



CHAPTER 3

Configuring the Global Controller

Last updated: February 5, 2009

This chapter contains the following topics:

- [Summary of Global Controller Configuration Tasks, page 3-1](#)
- [Global Controller–Local Controller Interoperability Information, page 3-2](#)
- [Adding Local Controllers, page 3-3](#)
- [Importing the Security Certificates, page 3-11](#)
- [Monitoring Local Controller Events from the Global Controller, page 3-15](#)
- [Preparing to Add and Discover Devices, page 3-15](#)
- [Adding Reporting Devices, page 3-16](#)
- [Configuring Supported Devices, page 3-17](#)
- [L2 Discovery and Mitigation, page 3-17](#)

Once you have performed the configuration tasks described in this chapter, a Global Controller administrator can create, edit, or delete user-defined settings and rules on the Global Controller and its monitored Local Controllers. These settings and rules include:

- Rules
- Reports and queries
- User, IP, and service management

Summary of Global Controller Configuration Tasks

To configure the Global Controller, you must perform several tasks before you can monitor the events and incidents reported by Local Controllers:

1. Configure the Global Controller to operate on your network. For more information on configuring the Global Controller to connect to your network, see the [Chapter 2, “Initial MARS Appliance Configuration.”](#)
2. Divide your network topology into locally controlled zones. For each zone identified, install and configure a Local Controller.
3. Add the reporting and mitigation devices in a zone to the Local Controller that monitors that zone. Also, configure the SNMP read-only community string settings for those devices to enable network discovery.

4. Add the zones to be monitored into Global Controller. Each zone is represented by a single Local Controller. By adding a Local Controller to the Global Controller, you are indicating that the Global Controller should monitor that local zone.



Note You can only add reporting devices to an active Local Controller.

5. Import the security certificate from each Local Controller into the Global Controller and vice versa. Sharing the security certificates among the appliances enables secure communications between a Local Controller and the Global Controller.
6. 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:

Protocol/Port	Function
TCP 22	Secure Shell (SSH)
TCP 443	Hyper Text Transport Protocol with Secure Sockets Layer (HTTPS)
TCP 8444	Cisco Proprietary data synchronization with Local Controller

Global Controller–Local Controller Interoperability Information

Feature History for MARS Appliance GC–LC Interoperability

Release Version	Description
4.3.1 / 5.3.1	Introduced interoperability for LCs running different MARS release versions than the GC
5.3.2	The MARS 25R, 25, and 55 are introduced.
6.0.1	The MARS 20R, 100E, and GCM become the MARS 20, 100, and GC respectively when reimaged with Release 6.0.1.


. [Table 3-1](#) lists which Local Controllers (20, 50, 100, 200, 25R, 25, 55, 110, 110R, 210) can interoperate with which Global Controllers (GC, GC2R, GC2).

[Table 3-2](#) lists the compatible releases required for a Global Controller to interoperate with a Local Controller. To interoperate, a Global Controller and a Local Controller must be running compatible releases of the MARS operating systems. A Global Controller cannot add a Local Controller running an incompatible release.

Table 3-1 Global Controller to Local Controller Interoperability Matrix (for Local Controllers running 6.0.X)

	20	50	100	200	25R	25	55	110R	110	210
GC (6.0.X)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GC2R (6.0.X)	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
GC2 (6.0.X)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 3-2 Release Requirements for Global Controller –Local Controller Interoperability

Release Versions—Global Controller ¹	Release Versions—Local Controllers
6.0.x	Local Controller must run an identical release version
5.3.x	Local Controller must run the identical release version of 5.3.x, or the corresponding release of 4.3.x.  Note The Local Controllers 25R, 25, and 55 require Release 5.3.2 or more recent.
5.2.x	Local Controller must run an identical release version
4.x.x	Local Controller must run an identical release version

1. Release 6.x operates on all MARS hardware platforms.
Release 5.x operates only on Global Controllers GC2R and GC2, and on Local Controller 25R, 25, 55, 110R, 110, and 210.
Release 4.x operates only on Global Controllers GC and GCM, and on Local Controllers 20R, 20, 50, 100E, 100, and 200.

