Common Administrative Tasks

This chapter contains the following sections:

Performing Administrative Tasks

You can perform most system administration tasks by using the System Administration menu in the graphical user interface (GUI). Some system administration features, however, are available only in the command-line interface (CLI).

In addition, you access the status-monitoring features of the appliance on the Monitor menu, which is described in chapter Monitoring System Status

> **Note**   Several of the features or commands described in this chapter can affect routing precedence. For more information, see IP Addresses, Interfaces, and Routing.

Cisco Content Security Management Appliances Licensing

Working with Feature Keys

Keys are specific to the serial number of your appliance and specific to the feature that you enable. You cannot reuse a key from one system on another system.

To perform the tasks described in this section from the command-line prompt, use the featurekey command.

To	Do This
• View all active feature keys for the appliance • View any feature keys that are pending activation • Search for new keys that have been issued • Install feature keys manually • Activate feature keys	Select **Management Appliance > System Administration > Feature Keys**. To add a new feature key manually, paste or enter the key into the Feature Key field and click **Submit Key.** An error message appears if the feature is not added (for example, if the key is incorrect); otherwise, the feature key is added to the list. If the appliance is configured to automatically download and install new keys as they are issued. the Pending Activation list is always empty.
Enable or disable automatic download and activation of feature keys	Select **Management Appliance > System Administration > Feature Keys Settings** By default, the appliance periodically checks for new keys.
Renew expired feature keys	Contact your Cisco representative

Virtual Appliance Licensing and Feature Keys

For information about appliance behavior upon license and feature key expiration, see the *Cisco Content Security Virtual Appliance Installation Guide* available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html

To view license information, use the show license command in the command-line interface (CLI.)

Smart Software Licensing

Overview

Smart Software Licensing enables you to manage and monitor Cisco Content Security Management 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.

- 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 Cisco Smart Software Manager Satellite.

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 classical licenses (traditional) should migrate their classical licenses to smart licenses.

  See https://video.cisco.com/detail/video/5841741892001/ convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic.

- 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-> 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.

License Reservation

You can reserve licenses for features enabled in Secure Email and Web Manager without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Email and Web Manager in a highly secured network environment with no communication to the Internet or external devices.

The feature licenses can be reserved in any one of the following modes:

- **Specific License Reservation (SLR)** – use this mode to reserve licenses for individual features (for example, 'Mail Handling') for a given time-period.

- **Permanent License Reservation (PLR)** – use this mode to reserve licenses for all features permanently.

For more information on how to reserve the licenses in Secure Email and Web Manager, see .

Device Led Conversion

After you register Secure Email and Web Manager with smart licensing, all existing, valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal.

Note   The DLC process is initiated if Secure Email and Web Manager contains valid feature licenses.

Note   After the DLC process is complete, you will not be able to convert the smart licenses to classic licenses. Contact Cisco TAC for assistance.

Note   The DLC process takes approximately an hour to complete.

You can view the status of the DLC process – 'success' or 'failed' in any one of the following ways:

- Device Led Conversion status field under the 'Smart Software Licensing Status' section in the **System Administration** > **Smart Software Licensing** page of the web interface.

- Conversion Status entry in the license_smart > status sub command in the CLI.

Note   When the DLC process fails, the system sends a system alert that details the reason for the failure. You need to fix the issue and then use the license_smart > conversion_start sub command in the CLI to manually convert the classical licenses to smart licenses.

Note   The DLC process is applicable only for classic licenses and not for the SLR or PLR modes of license reservation.

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 6
Step 2	Register the appliance with Cisco Smart Software Manager	Registering the Appliance with Cisco Smart Software Manager, on page 6
[Optional] Step 3	Reserve the feature licenses in Secure Email and Web Manager, if required.	Reserving Feature Licenses, on page 9
Step 4	Request for licenses (feature keys)	Requesting for Licenses, on page 7

Enabling Smart Software Licensing

Step 1   Choose **Managed Appliance > 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.

Note   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.

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.

Step 1   Go to **Managed Appliance > 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.

  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 5   Switch back to your appliance and paste the Product Instance Registration Token.

Step 6   Click **Register**.

Step 7   On the Smart Software Licensing page, you can check the Reregister this product instance if it is already registered check box to reregister your appliance. See Reregistering the Appliance with Smart Cisco Software Manager , on page 8.

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.

✎

Note   After you enabled smart software licensing and registered your content security gateway with the Cisco Smart Software Manager, the Cisco Cloud Services portal is automatically enabled and registered on your content security gateway.

Requesting for Licenses

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

Step 1   Choose **Management Appliance > 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**.

Note   By default the license for Mail Handling is available. You cannot activate, deactivate, or release this license. There is no evaluation period or out of compliance for Mail Handling license.

What to do next

When the licenses are overused or expired, they will go to 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

Step 1   Choose **Management Appliance > 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**.

Note   You cannot release the license for Mail Handling.

Deregistering the Appliance from Smart Cisco Software Manager

Step 1   Choose **Management Appliance > 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

Step 1   Choose **Management Appliance > 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 6 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 6 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.

Step 1   Choose **Management Appliance > 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**.

Reserving Feature Licenses

- Enabling License Reservation, on page 9

- Registering License Reservation, on page 10

- Updating License Reservation, on page 11

- Removing License Reservation, on page 12

- Disabling License Reservation, on page 13

Enabling License Reservation

Before you begin

Make sure you have already enabled the Smart Licensing mode in Secure Email and Web Manager.

Note   You can also enable the license reservation using the `license_smart` > `enable_reservation` sub command in the CLI. For more information, see the 'Smart Software Licensing' section in 'The Commands: Reference Examples' chapter of the CLI Reference Guide.

Step 1 Go to **System Administration** > **Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Select the **Specific/Permanent License Reservation** option.

Step 3 Click **Confirm**.

The license reservation (SLR or PLR) is enabled in Secure Email and Web Manager.

What to do next

- You need to register the license reservation. For more information, see Registering License Reservation, on page 10.

- You can disable the license reservation in Secure Email and Web Manager, if required. For more information, see Disabling License Reservation, on page 13.

Registering License Reservation

Before you begin

Make sure you have already enabled the required license reservation (SLR or PLR) in Secure Email and Web Manager.

Note You can also register the feature licenses using the `license_smart` > `request_code` and `license_smart` > `install_authorization_code` sub commands in the CLI.

Step 1 Go to **System Administration** > **Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Click **Register**.

Step 3 Click **Copy Code** to copy the request code.

Note You need to use the request code in the CSSM portal to generate an authorization code.

Note A system alert is sent every 24 hours to indicate that you need to install an authorization code.

Step 4 Click **Next**.

Note The request code is canceled when you click the Cancel button. You cannot install the authorization code (generated in the CSSM portal) in Secure Email and Web Manager. Contact Cisco TAC to assist you in removing the reserved license after the request code is canceled in Secure Email and Web Manager.

Step 5 Go to the CSSM portal to generate an authorization code to reserve licenses for specific or all features.

Note For more information on how to generate an authorization code, go to the *Inventory: License Tab > Reserve Licenses* section of the Help documentation at Smart Software Licensing Online Help (cisco.com).

Step 6 Paste the authorization code obtained from the CSSM portal in Secure Email and Web Manager in any one of the following ways:

- Select the **Copy and Paste authorizationc code** option and paste the authorization code in the text box under the 'Copy and Paste authorization code' option.

• Select the **Upload authorization code from the system** option and click **Choose File** to upload the authorization code.

Step 7   Click **Install Authorization Code**.

> **Note**   After you install the authorization code, you receive a system alert that indicates Smart Agent successfully installed the license reservation.

The license reservation (SLR or PLR) is registered in Secure Email and Web Manager. In SLR, only the reserved license is moved to the 'Reserved in Compliance' state. For PLR, all licenses in Secure Email and Web Manager are moved to the 'Reserved in Compliance' state.

> **Note**   The 'Reserved In Compliance:' state indicates that Secure Email and Web Manager is authorized to use the license.

What to do next

• [Applicable for SLR only]: You can update the license reservation, if required. For more information, see Updating License Reservation, on page 11.

• [Applicable for SLR and PLR]: You can remove the license reservation, if required. For more information, see Removing License Reservation, on page 12.

• You can disable the license reservation in Secure Email and Web Manager, if required. For more information, see Disabling License Reservation, on page 13.

Updating License Reservation

You can reserve license for a new feature or modify the existing license reservation for a feature.

> **Note**   You can only update the Specific License reservations and not the Permanent License reservations.

> **Note**   You can also update the license reservation using the `license_smart` > `reauthorize` sub command in the CLI.

Step 1   Go to the CSSM portal to generate an authorization code to update the already reserved licenses.

> **Note**   For more information on how to generate an authorization code, go to the *Inventory: Product Instances Tab > Update Reserved Licenses* section of the Help documentation at Smart Software Licensing Online Help (cisco.com).

Step 2   Copy the authorization code obtained from the CSSM portal.

Step 3   Go to **System Administration** > **Smart Software Licensing** page in Secure Email and Web Manager.

Step 4   Select **Reauthorize** from the 'Action' drop-down list and click **GO**.

Step 5   Paste the authorization code obtained from the CSSM portal in Secure Email and Web Manager in any one of the following ways:

   - Select the **Copy and Paste authorization code** option and paste the authorization code in the text box under the 'Copy and Paste authorization code' option.

   - Select the **Upload authorization code from the system** option and click **Choose File** to upload the authorization code.

Step 6   Click **Re-authorize**.

Step 7   Click **Copy Code** to copy the confirmation code.

   Note   You need to use the confirmation code in the CSSM portal to update the license reservations.

Step 8   Click **OK**.

Step 9   Add the confirmation code obtained from Secure Email and Web Manager in the CSSM portal.

   Note   For more information on how to add the confirmation code, go to the *Inventory: Product Instances Tab > Update Reserved Licenses* section of the Help documentation at Smart Software Licensing Online Help (cisco.com).

The license reservations are updated. The reserved license is moved to the 'Reserved in Compliance' state. The licenses that are not reserved are moved to the "Not Authorized" state.

Note   The 'Not Authorized' state indicates that Secure Email and Web Manager has not reserved any feature licenses.

What to do next

   - [Applicable for SLR and PLR]: You can remove the license reservation, if required. For more information, see Removing License Reservation, on page 12.

   - You can disable the license reservation in Secure Email and Web Manager. For more information, see Disabling License Reservation, on page 13 .

Removing License Reservation

You can remove the specific or permanent license reservation for the features enabled in Secure Email and Web Manager.

Note   You can also remove the license reservation using the `license_smart` > `return_reservation` sub command in the CLI.

Step 1   Go to **System Administration** > **Smart Software Licensing** page in Secure Email and Web Manager.

Step 2   Select **Return code** from the 'Action' drop-down list and click **GO**.

Step 3   Click **Copy Code** to copy the return code.

      Note   You need to use the return code in the CSSM portal to remove the license reservations.

      Note   An alert is sent to the user to indicate that Smart Agent successfully generated the return code for the product.

Step 4   Click **OK**.

Step 5   Add the return code obtained from Secure Email and Web Manager in the CSSM portal.

      Note   For more information on how to add the return code, go to the *Inventory: Product Instances Tab > Removing a Product Instance* section of the Help documentation at Smart Software Licensing Online Help (cisco.com).

The licenses reserved in Secure Email and Web Manager are removed and moved to the evaluation period.

Disabling License Reservation

You can disable the license reservation in Secure Email and Web Manager.

✎

Note   You can also disable the license reservation using the `license_smart` > `disable_reservation` sub command in the CLI.

Step 1   Go to **System Administration** > **Smart Software Licensing** page in Secure Email and Web Manager.

Step 2   Click **Change Type** under the 'Registration Mode' field.

Step 3   Click **Submit** in the 'Change registration mode' dialog box.

The license reservation is disabled on Secure Email and Web Manager.

Updating Smart Agent

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

Step 1   Choose **Management Appliance > 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

- [Applicable for SLR and PLR only]: Authorization code is installed after generation of request code.

- [Applicable for SLR and PLR only]: Authorization code is installed successfully.

- [Applicable for SLR and PLR only]: Return code is generated successfully.

- [Applicable for SLR only]: Reservation of specific feature license is expired.

- [Applicable for SLR only]: Frequency of alerts sent before expiry of specific feature license reserved.

Command Line Interface

license_smart

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

```
mail.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

```
mail.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%0AMDEzNTR8WlpCQ1lMbGGVMQWRx
OXhuenN4OWZDdktFckJLQzF5V3VVIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

Example: Status of Smart Licensing

```
mail.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

```
mail.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
Mail Handling	In Compliance
Content Security Management Master ISQ	In Compliance

Example: Setting the Smart Transport URL

```
mail.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.

```
mail.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. Content Security Management Centralized Tracking	Not Requested
2. Content Security Management Master ISQ	Not requested

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

Example: Releasing Licenses

```
mail.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. Content Security Management Centralized Tracking	In Compliance
2. Content Security Management Master ISQ	In Compliance

Example - Enabling and Registering License Reservation

In this example, you can use the `license_smart > enable_reservation` sub command to enable and register the license reservation on Secure Email and Web Manager.

```
mail.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.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Email and Web Manager.
[]> enable_reservation

Would you like to reserve license, then type "Y" else type "N" [Y/N] []> yes


License Reservation is enabled for the following machines:
mail1.example.com

License Reservation is enabled

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
[]> request_code


The generation of the request code is initiated...

Copy the request code obtained on your Secure Email and Web Manager and paste it in the
Cisco Smart Software Manager portal to select the required license

Request code: CD-ZSMA:BD20B624E904-B7HCL9scQ-DD

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

```
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Email and Web Manager.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web
Manager.
[]> install_authorization_code
1. Paste via CLI
2. Import the Authorization Code from a file

How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>7b654af6-9d60-46f5-a79-………………………………….PS/o+6</signature><udi>P:SMA,S:BE30B124E904
</udi></specificPLR>
^D
The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]>
```

Example - Updating License Reservation

In this example, you can use the `license_smart > reauthorize` sub command to reserve license for a new feature or modify the existing license reservation for a feature.

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]> reauthorize

1. Paste via CLI
2. Import the Authorization Code from a file
How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>6b684af8-4d20-42f5-ab89-…………………………………..</authorizationCode><signature>
MEYCIDS7IZQuLvMMmiXMH2eZOwf7cy6rjgc7kxBIja</signature><udi>P:SMA,S:BD660B174E904
</udi></specificPLR>
```

```
^D

The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager.

Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart Software
 Manager portal to update the specific reservation.

Confirmation code: 1f87b235

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]>
```

Example - Removing License Reservation

In this example, you can use the `license_smart` > `return_reservation` sub command to remove the specific
or permanent license reservation for the features enabled in Secure Email and Web Manager.

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]> return_reservation

After you return the license reservation, you cannot use any of the product features, if
the evaluation period has exceeded 90 days. After the 90 days
evaluation period, you must register your product with Cisco Smart Software Manager to
continue to use the product features. [N]> yes

The generation of the return code is initiated...

Copy the return code obtained on your Secure Email and Web Manager and paste it in the Cisco
 Smart Software Manager portal.

Return Code: C97xKY-otSY8D-ertAf-v-fbEu5q-APo

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
[]>

mail1.example.com>
```

Example - Disabling License Reservation

In this example, you can use the `license_smart` > `disable_reservation` sub command to disable the license reservation on Secure Email and Web Manager .

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Email and Web Manager.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web
Manager.
[]> disable_reservation


A request code for the specific or permanent reservation is generated on your Secure Email
 and Web Manager. If you want to disable the reservation, it cancels the request code.


Do you want to disable the specific or permanent reservation? [Y/N] []> yes

License Reservation is disabled for the following machines:
mail1.example.com

License Reservation is disabled

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.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Email and Web Manager.
[]>
```

Example - Enabling Device Led Conversion Process Manually

In this example, you can use the `license_smart` > `conversion_start` sub command to enable the Device Led Conversion (DLC) process manually on Secure Email and Web Manager.

```
mail.example.com > license_smart

Deregister Secure Email and Web Manager from the Cisco Smart Software Manager portal to
enable the license reservation

Choose the operation you want to perform:
- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart Licensing
[]> conversion_start
```

```
Do you want to start the process of converting your classic license keys to smart software
 licensing[Y/N]? []> yes
```

show_license

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: mail.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
Mail Handling	In Compliance
Content Security Management Master ISQ	In Compliance

cloudserviceconfig

Description

The **cloudserviceconfig** command is used to:

- This command is applicable only in Smart Licensing mode.

- Enable the Cisco Cloud Services portal on your appliance.

- Disable the Cisco Cloud Services portal on your appliance.

- Register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.

- Automatically register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.

- Deregister your Cisco Secure Email and Web Manager from the Cisco Cloud Services portal.

- Choose the Cisco Secure Cloud server to connect your appliance to the Cisco Cloud Services portal.

- Fetch the certificate and key from talos server used by the updater.

- Enable Cisco SecureX (or Cisco Threat Response) on your Cisco Secure Email and Web Manager. You must perform this using the General configuration settings.

- Disable Cisco SecureX or Cisco Threat Response on your Cisco Secure Email and Web Manager. You must perform this using the General configuration settings.

Usage

- **Commit**: This command does not require a 'commit.

- **Batch Command**: This command supports a batch format.

Example: Enabling Cisco Cloud Services on Appliance

In the following example, you can use the cloudserviceconfig > enable sub command to enable Cisco Cloud Services on your email gateway.

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

```
mail1.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.
mail1.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 GMT
mail1.example.com >
```

Example: Disabling Cisco Cloud Services on Appliance

In the following example, you can use the cloudserviceconfig > disable sub command to disable Cisco Cloud Services on your appliance.

```
mail1.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.
mail1.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
mail1.example.com >
```

Example: Registering Content Security Gateway with Cisco Cloud Services Portal

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is stage-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 Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> REGISTER

Enter a registration token key to register your appliance with the Cisco Cloud Service
portal.
[]> 90a92909fc3b1be666f180621146fea3

The appliance registration is in progress.
```

Example: Deregistering Content Security Gateway from Cisco Cloud Services Portal

In the following example, you can use the cloudserviceconfig > deregister sub command to deregister your appliance from the Cisco Cloud Services portal.

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is stage-api-sse.cisco.com

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.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> 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 Content Security Management appliance deregistration is in progress.
```

Example: Choosing Cisco Secure Cloud Server to connect Content Security Gateway 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 your email gateway to the Cisco Cloud Services portal.

