System Administration

This chapter contains the following sections:

Note Several of the features or commands described in this section will affect, or be affected by routing precedence. Please see *Appendix B "IP Addresses Interfaces and Routing"* for more information.

Management of the Appliance

The following tasks allow you to easily manage the common functions within the appliance .

Shutting Down or Rebooting the Appliance

After you shut down or reboot, you may restart the appliance later without losing any messages in the delivery queue.

You can use the s hutdown or reboot command in the CLI, or use the web interface:

Procedure

Step 1 Select **System Administration** > **Shutdown/Suspend**.

Step 2 In the **System Operations** section, choose **Shutdown** or **Reboot** from the **Operation** drop-down list.

Step 3 Enter a number of seconds to wait to allow open connections to complete before forcing them to close.

The default delay is thirty (30) seconds.

Step 4 Click **Commit**.

Suspending Email Receiving and Delivery

AsyncOS allows you to suspend receiving and delivering of emails. You can suspend:

- Receiving of emails on a particular listener or multiple listeners.
- Delivery of all emails or emails to a particular domain or multiple domains.

Use the suspend command in the CLI, or use the web interface:

Procedure

Step 1 Select **System Administration** > **Shutdown/Suspend**.

Step 2 Suspend receiving of emails on a particular listener or multiple listeners.

In the **Mail Operations** section, select the functions and/or listeners to suspend. If the appliance has multiple listeners, you can suspend email receiving on individual listeners.

Step 3 Suspend the delivery of all emails or emails to a particular domain or multiple domains. Depending on your requirements, do one of the following:

a. To suspend the delivery of all emails, in **Specify Domain(s)/Subdomain(s)** field, enter ALL, and press **Enter**.

b. To suspend the delivery of emails to a specific domain or subdomain, in **Specify Domain(s)/Subdomain(s)** field, enter the domain or subdomain name or IP address, and press **Enter**. Use comma-separated text to add multiple entries.

Step 4 Enter number of seconds to wait to allow open connections to complete before forcing them to close.

If there are no open connections, the system goes offline immediately.

The default delay is 30 seconds.

Step 5 Click **Commit**.

What to do next

When you are ready to resume suspended services, see Resuming Suspended Email Receiving and Delivery , on page 3.

Resuming Suspended Email Receiving and Delivery

Use the Shutdown/Suspend page or the r esume command to resume the suspended receiving and delivery of emails.

Procedure

Step 1 Select **System Administration** > **Shutdown/Suspend**.

Step 2 In the **Mail Operations** section, select the functions and/or listeners to resume.

If the appliance has multiple listeners, you can resume email receiving on individual listeners.

Step 3 Resume the delivery of all emails or emails to a particular domain or multiple domains.

In **Specify Domain(s)/Subdomain(s)** field, click the close icon on the intended entry.

Step 4 Click **Commit**.

Resetting to Factory Defaults

Caution Do not reset to factory defaults if you are not able to reconnect to the web interface or CLI using the Serial interface or the default settings on the Management port through the default Admin user account.

When physically transferring the appliance , you may want to start with factory defaults. Resetting to factory settings is extremely destructive, and it should only be used when you are transferring the unit or as a last resort to solving configuration issues. Resetting to factory defaults disconnects you from the web interface or CLI, disabling services that you used to connect to the appliance (FTP, SSH, HTTP, HTTPS), and even removing additional user accounts you had created. You can reset to factory default:

- On web interface, click the Reset button in the **System Administration > Configuration File** page, or click the Reset Configuration button in the **System Administration> System Setup Wizard**.
- On CLI, use the **`resetconfig`** command.

Note The **`resetconfig`** command only works when the appliance is in the offline state. The appliance returns to the online state after resetting to factory settings.

Next Steps

- Run the System Setup wizard. For more information, refer to Using the System Setup Wizard
- Turn on mail delivery to resume mail delivery.

Displaying the Version Information for AsyncOS

To determine which version of AsyncOS is currently installed on your appliance , use the System Overview page from the Monitor menu in the web interface (see System Status), or use the version command in the CLI.

Email Security Appliance Licensing

Feature Keys

On Cloud Email Security appliances , avoid changing feature key settings.

Adding and Managing Feature Keys

For physical appliances , feature keys are specific to the serial number of the appliance and specific to the feature being enabled (you cannot re-use a key from one system on another system).

To work with feature keys in the CLI, use the **`featurekey`** command.

Procedure

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

Step 2 Perform actions:

To	Do This
View the status of active feature keys	Look at the **Feature Keys for <serial number>** section.
View feature keys that have been issued for your appliance but are not yet activated	Look at the **Pending Activation** section. If you have enabled automatic download and activation, feature keys will never appear in this list.
Check for recently-issued feature keys	Click the **Check for New Keys** button in the Pending Activation section. This is useful if you have not enabled automatic download and activation of feature keys, or if you need to download feature keys before the next automatic check.
Activate an issued feature key	Select the key in the **Pending Activation** list and click **Activate Selected Keys.**
Add a new feature key	Use the **Feature Activation** section.

What to do next

Related Topics

- Automating Feature Key Download and Activation , on page 5
- Configuration File Page, on page 18

Automating Feature Key Download and Activation

You can set the appliance to automatically check for, download, and activate feature keys that are issued for this appliance .

Procedure

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

Step 2 Click **Edit Feature Key Settings**.

Step 3 To see frequency of checks for new feature keys, click the (?) help button.

Step 4 Specify settings.

Step 5 Submit and commit your changes.

What to do next

Related Topics

- Adding and Managing Feature Keys , on page 4

Expired Feature Keys

If a feature key is expiring, the appliance sends out alerts 90 days, 60 days, 30 days, 15 days, 5 days, one day prior to the key expiration, and at the time of key expiration. To receive these alerts, make sure that you have subscribed to the System Alerts. For more information, see Alerts, on page 39.

If the feature key for the feature you are trying to access (using the web interface) has expired, please contact your Cisco representative or support organization.

Smart Software Licensing

Overview

Smart Software Licensing enables you to manage and monitor 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.

Before you begin

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

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

Note A covered user is the total number of internet-connected employees, subcontractors, and other authorized individuals covered by your email gateway deployment (on-premises or cloud, whichever is applicable.)

For covered 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 covered 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 **Security Services -> Service updates**

Note For virtual covered 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.

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

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing, on page 8
Step 2	Register the appliance with Cisco Smart Software Manager	Registering the Appliance with Cisco Smart Software Manager, on page 8

	Do This	More Informaton
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 9

Enabling Smart Software Licensing

Procedure

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

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

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

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

Step 4 Commit your changes.

What to do next

After you enable Smart Software Licensing, all the features in the Classic Licensing mode will be automatically available in the Smart Licensing mode. If you are an existing covered 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 covered 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 covered users with active licenses in Classic Licensing mode will have evaluation period. If new virtual appliance covered 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.

Procedure

Step 1 Go to **System Administration** > **Smart Software Licensing** page in your email gateway.

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

Step 3 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 4 Switch back to your appliance and paste the Product Instance Registration Token.

Step 5 Click **Register**.

Step 6 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 10.

What to do next

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

Requesting for Licenses

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

Procedure

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

Step 2 Click **Edit Settings**.

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

Step 4 Click **Submit**.

Note By default the licenses for Mail Handling and Email Security Appliance Bounce Verification are available. You cannot activate, deactivate, or release these licenses.

There is no evaluation period or out of compliance for Mail Handling and Email Security Appliance Bounce Verification licenses. This is not applicable for virtual appliances .

What to do next

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

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

Deregistering the Appliance from Smart Cisco Software Manager

Procedure

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

Step 2 From the **Action** drop-down list, choose **Deregister** and click **Go**.

Step 3 Click **Submit**.

Reregistering the Appliance with Smart Cisco Software Manager

Procedure

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

Step 2 From the **Action** drop-down list, choose **Reregister** and click **Go**.

What to do next

See Registering the Appliance with Cisco Smart Software Manager, on page 8 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 to know how to change the transport settings.

Renewing Authorization and Certificate

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

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

Procedure

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

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

- Renew Authorization Now
- Renew Certificates Now

Step 3 Click **Go**.

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

Updating Smart Agent

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

Procedure

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

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

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

Smart Licensing in Cluster Mode

Note The cluster management of smart licensing feature happens only in the machine mode. In smart licensing cluster mode, you can log into any of the appliances and configure smart licensing feature. You can log into an appliance and access other appliances one by one in the cluster and configure the smart licensing feature without logging off from the first appliance.

For more information, see Centralized Management Using Clusters.

Cisco Email Security Virtual ApplianceVirtual Email Gateway License

To set up and license a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide* . This document is available from the location specified in .

Note You cannot open a Technical Support tunnel or run the System Setup Wizard before installing the virtual appliance license.

Virtual Appliance License Expiration

After the virtual appliance license expires, the appliance will continue to deliver mail without security services for 180 days. Security service updates do not occur during this period.

Alerts will be sent 180 days, 150 days, 120 days, 90 days, 60 days, 30 days, 15 days, 5 days, 1 day and 0 seconds before the license expires, and at the same intervals before the grace period ends. These alerts will be of type “System” at severity level “Critical.” To ensure that you receive these alerts, see Adding Alert Recipients, on page 40.

These alerts are also logged in the system log.

Individual feature keys may expire earlier than the virtual appliance license. You will also receive alerts when these approach their expiration dates.

Related Topics

- Reverting AsyncOS on Virtual Appliances May Impact the License , on page 35

Managing the Configuration File

All configuration settings within the appliance can be managed via a single configuration file. The file is maintained in XML (Extensible Markup Language) format.

You can use this file in several ways:

- 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 web interface for making configuration changes.
- You can upload entire configuration file via FTP access, or you can paste portions of or an entire configuration file directly into the CLI.
- Because the file is in XML format, an associated DTD (document type definition) 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.)

Managing Multiple Appliances with XML Configuration Files

- You can download an existing configuration file from one appliance , make changes to it, and upload it to a different appliance . This lets you manage an installation of multiple appliances more easily. Currently you may not load configuration files from C/X-Series appliances onto an M-Series appliance.
- You can divide an existing configuration file downloaded from one appliance into multiple subsections. You can modify those sections that are common among all applianceS (in a multiple appliance environment) and load them onto other appliances as the subsections are updated.

For example, you could use an appliance in a test environment for testing the Global Unsubscribe command. When you feel that you have configured the Global Unsubscribe list appropriately, you could then load the Global Unsubscribe configuration section from the test appliance to all of your production appliances .

Managing Configuration Files

To manage configuration files on your appliance , click the System Administration> Configuration File.

The Configuration File page contains the following sections:

- **Current Configuration** - used to save and export the current configuration file.
- **Load Configuration** - used to load a complete or partial configuration file.
- **End-User Safelist/Blocklist Database (Spam Quarantine)** - For information, see Using Safelists and Blocklists to Control Email Delivery Based on Sender and Backing Up and Restoring the Safelist/Blocklist.
- **Reset Configuration** - used to reset the current configuration back to the factory defaults (you should save your configuration prior to resetting it).