Adding Local Controllers

Follow these steps to add a Local Controller to the Global Controller:

- Step 1** Click **ADMIN > System Setup > Local Controller Management** to display the Zone Controller Information page, as shown in [Figure 3-1](#).

Figure 3-1 Zone Controller Information Page

Zone Controller Information

Page Refresh Rate: 15 minutes

Edit Delete Add Back Topo Sync Start/Stop Suspend/Resume Details...

Zone Name	Device Name	Zone Model	Zone Address	Version	Description	Status
LC133	pnmars	CS-MARS 20	10.1.1.133	4.2.1	LC133	Active (last checked: Tue Sep 05 12:25:03 PDT 2006)

1 to 1 of 1 25 per page

Edit Delete Add Back Topo Sync Start/Stop Suspend/Resume Details...

Step 2 Click **Add**.

A pop-up window appears in which you can add a Local Controller to the Global Controller.

Figure 3-2 Local Controller Information Page

Local Controller Information

Zone Name:

Zone Description:

LC IP Address:

Cancel Submit

Step 3 Enter values for the following settings:

- **Zone Name.** Enter a name for this zone. This name is used to uniquely identify the networks within this zone relative to other zones. For example, many companies use the same private network addresses behind NATed gateways. The zone combined with the network address allows you to reuse the same network address on your private networks.
- **Zone Description.** Enter a description of the zone
- **LC IP Address.** Enter the IP address of the Local Controller that monitors this zone.

Step 4 Click **Submit** to save the values.

Before the Global Controller can communicate with the Local Controller, you must import the security certificate into the Global Controller. For more information, see [Importing the Security Certificates](#), page 3-11.

Topology Synchronization

For the Global Controller to display a summarized and merged view of topology for its Local Controllers, topology data from all the Local Controllers must be pushed to the Global Controller. When you add a Local Controller to a Global Controller, the topology synchronization process begins and completes automatically.

When synchronized with Local Controllers, the Global Controller contains all the security and monitoring information of the Local Controllers (as displayed on **Admin > System Maintenance > Security and Monitor Devices**) and can display the combined topological maps of the Local Controllers with the following constraints:

- Devices common to Local Controllers are merged in the Global Controller topology. If you have a router listed on different Local Controllers, it only shows up once in topology graphs.
- Networks common to Local Controllers are not merged in the Global Controller topology, but are displayed as separate topologies even if they are the same network.

Topo Sync Start/Stop

When you change Local Controller topology or it otherwise becomes out-of-sync, you can re-synchronize the Local Controller and Global Controller by clicking **Topo Sync Start/Stop** on the Zone Controller Information Page. The **Status** field reports the current state of the synchronization process. [Table 3-3](#) lists and describes all possible status messages.

An out-of-sync condition can occur when unexpected errors or events (device, software, network, etc.) disrupt communication between the Local and Global Controllers.

Suspend/Resume

The **Suspend/Resume** button toggles the communication link on and off between the Global Controller and the Local Controller. When suspended, the Local Controller cannot communicate with the Global Controller.



Note

Incident, topology, and other information cannot be uploaded to the Global Controller when the Local Controller communication is suspended.

Table 3-3 Local Controller Status Messages on Zone Controller Page

Status Field Values	Description and Action
Active (last checked: <i>(Time_and_Date_last_checked)</i>)	The Local Controller is online, connected, and synchronized with the Global Controller.
Suspended	Communications between the Local Controller and the Global Controller have been manually halted with the Suspend/Resume button. To re-establish communication, select the Local Controller and click Suspend/Resume .
Synchronizing (<i>progress</i>)	The Global Controller and Local Controller are comparing and updating their topology information tables.

