence to RFC #2616. Compared to safe mode, in optimized mode the Web Proxy caches objects when no caching time is specified when a Last-Modified header is present. The Web Proxy caches negative responses.
3	Aggressive	The most caching and the least adherence to RFC #2616. Compared to optimized mode, aggressive mode caches authenticated content, ETag mismatches, and content without a Last-Modified header. The Web Proxy ignores the no-cache parameter.
4	Customized mode	Configure each parameter individually.

Step 4 If you chose option 4 (Customized mode), enter values (or leave at the default values) for each of the custom settings.

Step 5 Press **Enter** until you return to the main command interface.

Step 6 Commit your changes.

What to do next

Related Topics

- Web Proxy Cache, on page 82.

Web Proxy IP Spoofing

When the web proxy forwards a request, it changes the request source IP address to match its own address by default. This increases security, but you can change this behavior by implementing IP spoofing, so that requests appear to originate from client IP or any other routable custom IP address rather than from the Secure Web Appliance. You can configure Web Proxy IP Spoofing by creating IP spoofing profiles for custom IP addresses and adding them to the routing policies.

IP spoofing works for transparent and explicitly forwarded traffic. When the Web Proxy is deployed in transparent mode, you can configure the IP Spoofing Connection Type for transparently redirected connections only or for all connections (transparently redirected and explicitly forwarded). If explicitly forwarded connections use IP spoofing, you should ensure that you have appropriate network devices to route return packets back to the Secure Web Appliance.

When IP spoofing is enabled and the appliance is connected to a WCCP router, you must configure two WCCP services: one based on source ports and one based on destination ports.

IP spoofing profiles have a limitation when the HTTPS traffic is transparently redirected. See Accessing HTTPS Sites Using Routing Policies with URL Category Criteria.

Related Topics

- Creating IP Spoofing Profiles, on page 86
- Configuring Web Proxy Settings, on page 79
- Configuring WCCP Services

Creating IP Spoofing Profiles

Before you begin

Make sure that you have selected the proxy mode and IP spoofing connection type in the web proxy settings. For more information, see Configuring Web Proxy Settings, on page 79.

Procedure

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.
Step 2 Click **Add Profile**.
Step 3 Enter a name for the IP spoofing profile.
Step 4 Enter the IP address that you want to assign to the spoofing profile name.
Step 5 Submit and commit your changes.

What to do next

Add the IP spoofing profile to a routing policy. For more information, see Adding Routing Destination and IP Spoofing Profile to Routing Policy.

Related Topics

Editing IP Spoofing Profiles, on page 86
Deleting IP Spoofing Profiles, on page 87

Editing IP Spoofing Profiles

Note Once you update an IP spoofing profile, it will be updated in all the routing policies associated with that profile.

Procedure

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.
Step 2 Click the IP spoofing profile name link that you want to edit.

Step 3 Modify the profile details.

Step 4 Submit and commit your changes.

Deleting IP Spoofing Profiles

Procedure

Step 1 Choose **Web Security Manager** > **IP Spoofing Profiles**.

Step 2 Click the trash can icon corresponding to the IP spoofing profile that you want to delete.

Note
The appliance displays a warning if the IP spoofing profile that you are deleting is assigned to one or more routing policies. In this case, select a different IP spoofing profile to be assigned to all those affected routing policies.

Step 3 Submit and commit your changes.

Web Proxy Custom Headers

You can add custom headers to specific outgoing transactions to request special handling from destination servers. For example, if you have a relationship with YouTube for Schools, you can use a custom header to identify transaction requests to YouTube.com as coming from your network and as requiring special handling.

