



APPENDIX **B**

Troubleshooting

Revised: September 14, 2007, OL-14673-01

This appendix presents information that is helpful when troubleshooting the MARS Appliance. It lists expected services and error messages for each supported MARS Appliances. It explains how to collect and send support information to assist Cisco support in debugging such services are required. This appendix also provides guidance on retrieving lost license keys and running the web interface using a console connection. It includes the following topics:

- [Determine Version Information, page B-1](#)
- [Cannot Locate License Key, page B-2](#)
- [Cannot Recovery My Password, page B-2](#)
- [Cannot Delete a Device from MARS, page B-2](#)
- [Cannot Re-Add a Device to MARS, page B-2](#)
- [Cannot Add a Device to MARS, page B-2](#)
- [Cannot Rename Device in MARS, page B-2](#)
- [Collect Support Information, page B-2](#)
- [Access the GUI when the Network Is Down, page B-5](#)
- [Troubleshooting Global Controller-to-Local Controller Communications, page B-5](#)
- [List of Backend Services and Processes, page B-11](#)
- [Error Messages, page B-14](#)

Determine Version Information

Beginning with the 4.3.1 and 5.3.1 releases, the dynamic IPS signature updates is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail. To determine the version of MARS software and the IPS signature version, click **Help >About** on each appliance.

Cannot Locate License Key

For newer models of the MARS Appliance, the license key and serial numbers are both located on the exterior of the appliance. For information on locating the license key and serial number, see [Locating the License Key, page 1-7](#).

If you cannot locate your license key, contact the Cisco Licensing Team at licensing@cisco.com. You will need to provide the following information in the e-mail:

- Customer name
- Serial number of the MARS Appliance

Cannot Recovery My Password

See [Recovering a Lost Administrative Password, page 6-40](#).

Cannot Delete a Device from MARS

See [Delete a Device](#).

Cannot Re-Add a Device to MARS

If you cannot re-add a device to MARS, the device is likely already defined in one capacity or another. See [Delete a Device](#).

Cannot Add a Device to MARS

If you cannot add a device to MARS, the device has likely been defined during a topology discovery operation. You can address this issue by first deleting the device, and then adding it. See [Delete a Device](#).

Cannot Rename Device in MARS

You cannot directly rename a device. To do so you must first delete the device and then re-add it. See [Delete a Device](#).

Collect Support Information

As long as your appliance is running, you can provide Cisco support with log information that can assist in diagnosing any issues you are having with the appliance. Three options exist for collecting and sending this information:

- **Collect Summary Status from the MARS Database.** As of 4.3.1 and 5.3.1 releases, you can use the `get_mars_summary_info.sh` script to gather high-level statistics about a MARS Appliance's configuration and topology.

```
[pnadmin]$ script get_mars_summary_info.sh
Collecting MARS summary info from the DB in HTML format
Started at Fri Aug 24 11:08:58 PDT 2007
Use 'pnlog mailto' command to include it in the logs This may take several minutes to
complete. Use Ctrl+C in case you need to interrupt.
Completed at Fri Aug 24 11:10:20 PDT 2007 [pnadmin]$
```

After running the script, use the **pnlog mailto** command to e-mail the logs to yourself. You will see the files `get_mars_summary_info.html` and `get_mars_summary_info.run.log` in the log file named `error-logs.tar.gz` received with the other logs.

- From the CLI, you can use the **pnlog mailto** command. For more information on using this command, see [pnlog](#), page A-36.
- In the GUI, you can use the **Help > Feedback** option. For more information on using this option, see [Submitting Feedback and Reporting Errors](#), page B-3

Both options require that the appliance is connected to a network that can reach your SMTP server, and that the appliance is configured properly to send e-mail to that server. You can specify the e-mail gateway settings either on the Admin > System Setup > Configuration Information page or as an option the command line using the **pnlog mailto** command.

The **pnlog mailto** command packages and delivers the following information in a file named `error-logs.tar.gz`:

- C++ process logs
- System logs
- Java (GUI) logs
- Upgrade logs
- Current version
- Current model
- List of running processes

No passwords or network information is included in the `error-logs.tar.gz` file.

Submitting Feedback and Reporting Errors

If you receive an error in the web interface and the system recovers, a pink page appears allowing you to report the error to Cisco.



You can use either the Report Error button or the Feedback button that appears on every page to send feedback and error log files to the Cisco TAC. When you select the Feedback button, an e-mail message is sent to the e-mail address associated with the user account with which you are logged into the MARS web interface. You can forward this e-mail as needed. If you log in using an account that does not have an e-mail address associated with it, you will be prompted to enter an e-mail address.