Table 3-3 Local Controller Status Messages on Zone Controller Page

Status Field Values	Description and Action
Deleting in progress	The Global Controller is purging the selected Local Controller configuration and data from its database. If the Global and Local Controllers can communicate, the Local Controller is purging Global Controller configurations to change from monitor to standalone mode.
Not Responding (last checked: <i>Time_and_Date_last_checked</i>)	The Local Controller cannot be detected on the network. Check network status and connections.
Local Controller is online but is not responding (last checked: <i>Time_and_Date_last_checked</i>)	The Local Controller can be detected on the network, but does not respond. The problem or delay may clear, the status can return to Active.
Zone has standalone license	The Local Controller model indicated is not supported by the Global Controller.
Global controller license does not allow adding model PNMARS-100 for monitoring	The Local Controller model indicated is not supported by the Global Controller.
Global controller license does not allow adding model PNMARS-100X for monitoring	The Local Controller model indicated is not supported by the Global Controller.
Global controller license does not allow adding model PNMARS-200 for monitoring	The Local Controller model indicated is not supported by the Global Controller.
Zone version is different	The Global and Local Controllers are operating with different software versions. Update one or the other or both as appropriate.
Global license is Local Controller license	Enter the correct Global Controller license in the Global Controller at Admin > System Maintenance > Set License Key.
Global certificate not in LC or local certificate not on GC	Copy the Global Controller security certificate to the Local Controller, and the Local Controller security certificate to the Global Controller at Admin > System Maintenance > Certificates

Monitoring Communication between Local and Global Controllers

Communication status between the Local and Global Controller is displayed on the Global Controller Zone Information Page, as shown in [Figure 3-1](#), with the status messages described in [Table 3-3](#).

Feature History for MARS Appliance GC–LC Communication Monitoring

Release Version	Description
4.3.1 / 5.3.1	Events, Rules, and Reports introduced to monitor GC–LC communication
5.3.2	The MARS 25R, 25, and 55 are introduced.

In summary, communication problems between the Global Controller and Local Controllers are typically caused by one or more of the following events:

- Local Controller cannot connect to the Global Controller
- Local Controller certificate is not on the Global Controller or vice versa
- Local Controller and Global Controller are operating with incompatible MARS release versions

Monitoring the connection to the Global Controller from the Local Controller is accomplished by using syslogs, system rules and system reports designed to detect typical communication failure events.

Connection Event and Incident Monitoring

Every two minutes, a MARS process runs on the Local Controller to check the connection status, certificate information, and MARS release versions of itself and the Global Controller.

Syslogs are generated according to the following algorithm:

1. If the same error is found on three consecutive 2-minute checks, a syslog is generated as described in [Table 3-3](#) for Event IDs 1000059, 1000062, and 1000064.
2. If the same error is discovered in the next three consecutive 2-minute checks, a “continues to fail” syslog is generated, as described in [Table 3-3](#) for Event IDs 1000061, 1000063, and 1000065.
3. If the same error is detected in every subsequent 2-minute check for two hours, the “continues to fail” syslog reporting interval is lengthened to every eighteen minutes from every six minutes.
4. Whenever a discovered error is corrected (not detected), a “recovered” syslog is generated, as described in [Table 3-3](#) for Event ID 1000066.

The Local Controller sends the syslog messages to itself through the eth0 interface.

System Rules and System Reports

There are three system rules and two system reports of the Local Controller that can alert MARS users of communication issues with the Global Controller, as described in [Table 3-5](#) and [Table 3-6](#) respectively.

Table 3-4 Local Controller Events and Syslog Messages for Local Controller –Global Controller Communication

Event ID	Event Description and Raw Message	Device Event ID	Event Groups
1000059	CS-MARS LC failed to communicate with GC due to connectivity issue	PN-MARS: MARS-2-350050	OperationalError/CS-MARS OperationalStatusChange/CS-MARS
	%MARS-2-350050 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at <GC_IP_address>' due to connectivity issue for 3 times in the last 6 consecutive minutes. LC last successfully connected to GC at <date_time>.		
1000061	CS-MARS LC continues to fail to communicate with GC due to connectivity issue	PN-MARS: MARS-2-350051	Info/Misc/CS-MARS OperationalError/CS-MARS
	%MARS-2-350051 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at <GC_IP_address>' due to connectivity issue for <m> times in the last <n> consecutive minutes. LC last successfully connected to GC at <date_time>.		
1000062	CS-MARS LC failed to communicate with GC due to certificate mismatch	PN-MARS: MARS-2-350052	OperationalError/CS-MARS OperationalStatusChange/CS-MARS
	%MARS-2-350052 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at <GC_IP_address>' for 3 times in the last 6 consecutive minutes due to certificate mismatch. LC last successfully matched the certificates with GC at <date_time>.		