Note The private keys and certificates are included in unencrypted PEM format along with the configuration file with encrypted passphrase.

Related Topics

- Saving and Exporting the Current Configuration File, on page 14
- Loading a Configuration File, on page 15
- Mailing the Configuration File, on page 15
- Resetting the Current Configuration, on page 17

Saving and Exporting the Current Configuration File

Using the **Current Configuration** section of the **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.

The following information is not saved with the configuration file:

- Certificates used for secure communications with services used by the URL filtering feature.
- CCO User IDs and Contract ID saved on the Contact Technical Support page.

You can mask the user's passphrases by clicking the **Mask passphrases in the Configuration Files** checkbox. Masking a passphrase causes the original, encrypted passphrase to be replaced with "*****" in the exported or saved file. Please note, however, that configuration files with masked passphrases cannot be loaded back into AsyncOS.

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
- DK/DKIM signing keys
- 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.

Mailing the Configuration File

Use the Email file to field in the System Administration > Configuration File or use the m ailconfig command to email the current configuration to a user as an attachement.

Loading a Configuration File

Use the Load Configuration section of the **System Administration > Configuration File** page to load new configuration information into the appliance . You can also configure this in the command-line interface using the `loadconfig` command.

You can load information in one of three methods:

- Placing information in the `configuration` directory and uploading it.
- Uploading the configuration file directly from your local machine.
- Pasting configuration information directly.

Note Configuration files with masked passphrases cannot be loaded.

In cluster mode, you can either choose to load the configuration for a cluster or an appliance . For instructions to load cluster configuration, see Loading a Configuration in Clustered Appliances.

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 (document type definition) located in the `configuration` directory on your 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 either method, you can import an entire configuration file (the information defined between the highest level tags: `<config></config>`), or a *complete* and *unique* sub-section 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 this:

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

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosu

</config>
```

will cause validation errors, while uploading. This, however:

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

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosupport_enabled>

</config>
```

will not.

"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 this (including the declarations and `<config></config>` tags):

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

is allowed. However, a system can have multiple listeners defined, each with different Recipient Access Tables defined, so uploading only this:

```
<rat>

       <rat_entry>

              <rat_address>ALL</rat_address>

         <access>RELAY</access>

     </rat_entry>

</rat>
```

is considered ambiguous and 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.

If disk space allocations in the configuration file are smaller than the amount of data currently stored on the appliance , the oldest data will be deleted to meet the quota specified in the configuration file.

Empty vs. 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 this:

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

will remove all listeners from the system!

Caution When uploading or pasting subsections of a configuration file, you have the potential to disconnect yourself from the web interface or CLI and to 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 your configuration data prior to 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 will fail and alerts will be 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. Note that the encoding attribute is specified in the file whenever you issue the `showconfig` , `saveconfig` , or `mailconfig` commands:

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

Currently, only configuration files with this encoding can be loaded.

Related Topics

- Loading a Configuration in Clustered Appliances

Resetting the Current Configuration

Resetting the current configuration causes your appliance to revert back to the original factory defaults. You should save your configuration prior to resetting it. Resetting the configuration via this button in the GUI is not supported in a clustering environment.

See Resetting to Factory Defaults, on page 3.

Viewing the Configuration File

You can view the configuration file details using the `showconfig` command only. 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: IronPort 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.]
```

Configuration File Page

- Managing the Configuration File, on page 13
- Resetting to Factory Defaults, on page 3
- Backing Up and Restoring the Safelist/Blocklist

Managing Disk Space

- (Virtual Appliances Only) Increasing Available Disk Space , on page 18
- Viewing and Allocating Disk Space Usage , on page 19
- Managing Disk Space for the Miscellaneous Quota , on page 19
- Ensuring That You Receive Alerts About Disk Space , on page 20

(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.

To add disk space to the virtual appliance instance:

Note Disk space reduction is not supported. See the VMWare documentation for information.

Before You Begin

Carefully determine the disk space increase needed.

Procedure

Step 1 Bring down the 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. At time of release, this information for ESXi 5.5 was 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 Go to **System Administration > Disk Management** and verify that your change has taken effect.

Viewing and Allocating Disk Space Usage

You can optimize disk usage by allocating disk space on the appliance among the features that your deployment uses.

To	Do This
• View disk space quotas and current usage for each service • Reallocate disk space on your appliance at any time	Go to **System Administration > Disk Management**.
Manage data volume	• For reporting and tracking services and the spam quarantine, the oldest data will be deleted automatically. • For Policy, Virus and Outbreak quarantines, the default action configured in the quarantine will be taken. See Default Actions for Automatically Processed Quarantined Messages. • For the Miscellaneous quota, you must first manually delete data to reduce usage below the new quota you will set. See Managing Disk Space for the Miscellaneous Quota , on page 19.

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 **System Administration > Log Subscriptions** and: • Look to see which log directories 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**.

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 FTP, SSH, and SCP Access
Quota size	Go to **System Administration > Disk Management.**

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 Alerts, on page 39.

Disk Space and Centralized Management

Disk space management is available only in machine mode, not in group or cluster mode.

Managing Security Services

The Services Overview page lists the current service and rule versions of the following engines:

- Graymail
- McAfee
- Sophos

You can perform the following tasks in the Services Overview page:

- Manually update the engines. For more information, see Manually Updating the Engines, on page 21
- Rollback to previous version of the engine. For more information, see Rollback to Previous Version of Engine, on page 21

The **Auto Update** column shows the status of the automatic updates of a particular engine. If you want to enable or disable Automatic Updates, go to the **Global Settings** page of particular engine.

When automatic updates are disabled for a specific service engine, you will receive alerts periodically. If you want to change the alert interval, use the **Alert Interval for Disabled Automatic Engine Updates** option in the Security Services > Service Updates page.

Note Auto Updates are disabled automatically for the engine on which the rollback is applied.

Related Topics

- Manually Updating the Engines, on page 21
- Rollback to Previous Version of Engine, on page 21

• Viewing Logs, on page 21
• System Alerts, on page 46

Manually Updating the Engines

Procedure

Step 1 Go to **Security Services** > **Services Overview** page.

Step 2 Click **Update** in the **Available Updates** column for the latest service or rule version of the service engine.

Note The **Update** option is available only if new updates are available for the particular engine.

Rollback to Previous Version of Engine

Procedure

Step 1 Go to **Security Services** > **Services Overview** page.

Step 2 Click **Change** in the **Modify Versions** column.

Step 3 Select the required rule and service version of the update and click **Apply**.

The appliance rolls back the engine to the previous version.

Note A Service Updates includes the service version and the rule version together as a package.

Once you click **Apply**, the automatic updates for the particular engine is automatically disabled. To enable the automatic updates, go to the Global Settings page of the particular engine.

Viewing Logs

The information about engine rollback and disabling automatic updates is posted to the following logs:

- **Updater Logs**: Contains information about the engine rollback and automatic updating of the engine. Most information is at Info or Debug level.

  For more information, see Updater Log Example.

Service Updates

The following services require updates for maximum effectiveness:

- Feature Keys
- McAfee Anti-Virus definitions
- PXE Engine

- Sophos Anti-Virus definitions
- IronPort Anti-Spam rules
- Outbreak Filters rules
- Time zone rules
- URL categories (Used for URL filtering features. For details, see Future URL Category Set Changes)
- Enrollment client (Used for updating certificates needed for communication with cloud-based services used for URL filtering features. For information, see About the Connection to Talos Intelligence Services.)
- Graymail rules

Note Settings for the DLP engine and content matching classifiers are handled on the **Security Services** > **Data Loss Prevention** page. See About Updating the DLP Engine and Content Matching Classifiers for more information.

Service update settings are used for all services that receive updates except DLP updates. You cannot specify unique settings for any individual service except DLP updates.

To set up the network and the appliance to obtain these critical updates, see Setting Up to Obtain Upgrades and Updates , on page 22.

Setting Up to Obtain Upgrades and Updates

Options for Distributing Upgrades and Updates

There are several ways to distribute AsyncOS upgrade and update files to your appliances:

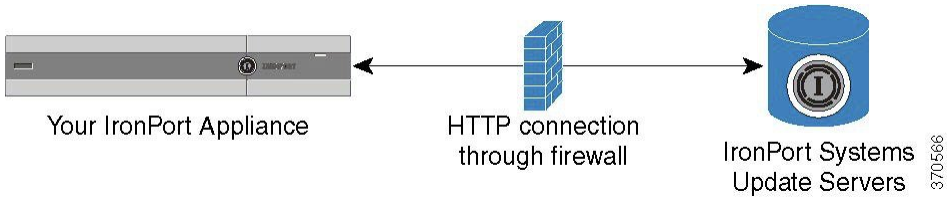
- Each appliance can download the files directly from the Cisco update servers. This is the default method.
- You can download the files from Cisco once, and then distribute them to your appliances from a server within your network. See Upgrading and Updating from a Local Server, on page 23.

To choose and configure a method, see Configuring Server Settings for Downloading Upgrades and Updates , on page 26.

Configuring Your Network to Download Upgrades and Updates from the Cisco Servers

The appliance connect directly to the Cisco update servers to find and download upgrades and updates:

Figure 1: Streaming Update Method



Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location instead. For more information, see Configuring the Appliance for Upgrades and Updates in Strict Firewall Environments, on page 23.

Create a firewall rule to allow downloading of upgrades from Cisco update servers on ports 80 and 443.

Configuring the Appliance for Upgrades and Updates in Strict Firewall Environments

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

Procedure

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

Step 2 Create a firewall rule to allow downloading of upgrades and updates from the static IP address on port 80.

Step 3 Choose **Security Services > Service Updates**.

Step 4 Click **Edit** Update Settings.

Step 5 On the Edit Update Settings page, in the “Update Servers (images)” section, choose Local Update Servers and enter the static URL received in step 1 in the Base URL field for AsyncOS upgrades and McAfee Anti-Virus definitions.

Step 6 Verify that IronPort Update Servers is selected for the “Update Servers (list)” section.

Step 7 Submit and commit your changes.

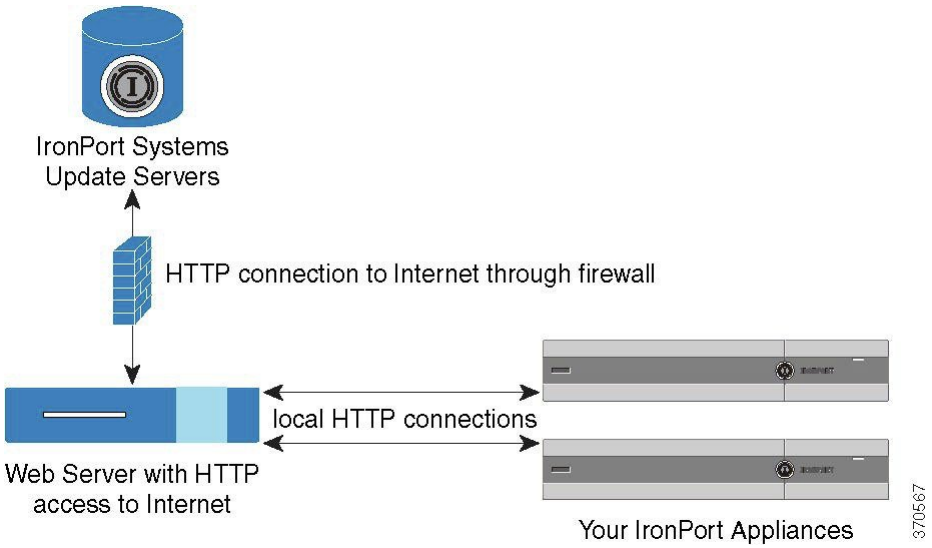
Upgrading and Updating from a Local Server

You can download AsyncOS upgrade images to a local server and host upgrades from within your own network rather than obtaining upgrades directly from Cisco’s update servers. Using this feature, an upgrade image is downloaded via HTTP to any server in your network that has access to the Internet. If you choose to download the upgrade image, you can then configure an internal HTTP server (an “update manager”) to host the AsyncOS images to your appliances.

Use a local server if your appliance does not have access to the internet, or if your organization restricts access to mirror sites used for downloads. Downloading AsyncOS upgrades to each appliance from a local server is generally faster than downloading from the Cisco IronPort servers.

Note Cisco recommends using a local server only for AsyncOS upgrades. If you use a local update server for security update images, the local server does not automatically receive security updates from Cisco IronPort, so the appliances in your network may not always have the most current security services.

Figure 2: Remote Update Method



Procedure

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

Step 2 Download the upgrade files.

Step 3 Configure the appliance to use the local server using either the **Security Services** > **Service Updates** page in the GUI or the **`updateconfig`** command in the CLI.

Step 4 Upgrade the appliance using either the **System Administration** > **System Upgrade** page or the upgrade command in the CLI.

Hardware and Software Requirements for Upgrading and Updating from a Local Server

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

- Internet access to the Cisco Systems update servers.
- A web browser (see Browser Requirements).

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 — which:
  - 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 an Upgrade Image on a Local Server

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 (for a physical appliance) or a VLN (for a virtual appliance) and the version number of the appliance . You will then be presented with a list of available upgrades. Click on the upgrade version that you want to download, and unzip the ZIP file in the root directory on the local server while keeping the directory structure intact. To use the upgrade image, configure the appliance to use the local server on the Edit Update Settings page (or use updateconfig in the CLI).

The local server also hosts an XML file that limits the available AsyncOS upgrades for the appliances on your network to the downloaded upgrade image. This file is called the "manifest." The manifest is located in the asyncos directory of the upgrade image ZIP file. After unzipping the ZIP file in the root directory of the local server, enter the full URL for the XML file, including the filename, on the Edit Update Settings page (or use updateconfig in the CLI).

For more information about remote upgrades, please see the Knowledge Base or contact your Cisco Support provider.

UpdatesThrough a Proxy Server

The appliance is configured (by default) to connect directly to Cisco's update servers to receive updates. This connection is made by HTTP on port 80 and the content is encrypted. If you do not want to open this port in your firewall, you can define a proxy server and specific port from which the appliance can receive updated rules.

If you choose to use a proxy server, you can specify an optional authentication and port.

Note If you define a proxy server, it will *automatically* be used for all service updates that are configured to use a proxy server. There is no way to turn off the proxy server for updates to any individual service.

Configuring Server Settings for Downloading Upgrades and Updates

Specify the server and connection information required to download upgrades and updates to your appliance .

You can use the same or different settings for AsyncOS upgrades and for service updates.

Before You Begin

Determine whether the appliance will download upgrades and updates directly from Cisco, or whether you will host these images from a local server on your network instead. Then set up your network to support the method you choose. See all topics under Setting Up to Obtain Upgrades and Updates , on page 22.

Procedure

Step 1 Choose **Security Services > Service Updates.**

Step 2 Click **Edit Update Settings**.

Step 3 Enter options:

Setting	Description
Update Servers (images)	Choose whether to download Cisco IronPort AsyncOS upgrade images and service updates from the Cisco IronPort update servers or a from a local server on your network. The default is the Cisco IronPort update servers for both upgrades and updates. To use the same settings for upgrades and updates, enter information in the visible fields. If 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 username and passphrase. To enter separate settings solely for AsyncOS upgrades and McAfee Anti-Virus definitions, click the **Click to use different settings for AsyncOS** link. **Note** Cisco Intelligent Multi-Scan requires a second local server to download updates for third-party anti-spam rules.

Setting	Description
Update Servers (lists)	To ensure that only upgrades and updates that are appropriate to your deployment are available to each appliance , Cisco IronPort generates a manifest list of the relevant files. Choose whether to download the lists of available upgrades and service updates (the manifest XML files) from the Cisco IronPort update servers or from a local server on your network. There are separate sections for specifying servers for updates and for AsyncOS upgrades. The default for upgrades and updates is the Cisco IronPort update servers. If you choose local update servers, enter the full path to the manifest XML file for each list, including the file name and HTTP port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, enter a valid user name and passphrase.
Automatic Updates	Enable automatic updates and the update interval (how often the appliance checks for updates) for Sophos and McAfee Anti-Virus definitions, Cisco Anti-Spam rules, Cisco Intelligent Multi-Scan rules, PXE Engine updates, Outbreak Filter rules, and time zone rules. Include a trailing s, m, or h to indicate seconds, minutes, or hours. Enter 0 (zero) to disable automatic updates. **Note** You can only turn on automatic updates for DLP using the **Security Services > Data Loss Prevention** page. However, you must enable automatic updates for all services first. See About Updating the DLP Engine and Content Matching Classifiers for more information.
Alert Interval for Disabled Automatic Engine Updates	Enter specific frequency of alerts to be sent when the 'Automatic Updates' feature is disabled for a specific engine. Include a trailing m, h, or d to indicate months, hours, or days. The default value is 30 days.
Interface	Choose which network interface to use when contacting the update servers for the listed security component updates. The available proxy data interfaces are shown. By default, the appliance selects an interface to use.
HTTP Proxy Server	An optional proxy server used for the services listed in the GUI. If you specify a proxy server, it will be used to update ALL services.
HTTPS Proxy Server	An optional proxy server using HTTPS. If you define the HTTPS proxy server, it will be used to update the services listed in the GUI.

Step 4 Submit and commit your changes.

Configuring Automatic Updates

Procedure

Step 1 Navigate to the **Security Services > Service Updates** page, and click **Edit Update Settings**.

Step 2 Select the check box to enable automatic updates.

Step 3 Enter an update interval (time to wait between checks for updates). Add a trailing **m** for minutes and **h** for hours. The maximum update interval is 1 hour.

Configuring the Appliance to Verify the Validity of Updater Server Certificate

The appliance can check the validity of Cisco updater server certificate every time the appliance communicates the updater server. If you configure this option and the verification fails, updates are not downloaded and the details are logged in Updater Logs.

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