The Report Error button allows you to send the error logs and information related to the triggering error. The error log facilitates debugging the error, and therefore it is the recommended option. However, this option requires that you provide a valid TAC case number to which the error log is attached.

TAC Case Number:

If this is a new case, please create a Cisco TAC Service Request by clicking here.


Email Log to TAC:

Message:

Please describe what actions produced the error:

190100

If you do not already have a valid case number, you are redirected to the Cisco TAC web site so you can create a new TAC case and obtain a valid case number.



[Logged In](#) | [Profile](#) | [Contacts & Feedback](#) | [Help](#) | [Site Map](#) | [Select a Location / Language](#)

HOME

TECHNICAL SUPPORT & DOCUMENTATION

TOOLS & RESOURCES

TAC Service Request Tool

Products & Services | [Ordering](#) | [Technical Support & Documentation](#) | [Learning & Events](#) | [Partners](#)

Tools & Resources

TAC Service Request Tool

Welcome to the TAC Service Request Tool.

The TAC Service Request Tool allows you to:

- Open severity 3 and 4 service requests and, after you describe your service request online, the tool recommends resources that may provide a solution immediately.
- Check the current status of open service requests
- Update open service requests with your own notes
- Attach files to open service requests
- View service requests closed within the last 18 months

If you have a severity 1 or 2 network-down emergency, open your service request by [telephone](#).

[Create a new TAC Service Request](#) [↗](#)

[Query a TAC Service Request](#) [↗](#)

190101

Access the GUI when the Network Is Down

While console connections enable you to perform basic network settings for an appliance, you must use the GUI to perform the majority of the configuration for the appliance. If you cannot connect to the appliance from hosts on your network, you can access the GUI using a computer by connecting a crossover cable to one of the Ethernet ports in the appliance.

To access the GUI using a console connection, follow these steps:

-
- Step 1** With the appliance running, connect a Cat 5 crossover cable to your computer's Ethernet port.
 - Step 2** Connect the Cat 5 crossover cable to the MARS Appliance's eth1 port. See [Hardware Descriptions—MARS 20, 20R, 50 200, GCm, and GC, page 1-4](#).
 - Step 3** Configure the computer's local TCP/IP settings to be on the same network as one of the Ethernet interfaces in the MARS Appliance. Pick an IP address other than the one used by the appliance on that interface.

It is possible that you specified the interface address for eth1 when you configured the interfaces using a console connection in [Specify the IP address and Default Gateway for the Eth0 Interface, page 5-7](#), and [Specify the IP Address and Default Gateway for the Eth1 Interface, page 5-8](#). However, the factory default setting for eth1 is 192.168.0.101.

**Tip**

You can use eth0 also; however, you must specify an address for your computer that works with the network settings that you specified in [Specify the IP address and Default Gateway for the Eth0 Interface, page 5-7](#).

Troubleshooting Global Controller-to-Local Controller Communications

The following sections provide information to assist in troubleshooting communications issues between a Global Controller and the Local Controllers it manages.

- [Communications Overview, page B-5](#)
- [Communication States, page B-6](#)
- [Required Open Ports, page B-6](#)
- [General Issues and Solutions, page B-7](#)

Communications Overview

A Global Controller and Local Controller can communicate if they are running on the same version of software. A version mismatch causes all communications to stop. For more information on configuring the communications, see [Configuring the Global Controller](#) of *User Guide for Cisco Security MARS Global Controller*.

When a Global Controller and Local Controller communicate, several types of data are synchronized:

- **Topology.** Topology configuration data includes the list of monitored devices, their interfaces, routes, and network groups. This data is sent from a Local Controller to the Global Controller every 30 seconds.
- **Configuration.** Configuration data includes custom parser definitions, event types, inspection rules, report definitions, and user accounts and roles that are defined on the Global Controller. This data is sent from the Global Controller to Local Controller every 30 seconds.
- **Report data.** Report result data is sent from a Local Controller to the Global Controller every 10 minutes. If a backlog exists on the Local Controller (for example, due to a communications failure), a block of report data is picked up 30 seconds after the previous block transmission completes until the backlog is clear.



Note For each schedule report (whether global or just a default system report), data is collected every 10 minutes and sent to the Global Controller, regardless of whether a report is scheduled within that interval.

- **Incident/firing event data.** This data is sent from the Local Controller to Global Controller every two minutes.

Communication States

When troubleshooting the communications, first verify that the Local Controller and Global Controller are communicating properly. From the web interface of the Global Controller, view the device state on the Admin > System Setup > Local Controller Information page. Understanding the communication state can assist you in diagnosing issues.

