



Troubleshooting Cisco MGC Node Manager

This section provides troubleshooting information for Cisco MGC Node Manager internal messages and for other common Cisco MGC Node Manager issues.

Troubleshooting Cisco MGC Node Manager Internal Messages

The following messages may be generated by Cisco MGC Node Manager itself and reflect errors in deployment, discovery, or configuration. See the next section, [“Solving Deployment and Discovery Errors” section on page C-5](#), for information on how to correct deployment and discovery errors.

Table 0-1 Cisco MGC Node Manager Internal Events.

| Message | Explanation | Action |
|--|---|---|
| (Cisco MGC host) Failed to collect active configuration | (1) FTP failed and the information is not getting to Cisco MGC Node Manager. (2) The device is not generating the information. | On the Cisco MGC host, run the prov-exp command to view the configuration information being generated. If it is OK, there is an FTP problem. If it is not OK, there is a problem with the Cisco MGC host. |
| <Host name>: Could not collect inventory: Login ID or password or security policy is invalid | Login or password is invalid for the deployed device, or the security policy attribute is mis-set. As a result, Cisco MGC Node Manager cannot fully discover the device. See Troubleshooting SSH-Related Errors, page C-6 for help in pinpointing the problem. | Correct the login, password, or security policy attribute information (Accounts dialog box) and rediscover the device. |
| <Host name>: Could not collect inventory: Password not specified | Password is not specified for the deployed device. As a result, Cisco MGC Node Manager cannot fully discover the device. | Correct the password information and rediscover the device. |

Table 0-1 Cisco MGC Node Manager Internal Events. (continued)

| Message | Explanation | Action |
|--|---|---|
| <Host name>: Could not get Host Device table. Check IP address and read-community string. | Cisco MGC Node Manager failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process not running on the device, or (3) the device is not reachable. | (1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |
| <Host name>: Could not get Host Files System. Check IP address and read-community string. | Cisco MGC Node Manager failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP agent or the fsagt process not running on the device, or (3) the device is not reachable. | (1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and fsagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |
| <Host name>: Could not get Host Storage table. Check IP address and read-community string. | Cisco MGC Node Manager failed to retrieve the device table from the device. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent or the hostagt process not running on the device, or (3) the device is not reachable. | (1) Check the SNMP read-community string and correct if needed. (2) Check that the snmpdm and hostagt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |
| BAMS is not configured to receive Call Data Records from any MGC Host | Since the BAMS server is not configured to collect data from any MGC Host, Cisco MGC Node Manager cannot deploy the device to the right MGC node, and its alarm status will not be propagated in the MGC-Node-View. | Check your BAMS configuration and check the MGC status. |
| Cannot get IF description from the interface table | The appropriate processes may not be running on the device. | On the Cisco MGC host, determine the process IDs by entering this command: ps-eflgrep agt Check that critagt, mibagt, hostagt, and snmpagt are running. If not, kill critagt and restart the processes. |

Table 0-1 Cisco MGC Node Manager Internal Events. (continued)

| Message | Explanation | Action |
|--|--|---|
| Could not get BAMS Poll table | Cisco MGC Node Manager failed to retrieve the BAMS configuration via SNMP. The problem may be (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, (3) the device is not reachable. As a result, Cisco MGC Node Manager cannot deploy the device to the correct MGC node. Thus, its alarm status will not be propagated in the MGC-Node-View. | (1) Check the SNMP community strings and correct if needed. (2) Check that the <code>snmpdm</code> and <code>sagt</code> processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <code><CEMF_ROOT>/logs/mgcController.log</code> . |
| Could not get IP Address table from <device name>. Check IP address and read-community string. | Cisco MGC Node Manager failed to retrieve the interface table from the device. The problem may be (1) wrong SNMP community strings, (2) Invalid IP Address, or (3) the device is not reachable. | (1) Check the SNMP read-community string and correct if needed. (2) Check the IP address. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |
| Could not get password for host <IP Address> | Password is not specified for the deployed MGC host. As a result, Cisco MGC Node Manager cannot fully discover the device. | Correct the password information and rediscover the device. |
| Failed to launch action <Action name>. Perhaps hostController is not running. | The most probable cause is that the Cisco MGC Node Manager process <code>hostController</code> is down while Cisco MGC Node Manager is trying to discover a MGC. | Verify that the <code>hostController</code> process is running. For example, enter: <pre>ps -ef grep hostController</pre> If the <code>hostController</code> is running, rediscover the device. If not, contact the TAC. |
| Miscellaneous error messages upon deployment such as, demons not running... | — | (1) Verify that the correct software release and patch are installed on the device. See the Installation Guide, Chapter 1, for details and links to up-to-date information. (2) Make sure that the device is running. For example, for the Cisco MGC, enter: <pre>/etc/init.d/CiscoMGC start</pre> If the device is already running, you get a message; if not, it should start. |