Table 3-4 Local Controller Events and Syslog Messages for Local Controller –Global Controller Communication

Event ID	Event Description and Raw Message	Device Event ID	Event Groups
1000063	CS-MARS LC continues to fail to communicate with GC due to certificate mismatch	PN-MARS: MARS-2-350053	Info/Misc/CS-MARS OperationalError/CS-MARS
	%MARS-2-350053 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at '<GC_IP_address>' for <m> times in the last <n> consecutive minutes due to certificate mismatch. LC last successfully matched the certificates with GC at <date_time>.		
1000064	CS-MARS LC failed to communicate with GC due to incompatible software/data versions	PN-MARS: MARS-2-350054	OperationalError/CS-MARS OperationalStatusChange/CS-MARS
	%MARS-2-350054 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at '<GC_IP_address>' for 3 times in the last 6 consecutive minutes due to incompatible software/data versions. LC version is <x1.y1.z1>. GC version is <x2.y2.z2>. LC last successfully had compatible software/data versions with GC at <date_time>.		
1000065	CS-MARS LC continues to fail to communicate with GC due to incompatible software/data versions	PN-MARS: MARS-2-350055	Info/Misc/CS-MARS OperationalError/CS-MARS
	%MARS-2-350055 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at '<GC_IP_address>' for <m> times in the last <n> consecutive minutes due to incompatible software versions. LC version is <x1.y1.z1>. GC version is <x2.y2.z2>. LC last successfully had compatible software/data versions with GC at <date_time>.		
1000066	CS-MARS Communication from LC to GC has recovered	PN-MARS: MARS-2-350056	Info/Misc/CS-MARS OperationalStatusChange/CS-MARS
	%MARS-2-350056 Communication has recovered from LC for zone '<LC_zone>' at '<LC_IP_address>' to GC at '<GC_IP_address>'. Communication was unsuccessful for <this_number_of> minutes.		

Table 3-5 Local Controller System Rules for Local Controller –Global Controller Communication

System Rule	Rule Description
System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue	<p>This rule fires if there is one or more repeated connectivity failure messages. Potentially, this could be a transient failure that may correct itself. The rule is a 3-offset rule as follows:</p> <p>(CS-MARS LC failed to communicate with GC due to connectivity issue</p> <p>FOLLOWED-BY</p> <p>CS-MARS LC continues to fail to communicate with GC due to connectivity issue)</p> <p>OR</p> <p>CS-MARS LC continues to fail to communicate with GC due to connectivity issue</p> <p>Each offset has a count of 1 and a time range of 10 minutes.</p>
System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch	<p>This rule is a one offset rule that matches against the event:</p> <p>CS-MARS LC failed to communicate with GC due to certificate mismatch</p> <p>The count is 1, the time range is 1 minute.</p>
System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions	<p>This rule is a one offset rule that matches against the event:</p> <p>CS-MARS LC failed to communicate with GC due to incompatible software/data versions</p> <p>The count is 1, the time range is 1 minute</p>

Table 3-6 Local Controller System Reports for Local Controller –Global Controller Communication

System Report	Report Description
Activity: CS-MARS LC-GC Communication Failures (Total View)	<p>Report scheduled for every hour.</p> <p>Query Type: Custom Columns ranked by Time, with “ANY” in all columns except Query, where event type matches any one of the communication failure events listed in Table 3-3 (Event IDs 1000059–1000065).</p> <p>The custom columns are ordered as Source Address, Event Type Set, Time Range and Raw Message.</p>
Activity: CS-MARS LC-GC Communication Recovered (Total View)	<p>On-demand report with a time range of 1 hour.</p> <p>Query Type: Custom Columns ranked by Time, with “ANY” in all columns except Query, where event type matches the event “CS-MARS Communication from LC to GC has recovered” (Event ID 1000066 in Table 3-3)</p> <p>The custom columns are ordered as Source Address, Event Type Set, Time Range, and Raw Message.</p>