Adding Custom Headers To Web Requests

Procedure

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> customheaders` commands to access the required submenus:

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
```

```
- EDIT - Edit entries
[]>
```

Step 3 Enter the required subcommand as follows:

Option	Description
`Delete`	Deletes the custom header you identify. Identify the header to delete using the number associated with the header in the list returned by the command.
`New`	Creates the header you provide for use with the domain or domains you specify. Example header: X-YouTube-Edu-Filter: ABCD1234567890abcdef (The value in this case is a unique key provided by YouTube.) Example domain: youtube.com
`Edit`	Replaces an existing header with one you specify. Identify the header to delete using the number associated with the header in the list returned by the command.

Step 4 Press **Enter** until you return to the main command interface.

Step 5 Commit your changes.

Web Proxy Bypassing

- Web Proxy Bypassing for Web Requests, on page 88
- Configuring Web Proxy Bypassing for Web Requests, on page 89
- Configuring Web Proxy Bypassing for Applications, on page 89

Web Proxy Bypassing for Web Requests

You can configure the Secure Web Appliance so that transparent requests from particular clients, or to particular destinations, bypass the Web Proxy.

Bypassing the web proxy allows you to:

- Prevent interference with non-HTTP-compliant (or proprietary) protocols that use HTTP ports but do not work properly when they connect to a proxy server.
- Ensure that traffic from a particular machine inside the network, such as a malware test machine, bypasses the Web Proxy and all its built-in security protection.

Bypassing only works for requests that are transparently redirected to the web proxy. The web proxy processes all requests that clients explicitly forward to it, whether the proxy is in transparent or forward mode.

Configuring Web Proxy Bypassing for Web Requests

Procedure

Step 1 Choose **Web Security Manager > Bypass Settings**.

Step 2 Click **Edit Bypass Settings**.

Step 3 Enter the addresses for which you wish to bypass the web proxy.

Note
When you configure /0 as a subnet mask for any IP in the bypass list, the appliance bypasses all the web traffic. In this case, the appliance interprets the configuration as 0.0.0.0/0.

Step 4 Choose the Custom URL Categories that you want to add to the proxy bypass list.

Note
You cannot set the web proxy bypass for Regular Expressions.

Note
Once you add the Custom URL Categories to the proxy bypass list, all the IP addresses and the domain names of the Custom URL categories are bypassed for both the source and destination.

Step 5 Submit and commit your changes.

Configuring Web Proxy Bypassing for Applications

Procedure

Step 1 Choose **Web Security Manager > Bypass Settings**.

Step 2 Click **Edit Application Bypass Settings**.

Step 3 Select the application(s) you wish to bypass scanning for.

Step 4 Submit and commit your changes.

Note
Webex bypass settings are only applicable to HTTPS traffic. However, for HTTP traffic the applications can be blocked via Access Policies.

Web Proxy Custom Headers Per Policy

You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. Each profile can have a maximum of 12 headers. You can also modify or delete the existing header profiles. You can add the header rewrite profile to an existing access policy to include the headers in all the transactions to which the particular access policy is applied.

The header rewrite profile feature enables the appliance to pass the user and group information to another upstream device after successful authentication. The upstream proxy considers the user as authenticated, bypasses further authentication, and provides access to the user based on the defined access policies.

- Creating Header Rewrite Profiles for HTTP Web Requests, on page 90
- Modifying Username and Group Header Formats , on page 91 (optional)
- Adding Header Profiles To Access Policy, on page 91

Recommend not to create web proxy custom headers using the CLI command `advancedproxyconfig -> customheader` from AsynOS verion 14.0 onwards.

Creating Header Rewrite Profiles for HTTP Web Requests

Procedure

Step 1 Choose **Web Security Manager** -> **HTTP Rewrite Profiles**

Step 2 Click **Add Profile**.

Step 3 Assign a unique name to the header rewrite profile that you want to create.

Step 4 In the **Headers** area, enter the following information:

Note