```
mail.example.com> updateconfig
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort 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
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
```

```
Enrollment Client Updates                              Cisco IronPort Servers
Support Request updates                                Cisco IronPort Servers
Service (list):                                        Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                        Cisco IronPort 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
[]>
```

Configuring the Email Gateway 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 appliance . By doing so, the appliance trusts the proxy server communication.

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

```
mail.example.com> updateconfig
...
...
...
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.
[]> 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-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.....................................
-----END CERTIFICATE-----
.
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.
[]>
```

Upgrading AsyncOS

Procedure

	Command or Action	Purpose
Step 1	If you have not yet done so, configure settings that apply to all update and upgrade downloads, and set up your network to support and optionally distribute these downloads.	Setting Up to Obtain Upgrades and Updates , on page 22
Step 2	Understand when an upgrade is available and determine whether to install it.	Notifications of Available Upgrades, on page 30
Step 3	Perform required and recommended tasks before each upgrade.	Preparing to Upgrade AsyncOS, on page 31 Upgrading Machines in a Cluster
Step 4	Perform the upgrade.	Downloading and Installing the Upgrade , on page 31

About Upgrading Clustered Systems

If you are upgrading clustered machines, please see Upgrading Machines in a Cluster.

About Batch Commands for Upgrade Procedures

Batch commands for upgrade procedures are documented in the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* at http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html.

Notifications of Available Upgrades

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 .

On clustered machines, actions apply only to the machine to which you are logged in.

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.**

Notifications of Available Upgrades

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 .

On clustered machines, actions apply only to the machine to which you are logged in.

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.**

Preparing to Upgrade AsyncOS

As a best practice, Cisco recommends preparing for an upgrade by taking the following steps.

Before you begin

Clear all the messages in your work queue. You cannot perform the upgrade without clearing your work queue.

Procedure

Step 1 Save the XML configuration file off-box. If you need to revert to the pre-upgrade release for any reason, you will need this file.

Step 2 If you are using the Safelist/Blocklist feature, export the list off-box.

Step 3 Suspend all listeners. If you perform the upgrade from the CLI, use the suspendlistener command. If you perform the upgrade from the GUI, listener suspension occurs automatically.

Step 4 Wait for the queue to empty. You can use the workqueue command to view the number of messages in the work queue or the rate command in the CLI to monitor the message throughput on your appliance .

Note Re-enable the listeners post-upgrade.

Downloading and Installing the Upgrade

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 IronPort 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 Setting Up to Obtain Upgrades and Updates , on page 22 and Configuring Server Settings for Downloading Upgrades and Updates , on page 26.
- If you will install the upgrade now, follow the instructions in Preparing to Upgrade AsyncOS, on page 31.
- If you are installing the upgrade in a clustered system, see Upgrading Machines in a Cluster.
- If you will only download the upgrade, there are no prerequisites until you are ready to install it.
- After you upgrade, you cannot use TLS v1.0 in FIPS mode. However, you can re-enable TLS v1.0 on the appliance , if necessary.

Procedure

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

Step 2 Click **Upgrade Options**.

Step 3 Click **Upgrade** to proceed with the upgrade process.

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

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

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:
  - Re-enable (resume) the listeners.
  - Save a configuration file for the new system. For information, see Managing the Configuration File, on page 13.
- After upgrade is complete, re-enable listeners.

Viewing Status of, Canceling, or Deleting a Background Download

Procedure

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

Step 2 Click **Upgrade Options**.

Step 3 Choose an option:

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

Step 4 (Optional) View the Upgrade Logs.

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 the Hardware Installation Guide.
- 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.

Procedure

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

Step 2 Sign in using an account with Administrator access.

Step 3 Enter the following commands:

```
remotepower
setup
```

Step 4 Follow the prompts to specify the following:

a. The dedicated IP address for this feature, plus netmask and gateway.

b. The username and passphrase required to execute the power-cycle command.

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

Step 5 Enter commit to save your changes.

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

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

What to do next

Related Topics

- Remotely Resetting Appliance Power

Reverting to a Previous Version of AsyncOS

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

Reversion Impact

Using the revert command on an appliance is a very destructive action. This command destroys all configuration logs and databases. Only the network information for the management interface is preserved--all other network configuration is deleted. In addition, reversion disrupts mail handling until the appliance is reconfigured. Because this command destroys network configuration, you may need physical local access to the appliance when you want to issue the revert command.

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

Reverting AsyncOS on Virtual Appliances May Impact the License

If you revert from AsyncOS 9.0 for Email to AsyncOS 8.5 for Email, the license does not change.

If you revert from AsyncOS 9.0 for Email to AsyncOS 8.0 for Email, there is no longer a 180-day grace period during which the appliance delivers mail without security features.

Feature key expiration dates do not change in either case.

Related Topics

- Virtual Appliance License Expiration , on page 13

Reverting AsyncOS

Procedure

Step 1 Ensure that you have the configuration file for the version you wish to revert to. Configuration files are not backwards-compatible. To do this, you can email the file to yourself or FTP the file. For information, see Mailing the Configuration File, on page 15.

Step 2 Save a backup copy of the current configuration of your appliance (with passphrases unmasked) on another machine.

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 Wait for the mail queue to empty.

Step 5 Log into the CLI of the appliance you want to revert.

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

Step 6 From the CLI, Issue the **`revert`** command.

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

Step 7 Wait for the appliance to reboot twice.

Step 8 After the machine reboots twice, use the serial console to configure an interface with an accessible IP address using the **`interfaceconfig`** command.

Step 9 Enable FTP or HTTP on one of the configured interfaces.

Step 10 Either FTP the XML configuration file you created, or paste it into the GUI interface.

Step 11 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 Commit your changes.

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

Configuring the Return Address for Appliance Generated Messages

It is recommended that you avoid changing return addresses on Cloud appliances .

You can configure the envelope sender for mail generated by AsyncOS for the following circumstances:

- Anti-Virus notifications
- Bounces
- DMARC feedback
- Notifications (notify() and notify-copy() filter actions)

- Quarantine notifications (and “Send Copy” in quarantine management)
- Reports
- All other messages

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.

You can modify the return address for system-generated email messages in the GUI or in the CLI using the addressconfig command.

Procedure

Step 1 Navigate to the System Administration > Return Addresses page.

Step 2 Click **Edit Settings**.

Step 3 Make changes to the address or addresses you want to modify

Step 4 Submit and commit your changes.

Setting Thresholds for System Health Parameters

Depending on your organization's requirements, you can configure the threshold for various health parameters of your appliance such as CPU usage, maximum messages in the workqueue, and so on. You can also configure the appliance to send alerts when the specified threshold values are crossed.

Note To configure the threshold for system health parameters using CLI, use the healthconfig command. For more information, see the CLI inline help or *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances* .

Before You Begin

Carefully determine the threshold values.

Procedure

Step 1 Click **System Administration** > **System Health**.

Step 2 Click **Edit Settings**.

Step 3 Configure the following options:

- Specify the threshold level for CPU usage (in percent).

  Also, specify if you want to receive an alert if the current CPU usage has crossed the configured threshold value. After the first alert is sent, if the CPU usage crosses the running average from the time the first alert was triggered by five percent in 15 minutes, an additional alert is sent.

  Note These alerts are triggered based only on the CPU usage of the mail handling process.

- Specify the threshold level for memory page swapping (in percent).

Also, specify if you want to receive an alert if the overall memory swap usage crosses the configured threshold value. After the first alert is sent, if the memory page swapping crosses the value that triggered the first alert by 150 percent or after a 15 minutes alert interval, an additional alert is sent. For example, if the threshold is set to 10,

- When the memory swap usage reaches 10.1%, the first alert is sent.
- When the memory swap usage reaches 15.1% in 15 minutes, one more alert is sent.

- Specify the threshold level for maximum messages in workqueue (in number of messages).

  Also, specify if you want to receive an alert if the number of messages in work queue has crossed the configured threshold value. After the first alert is sent, if the maximum messages in work queue crosses the value that triggered the first alert by 150 percent within 15 minutes, an additional alert is sent. For example, if the threshold is set to 1000,

  - When the maximum messages in work queue reached 1002, the first alert was sent.
  - When the maximum messages in work queue reached 1510 with 15 minutes, one more alert is sent.

Note All the alerts for this feature belong to the System Alert category.

Step 4 Submit and commit your changes.

What to do next

If you have configured alerts for this feature, make sure that you subscribe to the System Alerts. For instructions, see Adding Alert Recipients, on page 40.

Checking the Health of Appliance

You can use the health check functionality to check the health of your appliance . When you run the health check, the system analyzes historical data (up to three months) in the current Status Logs to determine the health of the appliance .

Note For the system to perform this analysis, the Status Logs must contain a minimum of one month of logging data.

To run the health check,

- On web interface, go to **System Administration** > **System Health** page and click **Run Health Check**.
- On CLI, run the command: **`healthcheck`** .

The analysis results will indicate whether system has experienced one or more of the following problems in the last few months:

- Resource conservation mode
- Delay in mail processing
- High CPU usage
- High memory usage
- High memory page swapping

If the health check is indicating that your appliance has experienced one or more of the above problems, consider reviewing and fine-tuning your system configuration. For more information, see: http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html .

Alerts

Alert messages are automatically-generated standard email messages that contain information about events occurring on the appliances . These events can be of varying levels of importance (or severity) from minor to major and pertain generally to a specific component or feature on your appliance . Alerts are generated by the appliance . You can specify, at a much more granular level, which alert messages are sent to which users and for which severity of event they are sent. Manage alerts via the System Administration > Alerts page in the GUI (or via the alertconfig command in the CLI).

Alert Severities

Alerts can be sent for the following severities:

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

AutoSupport

To allow Cisco to better support and design future system changes, the appliance can be configured to send Cisco Systems a copy of all alert messages generated by the system. This feature, called AutoSupport, is a useful way to allow our team 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 will 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, see Configuring Alert Settings, on page 41.

Alert Delivery

Alerts sent from the appliance to addresses specified in the Alert Recipient follow SMTP routes defined for those destinations

Since alert messages can be used to inform you of problems within your 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.

- 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 are not affected by bounce profiles or destination control limits.

Example Alert Message

```
Date: 23 Mar 2005 21:10:19 +0000


To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

Adding Alert Recipients

The alerting engine allows for granular control over which alerts are sent to which alert recipients. For example, you can configure the system to send only specific alerts to an alert recipient, configuring an alert recipient to receive notifications only when Critical (severity) information about the System (alert type) is sent.

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

Procedure

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

Step 2 Click **Add Recipient**.

Step 3 Enter the recipient's email address. You can enter multiple addresses, separated by commas.

Step 4 (Optional) If you want to receive software release and critical support notification alerts from Cisco Support, check the **Release and Support Notifications** checkbox.

Step 5 Select the alert types and severities that this recipient will receive.

Step 6 Submit and commit your changes.

Configuring Alert Settings

The following settings apply to all alerts.

Note Use the alertconfig CLI command to define the number of alerts to save on the appliance to view later.

Procedure

Step 1 Click **Edit Settings** on the Alerts page.

Step 2 Enter a Header From: address to use when sending alerts, or select Automatically Generated ("alert@<hostname>").

Step 3 Mark the checkbox if you want to specify the number of seconds to wait between sending duplicate alerts. For more information, see Sending Duplicate Alerts, on page 41.

- Specify the initial number of seconds to wait before sending a duplicate alert.
- Specify the maximum number of seconds to wait before sending a duplicate alert.

Step 4 You can enable AutoSupport by checking the IronPort AutoSupport option. For more information about AutoSupport, see AutoSupport, on page 39.

- If AutoSupport is enabled, the weekly AutoSupport report is sent to alert recipients set to receive System alerts at the Information level. You can disable this via the checkbox.

Step 5 Submit and commit your changes.

Alert Settings

Alert settings control the general behavior and configuration of alerts, including:

- The RFC 2822 Header From: when sending alerts (enter an address or use the default "alert@<hostname>"). You can also set this via the CLI, using the alertconfig -> from command.
- The initial number of seconds to wait before sending a duplicate alert.
- The maximum number of seconds to wait before sending a duplicate alert.
- The status of AutoSupport (enabled or disabled).
- The sending of AutoSupport's weekly status reports to alert recipients set to receive System alerts at the Information level.

Sending 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 and instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait

between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5 second wait would have alerts sent at 5 seconds, 15, seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, etc.

Eventually, the interval could become quite 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, etc.

Viewing Recent Alerts

The appliances saves the latest alerts so you can view them in both the GUI and the CLI in case you lose or delete the alert messages. These alerts cannot be downloaded from the appliance .

To view a list of the latest alerts, click the **View Top Alerts** button on the Alerts page or use the displayalerts command in the CLI. You can arrange the alerts in the GUI by date, level, class, text, and recipient.

By default, the appliance saves a maximum of 50 alerts to displays in the **Top Alerts** window. Use the alertconfig -> setup command in the CLI to edit the number of alerts that the appliance saves. If you want to disable this feature, change the number of alerts to 0.

Alert Descriptions

The following tables list alerts by classification, including the alert name (internal descriptor used by Cisco), actual text of the alert, description, severity (critical, information, or warning) and the parameters (if any) included in the text of the message. The value of the parameter is replaced in the actual text of the alert. For example, an alert message below may mention “$ip” in the message text. “$ip” is replaced by the actual IP address when the alert is generated.

Anti-Spam Alerts

The following table contains a list of the various anti-spam alerts that can be generated by AsyncOS, including a description of the alert and the alert severity.

Table 1: Listing of Possible Anti-Spam Alerts

Alert Name	Message and Description	Parameters
AS.SERVER.ALERT	$engine anti-spam - $message $tb Critical. Sent when the anti-spam engine fails.	'**engine**' - The type of anti-spam engine. '**message**' - The log message. '**tb**' - Traceback of the event.
AS.TOOL.INFO_ALERT	Update - $engine - $message Information. Sent when there is a problem with the anti-spam engine.	'**engine**' - The anti-spam engine name '**message**' - The message
AS.TOOL.ALERT	Update - $engine - $message Critical. Sent when an update is aborted due to a problem with one of the tools used to manage the anti-spam engine.	'**engine**' - The anti-spam engine name '**message**' - The message

Anti-Virus Alerts

The following table contains a list of the various Anti-Virus alerts that can be generated by AsyncOS, including a description of the alert and the alert severity.

Table 2: Listing of Possible Anti-Virus Alerts

Alert Name	Message and Description	Parameters
AV.SERVER.ALERT /AV.SERVER.CRITICAL	$engine antivirus - $message $tb Critical. Sent when there is a critical problem with the anti-virus scanning engine.	'**engine**' - The type of anti-virus engine. '**message**' - The log message. '**tb**' - Traceback of the event.
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb Information. Sent when an informational event occurs with the anti-virus scanning engine.	'**engine**' - The type of anti-virus engine. '**message**' - The log message. '**tb**' - Traceback of the event.
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb Warning. Sent when there is a problem with the anti-virus scanning engine.	'**engine**' - The type of anti-virus engine. '**message**' - The log message. '**tb**' - Traceback of the event.
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag Critical. Sent when anti-virus scanning produces an error while scanning a message.	'**mid**' - MID '**what**' - The error that happened. '**tag**' - Virus outbreak name if set.

