Centralized Policy, Virus, and Outbreak Quarantines

This chapter contains the following sections:

- Overview of Centralized Quarantines , on page 1
- Centralizing Policy, Virus, and Outbreak Quarantines , on page 3
- Managing Policy, Virus, and Outbreak Quarantines, on page 10
- Working with Messages in Policy, Virus, or Outbreak Quarantines, on page 17
- Troubleshooting Centralized Policy Quarantines , on page 24

Overview of Centralized Quarantines

Messages processed by certain filters, policies, and scanning operations on an Email Security appliance can be placed into quarantines to temporarily hold them for further action. You can centralize quarantines from multiple Email Security appliances on a Cisco Content Security Management appliance.

Benefits of centralizing quarantines include the following:

- You can manage quarantined messages from multiple Email Security appliances in one location.
- Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk.
- Centralized quarantines can be backed up as part of the standard backup functionality on the Security Management appliance.

Anti-virus scanning, Outbreak Filters, and Advanced Malware Protection (File Analysis) each have a single dedicated quarantine. You create policy quarantines to hold messages that are caught by message filtering, content filtering, and Data Loss Prevention policies.

For additional information about quarantines, see the documentation for your Email Security appliance.

Quarantine Types

Quarantine Type	Quarantine Name	Created by the System by Default?	Description	More Information
Advanced Malware Protection	File Analysis	Yes	Holds messages that are sent for file analysis, until a verdict is returned.	• Managing Policy, Virus, and Outbreak Quarantines • Working with Messages in Policy, Virus, or Outbreak Quarantines
Virus	Virus	Yes	Holds messages that may be transmitting malware, as determined by the anti-virus engine.	
Outbreak	Outbreak	Yes	Holds messages caught by Outbreak Filters as potentially being spam or malware.	
Policy	Policy	Yes	Holds messages caught by message filters, content filters, and DLP message actions. A default Policy quarantine has been created for you.	
	Unclassified	Yes	Holds messages only if a quarantine that is specified in a message filter, content filter, or DLP message action has been deleted. You cannot assign this quarantine to any filter or message action.	
	(Policy quarantines that you create)	No	Policy quarantines that you create for use in message filters, content filters, and DLP message actions.	

Quarantine Type	Quarantine Name	Created by the System by Default?	Description	More Information
Spam	Spam	Yes	Holds spam or suspected spam messages for the message's recipient or an administrator to review. The spam quarantine is not included in the group of policy, virus, and outbreak quarantines and is managed separately from all other quarantines.	Spam Quarantine

Centralizing Policy, Virus, and Outbreak Quarantines

Procedure

	Command or Action	Purpose
Step 1	If your Email Security appliance is in your DMZ and your Security Management appliance is behind your firewall, open a port in the firewall to allow the appliances to exchange centralized policy, virus, and outbreak quarantine data.	Firewall Information
Step 2	On the Security Management appliance, enable the feature.	Enabling Centralized Policy, Virus, and Outbreak Quarantines on the Security Management Appliance , on page 5
Step 3	On the Security Management appliance, allocate disk space for non-spam quarantines.	Managing Disk Space
Step 4	(Optional) • Create centralized policy quarantines on the Security Management appliance with desired settings. • Configure settings for the centralized virus and outbreak quarantines, and for the default policy quarantines. If you configure these settings before migration, you can refer to the existing settings on your Email Security appliances. You can also create required quarantines while configuring custom migration, or quarantines will be	• Configuring Policy, Virus, and Outbreak Quarantines , on page 12 • Checking the Settings of System-Created Quarantines , on page 12.

	Command or Action	Purpose
	created for you during automatic migration. All quarantines created during migration have default settings. Local quarantine settings are not retained in the centralized quarantine, even if the quarantine name is the same.	
Step 5	On the Security Management appliance, add Email Security appliances to manage, or select the Policy, Virus and Outbreak Quarantines option from the centralized services of an already-added appliance. • If your Email Security appliances are clustered, all appliances that belong to a particular level (machine, group, or cluster) must be added to the Security Management appliance before you enable centralized Policy, Virus and Outbreak Quarantines on any Email Security appliance in the cluster.	Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance, on page 6
Step 6	Commit your changes.	
Step 7	On the Security Management appliance, configure migration of existing policy quarantines from Email Security appliances.	Configuring Migration of Policy, Virus, and Outbreak Quarantines , on page 7
Step 8	On an Email Security appliance, enable the centralized policy, virus, and outbreak quarantines feature. • **Important** If you have policy, virus, and outbreak quarantines configured on an Email Security appliance, migration of quarantines and all their messages begins as soon as you commit this change.	See the "Centralizing Services on a Cisco Content Security Management appliance" chapter in the documentation for your Email Security appliance, specifically the following sections: • "About Migration of Policy, Virus, and Outbreak Quarantines" • "Centralizing Policy, Virus, and Outbreak Quarantines"
Step 9	Migrate additional Email Security appliances. • Only one migration process can be in progress at any time. Do not enable centralized policy, virus, and outbreak quarantines on another Email Security appliance until the previous migration is complete.	
Step 10	Edit centralized quarantine settings as needed. • Quarantines created during migration are created with default settings, not the settings in the originating local quarantines, even if the centralized and local quarantine names are the same.	Configuring Policy, Virus, and Outbreak Quarantines , on page 12