Deleting Local Controllers

To delete a Local Controller from the Global Controller and return the Local Controller to Standalone mode, do the following steps:

- Step 1** Click **ADMIN > System Setup > Local Controller Management**, to display the Zone Controller Information page, as shown in [Figure 3-3](#).

Figure 3-3 Zone Controller Information Page

The screenshot shows the Cisco MARS web interface for Zone Controller Information. At the top, there is a navigation bar with tabs for 'System Setup', 'System Maintenance', 'User Management', 'System Parameters', and 'Custom Setup'. Below this, there are buttons for 'Edit', 'Delete', and 'Add'. A table lists the zone controllers:

Zone Name	Device Name	Zone Model	Zone Address	Version	Description	Status
<input type="checkbox"/> LC1	LC1	CS-MARS 50	10.2.3.91	4.2.2	zone_LC1	Active (last checked: Tue Sep 05 14:23:01 PDT 2006)
<input type="checkbox"/> LC2	LC2	CS-MARS 20	10.2.3.92	4.2.2	zone_LC2	Active (last checked: Tue Sep 05 14:23:01 PDT 2006)

At the bottom of the table, there are buttons for 'Edit', 'Delete', 'Add', 'Back', 'Topo Sync Start/Stop', 'Suspend/Resume', and 'Details...'. The page also includes a footer with copyright information and a feedback button.

- Step 2** Click the checkbox of the Local Controller to delete, and click **Delete**.

A Yes/No confirmation dialog box appears. Click **Yes** to remove configuration info and data from the Global and Local Controllers.

If the status of the Local Controller is **Not Responding**, a Continue/Cancel dialog box appears. Because the Global Controller cannot communicate with the Local Controller, clicking **Continue** removes only the Local Controller data from the Global Controller. To remove the Global Controller configuration information from the Local Controller, you must execute a **pnreset -s** CLI command on the Local Controller as explained in the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/command/reference/cref1.html#wp1071420



Note If you do not remove the Global Controller configuration from the Local Controller, errors may occur when the Local Controller attempts to contact the Global Controller. Moreover, the Local Controller cannot be added to a Global Controller until it is reset.

The duration of the deletion process varies with the amount of data to be deleted. A duration of many minutes is possible.

Importing the Security Certificates

Security certificates are used for secure communications between a web browser and the Global Controller, as well as between the Global Controller and any Local Controllers that are managed by the Global Controller. Every Global Controller comes with a default certificate which is unique to each Global Controller. However, users could choose to modify the default certificate using the `sslcert` CLI command. For more information on using the `sslcert` command, see [sslcert](#), page 1-83 in the *Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x*.

Figure 3-4 Changing the Default Security Certificate

```

10.1.1.94 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles

Protego MARS - Mitigation and Response System

? for list of commands

[pnadmin]$ sslcert
Sslcert command will generate a new ssl certificate and restart jboss.
Please type YES if you want to proceed: YES
What is the common name of this device? (CN)
[Unknown]: pnsupport
What is the name of your organizational unit? (OU)
[Unknown]: protegonetworks
What is the name of your organization? (O)
[Unknown]: protego networks
What is the name of your City or Locality? (L)
[Unknown]: beautiful sunnyvale
What is the name of your State or Province? (SP)
[Unknown]: CA
What is the two-letter country code for this unit? (C)
[Unknown]: US
Certificate stored in file <server.cert>
Certificate was added to keystore
Restarting jboss ...
[pnadmin]$

```

If you wish to install the certificate to an Internet Explorer browser, you must do it during the Global Controller login process.