You can enter empty or null header value in Header Rewrite Profiles. When you save and commit the header with null or no value, the header is not included in the outgoing requests. For example, if you want to hide header `Via` to outbound server, add header-name `Via` to HTTP Rewrite Profiles with value `""`.

- **Header Name** — Enter the header name that you want to add to the HTTP requests. Example: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups, etc.
- **Header Value** —Enter the value to be included in the request header corresponding to the header name. Prefix the header variables with :
  - `$ReqMeta`— to fetch standard HTTP header variables such as client IP, user, group etc. For example, to include username in the request header, the format is `($ReqMeta[X-Authenticated-User])`
  - `$ReqHeader`— to use the values of the standard HTTP hearders or values of other headers defined under the same header rewrite profile.

    For example,

    ```
    Header1:32

    Header2: 44-($ReqHeader[Header1])-46
    ```

    Then the value of `Header 2` is `44-32-46`
- **Text Format**—Choose the text format for encoding. The available options are ASCII and UTF-8
- **Binary Encoding**— Choose whether you want binary encoding (Base64) or not for the request headers.

Note
Based on the server type, the appliance displays an error message if the size of the request header field sent exceeds the maximum limit of the server. For example, different server types support different header lengths:

- Apache 2.0, 2.2: 8k
- Nginx: 4k - 8k

- IIS(varies by version): 8K - 16K
- Tomcat: (varies by version) 8K

In case of user identification using ISE, the global X-authentication headers settings i.e., X-Authenticated-User and X-Authenticated-Groups, do not apply domain and authentication mechanism as prefix.

You can enter UTF+8 as `($ReqMeta[HTTP_header])` value even if you select text format as ASCII. Currenlty, the following headers support `($ReqMeta[HTTP_header])` :

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

The headers are not included in the outgoing requests, if the values of the headers are null. This happens when you do not :

- Enable proxy authentication
- Define groups in membership criteria for access policy, decryption policy, or routing policy.

Step 5 Submit and commit your changes.

Modifying Username and Group Header Formats

Procedure

Step 1 Choose **Web Security Manager** > **HTTP Rewrite Profiles**

Step 2 Click **Edit Settings**.

Step 3 Modify the formats.

Allowed formats are:

- Username -`$authMechanism://$domainName/$userName, $authMechanism:\\$domainName\$userName, $domainName/$userName, $domainName\$userName, $userName`
- Group- `$authMechanism://$domainName/$groupName, $authMechanism:\\$domainName\$groupName, $domainName/$groupName, $domainName\$groupName, $groupName`

  You can also modify the delimiter such as comma (,), colon (:), semicolon (;), backslash(\), vertical bar (|), and so on.

Step 4 Submit and commit your changes.

Adding Header Profiles To Access Policy

Before you begin

Configure access policy. See Creating a Policy.

Procedure

Step 1 Choose **Web Security Manager** > **Access Policies**

Step 2 In the Access Policies page, click the link for HTTP Rewrite Profile.

You can also create a new access policy and add the Header Rewrite profile to it. To create a new access policy, seeCreating a Policy

Step 3 Select the header rewrite profile that you want to add to the policy. After you add, the headers are included in the HTTP transaction to which the particular access policy is applied.

Step 4 Submit and commit your changes.

You can delete a header rewrite profile linked to an access policy. Before you delete, choose another profile and the selected profile will be applied to the access policies automatically.

Web Proxy Usage Agreement

You can configure the Secure Web Appliance to inform users that it is filtering and monitoring their web activity. The appliance does this by displaying an end-user acknowledgment page when a user first accesses a browser after a certain period of time. When the end-user acknowledgment page appears, users must click a link to access the original site requested or any other website.

Related Topics

- Notify End-Users of Proxy Actions

Domain Map

You can configure the Secure Web Appliance so that transparent HTTPS requests from particular clients, or to particular destinations, bypass the HTTPS Proxy.

You can use passthrough for applications that require traffic to pass through the appliance, without undergoing any modification, or certificate checks of the destination servers.