Alert Name	Message and Description	Parameters
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine.	'**mid**' - MID '**engine**' - The engine being used
	Critical. The scanning engine attempted to scan the message unsuccessfully because the message is malformed. The maximum number of retries has been exceeded, and the message will be processed without being scanned by this engine.	

Directory Harvest Attack Prevention (DHAP) Alerts

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

Table 3: Listing of Possible Directory Harvest Attack Prevention Alerts

Alert Name	Message and Description	Parameters
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.	
	Warning. Sent when a possible directory harvest attack is detected.	

Hardware Alerts

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

Table 4: Listing of Possible Hardware Alerts

Alert Name	Message and Description	Parameters
INTERFACE.ERRORS	Port $port: has detected $in_err input errors, $out_err output errors, $col collisions please check your media settings.	'**port**' - Interface name. '**in_err**' - The number of input errors since the last message. '**out_err**' - The number of output errors since the last message. '**col**' - The number of packet collisions since the last message.
	Warning. Sent when interface errors are detected.	
MAIL.MEASUREMENTS_FILESYSTEM	The $file_system partition is at $capacity% capacity	'**file_system**' - The name of the filesystem '**capacity**' - How full the filesystem is in percent.
	Warning. Sent when a disk partition is nearing capacity (75%).	

Alert Name	Message and Description	Parameters
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	The $file_system partition is at $capacity% capacity Critical. Sent when a disk partition reaches 90% capacity (and at 95%, 96%, 97%, etc.).	'**file_system**' - The name of the filesystem '**capacity**' - How full the filesystem is in percent.
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: $error Warning. Sent when a critical RAID-event occurs.	'**error**' - The text of the RAID error.
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: $error Information. Sent when a RAID-event occurs.	'**error**' - The text of the RAID error.

Spam Quarantine Alerts

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

Table 5: Listing of Possible Spam Quarantine Alerts

Alert Name	Message and Description	Parameters
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at $host:$port Information. Sent when AsyncOS was unable to connect to the (off-box) IP address.	'**host**' - address of off-box quarantine '**port**' - port to connect to on off-box quarantine
ISQ.CRITICAL	ISQ: $msg Critical. Sent when a critical spam quarantine error is encountered.	'**msg**' - message to be displayed
ISQ.DB_APPROACHING_FULL	ISQ: Database over $threshold% full Warning. Sent when the spam quarantine database is nearly full.	'**threshold**' - the percent full threshold at which alerting begins
ISQ.DB_FULL	ISQ: database is full Critical. Sent when the spam quarantine database is full.	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID $mid for $rcpt: $reason Warning. Sent when an email is not successfully deleted from the spam quarantine.	'**mid**' - MID '**rcpt**' - Recipient or "all" '**reason**' - Why the message was not deleted
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: $reason Warning. Sent when a notification message is not successfully sent.	'**reason**' - Why the notification was not sent

Alert Name	Message and Description	Parameters
ISQ.MSG_QUAR_FAILED	Warning. Sent when a message is not successfully quarantined.	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID $mid to $rcpt: $reason	'**mid**' - MID '**rcpt**' - Recipient or "all" '**reason**' - Why the message was not released
	Warning. Sent when a message is not successfully released.	
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason	'**mid**' - MID '**reason**' - Why the message was not released
	Warning. Sent when a message is not successfully released because the recipient is unknown.	
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties. Setting defaults	'**user**' - end user name
	Information. Sent when AsyncOS is unable to retrieve information about a user.	
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host	
	Information. Sent when AsyncOS is configured to reference an external quarantine, but the external quarantine is not defined.	

Safelist/Blocklist Alerts

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

Table 6: Listing of Possible Safelist/Blocklist Alerts

Alert Name	Message and Description	Parameters
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '$error'.	'**error**' - error reason
	Critical. Failed to recover the Safelist/Blocklist database.	
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: $current of $limit.	'**current**' - how much it has used, in MB '**limit**' - the configured limit, in MB
	Critical. The safelist/blocklist database exceeded the allowed disk space.	

System Alerts

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

Table 7: Listing of Possible System Alerts

Component/Alert Name	Message and Description	Parameters
AMP.ENGINE.ALERT	See Ensuring That You Receive Alerts About Advanced Malware Protection Issues	-
AMP.ENGINE.ALERT.WARN	Alert text: Failed to register the file analysis group name with Cisco Threat Grid server. Contact Cisco TAC for assistance. Alert level: WARNING. Description: Alert is sent when the email gateway fails to register the Appliance Group Name using the Smart Account ID with the Cisco Thread Grid server.	Parameter: reason for the failure
AsyncOS API Alerts	See "Alerts" section in the *AsyncOS API for Cisco Email Security Appliances - Getting Started Guide* .	-
Mailbox Auto Remediation Alerts	See "Alerts" section in Remediating Messages in Mailboxes	-
COMMON.APP_FAILURE	An application fault occurred: $error Warning. Sent when there is an unknown application failure.	'**error**' - The text of the error, typically a traceback.
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> Information: Automatic updates have been enabled for the particular engine <$engine>. You will now receive automatic engine updates for this engine.	'**$engine**' - The name of the Service Engine. The values can be: • Sophos • McAfee • Graymail
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<$level>: <$class> Information: Automatic updates have been disabled for the particular engine <$engine>. You will not receive any automatic updates for this engine, unless you enable automatic updates in the global setting page of the particular engine.	'**$engine**' - The name of the Service Engine. The values can be: • Sophos • McAfee • Graymail
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco sales representative. Warning. Sent when a feature key has expired.	'**feature**' - The name of the feature that is about to expire.

Component/Alert Name	Message and Description	Parameters
COMMON.KEY_EXPIRING_ ALERT	Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. Warning. Sent when a feature key is about to expire.	'**feature**' - The name of the feature that is about to expire. '**days**' - The number of days it will expire.
COMMON.KEY_FINAL_EXPIRING_ ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. Warning. Sent as a final notice that a feature key is about to expire.	'**feature**' - The name of the feature that is about to expire. '**days**' - The number of days it will expire.
KEYS.GRACE_EXPIRING_ ALERT	All security services licenses for this appliance have expired. The appliance will continue to deliver mail without security services for $days days. To renew security services licenses, Please contact your authorized Cisco sales representative. Critical. Sent periodically from the start of the grace period for virtual appliance license expiration.	'**days**' - The number of days remaining in the grace period at the time the alert was sent. For more information about the grace period, see Virtual Appliance License Expiration , on page 13.
KEYS.GRACE_FINAL_EXPIRING_ ALERT	This is the final notice. All security services licenses for this appliance have expired. The appliance will continue to deliver mail without security services for 1 day. To renew security services licenses, Please contact your authorized Cisco sales representative. Critical. Sent one day before the virtual appliance license expires.	For more information about the grace period, see Virtual Appliance License Expiration , on page 13.
KEYS.GRACE_EXPIRED_ALERT	Your grace period has expired. All security sevice have expired, and your appliance is non-functional. The appliance will no longer deliver mail until a new license is applied. To renew security services licenses, Please contact your authorized Cisco sales representative. Critical. Sent when the grace period for virtual appliance has expired.	For more information about the grace period, see Virtual Appliance License Expiration , on page 13.
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver. Unable to contact root servers. Warning. Sent when the appliance is unable to contact the root DNS servers.	

Component/Alert Name	Message and Description	Parameters
COMMON.INVALID_FILTER	Invalid $class: $error Warning. Sent when an invalid filter is encountered.	'**class**' - Either "Filter", "SimpleFilter", etc. '**error**' - Additional why-filter-is-invalid info.
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list. Warning. IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blocked list if more than 10 failed attempts occur within two minutes. When a user logs in successfully from the same IP address, that IP address is added to the allowed list. Addresses on the allowed list. are allowed access even if they are also on the blocked list. Entries are automatically removed from the blocked list after about a day.	**'ip'** - IP address from which a login attempt occurred.
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false Critical. Sent when an LDAP group query fails.	'**name**' - The name of the query.
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why Critical. Sent when an LDAP query fails completely (after trying all servers).	'**name**' - The name of the query. '**why**' - Why the error happened.
LOG.ERROR.*	Critical. Various logging errors.	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid matched the $rule_name rule. \n Details: $details Information. Sent every time when a Header Repeats rule evaluates to true .	'**mid**' - Unique identification number of the message. '**rule_name**' - The name of the rule that matched. '**details**' - More information about the message or the rule.

Component/Alert Name	Message and Description	Parameters
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server. Critical. Sent when an LDAP group query fails during per-recipient scanning.	
MAIL.QUEUE.ERROR.*	Critical. Various mail queue hard errors.	
MAIL.OMH.DELIVERY_RETRY	Subject - 'Alert: Message Delivery failed for $hostname. DANE verification failed for one or more Domain(s).' Message - The message delivery failed due to DANE verification failure for all mail exchange (MX) hosts in $hostname. The appliance will attempt message delivery again or bounce the message.	'host' - The host for which the DANE verification has failed.
MAIL.RES_CON_START_ALERT. MEMORY	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. RAM utilization for this system has exceeded the resource conservation threshold of $memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches $memory_threshold_halt%. Critical. Sent when RAM utilization has exceeded the system resource conservation threshold.	'**hostname**' - The name of the host. '**memory_threshold_start**' - The percent threshold where memory tarpitting starts. '**memory_threshold_halt**' - The percent threshold where the system will halt due to memory being too full.
MAIL.RES_CON_START_ALERT. QUEUE_SLOW	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput. Critical. Sent when the mail queue is overloaded and system resource conservation is enabled.	'**hostname**' - The name of the host.