	Command or Action	Purpose
Step 11	If message filters, content filters, and DLP message actions could not be automatically updated with the names of centralized quarantines, manually update those configurations on your Email Security appliances. • In 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.	See the documentation for message filters, content filters, and DLP Message Actions in the online help or user guide for your Email Security appliance.
Step 12	(Recommended) Specify an Email Security appliance to process released messages if the originating appliance is not available.	Designating an Alternate Appliance to Process Released Messages, on page 9
Step 13	If you delegate administration to custom user roles, you may need to configure access in a certain way.	Configuring Centralized Quarantine Access for Custom User Roles , on page 9

Enabling Centralized Policy, Virus, and Outbreak Quarantines on the Security Management Appliance

Before you begin

Complete any steps preceding this procedure in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3.

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

Step 2 Click **Enable**.

Step 3 Specify the interface and port for communication with Email Security appliances:

- Accept the default selections unless you have reason to change them.
- If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.
- Use the same port that you opened in the firewall.

Step 4 Click **Submit**.

What to do next

Return to the next step in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3.

Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance

To see an consolidated view of all quarantines on all Email Security appliances, consider adding all Email Security appliances before centralizing any quarantines.

Before you begin

Make sure you have completed all procedures to this point in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3.

Step 1 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 2 If you have already added the Email Security appliance to the list on this page:

a) Click the name of an Email Security appliance.

b) Select the **Policy, Virus, and Outbreak Quarantines** service.

Step 3 If you have not yet added the Email Security appliance:

a) Click Add Email Appliance.

b) In the Appliance Name and IP Address text fields, enter the appliance name and the IP address for the Management interface of the appliance you are adding.

Note If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.

c) The Policy, Virus and Outbreak Quarantines service is pre-selected.

d) Click **Establish Connection**.

e) Enter the user name and password for an administrator account on the appliance to be managed, and then click **Establish Connection**.

Note You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

f) Wait for the Success message to appear above the table on the page.

Step 4 Click **Submit**.

Step 5 Repeat this procedure for each Email Security appliance for which you want to enable Centralized Policy, Virus, and Outbreak Quarantines.

For example, add the other appliances in the cluster.

Step 6 Commit your changes.

What to do next

Return to the next step in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3.

Configuring Migration of Policy, Virus, and Outbreak Quarantines

Before you begin

- Make sure that you have completed all procedures to this point in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3
- For caveats and information about the migration process, see the "About Migration of Policy, Virus, and Outbreak Quarantines" section in the "Centralizing Services on a Cisco Content Security Management appliance" chapter in the documentation for your Email Security appliance.

Step 1 On the Security Management appliance, choose **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines**.

Step 2 Click **Launch Migration Wizard**.

Step 3 Choose a migration method:

If	Choose	Additional Information
• You want to migrate all existing policy quarantines from all associated Email Security appliances, and • Policy quarantines with the same names have identical settings on all Email Security appliances, and • You want to merge all policy quarantines with the same name on all Email Security appliances into a single centralized policy quarantine having that name.	Automatic	All centralized policy quarantines that are created using this process are automatically configured with default settings, regardless of the settings in the quarantines with the same names on the Email Security appliance. You must update those settings after migration.

If	Choose	Additional Information
• Policy quarantines with the same names have different settings on different Email Security appliances and you want to maintain the differences, or • You want to migrate some local quarantines and delete all others, or • You want to migrate local quarantines to centralized quarantines with different names or • You want to merge local quarantines with different names into a single centralized quarantine.	Custom	Any centralized policy quarantines that you create during migration, instead of before migration, will be configured with the default settings for new quarantines. You should update those settings after migration.

Step 4 Click **Next**.

Step 5 If you selected **Automatic**:

Verify that the policy quarantines to be migrated and other information on this page match your expectations.

Virus, Outbreak, and File Analysis quarantines will also be migrated.

Step 6 If you selected **Custom**:

- To select whether to show quarantines from all Email Security appliances or just one., choose an option from the **Show Quarantines from**: list.
- Select which local policy quarantines move to each centralized policy quarantine.
- Create additional centralized policy quarantines as needed. These will have default settings.
- Quarantine names are case-sensitive.
- Any quarantines remaining in the table on the left will not be migrated and will be deleted from the Email Security appliance upon migration.
- You can change the quarantine mapping by selecting a quarantine from the table on the right and clicking **Remove from Centralized Quarantine**.

Step 7 Click **Next** as needed.

Step 8 Submit and commit your changes.

What to do next

Return to the next step in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3.

Designating an Alternate Appliance to Process Released Messages

Normally, when a message is released from a centralized quarantine, the Security Management appliance returns it for processing to the Email Security appliance that originally sent it to the centralized quarantine.