Domain Map for Specific Applications

Before you begin

Ensure you have an identification policy defined for the devices that require pass through traffic to specific servers. See Classifying Users and Client Software for more information. Specifically, you must:

- Choose **Exempt from authentication/identification**.
- Specify the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets.

Procedure

Step 1 Enable HTTPS Proxy. See Enabling the HTTPS Proxy for more information.

Step 2 Choose **Web Security Manager** > **Domain Map**.

a) Click **Add Domain**.
b) Enter the **Domain Name** or the destination server.
c) Choose the order of the priority if there are existing domains specified.
d) Enter the IP addresses.
e) Click **Submit**.

Step 3 Choose **Web Security Manager** > **Custom and External URL Categories**.

a) Click **Add Category**.
b) Provide the following information.

Setting	Description
Category Name	Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups.
List Order	Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Category Type	Choose **Local Custom Category**.
Advanced	You can enter regular expressions in this section to specify additional sets of addresses. You can use regular expressions to specify multiple addresses that match the patterns you enter. See Regular Expressions for more information about using regular expressions.

c) Submit and commit the changes.

Step 4 Choose **Web Security Manager** > **Decryption Policies**.

a) Create a new decryption policy.
b) Choose the identification profile that you created for bypassing HTTPS traffic for specific applications.
c) In the **Advanced** panel, click the link for URL Categories.
d) In the **Add** column, click to add the custom URL category created in step 3.
e) Click **Done**.
f) In the Decryption Policies page, click the link for **URL Filtering**.
g) Choose **Pass Through**.
h) Submit and commit the changes.

You can use the **%(** format specifier to view access log information. See Customizing Access Logs for more information.

Note

- The Domain Map feature works in HTTPS Transparent mode.
- This feature does not work in Explicit mode and for HTTP traffic.

- Local Custom Category must be configured to allow the traffic using this feature.
- Enabling this feature will modify or assign the server name as per the server name configured in the Domain Map, even if SNI information is available.
- This feature does not block traffic based on domain name if that traffic matches the Domain Map and corresponding custom category, decryption policy and passthrough action are configured.
- Authentication does not work with this pass through feature. Authentication requires decryption, but traffic will not be decrypted in this case.
- UDP traffic is not monitored. You must configure UDP traffic not to come to the Secure Web Appliance, instead it should go directly through firewall to the internet for applications like WhatsApp, Telegram etc.
- WhatsApp, Telegram and Skype works in Transparent mode. However, some apps like WhatsApp do not work in Explicit mode due to restrictions on the app.

Client Options for Redirecting Web Requests

If you choose to have clients explicitly forward requests to the web proxy, you must also decide how to configure the clients to do this. Choose from the following methods:

- **Configure Clients Using Explicit Settings.** Configure clients with the web proxy hostname and port number. See individual client documentation for details on how to do this.



Note The web proxy port uses port numbers 80 and 3128 by default. Clients can use either port.

- **Configure Clients Using a Proxy Auto-Config (PAC) File.** PAC files provide clients with instructions on where to direct web requests. This options allows you to centrally manage subsequent changes to the proxy details.

If you choose to use PAC files, you must also choose where to store them and how clients will find them.

Related Topics

- Using PAC Files with Client Applications, on page 94

Using PAC Files with Client Applications

Options For Publishing Proxy Auto-Config (PAC) Files

You must publish PAC files where clients can access them. Valid locations are:

- **Web servers.**
- **Secure Web Appliance**.You can place PAC files on a Secure Web Appliance, which appears to clients as a web browser. The appliance also offers additional options to manage PAC files, including the ability to service requests that use different hostnames, ports, and file names.