When the Security Alert pop up appears, choose:

-
- Step 1** View Certificate.
 - Step 2** Install Certificate. Then click **Next**.
 - Step 3** Select *Automatically Select the Certificate Based on the Type of Certificate*. Then click **Next**.
 - Step 4** Complete the Certificate Import process by clicking **Finish**.
 - Step 5** Select **Yes** to add the certificate to the Root Store.

Figure 3-5 Global Controller Login Security Alert

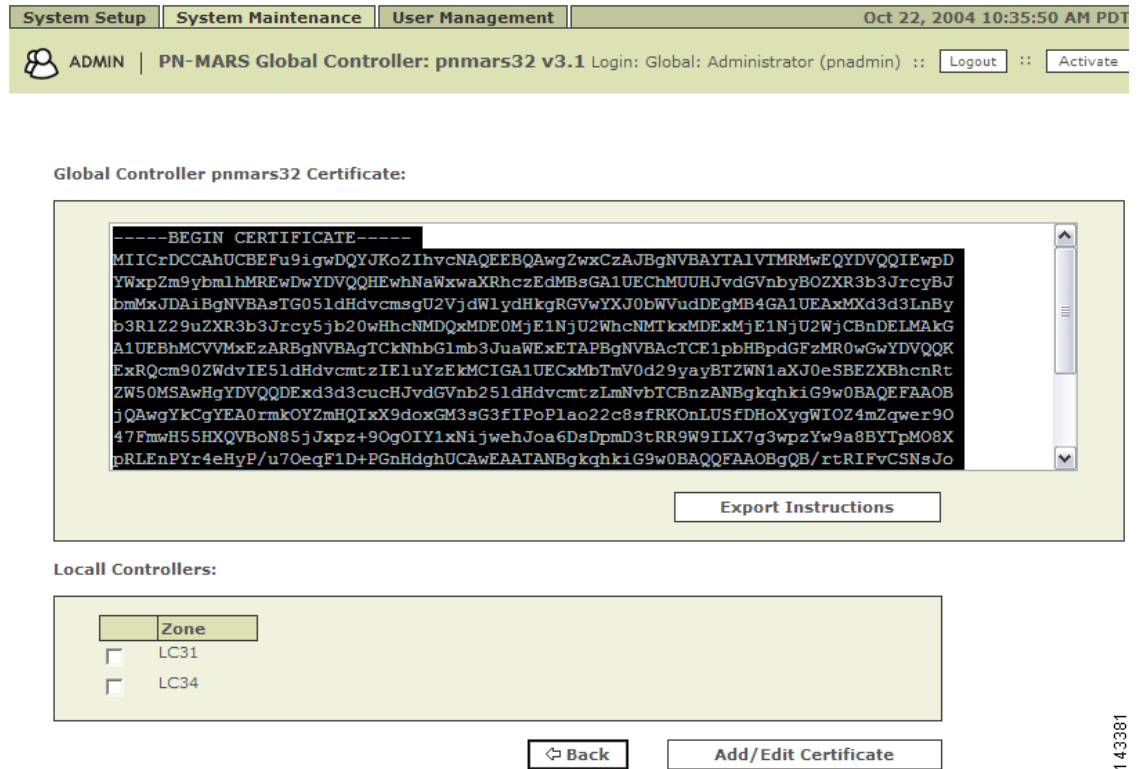
The security certificate is used for communication between a Global Controller and any Local Controllers that are managed by the Global Controller.

Although Global Controller and Local Controllers have default security certificates, the Global Controller certificate will need to be exported to all the Local Controllers manually. And all Local Controllers certificates will need to be exported to Global Controller.