The key states to check for when troubleshooting communications issues are as follows:

- **Active.** This state indicates that communications are operational. If you made a recent change, wait a minute for the system to process the change and then re-visit the page to obtain the updated state.



Note After adding a new Local Controller, the page briefly indicates the Active state even though you have not added the certificates. Re-visit the page to obtain the correct state.

- **Certificate Errors.** This state indicates the certificates are not configured correctly. If this state appears, validate the certificates on both the Local Controller and Global Controller. See [Importing the Security Certificates](#).
- **Synchronizing (progress).** This state results from triggering a full topology synchronization. A status indicator allows you to monitor the progress.

For a complete list of states and their meanings, see [Table 2-3, Local Controller Status Messages on Zone Controller Page](#).

Required Open Ports

When a Global Controller and Local Controller are separated by a firewall, open the following ports on both the inside and outside interfaces of the firewall to ensure proper operation of the Global Controller:

TCP Port	Function
22	Secure Shell (SSH) used by Local Controller for topology and device discovery
443	Hyper Text Transport Protocol with Secure Sockets Layer (HTTPS) use for user interface access
8444	Cisco Proprietary data synchronization between a Global Controller and Local Controllers.

General Issues and Solutions

The following symptoms and solutions address many synchronization errors.

**Tip**

Deleting and re-adding a Local Controller is rarely, if ever, the solution. This change also causes a full re-synchronization of topology data, resulting in an even longer downtime (possibly days). You should only delete a Local Controller if you want to permanently remove that Local Controller from the Global Controller.

Symptom	Possible Resolution
Local Controller/Global Controller communications fail.	Beginning with the 4.3.1 and 5.3.1 releases, the dynamic IPS signature updates is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail. To determine the version of MARS software and the IPS signature version, click Help >About on each appliance.
Local Controller/Global Controller communications does not appear to work but the state is Active.	<p>This issue can result from a backlog of data caused by a temporary disconnect of the Local Controller and Global Controller. Data synchronizes over time; therefore, the solution is to wait to verify the issue is correctly diagnosed. See Data is not synchronizing and the Local Controller and Global Controller were disconnected., page B-8</p> <p>Possible causes:</p> <p>A recent network outage caused a communication disconnect. The symptoms appear if the Local Controller receives a lot of data because, in such cases, the backlog can be large.</p> <p>A high usage MARS Appliance may not have adequate bandwidth between Local Controller/ Global Controller to ensure that the system stays synchronized.</p>
Data is not synchronizing and the Local Controller and Global Controller were disconnected.	<p>If a Local Controller\Global Controller pair is disconnected for a long period of time, the report and incident data will take a long time to transfer to the Global Controller. For each global report, data is gathered every 10 minutes and then transferred to the Global Controller. If the connectivity to the Global Controller is down, the Local Controller queues up pending data transfers. When connectivity is restored, it begins sending the report data.</p> <p>Configuration and topology data does not take as long as report and incident data, and it should synchronize in a reasonable amount of time.</p> <p>Note Communication link speeds vary; a saturated link could slow synchronization greatly relative to a lab environment.</p>

Symptom	Possible Resolution
A change in the Global Controller, such as adding a new global report or inspection rule, does not appear on a managed Local Controller.	Verify Activate was clicked. You must click Activate for Local Controller-based topological changes to be pushed to the Global Controller
No incidents appear in the Global Controller	This issue can result from a time synchronization mismatch. Make sure the Local Controller and Global Controller have the system times set properly as a time skew can cause incidents to not appear in the Summary page.
I deleted a Local Controller from the Global Controller when there were communication problems. How do I restore the Local Controller?	If the Local Controller was deleted from a Global Controller when communications were failing, use the pnreset -s command to reset the Local Controller to standalone mode. Then, you can add it to the Global Controller again. For more information, see pnreset, page A-38 .
A replacement Global Controller appliance has been restored. How do I restore communications with the Local Controllers?	Use the pnreset -g command on each Local Controller. This command removes the Global Controller data from a Local Controller, leaving Local Controller-specific data untouched. This option keeps the Global Controller connectivity information on the Local Controller intact, enabling the Local Controller to reconnect as soon as the Global Controller is restored (to purge this information, use the -s option). For more information, see pnreset, page A-38 . Note Use this option only when a Global Controller recovery is required.