- **Local machines.** You can place the PAC file locally on a client's hard disk. Cisco does not recommend this as a general solution, and it is not suited to automatic PAC file detection methods, but it can be useful for testing.

Related Topics

- Hosting PAC Files on the Secure Web Appliance, on page 95
- Specifying PAC Files in Client Applications, on page 96
- Hosting PAC Files on the Secure Web Appliance, on page 95
- Specifying PAC Files in Client Applications, on page 96

Client Options For Finding Proxy Auto-Config (PAC) Files

If you choose to use PAC files for your clients, you must also choose how clients will find the PAC files. You have two options:

- **Configure client with the PAC file location.** Configure the client with a URL that specifically points to the PAC file.
- **Configure clients to detect the PAC file location automatically.** Configure clients to find PAC files automatically using the WPAD protocol along with DHCP or DNS.

Automatic PAC File Detection

WPAD is a protocol that allows the browser determine the location of a PAC file using DHCP and DNS.

- **To use WPAD with DHCP**, you must set up option 252 on the DHCP server's with the url of the PAC file location. Not all browsers support DHCP, however.
- **To use WPAD with DNS**, you must configure a DNS record to point to the PAC file's host server.

You can configure either or both options. WPAD will first try to find PAC files using DHCP, and if it cannot, it will then try DNS.

Related Topics

- Detecting the PAC File Automatically in Clients, on page 97

Hosting PAC Files on the Secure Web Appliance

Procedure

Step 1 Choose **Security Services > PAC File Hosting**

Step 2 Click **Enable and Edit Settings**.

Step 3 (Optional) Complete the following basic settings:

Option	Description
PAC Server Ports	The ports that the Secure Web Appliance will use to listen for PAC file requests.
PAC File Expiration	Allows the PAC file to expire after a specified number of minutes in the browser's cache.

Step 4 Click **Browse** in the PAC Files section and select a PAC file from your local machine for upload to the Secure Web Appliance.

Note
If the file you select is called `default.pac` , you do not have to specify the file name when configuring its location in a browser. The Secure Web Appliance looks for a file called `default.pac` if no name is specified.

Step 5 Click **Upload** to upload the PAC file selected in step 4 to the Secure Web Appliance.

Step 6 (Optional) In the Hostnames for Serving PAC Files Directly section, configure hostnames and associated file names for PAC file requests that do not include a port number:

Option	Description
Hostname	The hostname that the PAC file request must include if the Secure Web Appliance is to service the request. As the request does not include a port number, it will be processed through the Web Proxy HTTP ports (e.g. port 80) and must be distinguishable as a PAC file request through this hostnamevalue.
Default PAC File for "Get/" Request through Proxy Port	The PAC file name that will be associated with the hostname on the same row. Request to the hostname will return the PAC file specified here. Only PAC files that have been uploaded are available for selection.
Add Row	Adds another row to specify additional hostnames and PAC file names.

Step 7 Submit and commit your changes.

Specifying PAC Files in Client Applications

- Configuring a PAC File Location Manually in Clients, on page 96
- Detecting the PAC File Automatically in Clients, on page 97

Configuring a PAC File Location Manually in Clients

Procedure

Step 1 Create and publish a PAC file.

Step 2 Enter a URL in your browser's PAC file configuration area that points to the PAC file location.

The following are valid URL formats if the Secure Web Appliance is hosting the PAC file:

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

where *WSAHostname* is the **hostname** value configured when hosting the PAC file on a Secure Web Appliance. Otherwise the URL format will depend on the storage location and, in some cases, on the client.

What to do next

- Hosting PAC Files on the Secure Web Appliance, on page 95

Detecting the PAC File Automatically in Clients

Procedure

Step 1 Create a PAC file called wpad.dat and publish it to a web server or Secure Web Appliance (the file must be placed in a web server's root folder if you intend using WPAD with DNS).

Step 2 Configure the web server to set up .dat files with the following MIME type:

```
application/x-ns-proxy-autoconfig
```

Note
A Secure Web Appliance does this for you automatically.

Step 3 To support DNS lookup, create an internally resolvable DNS name beginning with ' `wpad` ' (for example, `wpad.example.com`) and associate it with the IP address of the server hosting the `wpad.dat` file.

Step 4 To support DHCP lookup, configure your DHCP server's option 252 with the url of the wpad.dat file location (for example: " `http://wpad.example.com/wpad.dat` "). The URL can use any valid host address, including an IP address, and does not require a specific DNS entry.

What to do next

- Using PAC Files with Client Applications, on page 94
- Hosting PAC Files on the Secure Web Appliance, on page 95
- WPAD Not Working With Firefox

FTP Proxy Services

- Overview of FTP Proxy Services, on page 97
- Enabling and Configuring the FTP Proxy, on page 98

Overview of FTP Proxy Services

The web proxy can intercept two types of FTP requests:

- **Native FTP.** Native FTP requests are generated by dedicated FTP clients (or by browsers using built-in FTP clients). Requires the FTP proxy.
- **FTP over HTTP.** Browsers sometimes encode FTP requests inside HTTP requests, rather than using native FTP. Does not require the FTP proxy.

Related Topics

- Enabling and Configuring the FTP Proxy, on page 98
- Configuring FTP Notification Messages

Enabling and Configuring the FTP Proxy

Note To configure proxy settings that apply to FTP over HTTP connections, see Configuring Web Proxy Settings, on page 79.

Procedure

Step 1 Choose **Security Services** > **FTP Proxy**.

Step 2 Click **Enable and Edit Settings** (if the only available option is **Edit Settings** then the FTP proxy is already enabled).

Step 3 (Optional) Configure the basic FTP Proxy settings.

Property	Description
Proxy Listening Port	The port that the FTP Proxy will listen to for FTP control connections. Clients should use this port when configuring an FTP proxy (not as the port for connecting to FTP servers, which normally use port 21).
Caching	Whether of not data connections from anonymous users are cached. **Note** Data from non-anonymous users is never cached.
Server Side IP Spoofing	Allows the FTP Proxy to imitate the FTP server's IP address. This supports FTP clients that do not allow transactions when the IP address is different for the control and data connections.
Client IP Spoofing	Allows the FTP Proxy to imitate the FTP client's source IP address. When enabled, the FTP requests appear to originate from the FTP client rather than the FTP Proxy.
Authentication Format	Allows a choice of authentication format the FTP Proxy can use when communicating with FTP clients.
Passive Mode Data Port Range	The range of TCP ports that FTP clients should use to establish a data connection with the FTP Proxy for passive mode connections.
Active Mode Data Port Range	The range of TCP ports FTP servers should use to establish a data connection with the FTP Proxy for active mode connections. This setting applies to both native FTP and FTP over HTTP connections. Increasing the port range accommodates more requests from the same FTP server. Because of the TCP session TIME-WAIT delay (usually a few minutes), a port does not become available again for the *same* FTP server immediately after being used. As a result, any given FTP server cannot connect to the FTP Proxy in active mode more than *n* times in a short period of time, where *n* is the number of ports specified in this field.

Property	Description
Welcome Banner	The welcome banner that appears in FTP clients during connection. Choose from: • **FTP server message.** The message will be provided by the destination FTP server. This option is only available when the web proxy is configured for transparent mode, and only applies for transparent connections. • **Custom message.** When selected, this custom message is displayed for all native FTP connections. When not selected, this is still used for explicit forward native FTP connections.

Step 4 (Optional) Configure the advanced FTP Proxy settings:

Property	Description
Control Connection Timeouts	The maximum number of seconds the FTP Proxy waits for more communication in the control connection from an idle FTP client or FTP server when the current transaction has not been completed. • **Client side.** The timeout value for control connections to idle FTP clients. • **Server side.** The timeout value for control connections to idle FTP servers.