Component/Alert Name	Message and Description	Parameters
MAIL.RES_CON_START_ ALERT. QUEUE	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of $queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches $queue_threshold_halt%.	'**hostname**' - The name of the host. '**queue_threshold_start**' - The percent threshold where queue tarpitting starts. '**queue_threshold_halt**' - The percent threshold where the system will halt due to the queue being too full.
	Critical. Sent when queue utilization has exceeded the system resource conservation threshold.	
MAIL.RES_CON_START_ ALERT. WORKQ	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of $suspend_threshold. Listeners will be resumed once the work queue size has dropped to $resume_threshold. These thresholds may be altered via use of the 'tarpit' command on the system CLI.	'**hostname**' - The name of the host. '**suspend_threshold**' - Work queue size above which listeners are suspended. '**resume_threshold**' - Work queue size below which listeners are resumed.
	Information. Sent when listeners are suspended because the work queue size is too big.	
MAIL.RES_CON_START_ ALERT	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	'**hostname**' - The name of the host.
	Critical. Sent when the appliance enters "resource conservation" mode.	
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	'**hostname**' - The name of the host.
	Information. Sent when the appliance leaves 'resource conservation' mode.	
MAIL.URL_REP_ CLIENT.CATEGORY_CHANGE	See Future URL Category Set Changes.	—
MAIL.BEAKER_ CONNECTOR.CERTIFICATE_INVALID	See Troubleshooting URL Filtering.	
MAIL.BEAKER_CONNECTOR.ERROR_ FETCHING_CERTIFICATE		

Component/Alert Name	Message and Description	Parameters
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, $num msgs, $reason	‘**num**’ - The number of messages in the work queue. ‘**reason**’ - The reason the work queue is paused.
	Critical. Sent when the work queue is paused.	
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, $num msgs	‘**num**’ - The number of messages in the work queue.
	Critical. Sent when the work queue is resumed.	
NTP.NOT_ROOT	Not running as root, unable to adjust system time	
	Warning. Sent when the appliance is unable to adjust time because NTP is not running as root.	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID $mid - quarantine system unavailable	’**mid**’ - MID
	Critical. Sent when a message cannot be sent to a quarantine.	
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: $version; target $target_version)	’**version**’ - The schema version detected. ’**target_version**’ - The target schema version.
	Critical. Sent when a quarantine database cannot be updated.	
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the $file_system partition.	’**file_system**’ - The name of the filesystem.
	Critical. Sent when the disk space for quarantines is full.	
QUARANTINE.THRESHOLD_ALERT	Quarantine "$quarantine" is $full% full	’**quarantine**’ - The name of the quarantine. ’**full**’ - The percentage of how full the quarantine is.
	Warning. Sent when a quarantine reaches 5%, 50%, or 75% of capacity.	
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "$quarantine" is $full% full	’**quarantine**’ - The name of the quarantine. ’**full**’ - The percentage of how full the quarantine is.
	Critical. Sent when a quarantine reaches 95% of capacity.	
REPORTD.DATABASE_OPEN_FAILED_ALERT	The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	’**err_msg**’ - The error message raised
	Critical. Sent if the reporting engine is unable to open the database.	

Component/Alert Name	Message and Description	Parameters
REPORTD.AGGREGATION_ DISABLED_ALERT	Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	’**threshold**’ - The threshold value
	Warning. Sent if the system runs out of disk space. When the disk usage for a log entry exceeds the log usage threshold, reportd disables aggregation and sends the alert.	
REPORTING.CLIENT.UPDATE_ FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration).	’**duration**’ - Length of time the client has been trying to contact the reporting daemon. This is a string in a human readable format (’1h 3m 27s’).
	Warning. Sent if the reporting engine was unable to save reporting data.	
REPORTING.CLIENT.JOURNAL. FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	
	Critical. Sent if the reporting engine is unable to store new data.	
REPORTING.CLIENT.JOURNAL. FREE	Reporting Client: The reporting system is now able to handle new data.	
	Information. Sent when the reporting engine is again able to store new data.	
PERIODIC_REPORTS.REPORT_ TASK.BUILD_FAILURE	A failure occurred while building periodic report ‘$report_title’. This subscription has been removed from the scheduler.	‘**report_title**’ - the report title
	Critical. Sent when the reporting engine is unable to build a report.	
PERIODIC_REPORTS.REPORT_ TASK.EMAIL_FAILURE	A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.	’**report_title**’ - the report title
	Critical. Sent when a report could not be emailed.	
PERIODIC_REPORTS.REPORT_ TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report ’$report_title’. This subscription has been removed from the scheduler.	’**report_title**’ - the report title
	Critical. Sent when a report could not be archived.	

Component/Alert Name	Message and Description	Parameters
SENDERBASE.ERROR	Error processing response to query $query: response was $response	'**query**' - The query address. '**response**' - Raw data of response received.
	Information. Sent when an error occurred while processing a response from SenderBase.	
SMTPAUTH.FWD_SERVER_ FAILED_ ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why	'**ip**' - The IP of the remote server. '**why**' - Why the error happened.
	Warning. Sent when the SMTP Authentication forwarding server is unreachable.	
SMTPAUTH.LDAP_QUERY_ FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	Warning. Sent when an LDAP query fails.	
SYSTEM.HERMES_SHUTDOWN_ FAILURE. REBOOT	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot	'**error**' - The error that happened.
	Warning. Sent when there was a problem shutting down the system on reboot.	
SYSTEM.HERMES_SHUTDOWN_ FAILURE. SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down	'**error**' - The error that happened.
	Warning. Sent when there was a problem shutting down the system.	
SYSTEM.LOGIN_FAILURES_LOCK_ALERT	User "$user" is locked after $numlogins consecutive login failures. Last login attempt was from $rhost Information: Sent when the user account is locked because of maximum number of failed login attempts	'user' - The name of the user 'numlogins' - The configured alert threshold 'rhost' - The address of the remote host
SYSTEM.RCPTVALIDATION.UPDATE_ FAILED	Error updating recipient validation data: $why	'why' - The error message.
	Critical. Sent when a recipient validation update failed.	
SYSTEM.SERVICE_TUNNEL. DISABLED	Tech support: Service tunnel has been disabled	
	Information. Sent when a tunnel created for Cisco Support Services is disabled.	
SYSTEM.SERVICE_TUNNEL. ENABLED	Tech support: Service tunnel has been enabled, port $port	'**port**' - The port used for the service tunnel.
	Information. Sent when a tunnel created for Cisco Support Services is enabled.	

Component/Alert Name	Message and Description	Parameters
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list.	**'ip'** - IP address from which a login attempt occurred.
	Warning. IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blocked list if more than 10 failed attempts occur within two minutes. When a user logs in successfully from the same IP address, that IP address is added to the allowed list. Addresses on the allowed list are allowed access even if they are also on the blocked list . Entries are automatically removed from the blocked list after about a day.	
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text Warning. The appliance uses the watchdog service to monitor the health condition of the following engines: • Anti-Spam • Anti-Virus • Anti Malware Protection • Graymail If any of the above engines does not respond to the watchdog service for a certain duration, the watchdog service restarts the engine(s) and sends an alert to the administrator.	'**subject**'- Watchdog alert subject specific to the engine '**text**' - Watchdog alert text specific to the engine
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	Warning. Geolocation Update - the list of supported countries has changed. Added Countries - <$added> Deleted Countries - <$deleted> Review your HAT sender groups, Message Filters, and Content Filters settings accordingly.	'added' - The following countries are added: <iso_code1>:<country_name1>,<iso_code2>:<country_name2>, 'deleted' - The following countries are deleted: <iso_code1>:<country_name1>:<iso_code2>:<country_name2>,

Component/Alert Name	Message and Description	Parameters
MAIL.UPDATED_SHORT_URL_DOMAIN_LIST	Info. The list of shortened URL domains has been updated.. Added Domains: <$added_domains> Deleted Domains - <$deleted_domains>	'added_domains': The following domains are added: <domains_1>, <domain_2> 'deleted_domains' : The following domains are deleted: <domain_3>, <domain_4>
MAIL.DOMAINS_NOT_REACHABLE	Warning. The following domains are not reachable by the appliance for shortened URL support: <$domains> Check your firewall rules to allow your appliance to connect to these domains.	<$domains>: comma separated list of domains
MAIL.UPGRADE_CONFIG_CHANGE.ALERT	Info. Sent when the user configured value is changed by the system during the upgrade.	'**text**' - The Intelligent Multi-Scan and the Graymail global configuration settings have been modified during the upgrade. Please review the global settings for the Intelligent Multi-Scan and the Graymail configurations.
CERTIFICATE.CERT_EXPIRING_ALERT	Your certificate "$certificate" will expire in $days day(s). Alert level : WARNING	'**certificate**', 'The name of the certificate that is about to expire. '**days**', 'The number of days it will expire.'
CERTIFICATE.CERT_CRITICAL_EXPIRING_ALERT	Your certificate "$certificate" will expire in $days hour(s). Alert level : CRITICAL A 'CRITICAL' certificate validity period is less than 5 days.	'**certificate**', 'The name of the certificate that is about to expire. '**days**', 'The number of days with remaining time (HH:MM:SS), for example, 4 days 10:12:20 hour(s).'
CERTIFICATE.CERT_EXPIRED_ALERT	Your certificate "$certificate" has expired. Alert level : CRITICAL	'**certificate**', 'The name of the certificate that has expired.
MAIL.APP.NO_ACCESS_KEY	Alert text: 'Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date, add API AccessUID and API Access secret key.' Description: Alert is sent when a query for the APP expiry date failed because the API Access key and the secret key was not entered.	N/A
MAIL.APP.INVALID_KEY	Alert text: Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date because the API Access Key is invalid. You need to re-configure the API Access UID and secret key. Description: Alert is sent when a query for the APP expiry date failed because the API Access key and the secret key was not entered.	N/A

Component/Alert Name	Message and Description	Parameters
MAIL.APP.EXPIRED	Alert text: The Cisco Advanced Phishing Protection Cloud Service has expired and is disabled. Contact your Cisco Account Manager to renew the service and enable it. Description: The Cisco Advanced Phishing Protection Cloud Service has expired and is disabled. You need to renew the APP license and enable the APP service.	N/A
MAIL.APP.EXPIRY_REMINDER	Alert text: Cisco Advanced Phishing Protection Cloud Service expires on $eaas_expiry_date. You need to contact your Cisco Account Manager to renew the service. Description: Alert is sent each day, starting from three days before the expiry period.	Parameters: eaas_expiry_date eaas_expiry_date - date on which Cisco Advanced Phishing Protection Cloud Service will expire
MAIL.APP.SERVICE_ UNAVAILABLE	Alert text: Cisco Advanced Phishing Protection Cloud Service update. Unable to establish communication with the cloud service. Description: 'APP cloud service is unavailable because ten consecutive mails failed to forward to APP.	N/A
MAIL.APP.SERVICE_ AVAILABLE	Alert text: Cisco Advanced Phishing Protection Cloud Service update. Communication with the cloud service has been established. Description: APP cloud service is available.	N/A

Updater Alerts

The following table contains a list of the varius Updater alerts that can be generated by AsyncOS.

Table 8: Listing of Possible Updater Alerts

Alert Name	Message and Description	Parameters
UPDATER.APP.UPDATE_ ABANDONED	$app abandoning updates until a new version is published. The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage	**'app'** - The application name. **'attempts'** - The number of attempts tried.
	Warning. The application is abandoning the update.	

Alert Name	Message and Description	Parameters
UPDATER.UPDATERD. ANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold.	**'threshold'** - Human readable threshold string.
	Warning. Failed to acquire a server manifest.	
UPDATER.UPDATERD. RELEASE_NOTIFICATION	$mail_text	**'mail_text'** - The notification text. **'notification_subject'** - The notification text.
	Warning. Release notification.	
UPDATER.UPDATERD. UPDATE_FAILED	Unknown error occured: $traceback	**'traceback'** - The traceback.
	Critical. Failed to run an update.	

Outbreak Filter Alerts

The following table contains a list of the various Outbreak Filter alerts that can be generated by AsyncOS, including a description of the alert and the alert severity. Please note that Outbreak Filters can also be referenced in system alerts for quarantines (the Outbreak quarantine, specifically).

