Centralizing Services on a Cisco Secure Email and Web Manager (M-Series)

This chapter contains the following sections:

- Overview of Cisco Secure Email and Web Manager Services , on page 1
- Network Planning, on page 1
- Working with an External Spam Quarantine , on page 2
- About Centralizing Policy, Virus, and Outbreak Quarantines , on page 5
- Configuring Centralized Reporting, on page 9
- Configuring Centralized Message Tracking, on page 10
- Using Centralized Services , on page 11

Overview of Cisco Secure Email and Web Manager Services

The Cisco Secure Email and Web Manager (M-Series appliance) is an external or “off box” location that provides a single interface to certain services on multiple email gateways.

The Cisco Secure Email and Web Manager includes the following features:

- External spam quarantine. Holds spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.
- Centralized policy, virus, and outbreak quarantines. Provide a single location behind the firewall to store and manage messages quarantined by anti-virus scanning, outbreak filters, and policies.
- Centralized reporting. Run reports on aggregated data from multiple email gateways.
- Centralized tracking. Track email messages that traverse multiple email gateways.

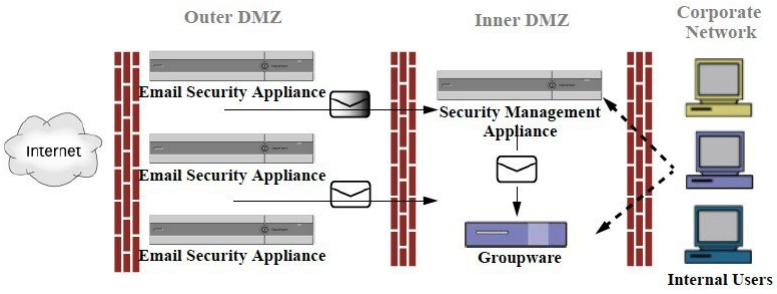
For complete information about configuring and using your Cisco Secure Email and Web Manager, see the Cisco Secure Email and Web Manager User Guide.

Network Planning

The Cisco Secure Email and Web Manager lets you separate the end-user interfaces (such as mail applications) from the more secure gateway systems residing in your various DMZs. Using a two-layer firewall can provide you with flexibility in network planning so that end users do not connect directly to the outer DMZ.

The following figure shows a typical network configuration incorporating Cisco Secure Email and Web Manager and multiple DMZs.

Figure 1: Typical Network Configuration with Cisco Secure Email and Web Manager



Large corporate data centers can share one Cisco Secure Email and Web Manager which acts as an external spam quarantine for one or more email gateways. Meanwhile, remote offices can maintain local spam quarantines on email gateways for local use.

Working with an External Spam Quarantine

- Mail Flow and External Spam Quarantine , on page 2
- Migrating from a Local Spam Quarantine to an External Quarantine, on page 3
- Enabling an External Spam Quarantine and External Safelist/Blocklist , on page 3
- Disabling the Local Spam Quarantine to Activate the External Quarantine , on page 4
- Troubleshooting an External Spam Quarantine , on page 5

Mail Flow and External Spam Quarantine

If your network is configured as described in Network Planning, on page 1, incoming mail from the Internet is received by appliances in the outer DMZ. Clean mail is sent along to the mail transfer agent (MTA) (groupware) in the inner DMZ and eventually to the end users within the corporate network.

Spam and suspected spam (depending on your mail flow policy settings) is sent to the spam quarantine on Cisco Secure Email and Web Manager. End users may then access the quarantine and elect to delete spam and release messages that they would like to have delivered to themselves. Messages remaining in the spam quarantine are automatically deleted after a configurable amount of time.

Messages that are released from the external quarantine on the Cisco Secure Email and Web Manager are returned to the originating email gateway for delivery. These messages do not normally pass through the following processes before delivery: HAT and other policy or scanning settings, RAT, domain exceptions, aliasing, incoming filters, masquerading, bounce verification, and the work queue.

An email gateway that is configured to send mail to a Cisco Secure Email and Web Manager will automatically expect to receive mail released from the Cisco Secure Email and Web Manager and will not reprocess those messages when they are received back. For this to work, the IP address of the Cisco Secure Email and Web Manager must not change. If the IP address of the Cisco Secure Email and Web Managerchanges, the receiving email gateway will process the message as it would any other incoming message. You should always use the same IP address for receiving and delivery on the Cisco Secure Email and Web Manager.