```
mail1.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.
mail1.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 Performing AutoRegistration using CLI for Smart Licensing

In the following example, you can use the command to display after you register once in smart licensing, the appliance performs auto registration in backend. If auto registration fails, you can see command for autoregistration in the CLI.

```
Autoregister Success/ and failure
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
```

```
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> AUTOREGISTER

The appliance failed to auto-register with the Cisco Cloud Service portal.
Reason: A request to generate a Smart Licensing payload from Cisco Smart Software Manager
failed.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> AUTOREGISTER

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

Example Download a Certificate and Key

In the following example, you can use the command to Fetch the certificate and key used by the updater from the TALOS server.

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com


Choose the operation you want to perform:
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> FETCHCERTIFICATE

Current Cisco Talos certificate is valid for 172 days

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

The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com
```

Example Client Certificate cloudserviceconfig

In the following example, you can use the command to upload the certificate and the key.

```
[]> clientcertificate

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.
```

```
-----BEGIN CERTIFICATE-----
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZFwzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJ
MIIDYzCCAkugAwIBAgIDCMvdMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYDVQQGEwJV
GlyOpFkbHg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
UzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNV
BAoTEkNpc2NvIFN5c3RlbXMgSW5jLjERMA8GA1UECxMIU2VjdXJpdHkxGzAZBgNV
BAMTElN0YWdlIEtleW1hc3RlciBDQTAeFw0xOTAyMTkwMzU3MzhaFw0yMjA0MDIw
2jgYEzrhGtZmx+hpAmHi1i8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qguqh7/bn6u8R9EMjzu4V+Rn54JZMTcJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIMP2SrqktLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGlyrQs6HIqIvMT
MzU3MzhaMEkxHTAbBgkqhkiG9w0BCQEWDnRlc3RAY2lzY28uY29tMRgwFgYDVQQD
DA9WTE5TTUExMjM0NTY3ODkxDjAMBgNVBAoMBWNpc2NvMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZFwzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJ
uT6K+qrTusUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTX1TXcY516jS
GlyOpFkbHg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
HRMEAjAAMAsGA1UdDwQEAwIHgDANBgkqhkiG9w0BAQsFAAOCAQEAOKYfiZfJg4rM
IWM73wz8u7Wtj97E6rGVgsj0D54fOKF6DmqHfyqPCuXns0Fl8nL1Da3ogslLwIrS
d5a1lfj/2r6NfbN0hjKN7/5PGBtcRyMDi86aUBoqahNmgCwDKTTJgoVTO0//a+Ca
2jgYEzrhGtZmx+hpAmHi1i8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qguqh7/bn6u8R9EMjzu4V+Rn54JZMTcJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIMP2SrqktLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGlyrQs6HIqIvMT
J1SwgurFWg==
-----END CERTIFICATE-----
^D

Paste Private Key.
Press CTRL-D on a blank line when done.
-----BEGIN RSA PRIVATE KEY-----
ZzSWnNAdMjtobo6dx1iMfbaWDd1Um+PIEiBXEy5z74btukQUGTI0DXsCgYEA36q3
gH/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB9OlPLkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqlZbFPHbddQGTIbCV4T1hyEcjNbyD2SSCIv5gxF70TBR5qD
14HT3PPt4HXpgcFw70NofNSnpNm63OhkW4SBNgkCgYEAs8Y4VMWA2WWEAFZhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVTk7kCEZLG7+vqzboSORPi98QXY1o/aBNhg
MIIEowIBAAKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJcVPlrZFw
NEnrtal7WnKNZz96nC1kaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
zTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1SarY6DhYNw
BHXHikhkl+8ibEB2K+XlQUPSCy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy
f3DsaHI6Yj7jYi4aI1ec7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkG58siV
Lt+psQKBgFjRVfNddwgcX5QaQXopYJWa/HFnWgH7jXgVFeR1Q9smq7L0Yk39GrxT
8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNLMpES7AmQ
itef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJuT6K+qrT
usUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTX1TXcY516jSGlyOpFkb
Hg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABAoIBAE+jQNqJoEmEwSvO
ENqmwcjYE5y3kK+rEt49ALlrS2dAunaZtq1Sl6Tr1XaMzgFJ07/JxDEnXuMQlqVL
KaTwWT4BTmvxMqVMdIH6GY0+99ShMT08OxVe3tnXc+m2c8nmX5dftLkcYC5yXNVb
bvtD2BR4eupNOrvj1N5P/+sYcNc4I7ZAAheGfhLc4oDTMiHIE5g6Dyvh7j+WIi9y
bpoU99fFV7jcGtql5AOUQtLUtuO6d1tk2WL1+m2qsX7uMkQ5ddM9vGbTRg0IkjRb
PVpshAK5j/RsQCUN6LlRq+SY7y18CllZ4MYWXu754KqMloK8UDarI+dKISyVskfe
69lNQ2ECgYEA5zLHTykFOA349MyliSQxIE6YsVL8tc1Ryf/PB69OoTY+vKUcmCZp
TzLPuEEbyzndAIW7FagVG5aYYFXD0kcUE9LUCCTl5bTOiYJM0YCGgsHnBpqUI7yI
ZzSWnNAdMjtobo6dx1iMfbaWDd1Um+PIEiBXEy5z74btukQUGTI0DXsCgYEA36q3
gH/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB9OlPLkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqlZbFPHbddQGTIbCV4T1hyEcjNbyD2SSCIv5gxF70TBR5qD
14HT3PPt4HXpgcFw70NofNSnpNm63OhkW4SBNgkCgYEAs8Y4VMWA2WWEAFZhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVTk7kCEZLG7+vqzboSORPi98QXY1o/aBNhg
NEnrtal7WnKNZz96nC1kaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
XEDpdHDalZZFpGDrf+wZraECgYB3cT1pe/Dnq43Aji+pEUuLdjIVp9Y9Gepk2XZU
BHXHikhkl+8ibEB2K+XlQUPSCy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy
```

```
f3DsaHI6Yj7jYi4aI1ec7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkG58siV
Lt+psQKBgFjRVfNddwgcX5QaQXopYJWa/HFnWgH7jXgVFeR1Q9smq7L0Yk39GrxT
Gu2acBalPQR474nW9394XqmPTJ5tYhf80nmT7JRwYEgE2C/flnDDea9YFoiX/yP3
fD4kLyDPgQ8utQwK7X7aK1PxdEIsXKZLcR6FoeT0wQj31gCG2igH
-----END RSA PRIVATE KEY-----
^DCertificate and key are stored successfully
```

Example: Enabling Cisco SecureX or Cisco Threat Response on Content Security Gateway

In the following example, you can use the clouderviceconfig > enablesecurecx sub command to enable Cisco SecureX or Cisco Threat Response on your appliance.

```
Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SECUREX - Configure Cisco SecureX/ Threat Response feature on your appliance
[]> SECUREX

The Cisco SecureX / Threat Response feature is currently disabled on your appliance.
Would you like to enable Cisco SecureX/ Threat Response feature [Y]>

Cloud Service is not enabled.
        Enter "cloudserviceconfig" for enabling Cisco Cloud service.
```

Example: Disabling Cisco SecureX or Cisco Threat Response from Content Security Gateway

In the following example, you can use the cloudserviceconfig >disablesecurex sub command to disable Cisco SecureX or Cisco Threat Response on your appliance.

```
sma> generalconfig


Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SECUREX - Configure Cisco SecureX/ Threat Response feature on your appliance
[]> SECUREX

The Cisco SecureX / Threat Response feature is currently enabled on your appliance.
Would you like to disable Cisco SecureX/ Threat Response feature [N]> Y

The Cisco SecureX / Threat Response feature is currently disabled on your appliance.
The Cisco Cloud Service is currently disabled on your appliance.
```

Smart Software Licensing Key Points for AsyncOS 14.0

- Cisco SecureX will be automatically enabled when you enable Cloud Services and Cisco Securex will be disabled when Cloud Services is disabled.

- Cisco SecureX and Cisco Threat Response option is now changed in the Web UI and you can enable or disable Cisco SecureX and Cisco Threat Response from **System Administration > General Settings**. You can also perform the same from CLI by using the **generalconfig** command.

- Cloud Service will be enabled and Appliance(SSE) will be registered automatically when smart software licensing is enabled and registered.

- In Classic Mode, Cloud Service will be in disabled state by default. You need to enable it manually and Cisco SecureX and Cisco Threat Response will be enabled. You must enable smart licensing mode for auto-registration to occur.

- After Enabling Smart Software Licensing, the Smart Agent is started and once the registration is completed, Cloud services will be enabled.

• You cannot perform an SSE auto registration when smart license is with evaluation mode.

Performing Maintenance Tasks Using CLI Commands

The operations and commands described in this section enable you to perform maintenance-related tasks on the Security Management appliance. This section describes the following operations and commands:

- shutdown
- reboot
- suspend
- suspendtransfers
- resume
- resumetransfers
- resetconfig
- version

Shutting Down the Security Management Appliance

To shut down your Security Management appliance, do the folliwng:

- Use the **Management Appliance > System Administration > Shutdown/Reboot** page.

  or

- Use the `shutdown` command at the command-line prompt.

Shutting down an appliance exits AsyncOS, which allows you to safely power down the appliance. You may restart the appliance at a later time without losing any messages in the delivery queue. You must enter a delay for the appliance to shut down. The default delay is 30 seconds. AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections.

Rebooting the Security Management Appliance

To reboot your Security Management appliance, use the Shutdown/Reboot page available on the System Administration menu in the GUI, or use the r eboot command in the CLI.

Rebooting your appliance restarts AsyncOS, which allows you to safely power down and reboot the appliance. You must enter a delay for the appliance to shut down. The default delay is 30 seconds. AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections. You may restart the appliance without losing any messages in the delivery queue.

Taking the Security Management Appliance Out of Service

If you want to take the appliance offline, for example to perform system maintenance, use one of the following commands:

Command	Description	Persistence
suspend	• Suspends transfer of quarantined messages from the Email Security appliance to the Security Management appliance. • Suspends delivery of messages released from quarantines. • Inbound email connections are not accepted. • Outbound email delivery is halted. • Log transfers are halted. • The CLI remains accessible.	Persists after reboot.
suspendtransfers	Suspends transfer of reporting and tracking data from managed email and web security appliances to the content security management appliance. This command also suspends receiving of quarantined messages from Email Security appliances. Use this command when preparing to bring a backup appliance into service as the primary appliance.	Persists after reboot.

You must enter a delay for the appliance when using these commands. The default delay is 30 seconds. AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections. If there are no open connections, service is suspended immediately.

To re-activate services that were halted by the suspend or suspendtransfers commands, use the resume or resumetransfers commands, respectively.

To determine the current online/suspended status of the management appliance, select **Management Appliance > System Administration > Shutdown/Reboot** in the web interface.

See also:

• "Suspending Email Delivery," "Resuming Email Delivery," "Suspending Receiving," and "Resuming Receiving" in the documentation or online help for your Email Security appliance.

CLI Examples: suspend and suspendtransfers Commands

```
sma.example.com> suspend
Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
sma.example.com>
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

Resuming from a Suspended State

The resume command returns the appliance to normal operating state after using the suspend or suspenddel command.

The resumetransfers command returns the appliance to normal operating state after using the suspendtransfers command.

CLI Examples: resume and resumetransfers Commands

```
sma.example.com> resume
Receiving resumed.
Mail delivery resumed.
sma.example.com>
sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

Resetting the Configuration to Factory Defaults

When physically transferring the appliance, or as a last resort for solving configuration issues, you may want to reset the appliance to factory defaults.

⚠️

Caution   Resetting the configuration will disconnect you from the CLI, disable services that you used to connect to the appliance (FTP, Telnet, SSH, HTTP, HTTPS), and remove user accounts.

To	Do This
• Reset all configurations to factory defaults • Clear all reporting counters But • Retain log files • Retain quarantined messages	1. Ensure that you can connect to the appliance after reset using the default admin user account and passphrase, either to the CLI using the serial interface or to the Management port using the default settings. See chapter Setup, Installation, and Basic Configuration for information about accessing an appliance having default settings. 2. Suspend service on the appliance. 3. Select **Management Appliance > System Administration > Configuration File** and click **Reset**. **Note** After resetting, the appliance automatically returns to the online state. If mail delivery was suspended before reset, delivery will be attempted again after the reset.
• Reset all configurations to factory defaults • Remove all data	Use the `diagnostic > reload` CLI command. **Caution** This command is NOT the same as the similar command used on a Cisco router or switch.

The resetconfig Command

```
mail3.example.com> suspend
Delay (seconds, minimum 30):
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com> resetconfig
Are you sure you want to reset all configuration values? [N]> Y
All settings have been restored to the factory default.
```

Displaying the Version Information for AsyncOS

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliances > Centralized Services > System Status**.

Step 3 Scroll to the bottom of the page and look under Version Information to see the version of AsyncOS that is currently installed.

Additionally, you can use the **version** command at the command-line prompt.

Enabling Remote Power Cycling

The ability to remotely reset the power for the appliance chassis is available only on 80- and 90- 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.

Before you begin

- Cable the dedicated Remote Power Cycle (RPC) port directly to a secure network. For information, see hardware documentation for your model, available from the location listed in Documentation.

- 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 the CLI reference guide.

Step 1   Use SSH, telnet, 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

[Remotely Resetting Appliance Power](#)

Monitoring System Health Using SNMP

AsyncOS supports system status monitoring via Simple Network Management Protocol (SNMP) versions v1, v2, and v3.

> • To enable and configure SNMP, use the `snmpconfig` command in the command-line interface.
>
> • MIBs are available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html use the latest available files.
>
> • The use of SNMPv3 with passphrase authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The `snmpconfig` command "remembers" this phrase the next time you run the command.
>
> • When setting up SNMP to monitor connectivity:
>
> When entering the url-attribute while configuring a connectivityFailure SNMP trap, determine whether the URL is pointing at a directory or a file.
>
> > • If it is a directory, add a trailing slash (/)
> >
> > • If it is a file, do not add a trailing slash

- Additional information about using SNMP with AsyncOS is available in the online help for your web or email security appliance.