Symptom	Possible Resolution
<p>The topology diagram is missing a device or other information.</p>	<p>To verify the issue is not the result of a slow link or catch up due to network downtime, add new device as a test. If the test device replicates after clicking Activate and waiting a few minutes, but the missing data still does not replicate, there could be an issue processing the transaction log.</p> <p>To manually re-synchronize the topology data, perform the following steps from the Global Controller web interface:</p> <ol style="list-style-type: none"> 1. Click Admin > Local Controller Management. 2. Select the Local Controller that has the issues and click the Topo Sync Start/Stop button. <p>The entire topology is copied from the Local Controller to the Global Controller. The size of this data set depends on the topology, but in very large cases, this operation can take several days. See Topology Synchronization .</p> <p>On the Local Controller Management page, the status indicates that data is being processed. As long as it is moving, progress is being made so continue to wait.</p> <p>Note Deleting and re-adding the Local Controller restarts this process and is not recommended</p>
<p>A topology change does not appear, the state is Active, and a reasonable amount of time has passed.</p>	<p>Initiate a full topology synchronization to re-push all topology.</p> <p>Note The time required to perform a full topology synchronization is not trivial; use this process only if topology data is missing on the Global Controller but more recent topology data has been transferred from the same Local Controller.</p>

Symptom	Possible Resolution
Configuration data (users, report definitions, rules, and event types) does not replicate from a Global Controller to Local Controller	<p>If the servers were disconnected, this symptom can result because it takes time to clear the backlog created during the downtime.</p> <p>To diagnose, create a new piece of data, such as a new user, and then click Activate. If, after a few minutes, the new user data replicates but the originally missing data does not, MARS has encountered an issue replaying that log. No configuration synchronization mechanism exists; therefore, you should following your technical support escalation process.</p>
None of the previous suggestions correct the error.	Use the pnlog command to collect log data and submit it to technical support to identify exceptions that may have the caused the error. See Collect Support Information, page B-2 .

List of Backend Services and Processes

You can obtain status on the following services and processes by entering **pnstatus** at the command line or by selecting Admin > System Maintenance > View Log Files to view backend system logs generated by the appliance. [Table B-1](#) lists the services and processes and provides a description of their role within MARS.



Note

All services should be running on a Local Controller. However, a Global Controller only has three services running: graphgen, pnarchiver, and superV—all other services are stopped.

Table B-1 MARS Services and Processes Descriptions

Service/Process Name	Description
pnparser	The pnparser service receives and parses events, SNMP MIBs and traffic flow logs generated by the reporting devices. It also uses network topology information to sessionize flows. The sessionization process involves grouping flows and other events for the same Layer 7 session that arrives within a small time frame. The network topology information is used to normalize the NAT-ed flows. Events belonging to the same session are assigned a session identifier.
ANOMALY service	The ANOMALY service performs statistical analysis of flows and other variables obtained via SNMP MIBs such as per-interface bandwidth, per-interface errors, and firewall connections. This service detects statistically significant anomalies in the data. In case of a detected anomaly, the ANOMALY service inserts a MARS generated “anomaly detected” event into the system.
autoupdate	The backend process that pulls and processes the IPS signature updates.

Table B-1 MARS Services and Processes Descriptions (continued)

LOGIC service	The LOGIC service correlates the parsed events according to a set of inspection rules. The inspection rules may be built in (that is, system defined) or defined by the user. Whenever a correlation rule is satisfied, the LOGIC service creates an incident containing the set of events satisfying the rule and forwards the incident for further analysis to process_postfire_srv.
process_postfire_srv	The process_postfire_srv service analyzes the incidents generated by the LOGIC service to determine whether they are false positives, identifies valid incidents that may represent potential attacks, and notifies the administrator. The service examines information from the following sources: <ul style="list-style-type: none"> • Built in event vulnerability data • Host information obtained from administrators or learned when process_postfire_srv probes hosts that have been attacked • Host Vulnerability information from vulnerability scanner results • Network topology paths and sessionized event data
LOADER service	The LOADER service efficiently stores the events and incidents into the database and compresses the data to be stored for archival purposes.
process_inlinerep_srv	The INLINE REPORT service performs in-memory computation of certain reports—this avoids the huge I/O penalty associated with database server computing these reports.
discover	The DISCOVERY service discovers the Layer 3 and Layer 2 network topology, NAT and ACL configuration from firewalls and routers. The service parses this information and stores it in the database in a unified vendor and device neutral form.
graphgen	The GRAPHGEN service creates network topology graphs, hotspot topology graphs, and topological attack paths for display by the web browser. The service also generates appropriate vendor and device-specific mitigation commands based on its derived knowledge about the attack path and all devices along the attack path.
GUI service	The GUI service provides the code used to display web pages that serve as the web interface for MARS. The service uses a JBOSS/Tomcat application server framework.
REPORTGEN service	The REPORTGEN service generates and sends the reports for the users. The service uses the JBOSS/Tomcat application server framework.

