Troubleshooting

This chapter contains the following sections:

- Collecting System Information , on page 1
- Troubleshooting Hardware Issues , on page 1
- Troubleshooting Feature Setup Issues , on page 1
- General Troubleshooting Resources , on page 2
- Troubleshooting Issues with Specific Functionality , on page 2
- Working with Technical Support, on page 3
- Running a Packet Capture, on page 7
- Remotely Resetting Appliance Power , on page 8

Collecting System Information

You can get information about your appliance and its status, including your serial number. Refer Monitoring System Status

Troubleshooting Hardware Issues

Lights on the front and/or rear panels of your hardware appliance indicate health and status of your appliance. For descriptions of these indicators, see the hardware guides such as the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide* available from the location specified in.

Specifications for your appliance, such as temperature ranges, are also available in these documents.

Note If you need to cycle power to your x80 or x90 appliance, wait at least 20 minutes for the appliance to come up (all LEDs are green) before pushing the power button.

Troubleshooting Feature Setup Issues

If you are experiencing difficulty configuring a feature successfully, see the summaries of the tasks you must complete for each feature. These include links to specific information for each.

- Setting Up Centralized Web Reporting and Tracking
- Setting Up Centralized Email Reporting
- Setting Up Centralized Message Tracking
- Setting Up the Centralized Spam Quarantine
- Centralized Policy, Virus, and Outbreak Quarantines
- Using Configuration Masters to Centrally Manage Web Security Appliances

General Troubleshooting Resources

General troubleshooting resources include:

- Recent alerts. See Viewing Recent Alerts.
- Log files. SeeLogging
- The Release Notes, including the Documentation Updates section. SeeDocumentation.
- The Cisco Bug Search Tool (instructions for access are in the Release Notes)
- Knowledge Base Articles (TechNotes)
- TheCisco Support Community

Troubleshooting Issues with Specific Functionality

See alsoTroubleshooting Feature Setup Issues , on page 1.

Web Security-Related Issues

- Troubleshooting All Reports
- Troubleshooting Web Reporting and Tracking
- Troubleshooting Configuration Management Issues
- Feature-related issues may also result from settings on your Web Security appliances. See the release notes and online help or user guide for your release at the location specified inDocumentation.

Email Security-Related Issues

- Troubleshooting All Reports
- Troubleshooting Message Tracking
- Troubleshooting Spam Quarantine Features
- Troubleshooting Centralized Policy Quarantines
- Feature-related issues may also result from settings on your Email Security appliances. See the release notes and online help or user guide for your release at the location specified inDocumentation.

General Issues

- If you are unable to load a configuration file, make sure your disk space quotas are larger than the current size of each function in the table on the **Management Appliance > System Administration > Disk Management** page.
- If you have recently upgraded and the online help appears to be outdated or you cannot find the information about a new feature, clear your browser cache and then reopen the browser window.
- Unexpected behavior can occur when configuring settings using the web interface if you are using multiple browser windows or tabs simultaneously.
- SeeResponding to Alerts , on page 3.
- SeeTroubleshooting Administrative User Access.

Responding to Alerts

- Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware, on page 3
- Additional Alert Descriptions , on page 3

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

Problem: You receive an alert with subject “Battery Relearn Timed Out” for 380 or 680 hardware.

Solution: This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-related alerts from the system, then you can safely ignore this alert.

Additional Alert Descriptions

For descriptions of additional alerts, see

- Hardware Alert Descriptions
- System Alert Descriptions

What to do next

- Managing Alerts

Working with Technical Support

- Opening or Updating a Support Case from the Appliance , on page 3
- Getting Support for Virtual Appliances , on page 4
- Enabling Remote Access for Cisco Technical Support Personnel , on page 4

Opening or Updating a Support Case from the Appliance

You can use this method to contact Cisco TAC or your own support services.

Before you begin

If you wish to contact Cisco TAC:

- If your issue is urgent, do not use this method. Instead, contact support using one of the other methods listed in Customer Support.
- Consider other options for getting help:
- When you open a support case using this procedure, the appliance configuration file is sent to Cisco Customer Support. If you do not want to send the appliance configuration, you can contact Customer Support using a different method.
- The appliance must be connected to the internet and able to send email.
- If you are sending information about an existing case, make sure you have the case number.

Procedure

Step 1 Log in to the appliance.

Step 2 Choose **Help and Support > Contact Technical Support**.

Step 3 Determine the recipients of the support request:

To send the request to Cisco TAC	Select the **Cisco Technical Support** check box.
To send the request only to your internal support desk	• Deselect the **Cisco Technical Support** check box. • Enter the email address of your support desk.
(Optional) To include other recipients	Enter email addresses.

Step 4 Complete the form.

Step 5 Click **Send**.

Getting Support for Virtual Appliances

If you file a support case for a Cisco content security virtual appliance, you must provide your Virtual License Number (VLN), your contract number, and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following table:

Functionality	PID	Description
All centralized web security functionality	SMA-WMGT-LIC=	—
All centralized email security functionality	SMA-EMGT-LIC=	

Enabling Remote Access for Cisco Technical Support Personnel

Only Cisco Customer Assistance can access your appliance using these methods.

• Enabling Remote Access for Cisco Technical Support Personnel , on page 4
• Enabling Remote Access to Appliances Without a Direct Internet Connection , on page 5
• Disabling a Tech Support Tunnel , on page 6
• Disabling Remote Access , on page 6
• Checking the Status of the Support Connection , on page 6

Enabling Remote Access to Appliances With an Internet Connection

Support accesses the appliance through an SSH tunnel that this procedure creates between the appliance and the upgrades.ironport.com server.