If the Email Security appliance that originated a message is not available, a different Email Security appliance can process and deliver released messages. You designate the appliance for this purpose.

Before you begin

- Verify that the alternate appliance can process and deliver released messages as expected. For example, configurations for encryption and antivirus rescanning should match the same configurations on your primary appliances.
- The alternate appliance must be fully configured for centralized policy, virus, and outbreak quarantines. Complete the steps in the table in Centralizing Policy, Virus, and Outbreak Quarantines , on page 3 for that appliance.

Step 1 On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

Step 2 Click the **Specify Alternate Release Appliance** button.

Step 3 Choose an Email Security appliance.

Step 4 Submit and commit your changes.

What to do next

Related Topics

Releasing Messages When an Email Security Appliance Is Unavailable , on page 10

Configuring Centralized Quarantine Access for Custom User Roles

In order to allow administrators with custom user roles to specify centralized policy quarantines in message and content filters and in DLP message actions on the Email Security appliance, you must grant those users access to the relevant policy quarantines on the Security Management appliance, and the custom user role names that you create on the Security Management appliance must match those on the Email Security appliance.

Related Topics

- Creating Custom Email User Roles

Disabling Centralized Policy, Virus, and Outbreak Quarantines

Generally, if you need to disable these centralized quarantines, you should do so on the Email Security appliance.

For information about disabling centralized policy, virus, and outbreak quarantines, including a list of impacts of doing so, see the online help or documentation for your Email Security appliance.

Releasing Messages When an Email Security Appliance Is Unavailable

Normally, when a message is released from a centralized quarantine, the Security Management appliance returns it for processing to the Email Security appliance that originally sent it to the centralized quarantine.

If the Email Security appliance that originated a message is not available, a different Email Security appliance can process and deliver released messages. You should designate an alternate release appliance for this purpose.

If the alternate appliance is unavailable, you can specify a different Email Security appliance as the alternate release appliance and that appliance will process and deliver queued messages.

After repeated unsuccessful attempts to reach an Email Security appliance. you will receive an alert.

Related Topics

- Designating an Alternate Appliance to Process Released Messages, on page 9

Managing Policy, Virus, and Outbreak Quarantines

- Disk Space Allocation for Policy, Virus, and Outbreak Quarantines , on page 10
- Retention Time for Messages in Quarantines , on page 11
- Default Actions for Automatically Processed Quarantined Messages , on page 12
- Checking the Settings of System-Created Quarantines , on page 12
- Configuring Policy, Virus, and Outbreak Quarantines , on page 12
- About Editing Policy, Virus, and Outbreak Quarantine Settings , on page 14
- Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned , on page 14
- About Deleting Policy Quarantines , on page 15
- Monitoring Quarantine Status, Capacity, and Activity , on page 15
- Alerts About Quarantine Disk-Space Usage , on page 16
- Policy Quarantines and Logging, on page 16
- About Distributing Message Processing Tasks to Other Users , on page 16

Disk Space Allocation for Policy, Virus, and Outbreak Quarantines

For information about allocating disk space, see Managing Disk Space.

Messages in multiple quarantines consume the same amount of disk space as a message in a single quarantine.

If Outbreak Filters and Centralized Quarantines are both enabled:

- All disk space on the Email Security appliance that would have been allocated to local policy, virus, and outbreak quarantines is used instead to hold copies of messages in the Outbreak quarantine, in order to scan those messages each time outbreak rules are updated.
- The disk space on the Security Management appliance for messages in the Outbreak quarantine from a particular managed Email Security appliance may be limited by the amount of available disk space for quarantined messages on that Email Security appliance.
- For more information about this situation, see Retention Time for Messages in Quarantines , on page 11

Related Topics

- Monitoring Quarantine Status, Capacity, and Activity , on page 15
- Alerts About Quarantine Disk-Space Usage , on page 16
- Retention Time for Messages in Quarantines , on page 11

Retention Time for Messages in Quarantines

Messages are automatically removed from the quarantine under the following circumstances:

- Normal Expiration—the configured retention time is met for a message in the quarantine. You specify a retention time for messages in each quarantine. Each message has its own specific expiration time, displayed in the quarantine listing. Messages are stored for the amount of time specified unless another circumstance described in this topic occurs.

  Note The normal retention time for messages in the Outbreak Filters quarantine is configured in the Outbreak Filters section of each mail policy, not in the outbreak quarantine.

- Early Expiration—messages are forced from quarantines before the configured retention time is reached. This can happen when:
  - The size limit for all quarantines, as defined in Disk Space Allocation for Policy, Virus, and Outbreak Quarantines , on page 10, is reached.

    If the size limit is reached, the oldest messages, regardless of quarantine, are processed and the default action is performed for each message, until the size of all quarantines is again less than the size limit. The policy is First In First Out (FIFO). Messages in multiple quarantines will be expired based on their latest expiration time.