To install a Global Controller security certificate on to Local Controllers, follow these steps:

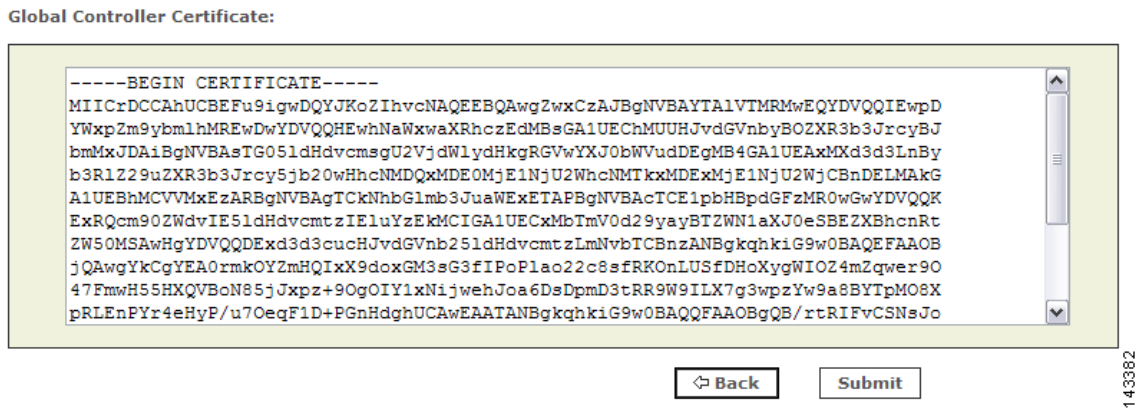
-
- Step 1** From the Global Controller, select **Admin > System Maintenance > Certificates**.
 - Step 2** Highlight the certificate, and press **Ctrl+C** to copy it.

Figure 3-6 Copy the Global Controller Security Certificate



- Step 3** Navigate to Local Controller **Admin > System Maintenance > Certificates**.
- Step 4** Paste the Global Controller certificate into the **Global Controller Certificate** box.
- Step 5** Repeat the process for all every Local Controller that the Global Controller is monitoring.

Figure 3-7 Apply the Global Controller Certificate to the Local Controller



To install a Local Controller security certificate on to the Global Controller, follow these steps:

- Step 1** From the Local Controller, select **Admin > System Maintenance > Certificates**.
- Step 2** Highlight the certificate and press **Ctrl+C** to copy it.

Figure 3-10 Apply the Local Controller Certificate to the Global Controller

System Setup | System Maintenance | User Management | Oct 22, 2004 10:41:16 AM PDT

ADMIN | PN-MARS Global Controller: pnmars32 v3.1 Login: Global: Administrator (padmin) :: Logout :: Activate

Local Controller LC31 Certificate:

```

-----BEGIN CERTIFICATE-----
MIICrDCCAhUCBEFvFuwwDQYJKoZIhvcNAQEEBQAwwZwxCzAJBgNVBAYTA1VTMRMwEQYDVQDEwPDB
YXxpZm9ybmlhMREwDwYDVQQHEWhNaWxwaXRhczEdMBsGA1UEChMUUHJvdGVnb3B3JrcyBJ
bmMxJDAiBgNVBAsTG051dHdvcmsqU2VjdWl1dHkgRGVwYXJ0bWVudDEgMB4GA1UEAxMxMDE3d3LnBy
b3R1Z29uZXR3b3Jrcy5jb20wHhcNMDQxMDE1MDAxNjQ0WhcNMTkxMDEyMDAxNjQ0WjCBnDELMAkG
A1UEBHMVVMXezARBgNVBAGTCkNhbG1mb3JuaWEXETAPBgNVBAcTCE1pbHpdGFZMR0wGwYDVQQK
ExRQcm90ZWdvIE51dHdvcmtzIEluYzEkMCIGA1UECzMbTmV0d29yaYBTZW51aXJ0eSBEZXBhcncRt
ZW50MSAwHgYDVQQDExd3d3cucHJvdGVnb251dHdvcmtzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwYkCgYEA07HrCqV1TiJhxSNBEJC0Y8zJIEyL+q4InQ2U4AmyPzOKfb6YnFwNt0h/28nlpBtc
j/OUSZBZydrIeU+zSyoB9AqfobWTKHulzDZzaXZ1qcJDO4ksGcWMDtPmluvB15sExCPyvxzf0gUg
19moSrBGX6aRnpuwBQyaD6/5jWQkTN8CAwEAATANBgkqhkiG9w0BAQQFAAOBgQCA2IxsWScA1T/8

```

Back Submit

143385

Monitoring Local Controller Events from the Global Controller

The various Local Controllers send summarized information to the Global Controller, which in turn compiles and collates it. There may be a reason you want to suspend, or temporarily hold back, information being sent from one of the Local Controllers. For example, if several of the Local Controller zones are compromised and sending many events at once, you may want to focus on isolating problems on one Local Controller at a time.