The Cisco Secure Email and Web Manager accepts mail for quarantining from the IP addresses specified in the spam quarantine settings. To configure the spam quarantine on the Security Management appliance, see the Cisco Secure Email and Web Manager User Guide.

Mail released by the Cisco Secure Email and Web Manager is delivered to the primary and secondary hosts (content security appliance or other groupware host) as defined in the spam quarantine settings (see the Cisco Secure Email and Web Manager User Guide). Therefore, regardless of the number of email gateways delivering mail to the Cisco Secure Email and Web Manager, all released mail, notifications, and alerts are sent to a single host (groupware or content security appliance). Take care not to overburden the primary host for delivery from the Cisco Secure Email and Web Manager.

Migrating from a Local Spam Quarantine to an External Quarantine

If you are currently using the local spam quarantine on an email gateway but would like to migrate to an external spam quarantine hosted on a Cisco Secure Email and Web Manager — while retaining access to the messages in the local quarantine — you should prevent new messages from entering the local quarantine during the transition.

Consider the following possible strategies:

- Configuring anti-spam settings — Configure the anti-spam settings on your mail policy specifying Cisco Secure Email and Web Manager as the alternate host. This action sends new spam to the external quarantine while still allowing access to the local quarantine.
- Setting a shorter expiration time — Configure the Schedule Delete After setting on the local quarantine to a shorter duration.
- Deleting all of the remaining messages — To delete all remaining messages in the local quarantine, disable the quarantine and the click the “Delete All” link on the local quarantines page (see Deleting Messages from the Spam Quarantine). This link only becomes available when a local spam quarantine with messages still contained in it has been disabled.

You should now be ready to enable the external quarantine and disable the local quarantine.

Note If both the local quarantine and the external quarantine are enabled, the local quarantine is used.

Enabling an External Spam Quarantine and External Safelist/Blocklist

You can enable only one external spam quarantine on an email gateway.

Before You Begin

- Review the information in Mail Flow and External Spam Quarantine , on page 2 .
- Review and take action on the information in Migrating from a Local Spam Quarantine to an External Quarantine, on page 3.
- Configure Cisco Secure Email and Web Manager to support the centralized spam quarantine and safelist/blocklist features. See the documentation for your Cisco Secure Email and Web Manager.
- If a different external spam quarantine was previously configured for the Email Security appliance, first disable the external spam quarantine setting.

Complete the following procedure on each email gateway.

Procedure

Step 1 Select **Security Services > Centralized Services > Spam Quarantine**.

Step 2 Click **Configure**.

Step 3 Select **Enable External Spam Quarantine**.

Step 4 In the Name field, enter the name of Cisco Secure Email and Web Manager

The name is not significant, and is used for reference only. For example, enter the hostname of Cisco Secure Email and Web Manager.

Step 5 Enter an IP address and port number.

These must match the IP address and port number that are specified on Cisco Secure Email and Web Manager in the Spam Quarantines Settings page (**Management Appliance > Centralized Services > Spam Quarantine**.)

Step 6 (Optional) Select the check box to enable the **External Safelist/Blocklist** feature, and specify the appropriate blocklist action.

Step 7 Submit and commit your changes.

Step 8 Repeat this procedure for each email gateway.

What to do next

If you have been using a local quarantine, see Disabling the Local Spam Quarantine to Activate the External Quarantine , on page 4.

Related Topics

- Local Versus External Spam Quarantine
- Spam Quarantine
- Managing Spam and Graymail
- How to Configure the Email Gateway to Scan Messages for Spam

Disabling the Local Spam Quarantine to Activate the External Quarantine

If you were using a local spam quarantine before enabling an external spam quarantine, you must disable the local quarantine in order to send messages to the external quarantine.

Before You Begin

Follow all directions, including information in the Before You Begin section, in Enabling an External Spam Quarantine and External Safelist/Blocklist , on page 3.

Procedure

Step 1 Select **Monitor > Spam Quarantine**.

Step 2 In the Spam Quarantine section, click the **Spam Quarantine** link.

Step 3 Deselect **Enable Spam Quarantine**.