Example: snmpconfig Command

```
sma.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: sma.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]> SMA.Administrator@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: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
sma.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

Backing Up Security Management Appliance Data

What Data Is Backed Up

You can choose to back up all data, or any combination of the following data:

- Spam quarantine, including messages and meta data
- Centralized policy, virus, and outbreak quarantines, including messages and meta data
- Email tracking (message tracking), including messages and meta data
- Web tracking
- Reporting (Email and Web)
- Safelist/blocklist

After the data transfer is finished, the data on the two appliances will be identical.

Configurations and logs are not backed up using this process. To back up those items, see Other Important Backup Tasks , on page 41.

Each backup after the first backup copies only the information generated since the last backup.

Restrictions and Requirements for Backups

Be sure to address the following restrictions and requirements before you schedule a backup:

Restriction	Requirement
AsyncOS version	The AsyncOS version of the source and target Security Management appliances must be the same. If there is a version incompatibility, upgrade appliances to the same release before scheduling a backup.
Target appliance on the network	The target appliance must be set up on the network. If the target appliance is new, run the System Setup Wizard to enter the necessary information. For instructions, see Setup, Installation, and Basic Configuration
Communication between source and target appliances	The source and target Security Management appliances must be able to communicate using SSH. Therefore: • Port 22 must be open on both appliances. By default, this port is opened when you run the System Setup Wizard. • The Domain Name Server (DNS) must be able to resolve the host names of both appliances using both A records and PTR records.
Target appliance must not be in service	Only the primary appliance should pull data from managed email and web security appliances. To ensure this, see Prevent the Target Appliance From Pulling Data Directly from Managed Appliances , on page 38. Also, cancel any scheduled configuration publishing jobs on the backup appliance.

Restriction	Requirement
Appliance capacity	The disk space capacity of the target appliance must be the same as or greater than the capacity of the source appliance. Disk space allocated to each type of data (reporting, tracking, quarantine, etc.) on the target appliance cannot be less than the corresponding allocation on the source appliance.
	You can schedule a backup from a larger source to a smaller target Security Management appliance as long as there is enough space on the target appliance for all of the data being backed up, for each type of data. If the source appliance is larger than the target appliance, you must reduce the space allocated on the source appliance to match the space available on the smaller target appliance.
	To view and manage disk space allocations and capacity, see Managing Disk Space , on page 79.
	For disk capacity of virtual appliances, see the *Cisco Content Security Virtual Appliance Installation Guide* .
Multiple, concurrent, and chained backups	Only one backup process can run at a time; a backup that is scheduled to run before a previous backup has been completed will be skipped and a warning sent.
	Data from a Security Management appliance can be backed up to a single Security Management appliance.
	Chained backup (a backup to a backup) is not supported.

Backup Duration

During a full initial backup, a backup of 800GB may take up to 10 hours. Daily backups, may take up to 3 hours each. Weekly and monthly backups may take longer. These numbers may vary.

After the initial backup, the backup process transfers only files that have changed since the last backup. Thus, subsequent backups should take less time than the initial backup. The time required for subsequent backups depends on the amount of data accumulated, how many files have changed, and to what extent the files have changed since the last backup.

Availability of Services During Backups

Backing up a Security Management appliance copies the active data set from the 'source' Security Management appliance to a 'target' Security Management appliance with minimum disruption on the originating 'source' appliance.

The phases of the backup process and their effect on the availability of services are as follows:

- Phase 1—Phase 1 of the backup process starts with the data transfer between the source and target appliances. During data transfer, services on the source appliance remain running, therefore data collection can still continue. However, services are shut down on the target appliance. Once the data transfer is complete from the source to target appliance, Phase 2 begins.
- Phase 2—When Phase 2 begins, services on the source appliance are shut down. Any differences that have collected during the data transfer between the source and target appliance since the initial shutdown are copied to the target appliance and services on both the source and the target appliances are returned to the state they were in when backup was initiated. This allows maintain maximum uptime on the source appliance and no data loss for either appliance.

During the backup, data availability reports may not work, and when viewing the message tracking results, the hostname for each message may be labeled as 'unresolved'.

If you try to schedule a report and forget that a backup is in progress, you can check the system status by choosing **Management Appliance > Centralized Services**. From this window you can see the warning at the top of the page that a system backup is in progress.

Interruption of a Backup Process

> **Note** If there is an unexpected reboot of the source appliance while a backup is being performed, the target appliance is unaware of this stoppage. You must cancel the backup on the target appliance.

If there is an interruption of the backup process and the backup process is not completed, the next time a backup is attempted, the Security Management appliance can start the backup process up from where it was stopped.

Canceling a backup in progress is not recommended, as the existing data will be incomplete and may not be usable until a subsequent backup is completed, especially if you receive an error. If you must cancel a backup in progress, be sure to run a complete backup as soon as possible to ensure that you always have a usable current backup.

Prevent the Target Appliance From Pulling Data Directly from Managed Appliances

Step 1 Access the command-line interface of the target appliance. For instructions, see Accessing the Command Line Interface.

Step 2 Run the `suspendtransfers` command.

Step 3 Wait for the prompt to reappear.

Step 4 Run the `suspend` command.

Step 5 Wait for the prompt to reappear.

Step 6 Exit the command-line interface of the target appliance.

Receiving Alerts About Backup Status

To receive alerts when backups are complete and be informed of any issues, configure the appliance to send you alerts of type System, severity Info. See Managing Alerts, on page 58.

Scheduling Single or Recurring Backups

You can schedule a single or recurring backup to occur at a predetermined time.

Note	A backup process will not start if there are any ongoing backups on the remote machine.

Before you begin

- Address the items in Restrictions and Requirements for Backups , on page 36.

- Make sure you disable two-factor authentication temporarily on the target appliance before you begin the backup process. Once the backup process is complete, you can enable two-factor authentication on the target appliance.

Step 1	Login, as administrator, to the command-line interface of the source appliance.
Step 2	At the command prompt, type **backupconfig**and press **Enter**.
Step 3	If the connection between source and target appliances is slow, turn on data compression:
	Type **setup** and enter **Y**.
Step 4	Type **Schedule** and press **Enter**.
Step 5	Type the IP address of the target Security Management appliance.
Step 6	Enter a meaningful name to identify the target appliance (up to 20 characters).
Step 7	Enter the admin user name and passphrase for the target appliance.
Step 8	Respond to prompts about which data you want to back up.
Step 9	To schedule a single backup, type **2** to Schedule a single backup and press **Enter**.
Step 10	To schedule a recurring backup:
	a) Type **1** to Setup Repeating Backup Schedule and press **Enter**.
	b) Choose the frequency for your periodic backup and press **Enter**.
Step 11	Type the specific date or day and time that you want the backup to start and press **Enter**.
Step 12	Type the name of the backup process.
Step 13	Verify that the backup was successfully scheduled: Type **View** and press **Enter** at the command prompt.
Step 14	See also Other Important Backup Tasks , on page 41.

Starting an Immediate Backup

Note	A backup process will not start if there are any ongoing backups on the target machine.

Before you begin

Meet all requirements in Restrictions and Requirements for Backups , on page 36.

Step 1	Login, as administrator, to the command-line interface of the source appliance.

Step 2   At the command prompt, type `backupconfig` and press **Enter**.

Step 3   If the connection between source and target appliances is slow, turn on data compression:

Type **setup** and enter **Y**.

Step 4   Type **Schedule** and press **Enter**.

Step 5   Type the IP address of the target Security Management appliance.

Step 6   Enter a meaningful name to identify the target appliance (up to 20 characters).

Step 7   Enter the admin user name and passphrase for the target appliance.

Step 8   Respond to prompts about which data you want to back up.

Step 9   Type **3** to Start a Single Backup Now and press **Enter**.

Step 10   Enter a meaningful name for the backup job.

The backup process begins in a few minutes.

Step 11   (Optional) To see the progress of the backup, type **Status** at the command-line prompt.

Step 12   See also Other Important Backup Tasks , on page 41.

Checking Backup Status

Step 1   Log in, as administrator, to the command-line interface of the primary appliance.

Step 2   At the command prompt, type **backupconfig** and press **Enter**.

To Check Status Of	Do This
A scheduled backup	Choose the View operation.
A backup in progress	Choose the Status operation.
	If you have configured alerts, check your email or see Viewing Recent Alerts , on page 60.

What to do next

Related Topics

Backup Information in Log Files , on page 40

Backup Information in Log Files

Backup logs record the backup process from start to finish.

Information about backup scheduling is in the SMA logs.

Related Topics

- Checking Backup Status , on page 40

Other Important Backup Tasks

Consider doing the following in order to prevent loss of items that are not backed up by the backup processes described in this section, and to speed setup of your replacement Security Management appliance in case of appliance failure:

- To save the settings from your primary Security Management appliance, see Saving and Importing Configuration Settings , on page 72. Save the configuration file to a safe location separate from your primary Security Management appliance.

- Save any Web Security appliance configuration files that you used to populate your Configuration Masters.

- To save log files from your Security Management appliance to an alternate location, see Log Subscriptions.

Additionally, you can set up a log subscription for Backup Logs. See Creating a Log Subscription in the GUI.

Making a Backup Appliance the Primary Appliance

If you are upgrading appliance hardware, or if you need to switch appliances for any other reason, use this procedure.

Before you begin

Review the information in Backing Up Security Management Appliance Data , on page 35.

Step 1 Save a copy of the configuration file from your old/primary/source appliance to a location that you can reach from the new appliance. See Saving and Importing Configuration Settings , on page 72.

Step 2 Run the System Setup Wizard on the new/backup/target appliance.

Step 3 Meet the requirements in Restrictions and Requirements for Backups , on page 36.

Step 4 Run a backup from the old/primary/source appliance. See instructions at Starting an Immediate Backup, on page 39.

Step 5 Wait for the backup to complete.

Step 6 Run the suspendtransfers and suspend commands on the old/primary/source appliance.

Step 7 Run a second backup to transfer last-minute data from the old/primary/source to the new/backup/target appliance.

Step 8 Import the configuration file into the new/backup/target appliance.

Step 9 Run the resumetransfers and resume commands on the new/backup/target appliance.

Do NOT run this command on the old/original primary/source appliance.

Step 10 Establish the connection between the new/backup/target appliance and the managed email and web security appliances:

Step 11 a) [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

b) Select **Management Appliance > Centralized Services > Security Appliances**.

c) Click an appliance name.

d) Click the **Establish Connection** button.

e) Click **Test Connection**.

f) Return to the list of appliances.

g) Repeat for each managed appliance.

Step 12 Verify that the new/target appliance is now functioning as the primary appliance:

Select **Management Appliance > Centralized Services > System Status** and check the status of data transfers.

Disaster Recovery on the Security Management Appliance

If your Security Management appliance unexpectedly fails, use the following procedure to restore security management services and your backed-up data, which you regularly save using the information in Backing Up Security Management Appliance Data , on page 35.

A typical appliance configuration might look as shown in the following figure:

Figure 1: Disaster Recovery: A Typical Environment
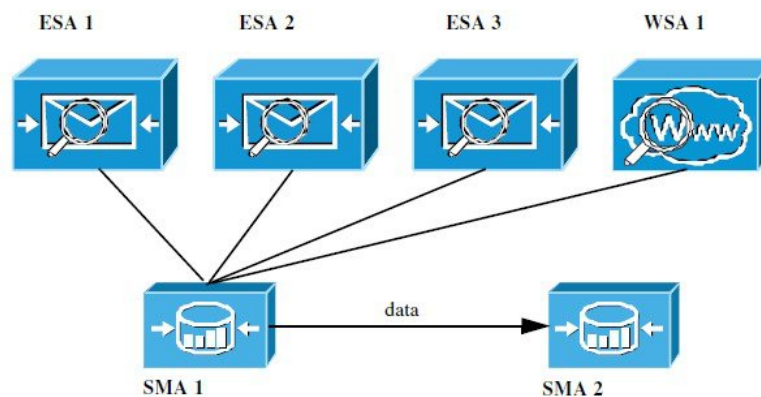
In this environment, SMA 1 is the primary Security Management appliance that is receiving data from ESAs 1-3 and WSA 1. SMA 2 is the backup Security Management appliance receiving backup data from SMA1.

In case of failure, you must configure SMA 2 to be your primary Security Management appliance.

To configure SMA 2 as your new primary Security Management appliance and restore service:

Procedure

	Command or Action	Purpose
Step 1	If you are using Centralized Policy, Virus, and Outbreak Quarantines: • On each Email Security appliance, disable the centralized quarantines.	See instructions for disabling Centralized Policy, Virus, and Outbreak Quarantines in the Email Security appliance documentation. This will create local quarantines on each Email Security appliance, which you will migrate later to the new Security Management appliance.
Step 2	Load onto your backup Security Management appliance (SMA2) the configuration file that you saved from your primary Security Management appliance (SMA1).	See Loading a Configuration File, on page 73.
Step 3	Recreate the IP address from the failed SMA 1 to be the IP address on SMA 2	a. On SMA 2 choose **Network > IP Interfaces > Add IP Interfaces**.

	Command or Action	Purpose
		b. On the **Add IP Interfaces** page, enter all of the relevant IP Interface information from the failed SMA1 into the text fields to recreate the interface on SMA 2. For more information about Adding IP Interfaces, see Configuring IP Interfaces.
Step 4	Submit and commit your changes.	
Step 5	Enable all applicable centralized services on the new Security Management appliance (SMA 2).	See Configuring Services on the Security Management Appliance.
Step 6	Add all appliances on to the new Security Management appliance (SMA 2). • Test to see that each appliance is enabled and working by establishing a connection to the appliances and testing the connections.	See About Adding Managed Appliances.
Step 7	If you are using Centralized Policy, Virus, and Outbreak Quarantines, configure quarantine migration on the new Security Management appliance, then enable and configure the migration on each applicable Email Security appliance.	See Centralizing Policy, Virus, and Outbreak Quarantines.
Step 8	If necessary, restore additional data.	See Other Important Backup Tasks , on page 41.

What to do next

After this process is complete, SMA 2 becomes the primary Security Management appliance. All data from ESAs 1-3 and WSA 1 now goes to SMA 2, as shown in the following figure:

Figure 2: Disaster Recovery: Final Result
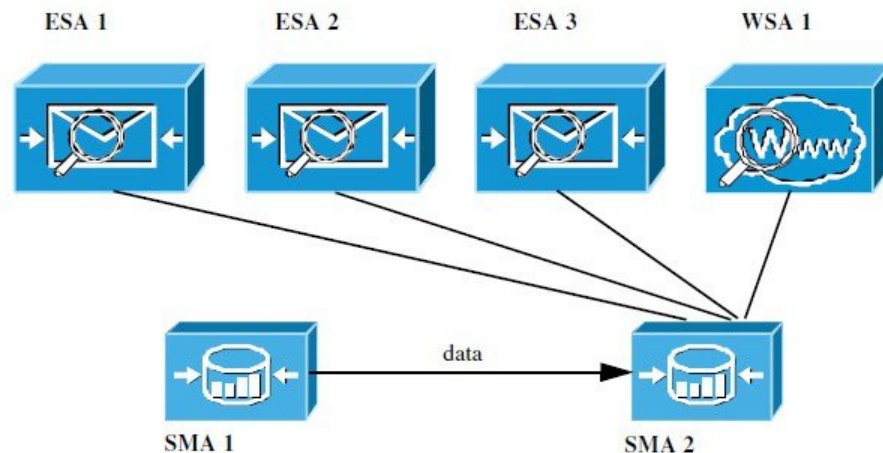
Upgrading Appliance Hardware

See Making a Backup Appliance the Primary Appliance , on page 41.

Upgrading AsyncOS

Batch Commands for Upgrades

Batch commands for upgrade procedures are documented in the CLI Reference Guide for AsyncOS for Email at http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

Determining Network Requirements for Upgrades and Updates

The update servers for Cisco content security appliances use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for AsyncOS upgrades. If you determine that your firewall settings require a static IP for upgrades, contact Cisco Customer support to obtain the required URL addresses.

Note If you have any existing firewall rules allowing download of legacy upgrades from upgrades.cisco.com ports such as 22, 25, 80, 4766, they will need to be removed and/or replaced with revised firewall rules.

Choosing an Upgrade Method: Remote vs. Streaming

Cisco provides two methods (or 'sources') for upgrading AsyncOS on your appliances:

- Streaming upgrades — Each appliance downloads the AsyncOS upgrades via HTTP directly from the Cisco content security update servers.
- Remote upgrades — You only download the upgrade image from Cisco one time, and then serve it to your appliances. Your appliances then download the AsyncOS upgrades from a server within your network.

You will configure the upgrade method in Configuring Upgrade and Service Update Settings, on page 47. Optionally, use the **updateconfig** command in the CLI.

Streaming Upgrade Overview

In Streaming upgrades, each Cisco Content Security appliance connects directly to the Cisco content security update servers to find and download upgrades:

Figure 3: Streaming Update Method
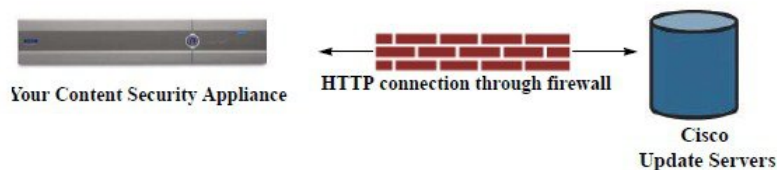
This method requires that your appliance contacts the Cisco content security update servers directly from the network.

Remote Upgrade Overview

You can also download and host updates to AsyncOS locally from within your own network (Remote Upgrade) rather than obtaining updates directly from the Cisco update servers (Streaming Upgrades). Using this feature, an encrypted update image downloaded via HTTP to any server in your network that has access to the Internet. If you choose to download the update image, you can then configure an internal HTTP server (an "update manager") to host the AsyncOS images to your Security Management appliances.

Figure 4: Remote Update Method
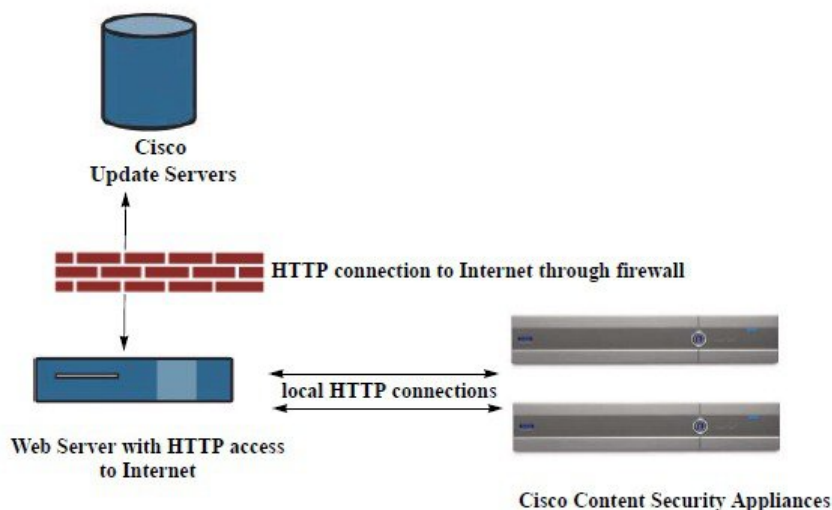
The basic process is as follows:

Step 1   Read the information in Hardware and Software Requirements for Remote Upgrades, on page 46 and Hosting a Remote Upgrade Image, on page 46.

Step 2   Configure a local server to retrieve and serve the upgrade files.

Step 3   Download the upgrade files.

Step 4   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 5   Choose **Management Appliance > System Administration > Update Settings**

From this page, choose to configure the appliance to use the local server.

Step 6   Choose **Management Appliance > System Administration > System Upgrade**

Step 7   Click **Available Upgrades**.

Note   From the command-line prompt you can also do the following: Run the **updateconfig** command then run the **upgrade** command.

For complete information, see Upgrading AsyncOS, on page 44.

Hardware and Software Requirements for Remote Upgrades

For *downloading* AsyncOS upgrade files, you must have a system in your internal network that has:

- Internet access to the update servers for Cisco content security appliances.
- A web browser.

Note   For this release, 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 update files, you must have a server in your internal network that has:

- A web server — for example, Microsoft IIS (Internet Information Services) or the Apache open source server — that:
  - 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 update image

Hosting a Remote Upgrade Image

After setting up a 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 and the version number of the Cisco Content Security appliance. You will then be presented with a list of available upgrades. Click the upgrade version that you want to download a zip file of the upgrade image. To use the upgrade image for AsyncOS upgrades, enter the base URL for your local server on the Edit Update Settings page (or use updateconfig in the CLI).

You can also host an XML file on a local server that limits the available upgrades for the Cisco Content Security appliances on your network to the version selected at http://updates.ironport.com/fetch_manifest.html . Your Cisco Content Security appliances still download the upgrade from the Cisco servers. If you want to host the upgrade list on a local server, download the zip file and extract the asyncos/phoebe-my-upgrade.xml file to the root directory of the local server. To use the upgrade list for AsyncOS upgrades, enter the full URL for the XML file on the Edit Update Settings page (or use updateconfig in the CLI).

For more information about remote upgrades, check the Knowledge Base (see Knowledge Base Articles (TechNotes)) or contact your support provider.

Important Differences in Remote Upgrading Method

Note these differences when upgrading AsyncOS from a local server (Remote upgrade) as opposed to the Streaming upgrade method:

- The upgrade installs immediately *while downloading* .
- A banner appears for 10 seconds at the beginning of the upgrade process. While this banner appears, you have the option to press Control-C to exit the upgrade process before downloading starts.

Configuring Upgrade and Service Update Settings

You can configure how the Cisco Content Security appliance downloads security services updates (such as time zone rules) and AsyncOS upgrades. For example, you can choose whether to download upgrades and updates dynamically from Cisco servers or from a local server onto which you have made the images available; configure the update interval; or disable automatic updates.

AsyncOS periodically queries the update servers for new updates to all security service components except for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades.

You can configure upgrade and updates settings in the GUI (see the following two sections) or using the updateconfig command in the CLI.

You can also configure upgrade notification settings.

Upgrade and Update Settings

The following table describes the update and upgrade settings you can configure.

Table 1: Update Settings for Security Services

Setting	Description
Update Servers (images)	Choose whether to download AsyncOS upgrade and service update software images, such as time zone rules and Feature Key updates, from the Cisco servers or a from a local web server. The default is the Cisco servers for both upgrades and updates. You might want to use a local web server if : - You need to download images to your appliance from a static address. See Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies , on page 48. - You want to download AsyncOS upgrade images to your appliance at your convenience. (You can still download service update images dynamically from the Cisco update servers.) When you choose a local update server, enter the base URL and port number for the servers used to download the upgrades and updates. If the server requires authentication, you can also enter a valid user name and passphrase. For more information, see Choosing an Upgrade Method: Remote vs. Streaming , on page 44 and Remote Upgrade Overview, on page 45.

Setting	Description
Update Servers (lists)	Choose whether to download the lists of available upgrades and service updates (the manifest XML files) from the Cisco servers or from a local web server. The default for both upgrades and updates is the Cisco servers. You can choose different settings for upgrades and for updates. If applicable, see Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies , on page 48. If you choose local update servers, enter the full path to the manifest XML file for each 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. For more information, see Choosing an Upgrade Method: Remote vs. Streaming , on page 44 and Remote Upgrade Overview, on page 45.
Automatic Updates	Choose whether or not to enable automatic updates for time zone rules. When enabled, enter the time to wait between checks for updates. Add a trailing **m** for minutes, **h** for hours, and **d** for days.
Interface	Choose which network interface to use when contacting the update servers for time zone rules and AsyncOS upgrades. The available proxy data interfaces are shown. By default, the appliance selects an interface to use.
HTTP Proxy Server	If an upstream HTTP proxy server exists and requires authentication, enter the server information and user name and passphrase here. Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI. This proxy server is also used to obtain File Analysis report details from the cloud. See also Requirements for File Analysis Report Details (Web reports) or Requirements for File Analysis Report Details (Email reports).
HTTPS Proxy Server	If an upstream HTTPS proxy server exists and requires authentication, enter the server information and user name and passphrase here. Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI. This proxy server is also used to obtain File Analysis report details from the cloud.. See also Requirements for File Analysis Report Details (Web reports) or Requirements for File Analysis Report Details (Email reports).

Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies

The AsyncOS update servers use dynamic IP addresses. If your environment has strict firewall policies which require static IP addresses, use the following settings on the Update Settings page:

Figure 5: Static URLs for Update Servers (images) Settings

Figure 6: Static URLs for Update Servers (list) Settings

Table 2: Static Addresses for Environments with Strict Firewall Policies

Section	Setting	Static URL/IP Address and Port
Update Servers (images):	Base URL (all services except Time zone rules and AsyncOS upgrades)	http://downloads-static.ironport.com 204.15.82.8 Port 80
	Base URL (Time zone rules)	downloads-static.ironport.com 204.15.82.8 Port 80
	Host (AsyncOS upgrades)	updates-static.ironport.com 208.90.58.25 Port 80
Update Servers (list):	For updates on physical hardware appliances: Full URL	update-manifests.ironport.com 208.90.58.5 Port 443
	For updates on virtual appliances: Full URL	update-manifests.sco.cisco.com Port 443
	For upgrades: Full URL	update-manifests.ironport.com 208.90.58.5 Port 443

☞

Important   You must configure the `update-manifests` URLs and port numbers using the `dynamichost` sub command of the `updateconfig` command in the CLI. This validates the service updates.

Configuring the Update and Upgrade Settings from the GUI

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > System Administration > Update Settings.**

Step 3   Click **Edit Update Settings**.

Use the descriptions in Upgrade and Update Settings, on page 47 to configure the settings in this procedure.

Step 4   In the **Update Servers (images)** section, specify the servers from which to download images for updates.

Step 5   Specify the server from which to download images for AsyncOS upgrades:

a)   At the bottom of the same section, click the **Click to use different settings for AsyncOS upgrades**link.

b)   Specify server settings for downloading images for AsyncOS upgrades.

Step 6   In the **Update Servers (list)** section, specify the servers for obtaining the list of available updates and AsyncOS upgrades.

The top subsection applies to updates. The bottom subsection applies to upgrades.

Step 7   Specify settings for Time Zone rules and interface.

Step 8   (Optional) Specify settings for Proxy Servers.

Step 9   Submit and commit your changes.

Step 10   Verify that your results are what you expect:

If you are not already looking at the Update Settings page, choose **Management Appliance > System Administration > Update Settings.**

Some URLs may append an "asyncos" directory to the server URL. You can ignore this discrepancy.

Upgrade Notifications

By default, users with administrator and technician privileges will see a notification at the top of the web interface when an AsyncOS upgrade is available for the appliance.

To	Do This
View more information about the latest upgrade	Hover over the upgrade notification.
View a list of all available upgrades	Click the down arrow in the notification.
Dismiss a current notification. The appliance will not display another notification until a new upgrade becomes available.	Click the down arrow, then select **Clear the notification**, then click **Close**.
Prevent future notifications (Users with Administrator privileges only.)	Go to **Management Appliance > System Administration > System Upgrade.**

Before You Upgrade: Important Steps

Before you begin

See network requirements at Determining Network Requirements for Upgrades and Updates , on page 44.

Step 1   Take steps to prevent or minimize data loss:

- Make sure the new appliance has sufficient disk capacity and the same or greater size allocations for each data type that will be transferred. See About Disk Space Maximums and Allocations, on page 81.

- If you have received any disk space warnings, resolve any disk space issues before upgrading.

Step 2   Save the XML configuration file off the appliance. See caveats at Saving and Exporting the Current Configuration File, on page 72.

If you need to revert to the pre-upgrade release for any reason, you will need this file.

Step 3   If you are using the Safelist/Blocklist feature, export the list off the appliance.

Click **Management Appliance > System Administration > Configuration File** and scroll down.

Step 4   Suspend the listeners using the **suspendlistener** command when running the upgrade from the CLI. If you perform the upgrade from the GUI, listener suspension occurs automatically.

Step 5   Drain the mail queue and the delivery queue.

Step 6   Verify that the upgrade settings are configured as you want them. See Configuring Upgrade and Service Update Settings, on page 47.

Upgrading AsyncOS

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

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 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.

Before you begin

- Choose whether you will download upgrades directly from Cisco or will host upgrade images from a server on your network. Then set up your network to support the method you choose. Then configure the appliance to obtain upgrades from your chosen source. See Choosing an Upgrade Method: Remote vs. Streaming , on page 44 and Configuring Upgrade and Service Update Settings, on page 47.

- Before installing the upgrade, follow the instructions in Before You Upgrade: Important Steps , on page 51.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > System Administration > System Upgrade**.

Step 3   Click **Upgrade Options**.

Step 4   Choose an option:

To	Do This
Download and install the upgrade in a single operation	Click **Download and Install**. If you have already downloaded an installer, you will be prompted to overwrite the existing download.
Download an upgrade installer	Click **Download only**. 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.

To	Do This
Install a downloaded upgrade installer	Click **Install**. This option appears only if an installer has been downloaded. The AsyncOS version to be installed is noted below the Install option.

Step 5   Unless you are installing a previously-downloaded installer, select an AsyncOS version from the list of available upgrades.

Step 6   If you are installing:

a) Choose whether or not to save the current configuration to the configuration directory on the appliance.

b) Choose whether or not to mask the passphrases in the configuration file.

> **Note**   You cannot load a configuration file with masked passphrases using the Configuration File page in the GUI or the `loadconfig` command in the CLI.

c) If you want to email copies of the configuration file, enter the email addresses to which you want to email the file. Use commas to separate multiple email addresses.

Step 7   Click **Proceed**.

Step 8   If you are installing:

a) Be prepared to respond to prompts during the process.

The process pauses until you respond.

A progress bar appears near the top of the page.

b) At the prompt, click **Reboot Now**.

> **Note**   Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted.

c) After about 10 minutes, access the appliance again and log in.

What to do next

- If the process was interrupted, you must start the process again.

- If you downloaded but did not install the upgrade:

  When you are ready to install the upgrade, follow these instructions from the beginning, including the prerequisites in the Before You Begin section, but choose the Install option.

- If you installed the upgrade, see .

Viewing Status of, Canceling, or Deleting a Background Download

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > System Administration > System Upgrade**.

Step 3   Click **Upgrade Options**.

Step 4   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.
	Upgrade status also appears in upgrade_logs.
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.

After Upgrading

After the upgrade is complete, complete the following:

- (For deployments with associated Email Security appliances) Re-enable the listeners.

- (For deployments with associated Web Security appliances) Configure your system to support the latest Configuration Master. See Using Configuration Masters to Centrally Manage Web Security Appliances.

- Consider saving your configuration. For more information, see Saving and Importing Configuration Settings , on page 72.

- Before viewing the online help after upgrade, clear your browser cache, exit the browser, then open it again. This clears the browser cache of any outdated content.

About Reverting to an Earlier Version of AsyncOS

You can revert to an to a previous qualified version of AsyncOS for emergency uses.

You can also revert to the currently running build if you want to clear all data on the appliance and start with a new, clean configuration.

Related Topics

Important Note About Reversion Impact

Using the revert command on a Cisco Content Security appliance is a very destructive action. This command permanently destroys all existing configurations and data. In addition, it disrupts mail handling until the appliance is reconfigured.

Reverting does not affect feature key or virtual appliance license expiration dates.

Reverting AsyncOS

Before you begin

- Back up or save any data that you want to preserve to a location off the appliance.

- You must have a configuration file for the version you want to revert to. Configuration files are *not* backwards-compatible.

- Because this command destroys all configuration, it is highly recommended that you have physical local access to the appliance when reverting.

- If quarantines are enabled on your Email Security appliances, disable centralization so that messages are quarantined locally on those appliances.

Step 1 Ensure that you have the configuration file for the version you want to revert to. Configuration files are not backwards-compatible.

Step 2 Save a backup copy of the current configuration of your appliance (with passphrases unmasked) on another machine. To do this, you can email the file to yourself or FTP the file. A simple way to do this is to run the `mailconfig` CLI command, which emails the current configuration file on your appliance to the specified email address.

Note   This is not the configuration file you will load after reverting.

Step 3 If you use the Safelist/Blocklist feature, export the Safelist/Blocklist database to another machine.

Step 4 Suspend any listeners on your Email Security appliances.

Step 5 Wait for the mail queue to empty.

Step 6 Log in to the CLI of the appliance you want to revert.

When you run the `revert` command, several warning prompts are issued. Once these warning prompts are accepted, the revert action takes place immediately. Therefore, do not begin the reversion process until after you have completed the prereversion steps.

Step 7 From the command-line prompt, type the `revert` command and respond to the prompts.

The following example shows the `revert` command:

Example:

```
m650p03.prep> revert
This command will revert the appliance to a previous version of AsyncOS.
WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preseved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases
unmasked)
- exported the Cisco Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
```

```
- waited for the mail queue to empty
Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired version.
Do you want to continue? yes
Are you sure you want to continue? yes
Available versions
=================
 1. 7.2.0-390
 2. 6.7.6-020
Please select an AsyncOS version: 1
You have selected "7.2.0-390".
Reverting to "testing" preconfigure install mode.
The system will now reboot to perform the revert operation.
```

Step 8   Wait for the appliance to reboot twice.

Step 9   Log in to the appliance using the CLI.

Step 10   Add at least one Web Security appliance and wait a few minutes to allow any URL Category updates to be downloaded from that appliance.

Step 11   After URL Category updates are completed, load the XML configuration file of the version you are reverting to.

Step 12   If you use the Safelist/Blocklist feature, import and restore the Safelist/Blocklist database.

Step 13   Reenable any listeners on your Email Security appliances.

Step 14   Commit your changes.

The reverted Cisco Content Security appliance should now run using the selected AsyncOS version.

Note   It may take 15 to 20 minutes before reversion is complete and console access to the Cisco Content Security appliance is available again.

About Updates

Service updates are periodically made available for download. To specify settings for these downloads, see Configuring Upgrade and Service Update Settings, on page 47

Related Topics

- Configuring Upgrade and Service Update Settings, on page 47

About URL Category Set Updates for Web Usage Controls

- Preparing For and Managing URL Category Set Updates
- URL Category Set Updates and Reports

Configuring the Appliance to Trust Proxy Server Communication

If you are using a non-transparent proxy server, you can add the CA certificate used to sign the proxy certificate to the email gateway. By doing so, the email gateway trusts the proxy server communication.

When Cisco Secure Email and Web Manager communicates with the updater servers to receive updates, a validation if the certificate is trusted is performed on the certificates that are used. To successfully validate the certificates used, you must include that updater server's Certificate Authority certificate into our Cisco

Secure Email and Web Manager for successful communication. To perform this, use the **updateconfig** > **trusted_certificates** . The options in the command include:

- Add- To add a certificate in CA

- List- To list all the certificates in CA

- Delete- To delete a certificate in CA

Use the updateconfig command to configure this option. The following example shows how to configure this option.

```
SMA> updateconfig

Service (images): Update URL:
--------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:
--------------------------------------------------------------------------------
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]> add

Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIIOUMAFHhzRskwDQYJKoZIhvcNAQELBQAwczELMAkGA1UE
BhMCSU4xCzAJBgNVBAgTAlROMQwwCgYDVQQHEwNDaG4xETAPBgNVBAoTCENBNQ053
aWxkMREwDwYDVQQLEwhDQUNOd2lsZDEjMCEGA1UEAwwaKi5jczIxLmRldml0LmNp
c2NvbGFicy5jb20wHhcNMjExMjE1MTE0NzAwWhcNMjIxMjE1MTE0NzAwWjBzMQsw
CQYDVQQGEwJJTjELMAkGA1UECBMCVE4xDDAKBgNVBAcTA0NobjERMA8GA1UEChMI
Q0FDTndpbGQxETAPBgNVBAsTCENBNQ053aWxkMSMwIQYDVQQDBoqLmNzMjEuZGV2
aXQuY2lzY29sYWJzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJPPBRGq0wHv/6ZLPOZ3jdEgzVS+dzXJSyhtMsgm/XrvIvjRH0MK3r++dtUgHMzz
le/WrxPKGphjtNsvF7ss58RRg3fiQCSQPX6nfBYc9v4A7rSdmKzYYFbBkGPeijLB
```

```
qwVyseMa3rifjv4Bucxw0M3ZrUqq7YfcZtxZhSEtxx8rT3A/uReIm/n1ERcZDclW
+GkfRxEdY3ZLpen/2sFiOAVMvAHlKRtK7kEhmo1TPQZ0h0UQFNDbl2ZWZZ6Nuv0I
Z6pUDNj1/+GoJyvSwl0qpetHxhdMtubMAAM8JQNvNkHgzOswsbN18F5at7cZ/KFI
HuvBUXKHV5pEX3hOdJxbuocCAwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUCNlXseZ5qBjqJtYv3sdCujJuqnAwHwYDVR0jBBgwFoAUCNlXseZ5qBjqJtYv
3sdCujJuqnAwCwYDVR0PBAQDAgGGMA0GCSqGSIb3DQEBCwUAA4IBAQBaq5KXw/wX
nzJpBnKPZuO4KNcIz9/A2Hil2ikWNBjfla1x/37OdTbh3IpHJ6n1OCeAkE5Ww7uX
amlUcWxvDk3Zn+tKysCU2Q1PYSxUHXtqH3rvWZDRglPkJUu420tnCg2fV1bulcJ1
xx6E95a9D1vCarfxvuINU50076gnypTMv9+lOFXCkvDgBOmkQpqswR5l519kmDZi
mt8CoknJN/iAENxM8b47262yXEc1X6ZN/OWa/x14OS3X0C0hikyg9HpUGDq+CigE
s5CBCOLDfe8G9kAPoTg2mVNT10xxQF1juobb6djmdB1Of8kqgKs2eWsD+MfKvNbG
ZzPGx4SUS2RZ
-----END CERTIFICATE-----
.
Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain
Name(FQDN) format ? [N]> y


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

Configuring the Return Address for Generated Messages

You can configure the envelope sender for mail generated by AsyncOS for the following types of cases:

- Bounce messages
- Reports

You can specify the display, user, and domain names of the return address. You can also choose to use the Virtual Gateway domain for the domain name.

Use the Return Addresses page available on the System Administration menu in the GUI, or use the **addressconfig** command in the CLI.

To modify the return address for system-generated email messages in the GUI, click **Edit Settings** on the Return Addresses page. Make changes to the address or addresses you want to modify, click **Submit,** and commit your changes.

Managing Alerts

The appliance sends you email alerts about events occurring on the appliance.

To	Do This
Have different types of alerts sent to different administrative users	Select **Management Appliance > System Administration > Alerts** If you enabled AutoSupport during system setup, the email address that you specified will receive alerts for all severities and classes by default. You can change the configuration at any time. Separate multiple addresses with commas.

To	Do This
Configure global settings for alerts, including: • Alert sender (FROM:) address • Controls for duplicate alerts • AutoSupport settings.	Select **Management Appliance > System Administration > Alerts** See About Duplicate Alerts , on page 60 See Cisco AutoSupport, on page 60
View a list of recent alerts Manage settings for this list	See Viewing Recent Alerts , on page 60
See a list of alerts and their descriptions	See: Hardware Alert Descriptions , on page 61. System Alert Descriptions , on page 61
Understand alert delivery mechanisms	See Alert Delivery, on page 59

Alert Types and Severities

Alert types include:

• Hardware alerts. See Hardware Alert Descriptions , on page 61.
• System alerts. See System Alert Descriptions , on page 61.
• Updater alerts.

Alerts can have the following severities:

• Critical: issue that requires immediate attention
• Warning: problem or error requiring further monitoring and potentially immediate attention
• Info: information generated in the routine functioning of this device

Alert Delivery

Because alert messages can be used to inform you of problems within your Cisco Content Security appliance, they are not sent using AsyncOS's normal mail delivery system. Instead, alert messages pass through a separate and parallel email system designed to operate even in the face of significant system failure in AsyncOS.

The alert mail system does not share the same configuration as AsyncOS, which means that alert messages may behave slightly differently from other mail delivery:

• Alert messages are delivered using standard DNS MX and A record lookups.

• They do cache the DNS entries for 30 minutes and the cache is refreshed every 30 minutes, so in case of DNS failure the alerts still go out.

• If your deployment includes Email Security appliances:

• Alert messages do not pass through the work queue, so they are not scanned for viruses or spam. They are also not subjected to message filters or content filters.

• Alert messages do not pass through the delivery queue, so they will not be affected by bounce profiles or destination control limits.

• [Optional - Only if TLS support is enabled in "alertconfig" and FQDN validation enabled in SSL Configuration settings]: Check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the server certificate, are in the FQDN format.

• [Optional - Only if TLS support is enabled in "alertconfig"]: Check whether the 'Common Name,' or 'SAN: DNS Name' fields, of the server certificate contain Hostname of the server. Reverse DNS name is used if IP is configured in Hostname field.

Viewing Recent Alerts

To	Do This
View a list of recent alerts	Users with administrator and operator access can choose **Management Appliance > System Administration > Alerts** and click the **View Top Alerts** button. Alerts appear even if there was a problem emailing them.
Sort the list	Click a column heading.
Specify the maximum number of alerts to save in this list	Use the alertconfig command in the command-line interface
Disable this feature	Use the alertconfig command in the command-line interface to set the maximum number of alerts to zero (0).

About Duplicate Alerts

You can specify the initial number of seconds to wait before AsyncOS will send a duplicate alert. If you set this value to 0, duplicate alert summaries are not sent; 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, and so on.

Eventually, the interval could become large. 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, and so on.

Cisco AutoSupport

To allow Cisco to better support and design future system changes, the Cisco Content Security appliance can be configured to send Cisco a copy of all alert messages generated by the system. This feature, called 'AutoSupport', is a useful way to allow Customer Support to be proactive in supporting your needs. AutoSupport also sends weekly reports noting the uptime of the system, the output of the **status** command, and the AsyncOS version used.

By default, alert recipients set to receive Information severity level alerts for System alert types receive a copy of every message sent to Cisco. This can be disabled if you do not want to send the weekly alert messages

internally. To enable or disable this feature, select **Management Appliance > System Administration Alerts** and click edit settings.

By default, if AutoSupport is enabled, the weekly AutoSupport report is sent to alert recipients set to receive system alerts at the Information level.