If you want to suspend the transmission of information from a Local Controller, follow these instructions:

- Step 1** In the Zone Controller Information page, select the Local Controller you want to suspend.
- Step 2** Click the **Suspend/Resume** button.

The Local Controller you selected disappears from the list of active Local Controllers, and its output is buffered until you select it and click **Suspend/Resume** again.

Follow the same procedure to resume output from the affected Local Controller.

Preparing to Add and Discover Devices

Before configuring the Global Controller to recognize reporting devices, be aware of the levels of operation supported by a Local Controller. To learn more about the levels of operation for the Local Controllers, see [Levels of Operation, page 3-1](#) in the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*

Adding Reporting Devices

After you have added the Global Controller's configuration information and rebooted it, you need to configure the third-party devices that report to the Global Controller. All of the event information that passes through these devices is distilled down and sessionized to the information that the Global Controller presents to you. The more information that you can provide for these devices, the clearer the picture you'll get when using the Global Controller.



Note

For a list of devices supported by the Global Controller, see the [Configuring Supported Devices, page 3-17](#).

Manual Configuration

In general, you have two choices for adding devices that you want to monitor into your Global Controller. You can create a seed file or you can add each device manually. Seed file support is limited to a few device types; see [Configuring Supported Devices, page 3-17](#).

When manually configuring devices, select the devices that are most interesting to you. Once added, you can come back and edit them as necessary. Manual configuration is also useful when you add or change a single security device on your network. See [Configuring Supported Devices, page 3-17](#) for more information about configuring individual devices.



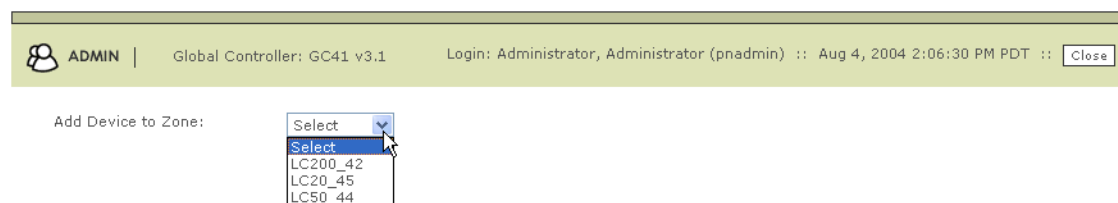
Note

Remember that you do not have to add all of the devices configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the Global Controller starts to report to you, and provide more details.

Add a Device Manually

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Figure 3-11 Selecting the Local Controller Zone



Step 2 Select the Local Controller **Zone** from the pull-down menu. This determines which Local Controller monitors the device. *You are then automatically logged into the Local Controller you have selected.* A pop-up window appears.

Figure 3-12 Entering the Device on the Local Controller

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: ▼

→ *Device Name:

→ *Reporting IP: ...

Step 3 Select the device from the pull-down menu.

Step 4 Enter the information needed to communicate with the device.

Step 5 Click the **Submit** button.

Newly added devices on the Local Controller are automatically discovered by the Global Controller.

For more information on installing individual devices, see [Preparing to Add and Discover Devices](#), page 3-15.

Configuring Supported Devices

For most of the security and monitoring devices that you have report to Global Controller, set up and configuration is three-part. You need to:

- Open communication channels to the device.
- Add the appropriate communication information to the Global Controller.
- Make sure that firewalls and routers sitting between the Global Controller and the reporting device are configured to let event traffic pass.

For devices that use agents, modules, or sensors, you need to perform a couple of extra steps.

L2 Discovery and Mitigation

For information on L2 device discovery and mitigation, see [Layer 2 Discovery and Mitigation](#), page 3-18 in the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.