    (Optional) You can configure individual quarantines to be exempt from release or deletion because of insufficient disk space. If you configure all quarantines to be exempt and the disk space reaches capacity messages will be held on the Email Security appliance until space is available on the Security Management appliance.

    Because the Security Management appliance does not scan messages, a copy of each message in the centralized outbreak quarantine is stored on the Email Security appliance that originally processed the message. This allows the Email Security appliance to rescan quarantined messages each time outbreak filter rules are updated, and tell the Security Management appliance to release messages that are no longer deemed a threat. Both copies of the outbreak quarantine should hold the same set of messages at all times. Therefore, in the rare situation when disk space on the Email Security appliance becomes full, then the copies of messages in the Outbreak quarantine on both appliances will expire early, even if the centralized quarantine still has space.

    You will receive alerts at disk-space milestones. See Alerts About Quarantine Disk-Space Usage , on page 16.

  - You delete a quarantine that still holds messages.

When a message is automatically removed from a quarantine, the default action is performed on that message. See Default Actions for Automatically Processed Quarantined Messages , on page 12.

Note In addition to the above scenarios, messages can be automatically removed from quarantine based on the result of scanning operations (outbreak filters or file analysis.)

Effects of Time Adjustments on Retention Time

- Daylight savings time and appliance time zone changes do not affect the retention period.
- If you change the retention time of a quarantine, only new messages will have the new expiration time.
- If the system clock is changed, messages that should have expired in the past will expire at the next most appropriate time.
- System clock changes do not apply to messages that are in the process of being expired.

Default Actions for Automatically Processed Quarantined Messages

The default action is performed on messages in a policy, virus, or outbreak quarantine when any situation described in Retention Time for Messages in Quarantines , on page 11, occurs.

There are two primary default actions:

- Delete—The message is deleted.
- Release—The message is released for delivery.

Upon release, messages may be rescanned for threats. For more information, see About Rescanning of Quarantined Messages , on page 23.

In addition, messages released before their expected retention time has passed can have additional operations performed on them, such as adding an X-Header. For more information, see Configuring Policy, Virus, and Outbreak Quarantines , on page 12.

Messages released from a centralized quarantine are returned to the originating Email Security appliance for processing.

Checking the Settings of System-Created Quarantines

Before you use quarantines, customize the settings of the default quarantines, including the Unclassified quarantine.

Related Topics

- Configuring Policy, Virus, and Outbreak Quarantines , on page 12

Configuring Policy, Virus, and Outbreak Quarantines

Before you begin

- If you are editing an existing quarantine, see About Editing Policy, Virus, and Outbreak Quarantine Settings , on page 14.
- Understand how messages in quarantines are automatically managed, including retention times and default actions. See Retention Time for Messages in Quarantines , on page 11, and Default Actions for Automatically Processed Quarantined Messages , on page 12.

- Determine which users you want to have access to each quarantine, and create users and custom user roles accordingly. For details, see Which User Groups Can Access Policy, Virus, and Outbreak Quarantines , on page 17.

Step 1 Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**.

Step 2 Do one of the following:

- Click **Add Policy Quarantine**.
- Click a quarantine to edit.

Step 3 Enter information.

Keep the following in mind:

- Changing the retention time of the File Analysis quarantine from the default of one hour is not recommended.
- If you do *not* want messages in this quarantine to be processed before the end of the Retention Period you specify, even when quarantine disk space is full, deselect **Free up space by applying default action on messages upon space overflow**.

  Do not select this option for all quarantines. The system must be able to make space by deleting messages from at least one quarantine.
- If you select **Release** as the default action, you can specify additional actions to apply to messages that are released before their retention period has passed:

Option	Information
Modify Subject	Type the text to add and specify whether to add it to the beginning or the end of the original message subject. For example, you might want to warn the recipient that the message may contain inappropriate content. **Note** In order for a subject with non-ASCII characters to display correctly it must be represented according to RFC 2047.
Add X-Header	An X-Header can provide a record of actions taken on a message. This can be helpful for example when handling inquiries about why a particular message was delivered. Enter a name and value. Example: Name = Inappropriate-release-early Value = True
Strip Attachments	Stripping attachments protects against viruses that may be in such files.

Step 4 Specify the users who can access this quarantine:

User	Information
Local Users	The list of local users includes only users with roles that can access quarantines. The list excludes users with Administrator privileges, because all Administrators have full access to quarantines.
Externally Authenticated Users	You must have configured external authentication.
Custom User Roles	You see this option only if you have created at least one custom user role with quarantine access.

Step 5 Submit and commit your changes.

What to do next

See Message Filters and Content Filters Page

- If you have not yet migrated quarantines from the Email Security appliance:

  You will assign these quarantines to message and content filters and DLP message actions as part of the migration process.

- If you have already migrated to centralized quarantines:

  Make sure your Email Security appliance has message and content filters and DLP message actions that will move messages to the quarantine. See the user guide or online help for the Email Security appliance.

About Editing Policy, Virus, and Outbreak Quarantine Settings

Note

- You cannot rename a quarantine.
- See also Retention Time for Messages in Quarantines , on page 11.