Hardware Alert Descriptions

Table 3: Hardware Alert Descriptions

Alert Name	Description	Severity
INTERFACE.ERRORS	Sent when interface errors are detected.	Warning
MAIL.MEASUREMENTS_FILESYSTEM	Sent when a disk partition is nearing capacity (75%).	Warning
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	Sent when a disk partition reaches 90% capacity (and at 95%, 96%, 97%, and so on).	Critical
SYSTEM.RAID_EVENT_ALERT	Sent when a critical RAID-event occurs.	Warning
SYSTEM.RAID_EVENT_ALERT_INFO	Sent when a RAID-event occurs.	Information

System Alert Descriptions

Table 4: System Alert Descriptions

Alert Name	Description	Severity
COMMON.APP_FAILURE	Sent when there is an unknown application failure.	Critical
COMMON.KEY_EXPIRED_ALERT	Sent when a feature key has expired.	Warning
COMMON.KEY_EXPIRING_ALERT	Sent when a feature key is about to expire.	Warning
COMMON.KEY_FINAL_EXPIRING_ALERT	Sent as a final notice that a feature key is about to expire.	Warning
DNS.BOOTSTRAP_FAILED	Sent when the appliance is unable to contact the root DNS servers.	Warning
COMMON.INVALID_FILTER	Sent when an invalid filter is encountered.	Warning

Alert Name	Description	Severity
IPBLOCKD.HOST_ADDED_TO_ALLOWED LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED LIST	Alert messages: • The host at \<IP address\> has been added to the blocked list because of an SSH DOS attack. • The host at \<IP address\> has been permanently added to the ssh allowed list. • The host at \<IP address\> has been removed from the blocked list. 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.	Warning
LDAP.GROUP_QUERY_FAILED_ALERT	Sent when an LDAP group query fails.	Critical
LDAP.HARD_ERROR	Sent when an LDAP query fails completely (after trying all servers).	Critical
LOG.ERROR.*	Various logging errors.	Critical
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	Sent when an LDAP group query fails during per-recipient scanning.	Critical
MAIL.QUEUE.ERROR.*	Various mail queue hard errors.	Critical
MAIL.RES_CON_START_ALERT.MEMORY	Sent when RAM utilization has exceeded the system resource conservation threshold.	Critical
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	Sent when the mail queue is overloaded and system resource conservation is enabled.	Critical

Alert Name	Description	Severity
MAIL.RES_CON_START_ALERT.QUEUE	Sent when queue utilization has exceeded the system resource conservation threshold.	Critical
MAIL.RES_CON_START_ALERT.WORKQ	Sent when listeners are suspended because the work queue size is too big.	Critical
MAIL.RES_CON_START_ALERT	Sent when the appliance enters "resource conservation" mode.	Critical
MAIL.RES_CON_STOP_ALERT	Sent when the appliance leaves "resource conservation" mode.	Critical
MAIL.WORK_QUEUE_PAUSED_NATURAL	Sent when the work queue is paused.	Critical
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	Sent when the work queue is resumed.	Critical
NTP.NOT_ROOT	Sent when the appliance is unable to adjust time because NTP is not running as root.	Warning
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	Sent when errors are found in the domain specification file.	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	Sent when the domain specification file is empty.	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	Sent when the domain specification file is not found.	Critical
REPORTD.DATABASE_OPEN_FAILED_ALERT	Sent if the reporting engine is unable to open the database.	Critical
REPORTD.AGGREGATION_DISABLED_ALERT	Sent if the system runs out of disk space. When the disk usage for a log entry exceeds the log usage threshold, reportd disables aggregation and sends the alert.	Warning
REPORTD.DATABASE_DELETION_ALERT	Sent if system checks and finds the export directory is not empty, then it prints the logline and tries to delete the directory in the next iteration.	Information
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Sent if the reporting engine was unable to save reporting data.	Warning

Alert Name	Description	Severity
REPORTING.CLIENT.JOURNAL.FULL	Sent if the reporting engine is unable to store new data.	Critical
REPORTING.CLIENT.JOURNAL.FREE	Sent when the reporting engine is again able to store new data.	Information
PERIODIC_REPORTS.REPORT_TASK. BUILD_FAILURE_ALERT	Sent when the reporting engine is unable to build a report.	Critical
PERIODIC_REPORTS.REPORT_TASK. EMAIL_FAILURE_ALERT	Sent when a report could not be emailed.	Critical
PERIODIC_REPORTS.REPORT_TASK. ARCHIVE_FAILURE_ALERT	Sent when a report could not be archived.	Critical
SENDERBASE.ERROR	Sent when an error occurred while processing a response from SenderBase.	Information
SMAD.ICCM.ALERT_PUSH_FAILED	Sent if a configuration push failed for one or more hosts.	Warning
SMAD.TRANSFER.TRANSFERS_STALLED	Sent if SMA logs are unable to fetch tracking data for two hours or reporting data for six hours.	Warning
SMTPAUTH.FWD_SERVER_FAILED_ALERT	Sent when the SMTP Authentication forwarding server is unreachable.	Warning
SMTPAUTH.LDAP_QUERY_FAILED	Sent when an LDAP query fails.	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	Sent when there was a problem shutting down the system on reboot.	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	Sent when there was a problem shutting down the system.	Warning
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Sent when a recipient validation update failed.	Critical
SYSTEM.SERVICE_TUNNEL.DISABLED	Sent when a tunnel created for Cisco Support Services is disabled.	Information
SYSTEM.SERVICE_TUNNEL.ENABLED	Sent when a tunnel created for Cisco Support Services is enabled.	Information

Changing Network Settings

This section describes the features used to configure the network operation of the appliance. These features give you direct access to the hostname, DNS, and routing settings that you configured using the System Setup Wizard in Running the System Setup Wizard.

The following features are described:

- `sethostname`

- DNS configuration (in the GUI and by using the `dnsconfig` command in the CLI)

- Routing configuration (in the GUI and by using the `routeconfig` and `setgateway` commands in the CLI)

- `dnsflush`

- Passphrase

Changing the System Hostname

The hostname is used to identify the system at the CLI prompt. You must enter a fully qualified hostname. The s ethostname command sets the name of the content security appliance. The new hostname does not take effect until you issue the commit command.

The sethostname Command

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

For the hostname change to take effect, you must enter the commit command. After you have successfully committed the hostname change, the new name appears in the CLI prompt:

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

The new hostname appears in the prompt as follows: mail3.example.com>

Configuring Domain Name System Settings

You can configure the Domain Name System (DNS) settings for your content security appliance through the Management Appliance > Network > DNS page in the GUI, or via the dnsconfig command.

You can configure the following settings:

- Whether to use the Internet's DNS servers or your own, and which server(s) to use
- Which interface to use for DNS traffic
- The number of seconds to wait before timing out a reverse DNS lookup
- Clearing the DNS cache

Specifying DNS Servers

AsyncOS can use the Internet root DNS servers, your own DNS servers, or the Internet root DNS servers and authoritative DNS servers that you specify. When using the Internet root servers, you may specify alternate servers to use for specific domains. Because an alternate DNS server applies to a single domain, it must be authoritative (provide definitive DNS records) for that domain.

AsyncOS supports "splitting" DNS servers when not using the Internet's DNS servers. If you are using your own internal server, you can also specify exception domains and associated DNS servers.

When setting up "split DNS," you should set up the in-addr.arpa (PTR) entries as well. For example, if you want to redirect ".eng" queries to the nameserver 1.2.3.4 and all the .eng entries are in the 172.16 network, then you should specify "eng,16.172.in-addr.arpa" as the domains in the split DNS configuration.

Multiple Entries and Priority

For each DNS server that you enter, you can specify a numeric priority. AsyncOS attempts to use the DNS server with the priority closest to 0. If that DNS server is not responding, AsyncOS attempts to use the server at the next priority. If you specify multiple entries for DNS servers with the same priority, the system randomizes the list of DNS servers at that priority every time it performs a query. The system then waits a short amount of time for the first query to expire or "time out" and then a slightly longer amount of time for the second, and so on. The amount of time depends on the exact total number of DNS servers and priorities that have been configured. The timeout length is the same for all IP addresses at any particular priority. The first priority gets the shortest timeout; each subsequent priority gets a longer timeout. Further, the timeout period is roughly 60 seconds. If you have one priority, the timeout for each server at that priority is 60 seconds. If you have two priorities, the timeout for each server at the first priority is 15 seconds, and each server at the second priority is 45 seconds. For three priorities, the timeouts are 5, 10, 45.

For example, suppose you configure four DNS servers, with two of them at priority 0, one at priority 1, and one at priority 2:

Table 5: Example of DNS Servers, Priorities, and Timeout Intervals

Priority	Server(s)	Timeout (Seconds)
0	1.2.3.4, 1.2.3.5	5, 5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS randomly chooses between the two servers at priority 0. If one of the priority 0 servers is down, the other is used. If both of the priority 0 servers are down, the priority 1 server (1.2.3.6) is used, and then, finally, the priority 2 (1.2.3.7) server.

The timeout period is the same for both priority 0 servers, longer for the priority 1 server, and longer still for the priority 2 server.

Using the Internet Root Servers

The AsyncOS DNS resolver is designed to accommodate the large number of simultaneous DNS connections required for high-performance email delivery.

Note	If you choose to set the default DNS server to something other than the Internet root servers, that server must be able to recursively resolve queries for domains for which it is not an authoritative server.

Reverse DNS Lookup Timeout

The Cisco Content Security appliance attempts to perform a "double DNS lookup" on all remote hosts connecting to a listener for the purposes of sending or receiving email. That is, the system acquires and verifies the validity of the remote host's IP address by performing a double DNS lookup. This consists of a reverse DNS (PTR) lookup on the IP address of the connecting host, followed by a forward DNS (A) lookup on the results of the PTR lookup. The system then checks that the results of the A lookup match the results of the PTR lookup. If the results do not match, or if an A record does not exist, the system uses only the IP address to match entries in the Host Access Table (HAT). This particular timeout period applies only to this lookup and is not related to the general DNS timeout discussed in Multiple Entries and Priority, on page 66.

The default value is 20 seconds. You can disable the reverse DNS lookup timeout globally across all listeners by entering '0' as the number of seconds. If the value is set to 0 seconds, the reverse DNS lookup is not attempted, and instead the standard timeout response is returned immediately.

DNS Alert

Occasionally, an alert may be generated with the message "Failed to bootstrap the DNS cache" when an appliance is rebooted. The message means that the system was unable to contact its primary DNS servers, which can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

Clearing the DNS Cache

The **Clear Cache** button from the GUI, or the d nsflush command (for more information about the dnsflush command, see the IronPort AsyncOS CLI Reference Guide, available from the location specified in Documentation), clears all information in the DNS cache. You may choose to use this feature when changes have been made to your local DNS system. The command takes place immediately and may cause a temporary performance degradation while the cache is repopulated.

Configuring DNS Settings via the Graphical User Interface

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > Network > DNS** page and click the **Edit Settings** button.

Step 3   Select whether to use the Internet's root DNS servers or your own internal DNS server(s), and specify authoritative DNS servers.

Step 4   If you want to use your own DNS server(s) or specify authoritative DNS servers, enter the server ID and click **Add Row.** Repeat this for each server. When entering your own DNS servers, specify a priority as well. For more information, see Specifying DNS Servers, on page 66.

Step 5   Choose an interface for DNS traffic.

Step 6   Enter the number of seconds to wait before canceling a reverse DNS lookup.

Step 7   Optionally, clear the DNS cache by clicking **Clear Cache.**

Step 8   Submit and commit your changes.

Configuring TCP/IP Traffic Routes

Some network environments require the use of traffic routes other than the standard default gateway. You can manage static routes in the GUI through the **Management Appliance > Network > Routing** page, or in the CLI by using the **routeconfig** command.

Managing Static Routes in the GUI

You can create, edit, or delete static routes by using the Management Appliance > Network > Routing page. You can also modify the default gateway from this page.

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   On the **Management Appliance** > **Network** > **Routing** page, click **Add Route** in the route listing. The Enter a name for the route.

Step 3   Enter the destination IP address.

Step 4   Enter the gateway IP address.

Step 5   Submit and commit your changes.

Modifying the Default Gateway (GUI)

Step 1   Click Default Route in the route listing on the Routing page.

Step 2   Change the gateway IP address.

Step 3   Submit and commit your changes.

Configuring the Default Gateway

You can configure the default gateway via the GUI through the Management Appliance > Network > Routing page (see Modifying the Default Gateway (GUI), on page 68) or via the setgateway command in the CLI.

Specifying a Secure Communication Protocol

- If you plan to upgrade from a lower AsyncOS version (for example, 13.6.x) with TLSv1.0 enabled, to AsyncOS 13.8.x and later, then TLSv1.0 is disabled and TLSv1.1 and TLSv1.2 are enabled by default. You need to enable TLSv1.0 method on your appliance after upgrade.

- From AsyncOS 13.8.x and later, there is no support for SSLv2 and SSLv3 methods.

- It is recommended to use TLSv1.1 and TLSv1.2 methods instead of SSLv3 and TLSv1.0. SSLv3 is not secure and you should not use it.

- You can choose the communication protocol to be used for each of the following:

    - Updater server

    - Web-based administrative interface to the appliance

    - LDAPS

Note By default, Update Servers, Web Interface, and LDAP servers use TLSv1.1 and TLSv1.2 methods on a newly installed appliance. SSLv3 is disabled for the end-user access to the spam quarantine.

- To view the currently selected protocols and available options, or to change protocols, use the sslconfig command in the command-line interface.

- Cisco update servers do not support SSLv3.

- If you are using a local (remote) update server, and for all other services and web browsers, the protocol you choose must be supported by and enabled on the server and tools you are using.

- One of the available options must be enabled for each service you use.

- Changes made using the sslconfig command require a Commit.

- Affected services will be briefly interrupted after you commit changes made using the sslconfig command.

Configuring the System Time

Note When gathering data for reports, the Security Management appliance applies the time stamp from the information that was set when you configured the time settings on the Security Management appliance. For information, see How the Security Management Appliance Gathers Data for Reports.

To set time-related settings using the command-line interface, use the ntpconfig , settime , and settz commands.

To	Do This
Set the system time	**Select Management Appliance > System Administration > Time Settings** See also Using a Network Time Protocol (NTP) Server, on page 70
Set the time zone	Select **Management Appliance > System Administration > Time Zone** See also: • Selecting a GMT Offset, on page 70 • Updating Time Zone Files, on page 71

Using a Network Time Protocol (NTP) Server

You can use a Network Time Protocol (NTP) server to synchronize the Security Management appliance system clock with other computers on your network or the internet.

The default NTP server is time.sco.cisco.com .

If you will use an external NTP server, including the default NTP server, open the required port through the firewall. See Firewall Information

Related Topics

- Configuring the System Time, on page 69
- Manually Updating Time Zone Files , on page 71

(Recommended) Setting Appliance System Time Using the Network Time Protocol (NTP)

This is the recommended time keeping method, especially if your appliance is integrated with other devices. All integrated devices should use the same NTP server.

You can use the `ntpconfig` command in the CLI to setup the time using the NTP server.

Step 1 Go to the **System Administration > Time Settings** page.

Step 2 Click **Edit Settings**.

Step 3 In the Time Keeping Method section, select **Use Network Time Protocol**.

Step 4 Enter an NTP server address and click **Add Row**. You can add multiple NTP servers.

Step 5 To delete an NTP server from the list, click the trash can icon for that server.

Step 6 Select an interface for NTP queries. This is the IP address from which NTP queries should originate.

Step 7 Select the **Use NTP Authentication** check box to ensure that a timestamp is generated by a trusted source, protecting NTP from malicious activity or interception.

Step 8 Submit and commit your changes.

Selecting a GMT Offset

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > Time Zone**.

Step 3 Click **Edit Settings**.

Step 4 Select GMT Offset from the list of regions. The Time Zone Setting page is updated to include GMT offsets in the Time Zone field.

Step 5 Select an offset in the Time Zone field. The offset refers to the number of hours that you add or subtract to or from Greenwich Mean Time (GMT) — the local time at the prime meridian. Hours preceded by a minus sign ("-") are west of the prime meridian. A plus sign ("+") indicates locations east of the prime meridian.

Step 6 Submit and commit your changes.

Updating Time Zone Files

Whenever there is a change in the time zone rules for any country, Time Zone files on the appliance must be updated.

Automatically Updating Time Zone Files

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > Update Settings**.

Step 3 Select the **Enable automatic updates for Time zone rules** check box.

Step 4 Enter an interval. Click the **?** help on the page for important information.

Step 5 Submit and commit your changes.

Manually Updating Time Zone Files

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > Time Settings**.

Step 3 Look at the **Time Zone File Updates** section.

Step 4 If there is an available time zone file update, click **Update Now**.

Configuration File Page

For Information About This Section	See
Saving the current configuration	Saving and Importing Configuration Settings , on page 72
Loading a saved configuration	Saving and Importing Configuration Settings , on page 72
End-User Safelist/Blocklist Database (Spam Quarantine)	Backing Up and Restoring the Safelist/Blocklist
Reset Configuration	Resetting the Configuration to Factory Defaults, on page 31

Saving and Importing Configuration Settings

Note The configuration file described in this section is used to configure Security Management appliances.

Most configuration settings for the Security Management appliance can be managed in a single configuration file. The file is maintained in Extensible Markup Language (XML) format.

You can use this file in several ways:

- In case of unexpected disaster to your primary Security Management appliance, you can quickly configure a second Security Management appliance to restore service.
- You can save the configuration file to a different system to back up and preserve crucial configuration data. If you make a mistake while configuring your appliance, you can "roll back" to the most recently saved configuration file.
- You can download the existing configuration file to view the entire configuration for an appliance quickly. (Many newer browsers include the ability to render XML files directly.) This may help you troubleshoot minor errors (like typographic errors) that may exist in the current configuration.
- You can download an existing configuration file, make changes to it, and upload it to the same appliance. This, in effect, "bypasses" both the CLI and the GUI for making configuration changes.
- You can upload an entire configuration file through FTP, or you can paste portions of a configuration file directly into the CLI.
- Because the file is in XML format, an associated document type definition (DTD) that describes all of the XML entities in the configuration file is also provided. You can download the DTD to validate an XML configuration file before uploading it. (XML validation tools are readily available on the Internet.)
- You can use the configuration file to speed configuration of another appliance, for example a cloned virtual appliance.

Managing Configuration Files

- Backing Up and Restoring the Safelist/Blocklist
- Resetting the Configuration to Factory Defaults, on page 31
- Rolling Back to a Previously Committed Configuration , on page 75

Saving and Exporting the Current Configuration File

Using the Current Configuration section of the **Management Appliance > System Administration > Configuration File** page, you can save the current configuration file to your local machine, save it on the appliance (placed in the configuration directory in the FTP/SCP root), or email it to the address specified.

Masking the passphrase

Optionally, mask the user's passphrases by selecting the check box. Masking a passphrase causes the original, encrypted passphrase to be replaced with "*****" in the exported or saved file.

Note Configuration files with masked passphrases cannot be loaded back into AsyncOS.

Encrypting the passphrase

You can encrypt the user's passphrases by clicking the Encrypt passphrases in the Configuration Files checkbox. The following are the critical security parameters in the configuration file that will be encrypted.

- Certificate private keys

- RADIUS passwords

- LDAP bind passwords

- Local users' password hashes

- SNMP password

- Outgoing SMTP authentication passwords

- PostX encryption keys

- PostX encryption proxy password

- FTP Push log subscriptions' passwords

- IPMI LAN password

- Updater server URLs

You can also configure this in the command-line interface using the `saveconfig` command.

Loading a Configuration File

The configuration file must have been saved from an appliance running the same AsyncOS version as the appliance on which you will load the configuration.

Configuration files with masked passphrases cannot be loaded.

Regardless of the method, you must include the following tags at the top of your configuration:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 ... your configuration information in valid XML
</config>
```

The closing </config> tag should follow your configuration information. The values in XML syntax are parsed and validated against the DTD located in the configuration directory on your Cisco Content Security appliance. The DTD file is named config.dtd . If validation errors are reported at the command line when you use the loadconfig command, the changes are not loaded. You can download the DTD to validate configuration files outside of the appliance before uploading them.

In any import method, you can import an entire configuration file (the information defined between the highest level tags: <config></config>), or a *complete* and *unique* subsection of the configuration file, as long as it contains the declaration tags (above) and is contained within the <config></config> tags.

"Complete" means that the entire start and end tags for a given subsection as defined by the DTD are included. For example, uploading or pasting the following code causes validation errors:

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

```
    <autosupport_enabled>0</autosu
</config>
```

However, uploading or pasting the following code does not cause validation errors:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
    <autosupport_enabled>0</autosupport_enabled>
</config>
```

"Unique" means that the subsection of the configuration file being uploaded or pasted is not ambiguous for the configuration. For example, a system can have only one hostname, so uploading the following code (including the declarations and <config></config> tags) is allowed:

```
<hostname>mail4.example.com</hostname>
```

However, a system can have multiple listeners defined, each with different Recipient Access Tables defined, so uploading only the following code is considered ambiguous:

```
    <rat>
        <rat_entry>
            <rat_address>ALL</rat_address>
            <access>RELAY</access>
        </rat_entry>
    </rat>
```

Because it is ambiguous, it is not allowed, even though it is "complete" syntax.

