Monitoring System Status

This chapter contains the following sections:

- About Security Management Appliance Status, on page 1
- Monitoring Service Status on the New Web Interface of the Appliance, on page 2
- Monitoring Security Management Appliance Capacity , on page 3
- Monitoring Status of Data Transfer From Managed Appliances , on page 4
- Viewing the Configuration Status of Your Managed Appliances, on page 5
- Monitoring Reporting Data Availability Status, on page 6
- Monitoring Email Tracking Data Status, on page 7
- Monitoring Capacity of Managed Appliances , on page 7
- Identifying Active TCP/IP Services , on page 7
- Replacing a Managed Appliance During Hardware Failure, on page 7

About Security Management Appliance Status

By default, the System Status page is the first page that appears when you access the Cisco Secure Email and Web Managerappliance from your browser. (To change the landing page, see Setting Preferences.)

To access the System Status page at any other time, select **Management Appliance > Centralized Services > System Status**.

Before you enable monitoring services and add a managed appliance, only the System Information section provides status information. If you have run the System Setup Wizard, enabled centralized services, and added managed appliances, the Centralized Services section and the Security Appliance Data Transfer Status section are populated with data.

Status information includes the following:

- **Centralized Services:**Status of each centralized service, including Processing Queue usage
- **System Uptime:** How long the appliance has been running
- **CPU Utilization:** Percentage of CPU capacity used by each monitoring service
- **System Version Information:** Model number, AsyncOS (operating system) version, build date, installation date, and serial number

Related Topics

- Monitoring the Processing Queue , on page 3
- Monitoring CPU Utilization , on page 3
- Monitoring Status of Data Transfer From Managed Appliances , on page 4

Monitoring Service Status on the New Web Interface of the Appliance

You can now monitor the status of your managed appliances and manage centralized services on the new web interface of your Secure Email and Web Manager appliance.

You can use the **Service Status** tab on the new web interface of your appliance to enable and disable centralized services such as email reporting, message tracking and quarantines.

The **Email Feature Status** section shows the services that are enabled and the number of licenses you have used for each service. Click **View Appliances** to view the number of added appliances. This redirects you to the legacy web interface of the appliance. For more information, see About Adding Managed Appliances

You can view the File Analysis details on the Service Status page of the new web interface of your appliance. You must join all managed appliances to the same appliance group in order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization.

You can enable and disable the following centralized services on the Service Status page:

- Centralized Reporting

  For more information, see Enabling Centralized Email Reporting on the New Web Interface.

- Centralized Message Tracking

  For more information, see Enabling Centralized Email Tracking on the New Web Interface.

- Centralized Spam Quarantines

  For more information, see the following:

  - Enabling and Configuring Spam Quarantine on the New Web Interface.
  - Notifying End Users About Quarantined Messages.
  - Configuring End-User Access to the Spam Quarantine.
  - Enabling Safelists and Blocklists on the New Web Interface.

- Centralized Policy, Virus and Outbreak Quarantines

  For more information, see Enabling Centralized Policy, Virus, and Outbreak Quarantines on the New Web Interface of the Appliance.

- Safelists and Blocklists

  For more information, see Enabling Safelists and Blocklists on the New Web Interface.

Monitoring Security Management Appliance Capacity

• Monitoring the Processing Queue , on page 3
• Monitoring CPU Utilization , on page 3

Monitoring the Processing Queue

You can periodically check the processing queue percentages used for email and web reporting and tracking to determine whether your appliance is running at optimal capacity.

The processing queue stores centralized reporting and tracking files as they await processing by the Security Management appliance. Normally, the Security Management appliance receives batches of reporting and tracking files for processing. The percentage of reporting or tracking files in the processing queue typically fluctuates as the files are transmitted from managed appliances and processed by the Security Management appliance.

Note Processing queue percentages gauge the number of files in the queue. They do not take file size into account. The percentages provide only a rough estimate of the Security Management appliance's processing load.