To change quarantine settings, choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines , and then click the name of a quarantine.

Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned

You can view the message filters, content filters, Data Loss Prevention (DLP) message actions, and DMARC verification profiles that are associated with a policy quarantine, and the Email Security appliance on which each is configured.

Step 1 Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**.

Step 2 Click the name of the policy quarantine to check.

Step 3 Scroll to the bottom of the page and view the **Associated Message Filters/Content Filters/DLP Message Actions**.

About Deleting Policy Quarantines

- Before you delete a policy quarantine, see if it is associated with any active filters or message actions. See Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned , on page 14.
- You can delete a policy quarantine even if it is assigned to a filter or message action.
- If you delete a quarantine that is not empty, the default action defined in the quarantine will be applied to all messages, even if you have selected the option not to delete messages if the disk is full. See Default Actions for Automatically Processed Quarantined Messages , on page 12.
- After you delete the quarantine associated with a filter or message action, any messages subsequently quarantined by that filter or message action will be sent to the Unclassified quarantine. You should customize the default settings of the Unclassified quarantine before you delete quarantines.
- You cannot delete the Unclassified quarantine.

Monitoring Quarantine Status, Capacity, and Activity

To View	Do This
Total space allocated for all non-spam quarantines	Choose **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines** and look in the first section on the page. To change allocations, see Managing Disk Space .
Currently available space for all non-spam quarantines	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** and look just below the table.
Total amount of space currently used by all quarantines	Choose **Management Appliance > Centralized Services > System Status**.
Amount of space currently used by each quarantine	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**, click the quarantine name, and look for this information in the table row directly below the quarantine name.
Total number of messages currently in all quarantines	Choose **Management Appliance > Centralized Services > System Status**.
Number of messages currently in each quarantine	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** and look at the table row for the quarantine.
Total CPU usage by all quarantines	Choose **Management Appliance > Centralized Services > System Status** and look in the System Information section.
Date and time when the last message entered each quarantine (excluding moves between policy quarantines)	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** and look at the table row for the quarantine.

To View	Do This
Date a policy quarantine was created	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**, click the quarantine name, and look for this information in the table row directly below the quarantine name. Creation date and creator name are not available for system-created quarantines.
Name of policy quarantine creator	
Filters and message actions associated with a policy quarantine	See Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned , on page 14.

Alerts About Quarantine Disk-Space Usage

An alert is sent whenever the total size of the policy, virus, and outbreak quarantine reaches or passes 75 percent, 85 percent, and 95 percent of its capacity. The check is performed when a message is placed in the quarantine. For example, if adding a message to a quarantine increases the size to or past 75 percent of the total capacity, an alert is sent.

For more information about Alerts, see Managing Alerts.

Policy Quarantines and Logging

AsyncOS individually logs all messages that are quarantined:

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

The message filter or Outbreak Filters feature rule that caused the message to be quarantined is placed in parentheses. A separate log entry is generated for each quarantine in which the message is placed.

AsyncOS also individually logs messages that are removed from quarantine:

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

The system individually logs messages after they are removed from all quarantines and either permanently deleted or scheduled for delivery, for example

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

When a message is re-injected, the system creates a new Message object with a new Message ID (MID). This is logged using an existing log message with a new MID “byline”, for example:

Info: MID 483 rewritten to 513 by Policy Quarantine

About Distributing Message Processing Tasks to Other Users

You can distribute message review and processing tasks to other administrative users. For example:

- The Human Resources team can review and manage the Policy Quarantine.
- The Legal team can manage the Confidential Material Quarantine.

You assign access privileges to these users when you specify settings for a quarantine. In order to add users to quarantines, the users must already exist.

Each user may have access to all, some, or none of the quarantines. A user who is not authorized to view a quarantine will not see any indication of its existence anywhere in the GUI or CLI listings of quarantines.

Related Topics

- Which User Groups Can Access Policy, Virus, and Outbreak Quarantines , on page 17
- Distributing Administrative Tasks

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

When you allow administrative users to access a quarantine, the actions that they can perform depend on their user group:

- Users in the Administrators or Email Administrators groups can create, configure, delete, and centralize quarantines and can manage quarantined messages.
- Users in the Operators, Guests, Read-Only Operators, and Help Desk Users groups, as well as custom user roles with quarantine management privileges, can search for, view, and process messages in a quarantine, but cannot change the quarantine's settings, create, delete, or centralize quarantines. You specify in each quarantine which of these users have access to that quarantine.
- Users in the Technicians group cannot access quarantines.

Access privileges for related features, such as Message Tracking and Data Loss Prevention, also affect the options and information that an administrative user sees on Quarantine pages. For example, if a user does not have access to Message Tracking, that user will not see message trackinginformation for quarantined messages.

Note: To allow custom user roles configured on the Security Management appliance to specify policy quarantines in filters and DLP message actions, see Configuring Centralized Quarantine Access for Custom User Roles , on page 9.