⚠️

Caution When uploading or pasting a configuration file or subsections of a configuration file, you have the potential to erase uncommitted changes that may be pending.

Empty Versus Omitted Tags

Use caution when uploading or pasting sections of configuration files. If you do not include a tag, then its value in the configuration is not modified when you load a configuration file. However, if you include an empty tag, then its configuration setting is cleared.

For example, uploading the following code removes all listeners from the system:

```
<listeners></listeners>
```

⚠️

Caution When uploading or pasting subsections of a configuration file, you can disconnect yourself from the GUI or CLI and destroy large amounts of configuration data. Do not disable services with this command if you are not able to reconnect to the appliance using another protocol, the Serial interface, or the default settings on the Management port. Also, do not use this command if you are unsure of the exact configuration syntax as defined by the DTD. Always back up the configuration data before loading a new configuration file.

Note About Loading Passphrases for Log Subscriptions

If you attempt to load a configuration file that contains a log subscription that requires a passphrase (for example, one that will use FTP push), the `loadconfig` command does not warn you about the missing passphrase. The FTP push fails and alerts are generated until you configure the correct passphrase using the `logconfig` command.

Note About Character Set Encoding

The "encoding" attribute of the XML configuration file must be " ISO-8859-1 " regardless of the character set you may be using to manipulate the file offline. The encoding attribute is specified in the file whenever you issue the showconfig , saveconfig , or mailconfig command:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

Resetting the Current Configuration

Resetting the current configuration causes your Cisco Content Security appliance to revert settings back to the original factory defaults. Save your configuration prior to resetting it.

See Resetting the Configuration to Factory Defaults, on page 31.

Rolling Back to a Previously Committed Configuration

You can roll back the configuration to a previously-committed configuration.

Use the rollbackconfig command in the command-line interface to choose one of the ten most recent commits.

If you enter No when prompted to commit a rollback, the rollback will be committed the next time you commit changes.

Only users with Administrator access can use the rollbackconfig command.

Note   No log messages or alerts will be generated when a previous configuration is restored.

Note   Certain commits, such as re-allocating disk space to a size insufficient to hold existing data, could result in data loss.

CLI Commands for Configuration Files

The following commands enable you to manipulate the configuration files:

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `rollbackconfig`
- `resetconfig` (see Resetting the Configuration to Factory Defaults, on page 31)
- `publishconfig`

- `backupconfig` (see Backing Up Security Management Appliance Data , on page 35)
- `trailblazerconfig`

The showconfig, mailconfig, and saveconfig Commands

For the configuration commands `showconfig` , `mailconfig` , and `saveconfig` , you are prompted to choose whether to include passphrases in the file that will be mailed or displayed. Choosing not to include passphrases leaves any passphrase field blank. You can choose not to include passphrases if you are concerned about security breaches. However, configuration files without passphrases fail when loaded using the `loadconfig` command. See Note About Loading Passphrases for Log Subscriptions, on page 75.

> **Note** When saving, showing, or mailing your configuration file if you choose to include passphrases (answer yes to "Do you want to include passphrases?"), the passphrases are encrypted. However, the private keys and certificates are included in unencrypted PEM format.

The `showconfig` command prints the current configuration to the screen.

```
mail3.example.com> showconfig
Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: model number
Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

Use the `mailconfig` command to email the current configuration to a user. A configuration file in XML format named config.xml will be attached to the message.

```
mail3.example.com> mailconfig
Please enter the email address to which you want to send
the configuration file.
[]> administrator@example.com
Do you want to include passphrases? Please be aware that a configuration
without passphrases will fail when reloaded with loadconfig.  [N]> y
The configuration file has been sent to administrator@example.com.
```

The `saveconfig` command on the Security Management appliance stores and saves all of the configuration master files (ESA) with a unique filename to the configuration directory.

```
mail3.example.com> saveconfig
Do you want to include passphrases? Please be aware that a configuration without passphrases

will fail when reloaded with loadconfig.  [N]> y
The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
 directory.
mail3.example.com>
```

The loadconfig Command

Use the `loadconfig` command to load new configuration information into the appliance. You can load information using one of two methods:

- Placing information in the configuration directory and uploading it
- Pasting configuration information directly into the CLI

See Loading a Configuration File, on page 73 for more information.

The rollbackconfig Command

See Rolling Back to a Previously Committed Configuration , on page 75.

The publishconfig Command

Use the `publishconfig` command to publish changes a configuration master. The syntax is as follows:

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

where *config_master* is a supported Configuration Master, as listed in the Compatibility Matrix in the Release Notes for this release at http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html . This keyword is required. The keyword *job_name* is optional and will be generated if it is not specified.

The keyword *host_list* is a list of host names or IP addresses for WSA appliances to be published, and will be published to all hosts assigned to the configuration master if not specified. The optional *host_ip* can be multiple host IP addresses, each separated by a comma.

To verify that the **publishconfig** command was successful, check the smad_logs file. You can also verify that the publish history was successful from the Security Management appliance GUI by choosing **Web > Utilities > Web Appliance Status**. From this page choose the web appliance that you want the publish history details. Additionally, you can go the Publish History page: **Web > Utilities > Publish > Publish History**.

The trailblazerconfig Command

You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.

You can see the inline help by using the following command on the CLI: `help trailblazerconfig`.

The syntax is as follows:

```
trailblazerconfig enable <https_port> <http_port>
```

```
trailblazerconfig disable
```

```
trailblazerconfig status
```

Where:

`'enable'` runs the trailblazer configuration on the default ports (HTTPS: 4431).

`'disable'` disables the trailblazer configuration

`'status'` checks the status of the trailblazer configuration.

☞

Important By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTPS ports are opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

The `trailblazerconfig` command helps you to avoid the following issues:

- Requiring to add multiple certificates for API ports in certain browsers.

- Redirecting to the legacy web interface when you refresh the Spam quarantine, Safelist or Blocklist page.

- Metrics bar on the Advanced Malware Protection report page does not contain any data.

✎

Note When you enable `trailblazerconfig` command on the appliance, the request URL will contain the `trailblazerconfig` HTTPS port number appended to the hostname.

The updatepvocert Command

You must use the `updatepvocert` command in the CLI to update the CA certificate of 2048 bits to enable Centralized Policy, Virus and Quarantines on the managed Cisco Email Security appliance that is in FIPS mode.

The Centralized Policy, Virus, and Outbreak Quarantines on the managed Email Security appliance is disabled when FIPS is enabled. From AsyncOS 13.0 onwards, appliances in FIPS mode uses a certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines. The earlier AsyncOS versions have certificates of size 1024 bits.

```
example.mail.com> updatepvocert
This command will recreate the PVO certificate and key of strength 2048 bits.
Also, the new certificate will be signed by a CA of strength 2048 bits.
Hermes process will restart post certificate update. No commit will be required.
Do you want to proceed with the certificate update? [Y]>

Certificate updated successfully. Hermes restart needed for the changes to be effective.
Do you want to restart hermes? []> Y

Enter the number of seconds to wait before abruptly closing connections. [30]>

Waiting for listeners to exit... Receiving suspended for euq_listener, cpq_listener. Waiting
 for outgoing deliveries to finish... Mail delivery suspended. Receiving resumed for
euq_listener, cpq_listener. Mail delivery resumed.
Hermes will be up in a moment. Run the status command for hermes.

example.mail.com >
```

Uploading Configuration Changes Using the CLI

Step 1 Outside of the CLI, ensure that you are able to access the configuration directory of the appliance. See IP Interfaces and Accessing the Appliance for more information.

Step 2 Place an entire configuration file or subsection of a configuration file in the configuration directory of the appliance, or edit an existing configuration that was created from the `saveconfig` command.

Step 3 Within the CLI, use the `loadconfig` command to load the configuration file you placed in the directory from Step 2, or paste the text (XML syntax) directly into the CLI.

In this example, a file named changed.config.xml is uploaded and the changes are committed:

Example:

```
mail3.example.com>
l
oadconfig
1. Paste via CLI
2. Load from file
[1]> 2
Enter the name of the file to import:
[]> changed.config.xml
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

In this example, a new configuration file is pasted directly at the command line. (Remember to press Ctrl-D on a blank line to end the paste command.) Then the System Setup Wizard is used to change the default hostname, IP address, and gateway information. (For more information, see Running the System Setup Wizard.) Finally, the changes are committed.

Example:

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 1
Paste the configuration file now. Press CTRL-D on a blank line when done.
[The configuration file is pasted until the end tag
</config>
. Control-D is entered on a separate line.]
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

Managing Disk Space

You can allocate available disk space among the features that your organization uses, up to the maximum available.

(Virtual Appliances Only) Increasing Available Disk Space

For virtual appliances running ESXi 5.5 and VMFS 5, you can allocate more than 2TB of disk space. For appliances running ESXi 5.1, the limit is 2 TB.

> **Note**   Disk space reduction in ESXi is not supported. See the VMWare documentation for information.

To add disk space to the virtual appliance instance:

Before you begin

Carefully determine the disk space increase needed.

Step 1   Bring down the Cisco Content Security Management appliance instance.

Step 2   Increase disk space using utilities or administrative tools provided by VMWare.

See information about changing the virtual disk configuration in the VMWare documentation.

Information for ESXi 5.5 is available here: http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

Step 3   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 4   Go to **Management Appliance > System Administration > Disk Management** and verify that your change has taken effect.

Viewing Disk Space, Quotas and Usage

To	Do This
View the total disk space available on the appliance	Select **Management Appliance > System Administration > Disk Management**. Look at the values shown for "Total Space Allocated" - for example, 184G of 204G.
View the amount of disk space allocated to and currently used by each of the Security Management appliance's monitoring services	Select **Management Appliance > System Administration > Disk Management**.
View the percentage of the quotas for quarantines that are currently used	Select **Management Appliance > Centralized Services > System Status** and look at the Centralized Services section.

About Disk Space Maximums and Allocations

Note   Centralized Reporting Disk Space on Security Management appliances is used for both Email and Web data. If you enable either Centralized Email Reporting or Centralized Web Reporting, all of the space is dedicated to the enabled feature. If you enable both, Email and Web reporting data share the space and space is allocated on a first-come basis.

- If you enable centralized web reporting but there is no disk space allocated for reporting, then centralized web reporting will not work until disk space is allocated.

- Before reducing the Miscellaneous quota below current usage levels, you should delete unneeded data. See Managing Disk Space for the Miscellaneous Quota , on page 81.

- For more information about how disk space is managed for policy, virus, and outbreak quarantines, see Disk Space Allocation for Policy, Virus, and Outbreak Quarantines and Retention Time for Messages in Quarantines.

- For all other data types, if you reduce the existing allocation below current usage, then the oldest data is deleted until all data fits within the new allocation amount.

- If the new quota is larger than the currently used disk space, you will not lose data.

- If you set the allocation to zero, no data is retained.

Ensuring That You Receive Alerts About Disk Space

You will begin to receive system alerts at warning level when Miscellaneous disk usage reaches 75% of the quota. You should take action when you receive these alerts.

To ensure that you receive these alerts, see Managing Alerts, on page 58.

Managing Disk Space for the Miscellaneous Quota

The Miscellaneous quota includes System data and User data. You cannot delete System data. User data that you can manage includes the following types of files:

To Manage	Do this
Log files	Go to **Management Appliance > System Administration > Log Subscriptions** and: • Click the Size column heading to see which logs consume the most disk space. • Verify that you need all of the log subscriptions that are being generated. • Verify that the log level is no more verbose than necessary. • If feasible, reduce the rollover file size.
Packet captures	Go to **Help and Support**(near the upper right side of your screen) > **Packet Capture**. Delete any unneeded captures.

To Manage	Do this
Configuration files (These files are unlikely to consume much disk space.)	FTP to the /data/pub directory on the appliance. To configure FTP access to the appliance, see Accessing the Appliance via FTP
Quota size	Go to **System Administration > Disk Management.**

Reallocating Disk Space Quotas

If disk space is allocated to features you do not use, or if the appliance frequently runs out of disk space for a particular feature and has excess space for other features, you can reallocate disk space.

If you require more space for all features, consider upgrading your hardware or allocating more disk space to your virtual appliance. See (Virtual Appliances Only) Increasing Available Disk Space , on page 80.

Before you begin

- Changing disk allocations may impact existing data or feature availability. See information at About Disk Space Maximums and Allocations, on page 81.
- You can temporarily create space in a quarantine by manually releasing or deleting messages from the quarantine.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > Disk Management**

Step 3 Click **Edit Disk Quotas.**

Step 4 On the **Edit Disk Quotas** page, enter the amount of disk space (in gigabytes) allocated to each service.

Step 5 Click **Submit.**

Step 6 Click **Commit** to commit your changes.

Managing Data Storage Time

You can now configure your Secure Email and Web Manager to store the messages (data) in the Centralized Email Tracking database based on the number of days.

Use the **Apply Data Storage Time** option in System Administration > Disk Management > Edit Data Disk Management page of the legacy web interface to configure the data storage time.

The 'Apply Data Storage Time' option is applicable in any one of the following scenarios:

- If the configured data disk storage limit is reached (for example 500 GB), the messages are automatically deleted from the database even before the configured data storage time is reached (for example, '40 days').

- If the configured data storage time limit is 40 days and a message that is older than the configured data storage time limit (for example, '41 days'), the message is automatically deleted even if the configured data disk storage limit is not reached (for example '500 GB).

Note You can also use the 'Manage data based on the storage time' statement in the diskquotaconfig > edit > Centralized Email Tracking sub command in the CLI to store messages in the Centralized Email Tracking database based on the number of days.

Important: From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. When you use the 'Apply Data Storage Time' option, the Splunk database that contains the email tracking data gets deleted automatically.

Action: Make sure you take a backup of the email tracking data (if required). You can use the backupconfig command in the CLI to perform the backup action. For more information, see Scheduling Single or Recurring Backups, on page 38.

Note If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see Cisco Secure Email and Web Virtual Appliance Installation Guide.

Before you begin

Make sure you have a valid feature key for the Centralized Email Tracking service.

Step 1   [New Web Interface Only] Click ⚙ on Secure Email and Web Manager to load the legacy web interface.

Step 2   Choose **Management Appliance** > **System Administration** > **Disk Management**.

Step 3   Click **Edit Disk Quotas**.

Step 4   Select **Apply Data Storage Time** under Centralized Email Tracking and enter a value in the given field to store the messages (data) in the Centralized Email Tracking database based on the number of days.

Step 5   Click **Submit**.

Step 6   Click **Commit** to commit your changes.

Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances

Note To receive alerts related to these thresholds, configure the thresholds on each managed Email Security appliance. For information, see information about configuring thresholds for system health in the user guide or online help for your Email Security appliance release. You can also run on-demand system health checks from individual appliances. See information about checking the health of your appliance in the user guide or online help for your Email Security appliance release.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Click **Management Appliance > System Administration > System Health**.

Step 3 Click **Edit Settings**.

Step 4 Configure options.

Option	Description
Overall CPU Usage	Default: 85%
Memory Page Swapping	Default: 5000 pages
Maximum Messages in Work Queue	Default: 500 messages

Step 5 Submit and commit your changes.

SSO Using SAML 2.0

About SSO and SAML 2.0

Cisco Content Security Management appliance now supports SAML 2.0 SSO so that the end users can access the Spam Quarantine using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization. For instance, you have enabled Ping Identity as your SAML identity provider (IdP) and has accounts on Rally, Salesforce, and Dropbox which have been SAML 2.0 SSO enabled. When you configure Cisco Content Security Management appliance to support SAML 2.0 SSO as a Service Provider (SP), end users will be able to sign in once and have access to all these services including Spam Quarantine.

SAML 2.0 SSO Workflow

The SAML 2.0 SSO workflow is displayed in the following figure:

Figure 7: SAML 2.0 SSO Workflow
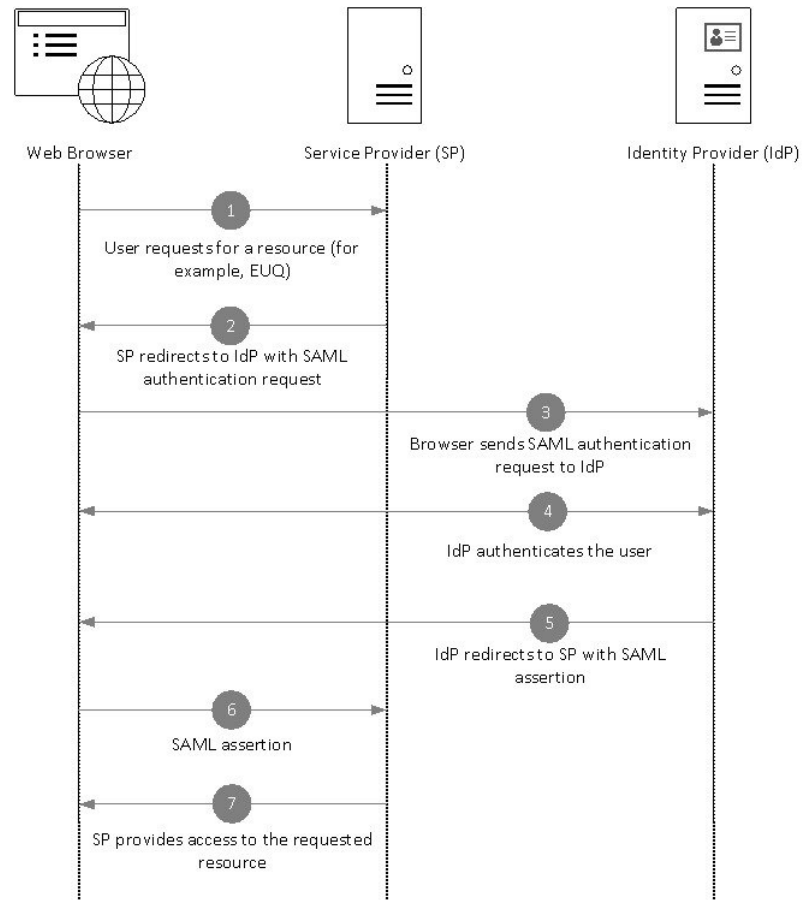
Workflow

1. The end user uses a web browser to request a resource from the service provider (your appliance). For example, the end user clicks on the spam quarantine link in a spam notification.

2. The service provider redirects the request to the web browser with SAML authentication request.

3. The web browser relays the SAML authentication request to the identity provider.

4. The identity provider authenticates the end user. The identity provider displays a login page to the end user and the end user logs in.

5. The identity provider generates the SAML assertion and sends it back to the web browser.

6. The web browser relays the SAML assertion to the service provider.

7. The service provider grants access to the requested resource.

Guidelines and Limitations for SAML 2.0

Logout

When end users log out of Spam Quarantine, they are not logged out of other SAML 2.0 SSO enabled applications.

General

You can configure only one instance of service provider and identity provider on Cisco Content Security Management appliance.

Spam Quarantine Access for Administrators

If you are enabling SSO for Spam Quarantine, keep in mind that the administrators will no longer be able to access the Spam Quarantine using the Spam Quarantine URL (http://<appliance_hostname>:<port>). Administrators can access the Spam Quarantine using the web interface (**Email > Message Quarantine > Spam Quarantine**).