Table B-1 *MARS Services and Processes Descriptions (continued)*

GC Exchange service	The Global Controller Exchange service communicates with the Global Controller and synchronizes the information between the two systems. The information that needs to be synchronized is: <ul style="list-style-type: none"> • Network topology discovered by the MARS appliances, • Report results generated by a MARS appliance • Incidents generated at a MARS appliance • Global objects (for example, networks, services, rules, reports, and queries) created at a Global Controller
pnarchiver	The pnarchiver service archives data stored in the database to an offline store via NFS. Both configuration data and dynamic events and incident data are archived. The archiving is done for both system recovery and forensics.
pndbpurger	The pndbpurger service deletes old data from the database to make room for new data.
superV	The superV service acts as a software watchdog for various MARS backend processes. It monitors resource usage of the various services and various consistency conditions and restarts the appropriate services whenever necessary. The superV service also provides an event bus for the MARS processes to send messages to each other.
device_monitor	The PNMONITOR service acts as a software watchdog for JBOSS and SUPERV. The operating system watches the health of PNMONITOR service.
csdam	This backend process is responsible for DTM and the management of IOS IPS signatures. It uses the IOS command line interface (CLI) over SSH or Telnet to issue SDF updates and retrieve current configuration information from the managed Cisco IOS IPS routers. This process was introduced in 4.1.
csips	This backend process uses RDEP to pull alerts from IDS 4.0 devices and SDEE to pull alerts from IPS 5.0 devices. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the two former processes named pnids40_srv and pnids50_srv.
csiosips	This backend process uses SDEE to pull alerts from IOS IPS devices using SDEE. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the former process named pniosips_srv.
cswin	This backend process uses MS-RPC to pull alerts alerts from Windows devices. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do. This process was introduced in version 4.2.2.

Table B-1 MARS Services and Processes Descriptions (continued)

pnmac	This backend process retrieves the mac addresses for the IP addresses found in sessions and incidents. It uses the STP information provided by the switches to which the sources and destinations are connected. MARS uses this data to perform port blocks or suggest the CLI commands required to block traffic from these MAC addresses.
device_monitor	This process uses SNMP to monitor the resources usage on the reporting devices and raises device anomalies (MARS events) when the usage exceeds the defined thresholds. The resources studied include CPU, memory, number of connections, and bandwidth used.
DbIncidentLoaderSrv	This process stores event/session data for fired incidents into the database after process_postfire_srv has performed false positive analysis.
pnesloader	This process stores event and session data in the database after pnparser has parsed and sessionized the recoeved data.
process_event_srv	This process is the rule processing engine. Compiles rules, receives events, computes the incidents that need to be fired and passes them on for notification and false positive analysis to process_postfire_srv.
process_query_srv	This process computes the results for multi-lined queries (queries that look like multi-line rules. For example, X followed by Y).

Error Messages

“Error ./pnarchiver Thread 2051:PN-0102:SQL error: ORA-01005: null password given; logon denied”

Issue: Problem with archiving to NFS server. The directories for the archiving are properly created on the server but those directories remain empty.

Workaround: An interoperability issue exists between MARS and CygWin NFS server running on Windows 2003 server. To work around such interoperability issues, replace the NFS server with Microsoft Windows Services for Unix. For more information, see [Configure the NFS Server on Windows, page 6-31](#).

Page cannot be found.

Issue: Upon logging in to the web interface, user receives a “Page cannot be found.” error and the URL in the address bar is of the format: `https://<IP_address>/j_security_check`.

Workaround: If you have the MSN Search Toolbar enabled in your browser, you must disable it before logging into MARS. To disable it, right-click on the toolbar and deselect MSN Search Toolbar. Alternatively, you can simply delete the `j_security_check` at the end of the URL string and press Enter.

Hangs on “Creating Oracle database”

Issue: When using the Recovery DVD, the system hangs on “Creating Oracle database.”

Workaround: This error can occur when, after reboot, the appliance is connected to a network. When the image is applied, the system hangs attempting to detect the factory default addresses on the network.

"Status: PN-0002: No message for PN-0216"

Issue: The message, "Status: PN-0002: No message for PN-0216", displays after configuring the data archive settings in the web interface.

Workaround. This error message appears when you've entered an incorrect IP address or directory path for the data archiving feature.