End users do not have see or have access to policy, virus, and outbreak quarantines.

Working with Messages in Policy, Virus, or Outbreak Quarantines

Related Topics

- Viewing Messages in Quarantines , on page 18
- Finding Messages in Policy, Virus, and Outbreak Quarantines , on page 18
- Manually Processing Messages in a Quarantine, on page 19
- Messages in Multiple Quarantines , on page 20
- Message Details and Viewing Message Content, on page 21
- About Rescanning of Quarantined Messages , on page 23
- The Outbreak Quarantine, on page 23

Viewing Messages in Quarantines

To	Do This
View all messages in a quarantine	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**. In the row for the relevant quarantine, click the blue number in the **Messages** column of the table.
View messages in the Outbreak quarantine	Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**. In the row for the relevant quarantine, click the blue number in the **Messages** column of the table. See Manage by Rule Summary Link, on page 24.
Navigate through the list of messages in a quarantine	Click Previous, Next, a page number, or double-arrow link. The double arrows take you to the first (<<) or last (>>) page in the listing.
Sort the list of messages in a quarantine	Click a column heading (except columns that could include multiple items or the “In other quarantines” column).
Resize table columns	Drag the divider between column headings.
View the content that caused the message to be quarantined	See Viewing Matched Content , on page 21.

Related Topics

- Quarantined Messages and International Character Sets, on page 18

Quarantined Messages and International Character Sets

For messages with subjects that contain characters from international character sets (double-byte, variable length, and non-ASCII encoded), the Policy Quarantine pages display subject lines in non-ASCII characters in their decoded form.

Finding Messages in Policy, Virus, and Outbreak Quarantines

Note

- Users can find and see only the messages in quarantines to which they have access.
- Searches in Policy, Virus, and Outbreak quarantines do not find messages in the spam quarantine.

Step 1 Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**.

Step 2 Click the **Search Across Quarantines** button.

Tip For the Outbreak Quarantine, you can also find all messages quarantined by each outbreak rule: Click the **Manage by Rule Summary** link in the Outbreak table row, and then click the relevant rule.

Step 3 (Optional) Enter other search criteria.

- For Envelope Sender and Envelope Recipient: You can enter any character(s). No validation of your entry is performed.
- Search results include only messages that match *all* of the criteria you specify. For example, if you specify an Envelope Recipient and a Subject, only messages that match the terms specified in both the Envelope Recipient *and* the Subject are returned.

What to do next

You can use the search results in the same way that you use the quarantine listings. For more information, see Manually Processing Messages in a Quarantine, on page 19.

Manually Processing Messages in a Quarantine

Manually processing messages means to manually select a Message Action for the message from the Message Actions page.

You can perform the following actions on messages:

- Delete
- Release
- Delay Scheduled Exit from quarantine
- Send a Copy of messages to email addresses that you specify
- Move a message from one quarantine to another

Generally, you can perform actions on messages in the lists that are displayed when you do the following. However, not all actions are available in all situations.

- From the list of quarantines on the **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** page or page, click the number of messages in a quarantine.
- Click **Search Across Quarantines**.
- Click a quarantine name and search within a quarantine.

You can perform these actions on multiple messages at one time by:

- Choosing an option from the pick list at the top of the list of messages.
- Selecting the check box beside each message listed on a page.
- Selecting the check box in the table heading at the top of a list of messages. This applies the action to all messages visible on the screen. Messages on other pages are not affected.

Additional options are available for messages in the outbreak quarantine. See information about the Manage by Rule Summary view in the chapter on Outbreak Filters in the online help or user guide for the *AsyncOS for Email Security Appliances*.

Related Topics

- Sending a Copy of the Message, on page 20
- About Moving Messages Between Policy Quarantines , on page 20
- Messages in Multiple Quarantines , on page 20
- Default Actions for Automatically Processed Quarantined Messages , on page 12

Sending a Copy of the Message

Only users who belong to the Administrators group may send copies of a message.

To send a copy of the message, enter an email address in the Send Copy To: field and click **Submit**. Sending a copy of a message does not cause any other action to be performed on the message.

About Moving Messages Between Policy Quarantines

You can manually move messages from one policy quarantine to another on a single appliance.

When you move a message to a different quarantine:

- The expiration time is unchanged. The message keeps the retention time of the original quarantine.
- The reason the message was quarantined, including the matched content and other relevant details, does not change.
- If a message is in multiple quarantines and you move the message to a destination that already holds a copy of that message, the expiration time and reason for quarantine of the moved copy of the message overwrite those of the copy of the message that was originally in the destination quarantine.

Messages in Multiple Quarantines

If a message is present in one or more other quarantines, the “In other quarantines” column in the quarantine message list will show “Yes,” regardless of whether you have permissions to access those other quarantines.

A message in multiple quarantines:

- Is not delivered unless it has been released from all of the quarantines in which it resides. If it is deleted from any quarantine, it will never be delivered.
- Is not deleted from any quarantine until it has been deleted or released from all quarantines in which it resides.