Table 9: Listing of Possible Outbreak Filter Alerts

Alert Name	Message and Description	Parameters
VOF.GTL_THRESHOLD_ALERT	Outbreak Filters Rule Update Alert:$text All rules last updated at: $time on $date.	'**text**' - Update alert text. '**time**' - Time of last update. '**date**' - Date of last update.
	Information. Sent when the Outbreak Filters threshold has changed.	
AS.UPDATE_FAILURE	$engine update unsuccessful. This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com. The specific error on the appliance for this failure is: $error	'**engine**' - The engine that failed to update. '**error**' - The error that happened.
	Warning. Sent when the anti-spam engine or CASE rules fail to update.	

Clustering Alerts

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

Table 10: Listing of Possible Clustering Alerts

Alert Name	Message and Description	Parameters
CLUSTER.CC_ERROR. AUTH_ERROR	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Machine does not appear to be in the cluster Critical. Sent when there was an authentication error. This can occur if a machine is not a member of the cluster.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped Warning. Sent when the connection to the cluster was dropped.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure Warning. Sent when the connection to the cluster failed.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR. FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection Critical. Sent when the appliance was unable to forward data to a machine in the cluster.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found Critical. Sent when the machine was unable to obtain a route to another machine in the cluster.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key Critical. Sent when there was an invalid SSH host key.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out Warning. Sent when the specified operation timed out.	'**name**' - The hostname and/or serial number of the machine. '**ip**' - The IP of the remote host. '**why**' - Detailed text about the error.

Alert Name	Message and Description	Parameters
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why Critical. Sent when the appliance could not obtain a valid IP address for another machine in the cluster.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR_NOIP. AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster Critical. Sent when there was an authentication error connecting to a machine in a cluster. This can occur if a machine is not a member of the cluster.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR_NOIP. DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped Warning. Sent when the machine was unable to obtain a valid IP address for another machine in the cluster and the connection to the cluster was dropped.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR_NOIP. FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure Warning. Sent when there was an unknown connection failure and the machine was unable to obtain a valid IP address for another machine in the cluster.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR_NOIP. FORWARD_FAILED	Error connecting to cluster machine $name - $error - whyerror:=Message forward failed, no upstream connection Critical. Sent when the machine was unable to obtain a valid IP address for another machine in the cluster and the appliance was unable to forward data to the machine.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
CLUSTER.CC_ERROR_NOIP. NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found Critical. Sent when the machine was unable to obtain a valid IP address for another machine in the cluster and it was unable to obtain a route to the machine.	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.

Alert Name	Message and Description	Parameters
CLUSTER.CC_ERROR_NOIP. SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
	Critical. Sent when the machine was unable to obtain a valid IP address for another machine in the cluster and was unable to obtain a valid SSH host key.	
CLUSTER.CC_ERROR_NOIP. TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out	'**name**' - The hostname and/or serial number of the machine. '**why**' - Detailed text about the error.
	Warning. Sent when the machine was unable to obtain a valid IP address for another machine in the cluster and the specified operation timed out.	
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name	'**name**' - The hostname and/or serial number of the machine. '**sections**' - List of cluster sections being sent.
	Critical. Sent when configuration data has gotten out of sync and has been sent to a remote host.	

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 via the System Setup Wizard (or the **systemsetup** command) in Using the System Setup Wizard.

The following features are described:

- **sethostname**
- DNS Configuration (GUI and via the **dnsconfig** command)
- Routing Configuration (GUI and via the **routeconfig** and **setgateway** commands)
- **dnsflush**
- Passphrase
- Network Access
- Login Banner

Changing the System Hostname

The hostname is used to identify the system. You must enter a fully-qualified hostname. To change the hostname:

- On the web interface, click Network> IP Interfaces, click the Management and in the Hostname, change the hostname.
- On the CLI, use the s ethostname command.

Note The new hostname does not take effect until you commit changes.

Configuring Domain Name System (DNS) Settings

You can configure the DNS settings for your appliance through the DNS page on the Network menu of the GUI, or via the d nsconfig command.

You can configure the following settings:

- whether to use the Internet's DNS servers or your own, and which specific server(s) to use
- which interface to use for DNS traffic
- the number of seconds to wait before timing out a reverse DNS lookup
- clear 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 you specify. When using the Internet root servers, you may specify alternate servers to use for specific domains. Since 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. So, 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 you enter, you can specify a numeric priority. AsyncOS will attempt to use the DNS server with the priority closest to 0. If that DNS server is not responding AsyncOS will attempt 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, etc. 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 will be 60 seconds. If you have two priorities, the timeout for each server at the first priority will be 15 seconds, and each server at the second priority will be 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 11: 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 will randomly choose between the two servers at priority 0. If one of the priority 0 servers is down, the other will be 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 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 only uses 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 62.

The default value is 20 seconds for each DNS server. When there are multiple entries for DNS servers, the total timeout value is (number of DNS servers multiplied by the Reverse DNS Lookup Timeout value) seconds. For example, if there are 8 DNS servers and the Reverse DNS Lookup Timeout value is 20 seconds, the total timeout value is (8 * 20) = 160 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. This also prevents the appliance from delivering mail to domains that require TLS-verified connections if the receiving host’s certificate has a common name (CN) that maps to the host’s IP lookup.

DNS Alert

Occasionally, an alert may be generated with the message “Failed to bootstrap the DNS cache” when an appliance is rebooted. The messages 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 CLI Reference Guide for AsyncOS for Cisco Email Security Appliances), 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

Procedure

Step 1 Select **Network > DNS**.

Step 2 Click **Edit Settings**.

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

Step 4 If you want to use your own DNS server(s) 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 62.

Step 5 If you want to specify alternate DNS servers for certain domains, enter the domain and the alternate DNS server IP address. Click **Add Row** to add additional domains.

Note You can enter multiple domains for a single DNS server by using commas to separate domain names. You can also enter multiple DNS servers by using commas to separate IP addresses.

Step 6 Choose an interface for DNS traffic.

Step 7 Enter the number of seconds to wait before cancelling a reverse DNS lookup.

Step 8 You can also clear the DNS cache by clicking **Clear Cache**.

Step 9 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.

The appliance can use both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) static routes.

You can manage static routes via the CLI, using the routeconfig command, or use the following procedure.

Procedure

Step 1 Select **Network > Routing**.

Step 2 Click **Add Route** for the type of static route you want to create (IPv4 or IPv6).

Step 3 Enter a name for the route.

Step 4 Enter the destination IP address.

Step 5 Enter the Gateway IP address.

Step 6 Submit and commit your changes.

Configuring the Default Gateway

You can configure the default gateway using the setgateway command in the CLI or use the following procedure.

Procedure

Step 1 Select **Network > Routing**.

Step 2 Click **Default Route** in the route listing for the Internet Protocol version you want to modify.

Step 3 Change the Gateway IP address.

Step 4 Submit and commit your changes.

Configuring SSL Settings

You can configure the SSL settings for the appliance using SSL Configuration Settings page or sslconfig command.

Procedure

Step 1 Click **System Administration** > **SSL Configuration Settings**.

Step 2 Click **Edit Settings**.

Important If you have upgraded from a lower AsyncOS version (for example, 12.0 or 12.1), the default SSL ciphers are changed in AsyncOS 13.x and later as follows:

- **For GUI HTTPS-**

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA
```

- **For Inbound SMTP -**

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA
```