How to Configure SSO on your Cisco Security Management Appliance

Procedure

	Command or Action	Purpose
Step 1	Review the prerequisites.	Prerequisites, on page 86
Step 2	Configure your appliance as a service provider.	Configure Cisco Content Security Management Appliance as a Service Provider, on page 87
Step 3	[On IDP] Configure the identity provider to work with your appliance.	Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 89
Step 4	Configure identity provider settings on your appliance.	Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 91
Step 5	Enable external authentication using SAML on your appliance.	Enable SAML Authentication, on page 92

Prerequisites

Supported Identity Providers

Verify whether the identity provider used by your organization is supported by Cisco Email Security Appliance. The following are the supported identity providers:

• Microsoft Active Directory Federation Services (AD FS) 2.0 and later

• Duo Access Gateway

• Azure AD

Certificates for Secure Communication

Obtain the following certificates that are required to secure the communication between your appliance and the identity provider:

- If you want your appliance to sign SAML authentication requests or if want your identity provider to encrypt SAML assertions, obtain a self-signed certificate or a certificate from a trusted CA and the associated private key.

- If you want the identity provider to sign SAML assertions, obtain the identity provider's certificate and import the same to your appliance. Your appliance will use this certificate to verify the signed SAML assertions.

Converting Certificates

Normally, the certificates obtained from the appliance are in .pfx format and must be converted to .pem format when you configure your appliance as a service provider.

To convert the certificates from .pfx format to .pem format, do the following:

- Download and install OpenSSL tool and import the certificate file (.pfx) obtained from your appliance.

- Run the following command to export the certificate in .pem format: `openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`

- Run the following command to export the private key in .pem format: `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`

- Run the following command to remove the passphrase from the private key: `openssl rsa -in key.pem -out server.key`

Configure Cisco Content Security Management Appliance as a Service Provider

Before you begin

Review the .

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > SAML**.

Step 3 Under the Service Provider section, click **Add Service Provider**.

Step 4 Enter the following details:

Field	Description
Profile Name	Enter a name for the service provider profile.
Configuration Settings	
Entity ID	Enter a globally unique name for the service provider (in this case, your appliance). The format of the service provider Entity ID is typically a URI.

Field	Description
Name ID Format	The format that the identity provider should use to specify the user in the SAML assertion. This field is not configurable. You will need this value while configuring the identity provider.
Assertion Consumer URL	The URL to which the identity provider should send the SAML assertion after authentication has successfully completed. In this case, this is the URL to your spam quarantine. This field is not configurable. You will need this value while configuring the identity provider.
SP Certificate	**Note** The private key must be in .pem format. **Signing Authentication Requests** If you want the appliance to sign the SAML authentication requests: **a.** Upload the certificate and the associated private key. **b.** Enter the passphrase for the private key. **c.** Select **Sign Request**. **Decrypt Encrypted Assertions** If you plan to configure your identity provider to encrypt SAML assertions: **a.** Upload the certificate and the associated private key. **b.** Enter the passphrase for the private key.
Sign Assertions	If you want the identity provider to sign the SAML assertions, select **Sign Assertions**. If you select this option, you must add the identity provider's certificate to the appliance. See Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 89.
Organization Details	Enter the details of your organization. Identity provider uses this information in the error logs.
Technical Contact	Enter the email address of the technical contact. Identity provider uses this information in the error logs.

Step 5   Click **Submit**.

Step 6   Note down the service provider metadata (Entity ID and Assertion Customer URL) displayed on the SSO Settings page and the Name ID Format displayed on the Service Provider Settings page. You will need these details while configuring the service provider settings on the identity provider.

Optionally, you can export the metadata as a file. Click **Export Metadata** and save the metadata file. Some identity providers allow you to load service provider details from a metadata file.

What to do next

Configure the identity provider to communicate with your appliance. See Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 89.

Configuring the Identity Provider to Communicate with Cisco Security Management Appliance

Before you begin

Make sure that you have:

- Configured your appliance as a service provider. See Configure Cisco Content Security Management Appliance as a Service Provider, on page 87.

- Copied the service provider metadata details or exported the metadata file. See Configure Cisco Content Security Management Appliance as a Service Provider, on page 87.

Step 1 On the identity provider, do one of the following:

- Manually configure the details of the service provider (your appliance).

- If your identity provider allows you to load the service provider details from a metadata file, import the metadata file.

If you have configured your appliance to sign the SAML authentication requests or you plan to encrypt SAML assertions, make sure that you add the relevant certificate to the identity provider.

For identity provider-specific instructions, see:

- Configure AD FS to Communicate with Cisco Security Management Appliance, on page 89.

- Configure Azure AD to Communicate with Cisco Security Management Appliance, on page 90.

- Configure Duo Access Gateway to Communicate with Cisco Security Management Appliance, on page 90.

Step 2 Note down the identity provider metadata or export the metadata as a file.

What to do next

Configure the identity provider settings on your appliance. See Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 89.

Configure AD FS to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to configure AD FS (2.0 and later) to communicate with your appliance. For complete and detailed instructions, see *Microsoft documentation*.

- Add the service provider's (appliance's) Assertion Consumer URL as a relaying party.

- Enter the service provider's (appliance's) Entity ID under Relaying Party Trusts > Properties > Identifiers > Relaying Party Identifier. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.

- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format under Relaying Party Trusts > Properties > Signature.

- If you plan to configure AD FS to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format under Relaying Party Trusts > Properties > Encryption.

- Set the Secure-hash Algorithm to SHA-1 under Relaying Party Trusts > Properties > Advanced.

- Add a custom rule to include SPNameQualifier in the response. The following is a sample custom rule:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer=
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =

"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

- Edit the Claim Rule and add an Issuance Transform Rule to send the LDAP attribute for email address as an outgoing claim type (email address). Also ensure that you add an Issuance Transform Rule to send the LDAP attribute for group attribute as an outgoing claim type (unspecified groups).

Configure Azure AD to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to Azure AD to communicate with your appliance. For complete and detailed instructions, see *Microsoft Azure AD Documentation*.

- Add the service provider's (appliance's) Assertion Consumer URL as the service provider identifier that receives and processes SAML assertions.

- Enter the service provider's (appliance's) Entity ID in the Azure Portal under Enterprise Application > New Application > Non-gallery application > Single Sign-On > Basic SAML Configuration. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.

- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) under SAML Signing Certificate section (Enterprise Application > New Application > Non-gallery application > Single Sign-On > SAML Signing Certificate).

- Configure a Group Claim under User Attributes and Claims section (Enterprise Application > New Application > Non-gallery application > Single Sign-On > User Attributes and Claims) and add the group attribute.

- Add users and groups under Enterprise Application > New Application > Non-gallery application > Users & Groups) to allow users to log in to the application based on the SAML assertion or response.

Configure Duo Access Gateway to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to Duo Access Gateway to communicate with your appliance. For complete and detailed instructions, see *Duo Security Documentation*.

- Add the service provider's (appliance's) Assertion Consumer URL as the service provider endpoint that receives and processes SAML assertions.

- Enter the service provider's (appliance's) Entity ID under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.

- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format when you configure the authentication source on the Duo Access Gateway.

- If you plan to configure Duo to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format when you configure the authentication source on the Duo Access Gateway.

- Select the NameID format as "unspecified" under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider > SAML Response.

- Set the Secure-hash Algorithm to SHA-256 under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider > SAML Response.

- Save the SAML - Service Provider Setting as a configuration file on the Duo Admin Panel and import the configuration file as a SAML application on the Duo Access Gateway.

Configure Identity Provider Settings on Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured the identity provider to communicate with your appliance. See Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 89.

- Copied the identity provider metadata details or the exported metadata file.

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance** > **System Administration** > **SAML**.

Step 3 Under the Identity Provider section, click **Add Identity Provider**.

Step 4 Enter the following details:

Field	Description
Profile Name	Enter a name for the identity provider profile.
Configuration Settings (Manually Configure Identity Provider Settings)	
Entity ID	Enter a globally unique name for the identity provider. The format of the identity provider Entity ID is typically a URI.
SSO URL	Specify the URL to which the service provider must send the SAML authentication requests.

Field	Description
Certificate	If the identity provider signs the SAML assertion, you must upload the identity provider's signing certificate.
Configuration Settings (Importing Identity Provider Metadata)	
Import IDP Metadata	Click **Import Metadata** and select the metadata file.

Step 5   Submit and commit your changes.

What to do next

Enable SAML Authentication

You can enable Single Sign On using SAML to authenticate users and assign groups of users to Cisco rules.

Before you begin

Make sure that you have configured the SAML profiles with Service Provider and Identity Provider settings. See How to Configure SSO on your Cisco Security Management Appliance, on page 86.

Step 1   Navigate to **Management Appliances > System Administration > Users**.

Step 2   Scroll down to the **External Authentication** section.

Step 3   Click **Enable**.

Step 4   Select the **Enable External Authentication** check box.

Step 5   Select **SAML** as the authentication type from the drop-down list.

Step 6   **(Optional)** In the **External Authentication Attribute Name Map** field, enter the attribute name to search from the Group Mapping.

The Attribute Name depends on the attributes that you configure for the Identity Provider. The appliance will search for matching entries of the Attribute Name in the **Group Mapping** field. This is optional and if you do not configure, the appliance will search for matching entries of all attributes present in the Group Mapping field.

Step 7   In the **Group Mapping** field, enter the group name attribute as defined in the SAML directory based on the predefined or custom user role. You can click **Add Row** to add multiple role mappings.

The Group Mapping must contain a group attribute. You can add 'Unspecified Groups' attribute to authenticate SAML assertions or response.

For more information on types of user roles, see Users Page.

Step 8   Submit and commit your changes.

What to do next

After you enable SAML external authentication, you can use the **Use Single Sign On** link on the login page of the appliance and enter the username to log in to the appliance.

How to Configure SSO for Spam Quarantine

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 93
Step 2	Configure your appliance as a service provider.	Configure Cisco Content Security Management Appliance as a Service Provider, on page 94
Step 3	[On IDP] Configure the identity provider to work with your appliance.	Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance
Step 4	Configure identity provider settings on your appliance.	Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 97
Step 5	Enable SSO for Spam Quarantine on your appliance.	Enable SSO for Spam Quarantine, on page 98
Step 6	Notify the end users about the new authentication mechanism.	

Prerequisites

- Verify whether the identity provider used by your organization is supported by Cisco Content Security Management Appliance. The following are the supported identity providers:

    - Microsoft Active Directory Federation Services (AD FS) 2.0

    - Ping Identity PingFederate 7.2

    - Cisco Web Security Appliance 9.1

- Obtain the following certificates that are required to secure the communication between your appliance and the identity provider:

    - If you want your appliance to sign SAML authentication requests or if want your identity provider to encrypt SAML assertions, obtain a self signed certificate or a certificate from a trusted CA and the associated private key.

    - If you want the identity provider to sign SAML assertions, obtain the identity provider's certificate. Your appliance will use this certificate to verify the signed SAML assertions.

Configure Cisco Content Security Management Appliance as a Service Provider

Before you begin

Review the .

Step 1   [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2   Choose **Management Appliance > System Administration > SAML**.

Step 3   Under the Service Provider section, click **Add Service Provider**.

Step 4   Enter the following details:

Field	Description
Profile Name	Enter a name for the service provider profile.
Configuration Settings	
Entity ID	Enter a globally unique name for the service provider (in this case, your appliance). The format of the service provider Entity ID is typically a URI.
Name ID Format	The format that the identity provider should use to specify the user in the SAML assertion. This field is not configurable. You will need this value while configuring the identity provider.
Assertion Consumer URL	The URL to which the identity provider should send the SAML assertion after authentication has successfully completed. In this case, this is the URL to your spam quarantine. This field is not configurable. You will need this value while configuring the identity provider.
SP Certificate	**Note** The private key must be in .pem format. **Signing Authentication Requests** If you want the appliance to sign the SAML authentication requests: **a.** Upload the certificate and the associated private key. **b.** Enter the passphrase for the private key. **c.** Select **Sign Request**. **Decrypt Encrypted Assertions** If you plan to configure your identity provider to encrypt SAML assertions: **a.** Upload the certificate and the associated private key. **b.** Enter the passphrase for the private key.

Field	Description
Sign Assertions	If you want the identity provider to sign the SAML assertions, select **Sign Assertions**. If you select this option, you must add the identity provider's certificate to the appliance. See Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 95.
Organization Details	Enter the details of your organization. Identity provider uses this information in the error logs.
Technical Contact	Enter the email address of the technical contact. Identity provider uses this information in the error logs.

Step 5   Click **Submit**.

Step 6   Note down the service provider metadata (Entity ID and Assertion Customer URL) displayed on the SSO Settings page and the Name ID Format displayed on the Service Provider Settings page. You will need these details while configuring the service provider settings on the identity provider.

Optionally, you can export the metadata as a file. Click **Export Metadata** and save the metadata file. Some identity providers allow you to load service provider details from a metadata file.

What to do next

Configure the identity provider to communicate with your appliance. See Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 95.

Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured your appliance as a service provider. See Configure Cisco Content Security Management Appliance as a Service Provider, on page 94.

- Copied the service provider metadata details or exported the metadata file. See Configure Cisco Content Security Management Appliance as a Service Provider, on page 94.

Step 1   On the identity provider, do one of the following:

- Manually configure the details of the service provider (your appliance).

- If your identity provider allows you to load the service provider details from a metadata file, import the metadata file.

If you have configured your appliance to sign the SAML authentication requests or you plan to encrypt SAML assertions, make sure that you add the relevant certificate to the identity provider.

For identity provider-specific instructions, see:

- Configure AD FS 2.0 to Communicate with Cisco Content Security Management Appliance, on page 96

- Configure PingFederate 7.2 to Communicate with Cisco Content Security Management Appliance, on page 96

- **Configuring the Appliance as an Identity Provider** section in the *User Guide for AsyncOS for Cisco Web Security Appliances* http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

Step 2   Note down the identity provider metadata or export the metadata as a file.

What to do next

Configure the identity provider settings on your appliance. See Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 97.

Configure AD FS 2.0 to Communicate with Cisco Content Security Management Appliance

The following are the high level tasks you need to perform to configure AD FS 2.0 to communicate with your appliance. For complete and detailed instructions, see Microsoft documentation.

- Add the service provider's (appliance's) Assertion Consumer URL as a relaying party.
- Enter the service provider's (appliance's) Entity ID under Relaying Party Trusts > Properties > Identifiers > Relaying Party Identifier. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.
- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format under Relaying Party Trusts > Properties > Signature.
- If you plan to configure AD FS to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format under Relaying Party Trusts > Properties > Encryption.
- Set the Secure-hash Algorithm to SHA-1 under Relaying Party Trusts > Properties > Advanced.

- Edit the Claim Rule and add an Issuance Transform Rule to send the LDAP attribute for email address as an outgoing claim type (email address).

- Add a custom rule to include SPNameQualifier in the response. The following is a sample custom rule:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
=
 c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<appliance-hostname>:83");
```

Configure PingFederate 7.2 to Communicate with Cisco Content Security Management Appliance

The following are the high level tasks you need to perform to configure PingFederate 7.2 to communicate with your appliance. For complete and detailed instructions, see Ping Identity documentation.

- Add your service provider's (appliance's) Assertion Consumer URL as an endpoint under protocol settings.
- Enter the service provider's (appliance's) Entity ID under SP Connection > General Info > Partner's Entity ID (Connection ID). Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.

- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate under Signature Verification section (SP Connection > Credentials > Signature Verification > Signature Verification Certificate).
- If you plan to configure PingFederate to send encrypted SAML assertions, upload the service provider's (appliance's) certificate under Signature Verification section (SP Connection > Credentials > Signature Verification > Select XML Encryption Certificate).
- Edit Attribute Contract to send the LDAP attribute- email address (Attribute Sources & User Lookup > Attribute Contract Fulfillment).

Configure Identity Provider Settings on Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured the identity provider to communicate with your appliance. See Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 95.

- Copied the identity provider metadata details or the exported metadata file.

Step 1 [New Web Interface Only] On the Security Management appliance, click ✿ to load the legacy web interface.

Step 2 Choose **Management Appliance** > **System Administration** > **SAML**.

Step 3 Under the Identity Provider section, click **Add Identity Provider**.

Step 4 Enter the following details:

Field	Description
Profile Name	Enter a name for the identity provider profile.
Configuration Settings (Manually Configure Identity Provider Settings)	
Entity ID	Enter a globally unique name for the identity provider. The format of the identity provider Entity ID is typically a URI.
SSO URL	Specify the URL to which the service provider must send the SAML authentication requests.
Certificate	If the identity provider signs the SAML assertion, you must upload the identity provider's signing certificate.
Configuration Settings (Importing Identity Provider Metadata)	
Import IDP Metadata	Click **Import Metadata** and select the metadata file.

Step 5 Submit and commit your changes.

What to do next

Enable SSO for Spam Quarantine, on page 98

Enable SSO for Spam Quarantine

Before you begin

Make sure that you have:

- Configured all the settings on **Management Appliance** > **System Administration** > **SAML** page.

- Enabled Spam Quarantine. See Spam Quarantine.

Step 1	[New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.
Step 2	Choose **Management Appliance** > **Centralized Services** > **Spam Quarantine**.
Step 3	Click **Edit Settings** and scroll down to the End-User Quarantine Access section.
Step 4	Make sure that you have enabled End-User Quarantine Access.
Step 5	Set the End-User Authentication method to **SAML2.0**.
Step 6	(Optional) Specify whether to display message bodies before messages are released.
Step 7	Submit and commit your changes.

What to do next

Notify the end users about the new authentication mechanism.

Configuring OpenID Connect 1.0 on Cisco Content Security Management for AsyncOS APIs

Overview

The Cisco Content Security Management Appliance supports integration with applications or clients that use Identity Providers (IDPs) with OpenID Connect 1.0 authentication to connect seamlessly with AsyncOS APIs available in your appliance. Currently, your appliance has been certified with OpenID Connect using Microsoft AD FS only.

Workflow

In the following workflow, AD FS is used as an identity provider, external application as a client, and your appliance as a resource provider.

Steps:

1. In the following workflow, AD FS is used as an identity provider, external application as a client, and your appliance as a resource provider, see Configuring OpenID Connect on Appliance, on page 100.

2. [One-time activity] The appliance fetches the OpenID Connect configuration metadata and the required keys to validate the access token based on the configuration done in step1.

3. Obtain the access token after you authenticate the external application with AD FS. For more information on how to authenticate and receive the access token, see your Authentication Provider or Identity Provider documentation.

4. Send the API request along with the access token to the appliance.

5. The appliance validates the access token in the API request using the key set retrieved from step2.

6. The appliance validates the required claim (issuer, audience) in the access token.

7. The appliance uses the role claim value to authorize and allocate the user role privileges to access the AsyncOS APIs.

8. The appliance provides an appropriate response for the AsyncOS API request.

Sample Access Token

The following is the format of a sample access token:

Header

alg:RSA256

typ:JWT

[….]

Payload

claim:aud: CiscoEmailAPICaller

claim:iss:http://adfsserver/adfs/services/trust

claim:iat: 1594712147

claim:exp: 1594712807

claim: CustomOrgIdentifier: MyCustomOrgId

claim: LastName: Fernandes

claim: FirstName: Erik

claim: Email: http://erik.fernandes@customorg.com

claim: Role: LogCollector

claim: Role: ReadOnly

[.....]

The appliance supports the validation of access tokens signed by the following algorithms only:

- RSA256

- RSA384

- RSA512

Prerequisites

Make sure that you have met the following prerequisites before you configure your appliance with OpenID Connect:

- The authentication provider used by your organization is supported by the appliance.

- The application can authenticate with the authentication provider and retrieve the access token.

- The appliance can connect to the authentication provider over HTTPs to fetch the OpenID Connect metadata configuration.

Configuring OpenID Connect on Appliance

Before you begin

Make sure that you have the following:

- A valid access token issued by the authentication provider (based on your authentication provider setup).

- The access token must include the role information to allow the appliance to perform the required authorization checks.

Step 1 Click **System Administration** > **OpenID Connect** .

Step 2 Click **Edit Settings**

Step 3 Enter the required parameters described in the following table to configure OpenID Connect:

OpenID Connect Parameters	Description
Identity Provider Metadata URL	Enter the identity provider URL used to fetch the OpenID Connect configuration metadata. The metadata is used to validate the access token.
	The following is an example of an identity provider URL -https://example.com/adfs/ .well-known/openid-configuration
Issuer	Enter the value of the issuer of the access token.
	Note The value must match the issuer claim value of the access token when validating the access token.
	The following is an example of an issuer -http://example.com/adfs/services/trust

OpenID Connect Parameters	Description
Audience	Enter the value of the audience that must match the audience claim value of the access token. **Note** Click **Add Row** if you want to add more than one audience value.
Claim Name	Enter the name of the claim in the access token, which contains the user role information. The claim name is used to retrieve the role information from the access token.
Identity Provider to Appliance Role Mapping	Enter a user group role defined in the Identity Provider server and choose a corresponding local user role configured in the appliance to map both roles. **Note** Click **Add Row** if you want to add more than one role mapping record.

Step 4   Submit and commit your changes.

What to do next

Include the access token in the Authorization Bearer header of the AsyncOS API call and send the API request.

The following is an example of invoking an AsynOS API with the access token in the Authorization Bearer header of the API.