Because a user wanting to release a message may not have access to all of the quarantines in which it resides, the following rules apply:

- A message is not released from any quarantine until it has been released from all of the quarantines in which it resides.
- If a message is marked as Deleted in any quarantine, it cannot be delivered from any other quarantine in which it resides. (It can still be released.)

If a message is queued in multiple quarantines and a user does not have access to one or more of the other quarantines:

- The user will be informed whether the message is present in each of the quarantines to which the user has access.
- The GUI shows only the scheduled exit time from the quarantines to which the user has access. (For a given message, there is a separate exit time for each quarantine.)
- The user will not be told the names of the other quarantine(s) holding the message.
- The user will not see matched content that caused the message to be placed into quarantines that the user does not have access to.
- Releasing a message affects only the queues to which the user has access.
- If the message is also queued in other quarantines not accessible to the user, the message will remain in quarantine, unchanged, until acted upon by users who have the required access to the remaining quarantines (or until the message is released "normally" via early or normal expiration).

Message Details and Viewing Message Content

Click on the subject line of a message to view that message's content and to access the Quarantined Message page.

The Quarantined Message page has two sections: Quarantine Details and Message Details.

From the Quarantined Message page, you can read the message, select a Message Action, or send a copy of the message. You can also see if a message will be encrypted upon release from the quarantine due to the Encrypt on Delivery filter action.

The Message Details section displays the message body, message headers, and attachments. Only the first 100 K of the message body is displayed. If the message is longer, the first 100 K is shown, followed by an ellipsis (...). The actual message is not truncated. This is for display purposes only. You can download the message body by clicking [message body] in the Message Parts section at the bottom of Message Details. You can also download any of the message's attachments by clicking the attachment's filename.

If you view a message that contains a virus and you have desktop anti-virus software installed on your computer, your anti-virus software may complain that it has found a virus. This is not a threat to your computer and can be safely ignored.

To view additional details about the message, click the **Message Tracking** link.

Note For the special Outbreak quarantine, additional functionality is available. See The Outbreak Quarantine, on page 23.

Related Topics

- Viewing Matched Content , on page 21
- Downloading Attachments , on page 22

Viewing Matched Content

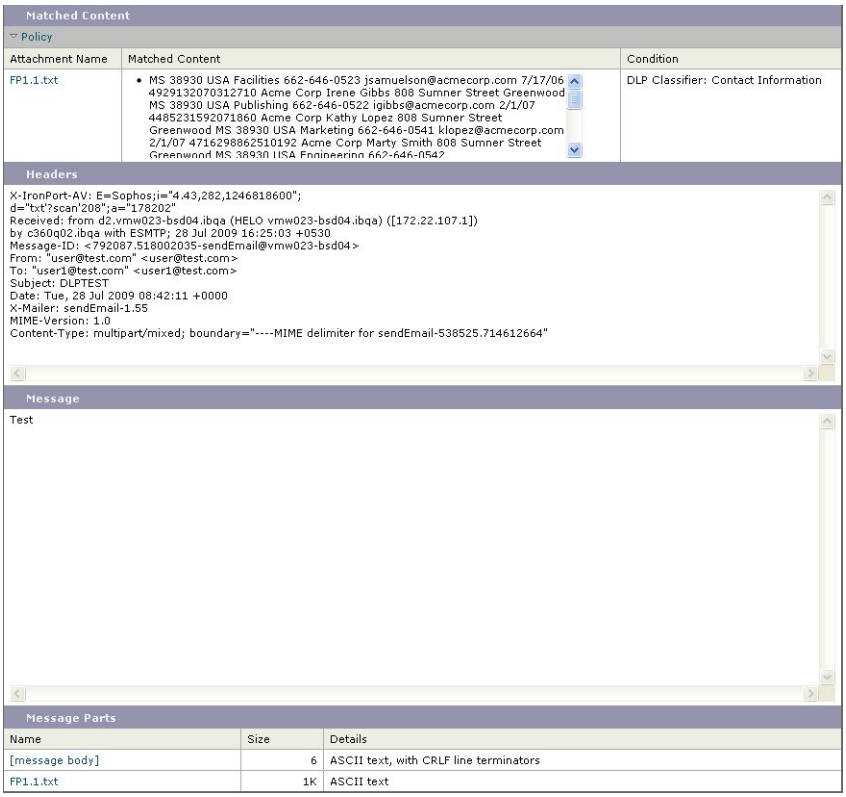
When you configure a quarantine action for messages that match Attachment Content conditions, Message Body or Attachment conditions, Message body conditions, or the Attachment content conditions, you can view the matched content in the quarantined message. When you display the message body, the matched

content is highlighted in yellow, except for DLP policy violation matches. You can also use the $MatchedContent action variable to include the matched content from message or content filter matches in the message subject.

If the attachment contains the matched content, the attachment's contents are displayed, as well as the reason it was quarantined, whether it was due to a DLP policy violation, content filter condition, message filter condition, or Image Analysis verdict.