Ignore any warnings to adjust mail policies as a result of this change. Mail policies automatically send messages to the external spam quarantine if you have configured the external quarantine settings.

Step 4 Submit and commit your changes.

Troubleshooting an External Spam Quarantine

Problem: Messages released from Cisco Secure Email and Web Manager are unnecessarily reprocessed by the email gateway.

Solution: This can occur if the IP address of Cisco Secure Email and Web Manager has changed. See Mail Flow and External Spam Quarantine , on page 2.

About Centralizing Policy, Virus, and Outbreak Quarantines

- Centralized Policy, Virus, and Outbreak Quarantines , on page 5
- About Migration of Policy, Virus, and Outbreak Quarantines , on page 6
- Centralizing Policy, Virus, and Outbreak Quarantines , on page 7
- About Disabling Centralized Policy, Virus, and Outbreak Quarantines, on page 8
- Troubleshooting Centralized Policy, Virus, and Outbreak Quarantines , on page 9

Centralized Policy, Virus, and Outbreak Quarantines

You can centralize policy, virus, and outbreak quarantines on a Cisco Secure Email and Web Manager. Messages are processed by email gateways but are stored in quarantines on Cisco Secure Email and Web Manager.

Centralizing policy, virus, and outbreak quarantines offers the following benefits:

- Administrators can manage quarantined messages from multiple email gateways in one location.
- Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk.
- Centralized quarantines can be backed up using the standard backup functionality on Cisco Secure Email and Web Manager.

For complete information, see the user guide or online help for your Cisco Secure Email and Web Manager.

Restrictions and Limitations of Centralized Policy, Virus, and Outbreak Quarantines

- On each email gateway, either all policy, virus, and outbreak quarantines must be centralized or all must be stored locally.
- Because scanning engines are not available on Cisco Secure Email and Web Manager, you cannot manually test messages in policy, virus, or outbreak quarantines for viruses.

Requirements for Centralized Policy, Virus, and Outbreak Quarantines in Cluster Configurations

You can enable centralized policy, virus, and outbreak quarantines at any level for clustered appliances.

Requirements:

- Before you enable centralized policy, virus, and outbreak quarantines on an email gateway at a particular level (machine, group, or cluster), all appliances that belong to the same level must first be added to Cisco Secure Email and Web Manager.
- Content and message filters and DLP message actions must be configured at the same level and not overridden at any level below that level.
- Centralized policy, virus, and outbreak quarantines settings must be configured at the same level and not be overridden at any level below the configured level.
- Ensure that the interface to be used for communications with Cisco Secure Email and Web Manager has the same name on all appliances in the group or cluster.

For example:

If you want to enable centralized policy, virus, and outbreak quarantines at the cluster or group level, but an email gateway which is connected to the cluster has these settings defined at the machine level, you must remove the centralized quarantines settings configured at the machine level before you can enable the feature at the cluster or group level.

About Migration of Policy, Virus, and Outbreak Quarantines

When you centralize policy, virus, and outbreak quarantines, existing policy, virus, and outbreak quarantines on your email gateway migrate to Cisco Secure Email and Web Manager.

You will configure migration on Cisco Secure Email and Web Manager, but migration occurs when you commit the change enabling centralized policy, virus, and outbreak quarantines on the email gateway.

As soon as you commit this change, the following occur:

- Local policy, virus, and outbreak quarantines on the email gateway are disabled. All new messages entering these quarantines will be quarantined on Cisco Secure Email and Web Manager.
- Migration of existing non-spam quarantines to Cisco Secure Email and Web Manager begins.
- All local policy, virus, and outbreak quarantines are deleted. If you configured a custom migration, any local policy quarantines that you chose not to migrate are also deleted. For effects of deleting policy quarantines, see About Deleting Policy Quarantines.
- A message that was in multiple quarantines before migration will be in the corresponding centralized quarantines after migration.
- Migration happens in the background. The amount of time it takes depends on the size of your quarantines and on your network. When you enable centralized quarantines on the email gateway, you can enter one or more email addresses that will receive notification when migration is complete.
- The settings in the centralized quarantine, not those of the originating local quarantine, apply to the messages. However, the original expiration time still applies to each message.

Note All centralized quarantines that are automatically created during migration have the default quarantine settings.