Step 1 [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.

Step 2 On the Security Management appliance, choose **Management Appliance > Centralized Services > System Status**.

Step 3 In the **Centralized Services** section at the top of the page, look at the Processing Queue percentages for:

a) Centralized Reporting (Email Security subsection)
b) Centralized Message Tracking
c) Centralized Reporting (Web Security subsection)

Step 4 If the processing queue usage percentages remain consistently high over several hours or days, then the system is running at or beyond capacity.

In that case, consider removing some of the managed appliances from the Security Management appliance, installing additional Security Management appliances, or both.

Monitoring CPU Utilization

To view the percentage of its CPU capacity that the Security Management appliance is using for each centralized service:

Step 1 [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.

Step 2 Select **Management Appliance > Centralized Services > System Status**.

Step 3 Scroll to the **System Information** section and view the **CPU Utilization** subsection.

The CPU Utilization percentages indicate the portion of the Security Management appliance's CPU processing that is devoted to each of the main centralized services. Utilization percentages for some services may be combined. For example, email reporting are combined under "Reporting Service" while spam, policy, virus, and outbreak quarantines are combined under "Quarantine Services." Other operations of the Security Management appliance are grouped under the general heading "Security Management appliance."

Step 4 Refresh the browser display to view the most recent data.

The CPU utilization percentages change constantly.

Monitoring Status of Data Transfer From Managed Appliances

To perform centralized management functions, the Security Management appliance relies on the successful transfer of data from the managed appliances to the Security Management appliance. The Security Appliance Data Transfer Status section provides status information about each appliance that is managed by the Security Management appliance.

By default, the Security Appliance Data Transfer Status section displays up to ten appliances. If the Security Management appliance manages more than ten appliances, you can use the Items Displayed menu to select the number of appliances to display.

Note Summary information about data transfer status appears in the Services section at the top of the System Status page. The Security Appliance Data Transfer Status section provides appliance-specific data transfer status.

In the Security Appliance Data Transfer Status section of the System Status page, you can view connection status issues for specific appliances. For detailed information about the status of each service on an appliance, click the appliance name to view the Data Transfer Status page for the appliance.

The Data Transfer Status: *Appliance_Name* page shows when the last data transfer occurred for each monitoring service.

The data transfer status for Email Security appliances can be one of the following values:

- **Not enabled:**The monitoring service is not enabled on the Email Security appliance.
- **Never connected:** The monitoring service is enabled on the Email Security appliance, but no connection has been established between the Email Security appliance and the Security Management appliance.
- **Waiting for data:** The Email Security appliance has connected to the Security Management appliance, which is waiting to receive data.
- **Connected and transferred data:**A connection was established between the Email Security appliance and the Security Management appliance, and data were successfully transferred.
- **File transfer failure:** A connection was established between the Email Security appliance and the Security Management appliance, but the data transfer failed.

The data transfer status for Web Security appliances can be one of the following values:

- **Not enabled:** The centralized configuration manager is not enabled for the Web Security appliance.

- **Never connected:** The centralized configuration manager is enabled for the Web Security appliance, but no connection has been established between the Web Security appliance and the Security Management appliance.
- **Waiting for data:** The Web Security appliance has connected to the Security Management appliance, which is waiting to receive data.
- **Connected and transferred data:** A connection was established between the Web Security appliance and the Security Management appliance, and data were successfully transferred.
- **Configuration push failure:** The Security Management appliance attempted to push a configuration file to the Web Security appliance, but the transfer failed.
- Configuration push pending: The Security Management appliance is in the process of pushing a configuration file to the Web Security appliance.
- Configuration push success: The Security Management appliance successfully pushed a configuration file to the Web Security appliance.

Data transfer issues can reflect temporary network problems or appliance configuration issues. The statuses of "Never connected" and "Waiting for data" are normal, transient statuses when you first add a managed appliance to the Security Management appliance. If the status does not eventually change to "Connected and transferred data," then the data transfer status might indicate a configuration issue.