Data Connection Timeouts	How long the FTP Proxy waits for more communication in the data connection from an idle FTP client or FTP server when the current transaction has not been completed. • **Client side.** The timeout value for data connections to idle FTP clients. • **Server side.** The timeout value for data connections to idle FTP servers.

Step 5 Submit and commit your changes.

What to do next

- Overview of FTP Proxy Services, on page 97

SOCKS Proxy Services

- Overview of SOCKS Proxy Services, on page 99
- Enabling Processing of SOCKS Traffic, on page 100
- Configuring the SOCKS Proxy, on page 100
- Creating SOCKS Policies, on page 101

Overview of SOCKS Proxy Services

The Secure Web Appliance includes a SOCKS proxy to process SOCKS traffic. SOCKS policies are the equivalent of access policies that control SOCKS traffic. Similar to access policies, you can make use of Identification Profiles to specify which transactions are governed by each SOCKS policy. Once SOCKS policies are applied to transactions, routing policies can then govern routing of the traffic.

Note the following regarding the SOCKS proxy:

- The SOCKS protocol only supports direct forward connections.

- The SOCKS proxy does not support (will not forward to) upstream proxies.
- The SOCKS proxy does not support scanning services, which are used by Application Visibility and Control (AVC), Data Loss Prevention (DLP), and malware detection.
- The SOCKS proxy does not support policy tracing.
- The SOCKS proxy does not decrypt SSL traffic; it tunnels from client to server.

Enabling Processing of SOCKS Traffic

Before you begin

Enable the Web Proxy.

Procedure

Step 1 Choose **Security Services** > **SOCKS Proxy**.
Step 2 Click **Edit Settings**.
Step 3 Select **Enable SOCKS Proxy**.
Step 4 **Submit** and **Commit** Changes.

Configuring the SOCKS Proxy

Procedure

Step 1 Choose **Security Services** > **SOCKS Proxy**.
Step 2 Click **Edit Settings**.
Step 3 Select **Enable SOCKS Proxy**.
Step 4 Configure the basic and advanced SOCKS Proxy settings.

SOCKS Proxy	Enabled.
SOCKS Control Ports	Ports that accept SOCKS requests. Default is 1080.
UDP Request Ports	UDP ports on which the SOCKS server should listen. Default is 16000-16100.
Proxy Negotiation Timeout	Time to wait (in seconds) to send or receive data from a SOCKS client in the negotiation phase. Default is 60.
UDP Tunnel Timeout	Time to wait (in seconds) for data from a UDP client or server before closing the UDP tunnel. Default is 60.

Creating SOCKS Policies

Procedure

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

Step 2 Click **Add Policy**.

Step 3 Assign a name in the **Policy Name** field.

Note
Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 (Optional) Add a description.

Step 5 In the **Insert Above Policy** field, choose where in the SOCKS policies table to insert this SOCKS policy.

Note
When configuring multiple SOCKS policies, determine a logical order for each policy. Order your policies to ensure that correct matching occurs.

Step 6 In the **Identities and Users** section, choose one or more Identities to apply to this policy group.

Step 7 (Optional) Expand the Advanced section to define additional membership requirements.

Proxy Ports	The port configured in the browser. (Optional) Define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port. **Note** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the SOCKS policy group level.
Subnets	(Optional) Define policy group membership by subnet or other addresses. You can choose to use the **addresses** that may be **defined** with the associated **Identity**, or you can enter **specific addresses** here. **Note** If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity's addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.
Time Range	(Optional) Define policy group membership by time range: **a.** Select a time range from the **Time Range** field. **b.** Specify whether this policy group should apply to the times inside or outside the selected time range.

Step 8 Submit and Commit Changes.

What to do next

- (Optional) Add an Identity for use with SOCKS Policies.
- Add one or more SOCKS Policies to manage SOCKS traffic.

Troubleshooting Intercepting Requests

- URL Categories Do Not Block Some FTP Sites
- Large FTP Transfers Disconnect
- Zero Byte File Appears On FTP Servers After File Upload
- Unable to Route FTP Requests Via an Upstream Proxy
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication
- User Matches Global Policy for HTTPS and FTP over HTTP Requests