Centralizing Policy, Virus, and Outbreak Quarantines

Before you begin

Note Perform this procedure during a maintenance window or off-peak hours.

- You must first configure your Cisco Secure Email and Web Manager for centralized policy, virus, and outbreak quarantines. See the table in the "Centralizing Policy Virus, and Outbreak Quarantines" section in the "Centralized Policy, Virus, and Outbreak Quarantines" chapter in the online help or user guide for Cisco Secure Email and Web Manager.
- If the space allocated to centralized quarantines on Cisco Secure Email and Web Manager will be smaller than the amount of space that your existing local quarantines collectively occupy, messages will be expired early based on the quarantine settings on Cisco Secure Email and Web Manager. Before migration, consider taking manual action to reduce quarantine sizes. For more information about early expiration, see Default Actions for Automatically Processed Quarantined Messages.
- If you have chosen automatic migration, or configured custom migration to create centralized quarantines during migration, consider noting the current quarantine settings on your email gateways in order to use them as guidelines for configuring the centralized quarantines.
- If your email gateways are deployed in a cluster configuration, see Requirements for Centralized Policy, Virus, and Outbreak Quarantines in Cluster Configurations , on page 5.
- Be aware of the changes that will occur as soon as you commit the changes in this procedure. See About Migration of Policy, Virus, and Outbreak Quarantines , on page 6.

Procedure

Step 1 Choose **Security Services > Centralized Services > Policy, Virus, and Outbreak Quarantines**.

Step 2 Click **Enable**.

Step 3 Enter the interface and port to use for communication with Cisco Secure Email and Web Manager.

Make sure the interface and port are reachable from Cisco Secure Email and Web Manager.

If your email gateways are clustered, the interface you select must be available on all machines in the cluster.

Step 4 To receive notification when migration is complete, enter one or more email addresses.

Step 5 Verify the information about quarantines to be migrated to be sure that this is what you want.

Step 6 If you are completing a Custom migration, note any quarantines that will be deleted when you commit the changes in this procedure.

Step 7 Verify that the information about content and message filters and DLP message actions to be updated is as you expect it to be.

Note
For cluster configurations, filters and message actions can be automatically updated on a particular level only if filters and message actions are defined at that level and not overridden at any level below that level. After migration, you may need to manually reconfigure filters and message actions with centralized quarantine names.

Step 8 If you need to reconfigure migration mapping:

a) Return to Cisco Secure Email and Web Manager.
b) Reconfigure the migration mapping.

   On Cisco Secure Email and Web Manager, select a quarantines to remap, then click **Remove from Centralized Quarantine**. Then you can remap the quarantine.

c) Commit the new migration configuration on Cisco Secure Email and Web Manager.
d) Start this procedure from the beginning.

   Important! Be sure to reload the **Security Services > Centralized Services > Policy, Virus, and Outbreak Quarantines** page.

Step 9 Click **Submit**.

Step 10 If you need to reconfigure migration mapping, follow the procedure in Step 8.

Step 11 Commit your changes.

Note
While migration is in progress, avoid making configuration changes on email gateway or Cisco Secure Email and Web Manager.

Step 12 Look at the top of the page to monitor migration status, or, if you entered an email address when configuring migration, await the email notifying you that migration is complete.

What to do next

Perform the remaining tasks described in the table in the "Centralizing Policy, Virus, and Outbreak Quarantines" topic in the online help or user guide for Cisco Secure Email and Web Manager.

Related Topics

- Which User Groups Can Access Policy, Virus, and Outbreak Quarantines

About Disabling Centralized Policy, Virus, and Outbreak Quarantines

When you disable centralized policy, virus, and outbreak quarantines on the email gateway:

- Local quarantines are automatically enabled on the email gateway.
- System-created quarantines and quarantines that are referenced by message filters, content filters, and DLP message actions are automatically created on the email gateway. The Virus, Outbreak, and Unclassified quarantines are created with the same settings that they had before quarantines were centralized, including assigned user roles. All other quarantines are created with default settings.
- Newly quarantined messages go immediately to local quarantines.
- Messages in the centralized quarantine at the time it is disabled remain there until one of the following occurs:
  - Messages are manually deleted or automatically deleted when they expire.
  - Messages are manually or automatically released, if one of the following is also true:

* An alternate release appliance is configured on Cisco Secure Email and Web Manager. See the online help or documentation for Cisco Secure Email and Web Manager.