When you view messages in the local quarantine that have triggered message or content filter rules, the GUI may display content that did not actually trigger the filter action (along with content that triggered the filter action). The GUI display should be used as a guideline for locating content matches, but does not necessarily reflect an exact list of content matches. This occurs because the GUI uses less strict content matching logic than is used in the filters. This issue applies only to the highlighting in the message body. The table that lists the matched strings in each part of the message, along with the associated filter rule, is correct.

Figure 1: Matched Content Viewed in the Policy Quarantine



Downloading Attachments

You can download a message attachment by clicking the attachment's file name in the Message Parts or Matched Content section. AsyncOS displays a warning that attachments from unknown sources may contain viruses and asks you if you want to continue. Download attachments that may contain viruses at your own risk. You can also download the message body by clicking [message body] in the Message Parts section.

About Rescanning of Quarantined Messages

When a message is released from all queues in which is has been quarantined, the following rescanning occurs, depending on the features enabled for the appliance and for the mail policy that originally quarantined the message:

- Messages released from Policy and Virus quarantines are rescanned by the anti-virus engine.
- Messages released from the Outbreak quarantine are rescanned by the anti-spam and anti-virus engines. (For information about rescanning of messages while in the Outbreak quarantine, see Outbreak Filters Page the chapter on Outbreak Filters in the online help or user guide for the Email Security appliance.)
- Messages released from the File Analysis quarantine are rescanned for threats.
- Messages with attachments are rescanned by the file reputation service upon release from Policy, Virus, and Outbreak quarantines.

Upon rescanning, if the verdict produced matches the verdict produced the previous time the message was processed, the message is not re-quarantined. Conversely, if the verdict is different, the message could be sent to another quarantine.

The rationale is to prevent messages from looping back to the quarantine indefinitely. For example, suppose a message is encrypted and therefore sent to the Virus quarantine. If an administrator releases the message, the anti-virus engine will still not be able to decrypt it; however, the message should not be re-quarantined or a loop will be created and the message will never be released from the quarantine. Since the two verdicts are the same, the system bypasses the Virus quarantine the second time.

The Outbreak Quarantine

The Outbreak quarantine is present when a valid Outbreak Filters feature license key has been entered. The Outbreak Filters feature sends messages to the Outbreak quarantine, depending on the threshold set. For more information, see the Outbreak Filters chapter in the online help or user guide for the Email Security appliance.

The Outbreak quarantine functions just like other quarantines—you can search for messages, release or delete messages, and so on.

- Standard
- Rule Summary

The Outbreak quarantine has some additional features not available in other quarantines: the Manage by Rule Summary link, the Send to Cisco feature when viewing message details, and the option to sort messages in search results by the Scheduled Exit time.

If the license for the Outbreak Filters feature expires, you will be unable to add more messages to the Outbreak quarantine. Once the messages currently in the quarantine have expired and the Outbreak quarantine becomes empty, it is no longer shown in the Quarantines listing in the GUI.

Related Topics

- Rescanning Messages in an Outbreak Quarantine , on page 24
- Manage by Rule Summary Link, on page 24
- Reporting False Positives or Suspicious Messages to Cisco Systems, on page 24

Rescanning Messages in an Outbreak Quarantine

Messages placed in the Outbreak quarantine are automatically released if newly published rules deem the quarantined message no longer a threat.

If anti-spam and anti-virus are enabled on the appliance, the scanning engines scan every message released from the Outbreak quarantine based on the mail flow policy that applies to the message.

Manage by Rule Summary Link

Click the Manage by Rule Summary link next to the Outbreak quarantine in the quarantine listing to view the Manage by Rule Summary page. You can perform message actions (Release, Delete, Delay Exit) on all of the messages in the quarantine based on which outbreak rule caused the message to be quarantined. This is ideal for clearing out large numbers of messages from the Outbreak quarantine. For more information, see information about the Manage by Rule Summary view in the Outbreak Filters chapter in the online help or user guide for the Email Security appliance

Reporting False Positives or Suspicious Messages to Cisco Systems

When viewing message details for a message in the Outbreak quarantine, you can send the message to Cisco to report false positives or suspicious messages.

Step 1 Navigate to a message in the Outbreak quarantine.

Step 2 In the Message Details section, select the **Send a Copy to Cisco Systems** check box.

Step 3 Click **Send**.

Troubleshooting Centralized Policy Quarantines

- Administrative User Cannot Choose Quarantines in Filters and DLP Message Actions, on page 24
- Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned , on page 25

Administrative User Cannot Choose Quarantines in Filters and DLP Message Actions

Problem

Administrative users cannot see or choose quarantines in content and message filters or DLP actions on the Email Security appliance.

Solution

See Configuring Centralized Quarantine Access for Custom User Roles , on page 9

Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned

Problem

Messages released from the Outbreak Quarantine should be scanned again before delivery. However, some contaminated messages have been delivered from the quarantine.

Solution

This can occur under the situation described in About Rescanning of Quarantined Messages , on page 23