Before you begin

Identify a port that can be reached from the internet. The default is port25 which will work in most environment . Connections over this port are allowed in most firewall configurations.

Procedure

Step 1 Log in to the appliance.
Step 2 From the top right side of the GUI window, choose **Help and Support > Remote Access**.
Step 3 Click **Enable**.
Step 4 Enter information.
Step 5 Click **Submit**.

What to do next

When remote access for support personnel is no longer required, seeDisabling a Tech Support Tunnel , on page 6.

Enabling Remote Access to Appliances Without a Direct Internet Connection

For appliances without a direct internet connection, access is made through a second appliance that is connected to the internet.

Before you begin

- The appliance must be able to connect on port 22 to a second appliance that is connected to the internet.
- On the appliance with the internet connection, follow the procedure inEnabling Remote Access to Appliances With an Internet Connection , on page 5 to create a support tunnel to that appliance.

Procedure

Step 1 From the command-line interface of the appliance requiring support, enter the `techsupport` command.
Step 2 Enter `sshaccess` .

Step 3 Follow the prompts.

What to do next

When remote access for support personnel is no longer required, see the following:

- Disabling Remote Access , on page 6
- Disabling a Tech Support Tunnel , on page 6

Disabling a Tech Support Tunnel

An enabled techsupport tunnel remains connected to upgrades.ironport.com for 7 days. After that time, established connections will not be disconnected but will be unable to re-attach to the tunnel once disconnected.

Procedure

Step 1 Log in to the appliance.

Step 2 From the top right side of the GUI window, choose **Help and Support > Remote Access**.

Step 3 Click **Disable**.

Disabling Remote Access

A remote access account that you create using the techsupport command remains active until you deactivate it.

Procedure

Step 1 From the command-line interface, enter the `techsupport` command.

Step 2 Enter `sshaccess` .

Step 3 Enter `disable` .

Checking the Status of the Support Connection

Procedure

Step 1 From the command-line interface, enter the `techsupport` command.

Step 2 Enter status .

Running a Packet Capture

Packet Capture allows support personnel to see the TCP/IP data and other packets going into and out of the appliance. This allows Support to debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance.

Procedure

Step 1 Choose **Help and Support > Packet Capture**.

Step 2 Specify packet capture settings:

a) In the **Packet Capture Settings** section, click **Edit Settings**.

b) (Optional) Enter duration, limits, and filters for the packet capture.

Your Support representative may give you guidance on these settings.

If you enter a capture duration without specifying a unit of time, AsyncOS uses seconds by default.

In the Filters section:

- Custom filters can use any syntax supported by the Unix `tcpdump` command, such as host 10.10.10.10 && port 80 .
- The client IP is the IP address of the machine connecting to the appliance, such as a mail client sending messages through the Email Security appliance.
- The server IP is the IP address of the machine to which the appliance is connecting, such as an Exchange server to which the appliance is delivering messages.

You can use the client and server IP addresses to track traffic between a specific client and a specific server, with the Email Security appliance in the middle.

c) Click **Submit**.

Step 3 Click **Start Capture**.

- Only one capture may be running at a time.
- When a packet capture is running, the Packet Capture page shows the status of the capture in progress by showing the current statistics, such as file size and time elapsed.
- The GUI only displays packet captures started in the GUI, not from the CLI. Similarly, the CLI only displays the status of a current packet capture run started in the CLI.
- The packet capture file is split into ten parts. If the file reaches the maximum size limit before the packet capture ends, the oldest part of the file is deleted (the data is discarded) and a new part starts with the current packet capture data. Only 1/10 of the packet capture file is discarded at a time.
- A running capture started in the GUI is preserved between sessions. (A running capture started in the CLI stops when the session ends.)

Step 4 Allow the capture to run for the specified duration, or, if you have let the capture run indefinitely, manually stop the capture by clicking **Stop Capture**.

Step 5 Access the packet capture file:

- Click the file in the **Manage Packet Capture Files** list and click **Download File**.

- Use FTP or SCP to access the file in the captures subdirectory on the appliance.

What to do next

Make the file available to Support:

- If you allow remote access to your appliance, technicians can access the packet capture files using FTP or SCP. SeeEnabling Remote Access for Cisco Technical Support Personnel , on page 4.
- Email the file to Support.

Remotely Resetting Appliance Power

If the appliance requires a hard reset, you can reboot the appliance chassis remotely using a third-party Intelligent Platform Management Interface (IPMI) tool.

Restrictions

- Remote power cycling is available only on certain hardware.

  For specifics, seeEnabling Remote Power Cycling.

- If you want be able to use this feature, you must enable it in advance.

  For details, seeEnabling Remote Power Cycling.

- Only the following IPMI commands are supported:

  ```
  status, on, off, cycle, reset, diag, soft
  ```

  Issuing unsupported commands will produce an “insufficient privileges” error.

Before you begin

- Obtain and set up a utility that can manage devices using IPMI version 2.0.
- Understand how to use the supported IPMI commands. See the documentation for your IPMI tool.

Procedure

Step 1 Use IPMI to issue a supported power-cycling command to the IP address assigned to the Remote Power Cycle port, which you configured earlier, along with the required credentials.

For example, from a UNIX-type machine with IPMI support, you might issue the command:

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

where `192.0.2.1` is the IP address assigned to the Remote Power Cycle port and remoteresetuser and passphrase are the credentials that you entered while enabling this feature.

Step 2 Wait at least eleven minutes for the appliance to reboot.