* Centralized quarantines are again enabled on the email gateway.

Disabling Centralized Policy, Virus, and Outbreak Quarantines

Before you begin

- Understand the impacts of disabling centralized policy, virus, and outbreak quarantines.
- Do one of the following:
  - Process all messages that are currently in centralized policy, virus, and outbreak quarantines.
  - Ensure that you have designated an alternate release appliance to process messages that are released from the centralized quarantine after you disable it. For information, see the online help or user guide for your Cisco Secure Email and Web Manager.

Procedure

Step 1 On the email gateway, choose **Security Services > Centralized Services > Policy, Virus, and Outbreak Quarantines**.

Step 2 Disable centralized policy, virus, and outbreak quarantines.

Step 3 Submit and commit the change.

Step 4 Customize the settings of the newly created local quarantines.

Troubleshooting Centralized Policy, Virus, and Outbreak Quarantines

If a Cisco Secure Email and Web Manager Goes Out of Service

If Policy, Virus, and Outbreak Quarantines are centralized on a Cisco Secure Email and Web Manager that goes out of service, you should disable these centralized quarantines on the email gateway.

If you deploy a replacement Cisco Secure Email and Web Manager, you must reconfigure quarantine migration on Cisco Secure Email and Web Manager and on each email gateway. See the table in the "Centralizing Policy Virus, and Outbreak Quarantines" section in the "Centralized Policy, Virus, and Outbreak Quarantines" chapter in the online help or user guide for Cisco Secure Email and Web Manager.

Configuring Centralized Reporting

Before you begin

- Enable and configure centralized reporting on a Cisco Secure Email and Web Manager. See prerequisites and instructions in Cisco Secure Email and Web Manager User Guide.
- Ensure that sufficient disk space is allocated to the reporting service on Cisco Secure Email and Web Manager.

Procedure

Step 1 Click **Security Services > Reporting**.

Step 2 In the Reporting Service section, select the Centralized Reporting option.

Step 3 Submit and commit your changes.

Requirements for Advanced Malware Protection Reporting

For required configurations for full reporting on Advanced Malware Protection (file reputation and file analysis) features on Cisco Secure Email and Web Manager, see the information about Advanced Malware Protection reports in the email reporting chapter of the online help or user guide for your version of Cisco Secure Email and Web Manager software.

Availability of Reporting Information after Changing to Centralized Reporting

When centralized reporting is enabled on an email gateway:

- Existing data on the email gateway for the monthly report is not transferred to Cisco Secure Email and Web Manager.
- Archived reports on the email gateway are not available.
- The email gateway stores only a week's worth of data.
- New data for the monthly and yearly reports is stored on Cisco Secure Email and Web Manager.
- Scheduled reports on the email gateway are suspended.
- You can no longer access the scheduled report configuration page on the email gateway.

About Disabling Centralized Reporting

If you disable centralized reporting on the email gateway, the email gateway begins storing new monthly report data, scheduled reports resume, and you can access its archived reports. After disabling centralized reporting, the appliance only displays data for the past hour and day, but not the past week or month. This is temporary. The appliance will display the reports for the past week and month after it accumulates enough data. If the email gatewayEmail Security appliance is placed back into centralized reporting mode, it will display data for the past week in the interactive reports.

Configuring Centralized Message Tracking

Before you begin

Note You cannot enable both centralized and local tracking on an email gateway.

Procedure

Step 1 Click **Security Services > Message Tracking**.

Step 2 In the Message Tracking Service section, click **Edit Settings**.

Step 3 Select the **Enable Message Tracking Service** check box.

Step 4 Select the Centralized Tracking option.

Step 5 (Optional) Select the check box to save information for rejected connections.

Note
Saving tracking information for rejected connections can adversely affect the performance of Cisco Secure Email and Web Manager.

Step 6 Submit and commit your changes.

What To Do Next

To use centralized tracking, you must enable the feature on the email gateways *and* Cisco Secure Email and Web Manager. To enable centralized tracking on S Cisco Secure Email and Web Manager, see Cisco Secure Email and Web Manager User Guide.

Using Centralized Services

For instructions on using centralized services, see the Cisco Secure Email and Web Manager User Guide.