- **For Outbound SMTP -**

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:
!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:
-aNULL:-EXPORT:-IDEA
```

Step 3 Depending on your requirements, do the following:

- Set GUI HTTPS SSL settings. Under GUI HTTPS, specify the SSL methods and ciphers that you want to use.
- Set Inbound SMTP SSL settings. Under Inbound SMTP, specify the SSL methods and ciphers that you want to use.
- Set Outbound SMTP SSL settings. Under Outbound SMTP, specify the SSL methods and ciphers that you want to use.

- Set other TLS Client Services. Under 'Other TLS Client Services,' the TLS v1.0 method is disabled by default if your appliance is in the non-FIPS mode. You can enable the TLS v1.0 method on your appliance for the following TLS client services - 'LDAP' and 'Updater.'

Keep in mind that,

- [In non-FIPS mode] You cannot enable TLS v1.0 and v1.1 methods simultaneously. However, you can enable these methods in conjunction with TLS v1.2 method.
- If you plan to upgrade from a lower AsyncOS version (for example, 12.x or 13.0) in non-FIPS mode with TLS v1.0 enabled, to AsyncOS 13.5.1 and later, then TLS v1.0 is disabled by default. You need to enable TLS v1.0 method on your appliance after upgrade.
- From AsyncOS 13.5.1 and later, there is no support for SSLv2 and SSL v3 methods.
- There is no support for the TLS v1.0 method if your appliance is in the FIPS mode.
- The TLS v1.0 method is disabled by default if your appliance is in the non-FIPS mode.

Step 4 Click **Submit**.

Step 5 Click **Commit Changes**.

Single Sign-On (SSO) Using SAML 2.0

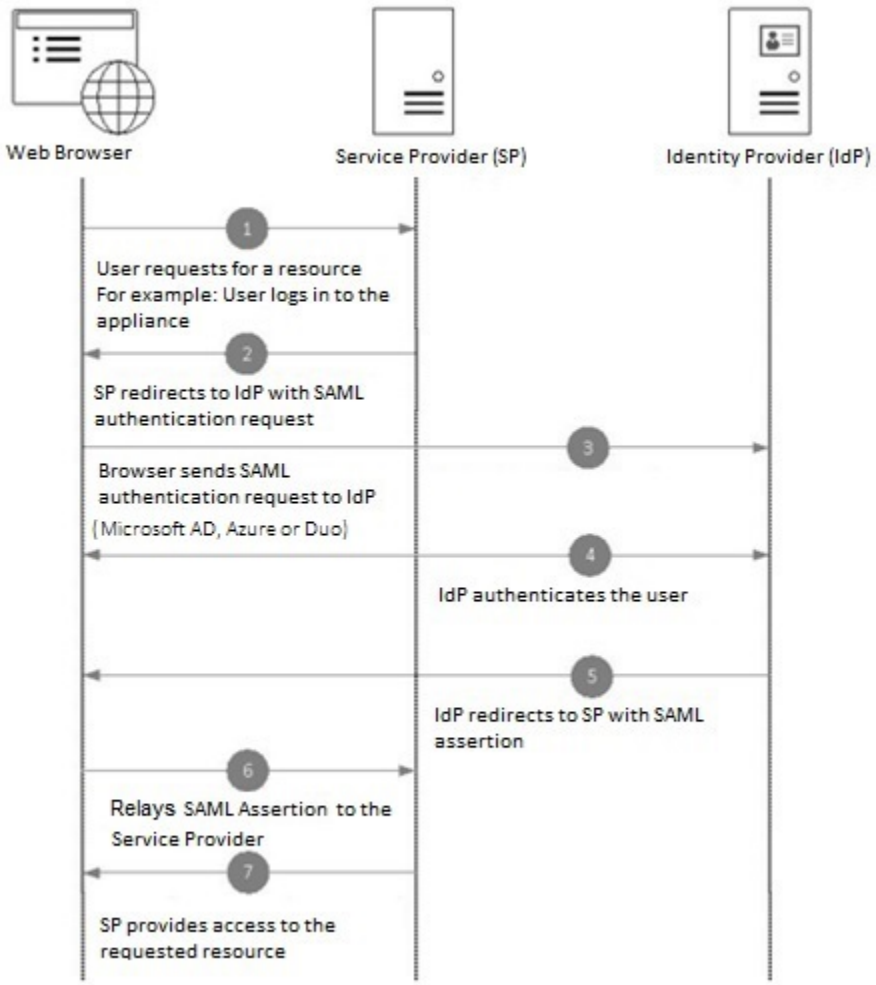
About Single Sign-On (SSO) and SAML 2.0

The appliance now supports SAML 2.0 SSO so that the administrative users can log in to the web interface of the appliance using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization. For instance, if you enable Duo, Microsoft AD FS or Azure as your SAML Identity Provider (IdP), then you can configure your appliance as a Service Provider (SP) to support SAML 2.0 SSO. Users can sign in once and have access to all SAML 2.0 SSO enabled services.

SAML 2.0 SSO Workflow

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

Figure 3: SAML Workflow



Guidelines and Limitations for SAML 2.0

General

You can use Single Sign-On using SAML only on the graphical user interface (GUI). You can use the GUI and the command line interface (CLI) to configure SAML profiles.

You can configure only one instance of service provider and identity provider on the appliance .

Logout

When a user logs out of the appliance , they are not logged out of other SAML 2.0 SSO enabled applications.

Limitations

You cannot configure SAML profiles at cluster level. All SAML configurations are restricted to machine level.

How to Configure SSO on your Appliance

Procedure

	Command or Action	Purpose
Step 1	Review the prerequisites.	Prerequisites, on page 68
Step 2	Configure your appliance as a service provider.	Configuring Appliance as a Service Provider, on page 69
Step 3	[On IDP] Configure the identity provider to work with your appliance .	Configuring the Identity Provider to Communicate with Appliance , on page 72
Step 4	Configure identity provider settings on your appliance .	Configure Identity Provider Settings on Appliance , on page 74
Step 5	Enable External Authentication using SAML on your appliance .	Enable SAML Authentication

Prerequisites

- Supported Identity Providers, on page 68
- Certificates for Secure Communication, on page 69

Supported Identity Providers

Verify whether the identity provider used by your organization is supported by the appliance . The following are the pre-qualified identity providers:

- Microsoft Active Directory Federation Services (AD FS) 2.0 and later
- Duo Access Gateway
- Azure AD

Note You can use any standard SAML 2.0 identity provider to configure SSO using SAML on your email gateway.

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

To create and export certificates from your appliance , see Working with 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`

Configuring Appliance as a Service Provider

Note The service provider settings on the identity provider is configured based on the service provider configurations on the appliance .

Before you begin

Make sure that you review the Prerequisites, on page 68.

Procedure

Step 1 Log in to your appliance using the web interface.

Step 2 Navigate to **System Administration > SAML**.

Step 3 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 service provider settings on the identity provider.
Assertion Consumer URL	Enter the URL to which the identity provider should send the SAML assertion after authentication has successfully completed. The Assertion Consumer URL is the URL that is used to access your appliance . You will need this value while configuring the service provider settings on the identity provider.

Field	Description
SP Certificate	You can choose to import service provider certificates in any one of the following ways: • Select a signed certificate available on your appliance , from the drop-down list. • Import a certificate and the associated private key. The certificate must be in (.cert) format and the private key in (.key) format. • Import a certificate in PKCS #12 file format. Password is mandatory for PKCS #12 format certificates. (Optional) **Signing Authentication Requests** If you want the appliance to sign the SAML authentication requests: **a.** Upload the certificate obtained from the appliance and the associated private key. You must upload the certificate in (**.cert**) format. For more information, see Certificates for Secure Communication, on page 69. **b.** Enter the passphrase for the private key. **c.** Select **Sign Requests**. (Optional) **Decrypt Encrypted Assertions** If you plan to configure your identity provider to encrypt SAML assertions: **a.** Upload the certificate obtained from the appliance and the associated private key. **b.** Enter the passphrase for the private key. **Note** The private key must be in **.key** format. For information on the usage of certificates, see Certificates for Secure Communication, on page 69.
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 Identity Provider Settings on Appliance , on page 74.
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** and commit your changes.

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. After you configure the settings, 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 Appliance , on page 72.

Configuring the Identity Provider to Communicate with Appliance

Before you begin

Make sure that you have:

- Configured your appliance as a service provider. See Configuring Appliance as a Service Provider, on page 69.
- Copied the service provider metadata details or exported the metadata file. See Configuring Appliance as a Service Provider, on page 69.

Procedure

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 Appliance , on page 73.
- Configure Duo Access Gateway to Communicate with Appliance , on page 73.
- Configure Azure AD to Communicate with Appliance , on page 74.

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 Appliance , on page 74.

Configure AD FS to Communicate with 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 Duo Access Gateway to Communicate with 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 Azure AD to Communicate with 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/or groups under Azure Application created for SAML > Users & Groups to control users who can login to this Azure SAML application..

Configure Identity Provider Settings on 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 Appliance , on page 72.
- Copied the identity provider metadata details or exported the identity provider metadata as file.

Procedure

Step 1 Log in to your appliance on the web interface.

Step 2 Navigate to **System Administration > SAML**.

Step 3 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 SAML Authentication.

Configuring OpenID Connect 1.0 on Email Gateway for AsyncOS APIs

Overview

The Cisco Secure Email Gateway 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 email gateway. Currently, your email gateway 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 email gateway as a resource provider.

Steps:

1. [One-time activity] Configure yor email gateway to validate the access token. For more information, see Configuring OpenID Connect on Email Gateway, on page 77.
2. [One-time activity] The email gateway 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 email gateway.
5. The email gateway validates the access token in the API request using the key set retrieved from step2.
6. The email gateway validates the required claim (issuer, audience) in the access token.
7. The email gateway uses the role claim value to authorize and allocate the user role privileges to access the AsyncOS APIs.
8. The email gateway 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: erik.fernandes@customorg.com
claim: Role: LogCollector
claim: Role: ReadOnly
[...]
```

The email gateway 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 email gateway with OpenID Connect:

- The authentication provider used by your organization is supported by the email gateway.
- The application can authenticate with the authentication provider and retrieve the access token.
- The email gateway can connect to the authentication provider over HTTPs to fetch the OpenID Connect metadata configuration.

Configuring OpenID Connect on Email Gateway

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 email gateway to perform the required authorization checks.

Procedure

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 Open ID 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 email gateway 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://esa.com/esa/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'

--header 'Authorization: Bearer <add access_token here>’
```

System Time

It is recommended that you avoid changing the time settings on the appliance .

To set the System Time on your appliance , set the Time Zone used, or select an NTP server and query interface, use the Time Zone or Time Settings page from the System Administration menu in the GUI or use the following commands in the CLI: ntpconfig , settime , and settz .

You can also verify the time zone files used by AsyncOS on the **System Administration > Time Settings** page or using the tzupdate CLI command.

Selecting a Time Zone

The Time Zone page (available via the System Administration menu in the GUI) displays the time zone for your appliance . You can select a specific time zone or GMT offset.

Procedure

Step 1 Click **Edit Settings** on the **System Administration > Time Zone** page.
Step 2 Select a Region, country, and time zone from the pull-down menus.
Step 3 Submit and commit your changes.

Selecting a GMT Offset

Procedure

Step 1 Click **Edit Settings** on the **System Administration > Time Zone** page.
Step 2 Select GMT Offset from the list of regions.
Step 3 Select an offset in the Time Zone list. The offset refers to the amount of hours that must be added/subtracted in order to reach GMT (the Prime Meridian). Hours preceded by a minus sign ("-") are east of the Prime Meridian. A plus sign ("+") indicates west of the Prime Meridian.
Step 4 Submit and commit your changes.

Editing Time Settings

You can edit the time settings for the appliance using one of the following methods:

- (Recommended) Setting Appliance System Time Using the Network Time Protocol (NTP), on page 79
- Setting Appliance System Time Manually , on page 80

(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.

Procedure

Step 1 Navigate 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 Submit and commit your changes.

Setting Appliance System Time Manually

This time keeping method is generally not recommended. Use a Network Time Protocol server instead.

Procedure

Step 1 Navigate to the System Administration > Time Settings page.
Step 2 Click **Edit Settings**.
Step 3 In the Time Keeping Method section, select Set Time Manually.
Step 4 Enter the month, day, year, hour, minutes, and seconds.
Step 5 Select A.M or P.M.
Step 6 Submit and commit your changes.

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.
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.
View or build a custom reporting page	See My Dashboard Page.

Setting User Preferences

Local users can define preference settings, such as language, specific to each account. These settings apply by default when the user first logs into the appliance . The preference settings are stored for each user and are the same regardless from which client machine the user logs into the appliance .

When users change these settings but do not commit the changes, the settings revert to the default values when they log in again.

Note This feature is not available to externally-authenticated users. These users can choose a language directly from the Options menu.

Procedure

Step 1 Log into the appliance with the user account for which you want to define preference settings.

Step 2 Choose **Options** > **Preferences**. The options menu is at the top right side of the window.

Step 3 Click **Edit Preferences**.

Step 4 Configure settings:

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

Step 5 Submit and commit your changes.

Step 6 Click the **Return to previous page** link at the bottom of the page.

General Settings

You can edit the following general settings for the appliance :

- Overriding Internet Explorer Compatibility Mode, on page 81
- Collecting Usage Statistics of the Appliance on the New Web Interface , on page 82

Overriding Internet Explorer Compatibility Mode

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.

Procedure

Step 1 Click System **Administration** > **General Settings**.

Step 2 Select **Override IE Compatibility Mode** check box.

Step 3 Submit and commit your changes.

Collecting Usage Statistics of the Appliance on the New Web Interface

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 .

Usage Analytics is enabled on the appliance by default. If you want to disable Usage Analytics, do the following:

Procedure

Step 1 Click System **Administration** > **General Settings**.

Step 2 Clear the **Usage Analytics** check box.

Step 3 Submit and commit your changes.

Configuring Maximum HTTP Header Size

You can now use the `adminaccessconfig > maxhttpheaderfieldsize` command in the CLI to configure the maximum HTTP header size of an HTTP request sent to the appliance .

The default value for the HTTP header field size is 4096 (4 KB) and the maximum value is 33554432 (32 MB).

Restarting and Viewing Status of Service Engines

You can use the `diagnostic > services`sub command in the CLI to:

- Restart the service engines enabled on your appliance without having to reboot your appliance .
- View the status of service engines enabled on your appliance .

For more information, refer to the CLI Reference Guide for Email Security Appliance .