If the "File transfer failure" status appears for an appliance, monitor the appliance to determine if the failure was caused by a network issue or by a problem with the appliance configuration. If no network issues prevent data transfer and the status does not change to "Connected and transferred data," then you might need to change the appliance configuration to enable data transfer.

Viewing the Configuration Status of Your Managed Appliances

You can view the configuration status of your managed appliances in one of the following ways:

- [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.
- On the Security Management appliance, choose **Management Appliance > Centralized Services > System Status**.

The Centralized Service Status section shows which services are enabled and how many licenses you have used for each service. The Security Appliances section lists the appliances you have added. Check marks indicate the enabled services, and the Connection Established? column shows whether or not file transfer access is properly configured.

Related Topics

- Designating an Alternate Appliance to Process Released Messages
- About Adding Managed Appliances

Additional Status Information for Web Security Appliances

For additional status information about Web Security appliances, see Viewing Status of Individual Web Security Appliances.

Monitoring Reporting Data Availability Status

The Security Management appliance enables you to monitor the availability of reporting data for a specified time period. See the appropriate section for your appliance:

• Monitoring Email Security Reporting Data Availability, on page 6

Monitoring Email Security Reporting Data Availability

To monitor reporting data from your Email Security appliances on the Security Management appliance, view the **Email > Reporting > Reporting Data Availability** page.

From the **Reporting Data Availability** page, you can view the percentage of reporting data that the Security Management appliance received from your Email Security appliances over a specified period of time. A bar chart indicates the completeness of the data received during the time range.

You can monitor reporting data availability for the preceding day, week, month, or year. If the Security Management appliance received less than 100% of the reporting data from the Email Security appliances, you can tell immediately that your data may be incomplete. Use the data availability information to validate reporting data and to troubleshoot system problems.

Monitoring Web Security Reporting Data Availability

To monitor reporting data from your Web Security appliances on the Security Management appliance, view the **Web > Reporting > Data Availability** page.

From the Data Availability page you can update and sort data to provide real-time visibility into resource utilization and web traffic trouble spots.

Note In the Web Reporting Data Availability window, Web Reporting will show disabled only if **both** Web Reporting and Email Reporting are disabled.

All data resource utilization and web traffic trouble spots are shown from this page. By clicking on one of the listed Web Security appliance links, you can view reporting data availability for that appliance.

You can monitor reporting data availability for the preceding day, week, month, or year. If the Security Management appliance received less than 100% of the reporting data from the Web Security appliances, you can tell immediately that your data may be incomplete. Use the data availability information to validate reporting data and to troubleshoot system problems.

If data availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: “Some data in this time range was unavailable.” If there are no gaps present, nothing appears.

See the Data Availability Page for more information on the Data Availability page on the Web Security appliance.

Monitoring Email Tracking Data Status

To monitor the status of email tracking data, view the **Email > Message Tracking > Message Tracking Data Availability** page.

Monitoring Capacity of Managed Appliances

You can monitor capacity of your managed appliances from the Security Management appliance. You can check the collective capacity of all Email or Web Security appliances and the capacity of each individual appliance.

To View Capacity of	See
Managed Web Security appliances	System Capacity Page
Managed Email Security appliances	System Capacity Page

Identifying Active TCP/IP Services

To identify active TCP/IP services used by your Security Management appliance, use the tcpservices command in the command line interface.

Replacing a Managed Appliance During Hardware Failure

If you have to replace a managed appliance due to a hardware failure or other reasons, the data from the replaced appliance will not be lost, but the data will not be displayed correctly on the Security Management appliance.

Upon replacing a managed appliance, add the new appliance to the list of hosts on the SMA, and connect it to the new appliance. If the IP address remains the same, change the IP on the old host entry to a non existing value.