```
curl --location --request
GET 'https://sma.com/sma/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'
--header 'Authorization: Bearer <add access_token here>'
```

Configuring OpenID Connect on Appliance using CLI

Use the **oidcconfig** command to perform the following tasks:

- Configure OpenID Connect on your email gateway for AsyncOS APIs.

- Delete OpenID Connect configuration settings on your email gateway.

Customizing Your View

Using Favorite Pages

(Locally-authenticated administrative users only.) You can create a quick-access list of the pages you use most.

To	Do This
Add pages to your favorites list	Navigate to the page to add, then choose **Add This Page To My Favorites** from the My Favorites menu near the top right corner of the window. No commit is necessary for changes to My Favorites.
Reorder favorites	Choose **My Favorites > View All My Favorites** and drag favorites into the desired order.
Edit favorite page, name, or description	Choose **My Favorites > View All My Favorites** and click the name of the favorite to edit.
Delete favorites	Choose **My Favorites > View All My Favorites** and delete favorites.
Go to a favorite page	Choose a page from the **My Favorites** menu near the top right corner of the window.
Return to the main interface	Choose any favorite, or click the **Return to previous page** at the bottom of the page.

Setting Preferences

Administrative users configured on the Security Management appliance

Locally-authenticated users can choose the following preferences, which apply each time the user logs in to the Security Management appliance:

- Language (applies to the GUI)

- Landing page (the page displayed after login)

- Default time range for report pages (available options are a subset of the time ranges available for Email and Web reporting pages)

- Number of rows visible in tables on report pages

Exact options depend on the user role.

To set these preferences, choose **Options > Preferences**. (The Options menu is at the top right side of the GUI window.) Submit your changes when done. Commit is not required.

Tip To return to the page you were viewing before you accessed the Preferences page, click the **Return to previous page** link at the bottom of the page.

Externally authenticated users

Externally authenticated users can choose the display language directly in the Options menu.

General Settings

Monitoring Web Usage Analytics

Usage Analytics is used to provide insight into your site activity data for analytical statistics. If Usage Analytics is enabled, the appliance collects the feature usage data of the appliance on the new web interface. The usage statistics are used to analyze and provide insight to improve the user experience of the appliance.

Step 1 [New Web Interface Only] On the Security Management appliance, click ✿ to load the legacy web interface.

Step 2 Choose **Management Appliance** > **System Administration** > **General Settings**.

Step 3 Click on **Edit Settings**.

Step 4 Select the **Enable** check box in the Usage Analytics field.

Step 5 Submit and commit your changes.

Improving Web Interface Rendering

For better web interface rendering, Cisco recommends that you enable Internet Explorer Compatibility Mode Override.

Note If enabling this feature is against your organizational policy, you may disable this feature.

Step 1 [New Web Interface Only] On the Security Management appliance, click ✿ to load the legacy web interface.

Step 2 Choose **Management Appliance** > **System Administration** > **General Settings**.

Step 3 Click on **Edit Settings**.

Step 4 Select the **Enable** check box in the Override IE Compatibility Mode field.

Step 5 Submit and commit your changes.

Restarting and Viewing Status of Services Enabled on Appliance

You can use the `diagnostic > services` sub command in the CLI to:

- Restart the services enabled on your appliance without having to reboot your appliance.

- View the status of the services enabled on your appliance.

Example: Viewing Status of Reporting Service

In the following example, the `services` command is used to view the status of the reporting service enabled on your appliance.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> reporting

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Reporting has been up for 28d 20h 45m 35s.
```

Example: Restarting the Message Tracking Service

In the following example, the `services` command is used to restart the message tracking service enabled on your appliance.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> tracking

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

Managing Lists of Certificate Authorities

The appliance uses stored trusted certificate authorities to verify a certificate from a remote domain to establish the credentials of the domain. You can configure the security management appliance to use the following trusted certificate authorities:

- System list- The appliance has a pre-installed list of trusted certificate authorities. This is called the system list.

- Custom list- You can customize a list of trusted certificate authorities, and then import the custom list into the appliance.

Note You can use either the system list or the customized list, or both to verify certificate from a remote domain.

Manage the lists using the **Network > Certificates > Edit Certificate Authorities** page in the GUI or the **certconfig** > **certauthority** command in the CLI.

On the **Network > Certificates > Edit Certificate Authorities** page, you can perform the following tasks:

- Choose whether or not to use the system list. You can enable or disable the system list. For more information, see Disabling the System Certificate Authority List, on page 105.

- Choose whether or not to use a custom certificate authority list. You can enable the appliance to use a custom list and then import the list from a text file. For more information, see Importing a Custom Certificate Authority List, on page 106 .

- Export the list of certificate authorities. You can export either the system or customized list of certificate authorities to a location in your local drive. For more information, see Exporting a Certificate Authority List, on page 106.

On the **Network > Certificates > Manage Trusted Root Certificates** page, you can perform the following tasks:

- View the custom and system list of certificates. For more information, see Displaying Trust Root Certificate, on page 107.

- Delete an existing certificate. You can delete a custom certificate that you have imported. For more information,see Deleting Custom Certificate, on page 107

Disabling the System Certificate Authority List

The pre-installed system certificate authorities list cannot be removed from the appliance, but you can enable or disable it. You can disable it to allow the appliance to only use your list to verify certificates from remote hosts.

Procedure

	Command or Action	Purpose
Step 1	Navigate to the **Network > Certificates** page.	
Step 2	Click **Edit Settings** in the Certificate Authorities section.	
Step 3	Click **Disable** for the System List.	
Step 4	Submit and commit your changes.	

Importing a Custom Certificate Authority List

You can create a custom list of trusted certificate authorities and import it onto the appliance. The file must be in the PEM format and include certificates for the certificate authorities that you want the appliance to trust.

Step 1 Click **Network > Certificate**.

Step 2 Click **Edit Settings**.

Step 3 Choose the **Enable** radio button.

Step 4 Click **Choose File** in Custom List.

Step 5 Browse to the location where the certificate resides, and click **Ok**.

Step 6 [Optional] Select the FQDN Validation check box to allow the email gateway to check whether the 'Common Name', 'SAN: DNS Name' fields, or both present in the certificate, are in the FQDN format.

Step 7 Click **Submit**.

Note Below checks will done on CA import,

- Expiry

- Duplication

- CA flag is present and Set to "True"

- Root Certificate Authority is present if importing Intermediate Certificate Authority is imported.

Exporting a Certificate Authority List

If you want to use only a subset of the trusted certificate authorities in the system or edit an existing custom list.

Note You can export the custom list to a .txt file, edit to add or remove certificate authorities, and then import the file back onto the appliance as a custom list.

Step 1   Click **Network > Certificate**.

Step 2   Click **Edit Settings**.

        The Edit Settings list the custom and Cisco trusted root certificates.

Step 3   Click the Certificate name.

Step 4   Click **Export** to export the certificate.

Displaying Trust Root Certificate

Step 1   Click **Network > Certificate**.

Step 2   Click **Manage Trusted Root Certificates**.

        The Manage Trusted Root Certificates lists the custom and Cisco trusted root certificates.

Step 3   Check the **Override Trust** check box to override the trust.

Step 4   Click **Submit**.

        In the Manage Trusted Root Certificates page, you can click on Download Certificate to download and store the certificate to your local machine.

Deleting Custom Certificate

Step 1   Click **Network > Certificate**.

Step 2   Click **Manage Trusted Root Certificates**.

        The Manage Trusted Root Certificates lists the custom certificates.

Step 3   Click **Delete** to delete a custom trusted root certificate.

Step 4   Click **Submit**.

Receiving and Delivering Messages with Internationalised Domain Names (IDNs)

The Cisco Secure Email and Web Manager can receive and deliver messages with email addresses that contain IDN domains.

Currently, your email gateway provides support of IDN domains for the following languages only:

Indian Regional Languages: Hindi, Tamil, Telugu, Kannada, Marati, Punjabi, Malayalam, Bengali, Gujarati, Urdu, Assamese, Nepali, Bangla, Bodo, Dogri, Kashmiri, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, and Tulu.

European and Asian Languages: French, Russian, Japanese, German, Ukrainian, Korean, Spanish, Italian, Chinese, Dutch, Thai, Arabic, and Kazakh.

Related Topics

Prerequisites IDN

Make sure you have met the following prerequisites before you use the Internationalised Domain Names (IDN) feature:

- All incoming messages must have IDNs encoded in UTF-8.

  For Example: An MTA that sends messages to the email gateway must support IDNs and make sure the domains in the messages are in the UTF-8 format.

- All outgoing messages must have IDNs encoded in UTF-8, and the destination server must accept and support IDNs accordingly.

  For Example: An MTA that accepts messages from the email gateway must support IDNs and domains encoded in the UTF-8 format.

- In all applicable DNS records, IDNs must be configured using the Punycode format

  For Example: When you configure an MX record for an IDN, the domain in the DNS record must be in the Punycode format.

Features Configurable using IDN Domains in Cisco Secure Email and Web Manager

For this release, you can only configure the following features using IDN domains in your Cisco Secure Email and Web Manager :

- **SMTP Routes Configuration Settings:**

  - Add or edit IDN domains.

  - Export or import SMTP routes using IDN domains.

- **DNS Configuration Settings:** Add or edit the DNS server using IDN domains.

- **Reporting Configuration Settings:** View IDN data - usernames, email addresses, and domains) in the reports.

- **Message Tracking Configuration Settings:** View IDN data- usernames, email addresses, and domains) in message tracking.

- **Policy, Virus, and Outbreak Quarantine Configuration Settings:**

- View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine.

- View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware.

- View messages with IDN domains caught by message filters, content filters, and DLP message actions.

- **Spam Quarantine Configuration Settings:**

  - View messages with IDN domains detected as spam or suspected spam.

  - Add email addresses with IDN domains to the safelist and blocklist categories.

- **End User Quarantine-** IDN support with Authentication Mode as NONE. Other auth modes are not supported in this phase.

FQDN

A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the internet. For a X.509 certificate, the FQDN validation validates the common name field (CN) of that certificate's subject distinguished name and the subjectAltName extension of type dNSName (SAN:dNSName). AsyncOS validates the domain name and the certificates for the common name and SAN:dNSName in its fields. Preferably the SAN:dNSName names are used. Examples of valid FQDN include example.com, *.example.com.

The criteria for FQDN compliance includes:

- Either the CN or the SAN:dNSName should be present in the certificate and AsyncOS mandates that either one should be FQDN compliant.

- Both the CN and SAN:dNSName are present in the certificate and AsyncOS mandates that both should be FQDN compliant.

The variants include:

- Validation on Peer Certificate, on page 109

- Custom CA Validation, on page 110

- Appliance Certificate Validation, on page 111

When you perform an add or import of the appliance certificate, Cisco Secure Email and Web Manager performs FQDN validation on the certificate when its FQDN validation is enabled and during the peer certificate validation of the server. All detailed logging is tracked in the Cisco Secure Email and Web Manager system.current or gui.current log files. However; Cisco Secure Email and Web manager does not enable you to import a certificate that does not have a common name (CN) and has an alternate subject name without a critical extension.

Validation on Peer Certificate

AsyncOS provides a common configuration to control FQDN validation for all services under SSL configuration, for example TLS. However, you must enable the FQDN service manually.

- Validation on Peer Certificate Using the GUI, on page 110

Validation on Peer Certificate Using the GUI

Step 1   Go to **System Administration > SSL Configuration** page.

Step 2   Click **Edit Settings.**

Step 3   Check the **Enable** checkbox listed with Peer Certificate FQDN Validation.

Step 4   Click **Submit.**

Validation on Peer Certificate Using the CLI

You must enter the sslconfig command to perform a validation on peer certificate.

Before you begin

prompt> sslconfig

```
Disabling SSLv3 is recommended for best security.
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be
sequential. So to avoid communications errors, always select a contiguous set
of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1
disabled.
Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater and LDAP.
```

Custom CA Validation

AsyncOS enables you to perform a FQDN validation when you import the custom certificate authority into the appliance. You must enable the validation manually.

Step 1   Enter the command CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT

```
Enter in the command-line interface the CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT command
```

Step 2   Enter the filename of the file you want to import.

```
Enter the name of the file on machine "appliance" to import:
[]> filename.pem
```

Step 3   Confirm if you want to check for FQDN.

```
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN) format ? [N]> y
```

Appliance Certificate Validation

AsyncOS enables you to perform a FQDN validation when you import the appliance certificate into the appliance. You must enable the validation manually.

Step 1 Enter the CERTCONFIG > CERTIFICATE > SETUP command.

```
Prompt>  CERTCONFIG > CERTIFICATE > SETUP >
```

Step 2 Enter if you want the intermediate certificate.

```
Do you want to add an intermediate certificate? [N]>
```

Step 3 Enter if you want to check for FQDN.

```
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN) format ? [N]> y
```

Single Pane of Glass

The Single Pane of Glass (SPoG) feature enables you to access Cisco Secure Email and Web Manager details on a single primary Cisco Secure Email and Web Manager. You must ensure that you have multiple Cisco Secure Email and Web Manager units connected to a primary Cisco Secure Email and Web Manager unit. You can view information for example Monitoring, Tracking, Quarantine of the secondary Cisco Secure Email and Web Manager units on a primary unit. However, to perform this, you must enable the configuration using the command line interface of the primary Cisco Secure Email and Web Manager.

Before you begin

Make sure all the Secure Email and Web Manager devices have the same version.

To enable the drop-down and gather information in the primary Cisco Secure Email and Web Manager unit, you must use the **smaapplianceconfig** command.

Once you enable the configuration, you can view the details of the secondary Cisco Secure Email and Web Managers in the primary unit, see

Note When you enable or disable SPoG, the session of all the users concurrently logged into NGUI becomes invalid, and a new request to the server logs them out. The users must log in again.

Also, if a Secure Email and Web Manager is added to SPoG or deleted from SPoG, and you are currently logged into the NGUI of the same Secure Email and Web Manager, then you will be logged out due to a change in the flow of JWT validation.

Using the **smaapplianceconfig** command you can:

SPoG Add a Cisco Secure Email and Web Manager

The following example shows how you can add a Cisco Secure Email and Web Manager.

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ====== ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> ADD
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[]> vm21sma0062.cs21
Enter a name to identify this appliance
[]> SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Enter the login credentials for an administrator or an operator account on the appliance.
This will be used to obtain an SSH key for file transfers.
Username:
[]> admin
Passphrase:
[]>
Appliance 10.10.3.62 added.
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> added vm21sma0062.cs21
Changes committed: Tue Apr 27 10:28:01 2021 GMT
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
```

```
= =========== ======= ============= ========= ======== ===========
1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
```

SPoG Edit a Cisco Secure Email and Web Manager

The following example shows how you can edit a secondary Cisco Secure Email and Web Manager connection parameters.

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> EDIT
Enter the name or number of the appliance you wish to edit.
[]> 3
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[10.10.3.62]>
Enter a name to identify this appliance
[SMA0062]> Tracking_SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Appliance 10.10.3.62 was edited
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============= ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA63" at address 10.10.3.63:
------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Would you like Email Reporting to be enabled on this appliance? [N]>
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]>
Services for appliance "SMA63" at address 10.10.3.63:
```

```
------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> services
Enter the name or number of the appliance you wish to configure.
[]> 3
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
------------------------------------------------------------------------
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Would you like Email Reporting to be enabled on this appliance? [Y]> N
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]> N
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Disabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============= ========= ======== ===========
1 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> use vm21sma0062.cs21 for tracking
Changes committed: Tue Apr 27 10:32:32 2021 GMT
```

SPoG Delete a Cisco Secure Email and Web Manager

The following example shows how you can delete a Cisco Secure Email and Web Manager.

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
```

```
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============== ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> DELETE
Enter the name or number of the appliance you wish to delete.
[]> 3
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ====== ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> deleting Tracking_SMA0062
Changes committed: Tue Apr 27 10:37:12 2021 GMT
vm21sma0061.cs21>
```

SPoG Enable Services on a Cisco Secure Email and Web Manager

The following example shows how you can enable services on a Cisco Secure Email and Web Manager.

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA0062" at address 10.10.3.62:
--------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Disabled
Spam Quarantines service: Disabled
Would you like Email Reporting to be enabled on this appliance? [N]> Y
Would you like Email Tracking to be enabled on this appliance? [N]> Y
Would you like Spam Quarantines to be enabled on this appliance? [N]> Y
Services for appliance "SMA0062" at address 10.10.3.62:
```

```
------------------------------------------------------------------------
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> anabled services on vm21sma0062.cs21
Changes committed: Tue Apr 27 10:29:17 2021 GMT
vm21sma0061.cs21>
```

SPoG Viewing details on primary Cisco Secure Email and Web Manager

To view the details of the secondary units, you must:

- Navigate to the Quarantine page of the primary Cisco Secure Email and Web Manager unit.

- Select the secondary Cisco Secure Email and Web Manager from the **View SMA** drop down.

You can now view the data corresponding to the selected secondary Cisco Secure Email and Web Manager on your primary unit.

You can also view the same in both the Tracking and Monitoring pages after you enable using the **services** sub command in the **smaapplianceconfig** command.