Table 0-1 Cisco MGC Node Manager Internal Events. (continued)

| Message | Explanation | Action |
|--|---|---|
| No IP addresses defined on this device. All traps from it will be ignored. | Cisco MGC Node Manager failed to find any address on this device via SNMP. The problem may be: (1) wrong SNMP community strings, (2) SNMP Agent does not run on the device, or (3) the device is not reachable. | (1) Check the SNMP community strings and correct if needed. (2) Check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |
| Subrack discovery failed. Check logs | Cisco MGC Node Manager failed to discover components on the device. The problem may be: (1) Wrong SNMP community strings. (2) SNMP Agent does not run on the device. (3) The device is not reachable. | (1) Check the SNMP community strings and correct if needed. (2) If MGC or BAMS, check that the snmpdm and mib2agt processes are running. (3) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. For more information, refer to the log file <CEMF_ROOT>/logs/mgcController.log. Verify that the correct software release and patch are installed on the device. See the Installation Guide, Chapter 1 for details and links to up-to-date information. |
| The IP Address <IP Address> is not reachable. | Cisco MGC Node Manager failed to do SNMP ping with this address. | Check the network connection. |
| This device is not reachable. | Cisco MGC Node Manager cannot reach the device using SNMP. If the device has multiple IP addresses, then all of them are unreachable. | (1) Check the SNMP community strings and correct if needed. (2) Attempt to access the device using ping. If it is unreachable, there may be a problem in the network connection. |

Table 0-2 Seed File Deployment Errors

| Message | Explanation | Action |
|--|----------------------------------|--------|
| Unknown device specified | — | — |
| Unbalanced braces | — | — |
| Duplicate object names | — | — |
| Missing required attribute: <i>Attribute</i> | A required attribute is missing. | — |

Table 0-2 Seed File Deployment Errors (continued)

| Message | Explanation | Action |
|---|---|---|
| Component is not valid: <i>COMPONENT</i> | Device information supplied is syntactically incorrect. | Check and fix device syntax in seed file. |
| Expected attribute value. Found | A required value is missing | — |

Solving Deployment and Discovery Errors

If you receive errors when deploying a seed file, check the information in [Table 0-2](#) and correct the problem in the file. See [Chapter 5, “Deploying Your Network in Cisco MGC Node Manager,” “Deploying a Network Using a Seed File” section on page 5-9](#) for details.

If you receive a message about a problem in manual device deployment or during the discovery process, use these procedures to change the deployment information or rediscover network elements

Changing Password or Community Strings

To change the password or community strings for a device:

-
- Step 1** In the Map Viewer, select the object and right-click.
 - Step 2** From the pull-down menu, choose **Accounts**. You see the Accounts dialog box.
 - Step 3** On the Accounts tab, check and if needed change the password.
 - Step 4** On the SNMP tab, check and if needed change the SNMP community strings.
 - Step 5** Click the **Save** button on the toolbar. Close the dialog box.
 - Step 6** If you changed the community strings to any device or the password for the MGC host, rediscover the device as described in the [“Rediscovering a Device After a Problem” section on page C-6](#).
-

Changing IP Address

If the wrong IP address was entered, the device must be redeployed. Use the following steps to redeploy a device:

-
- Step 1** In the Map Viewer, select the object and right-click.
 - Step 2** From the pull-down menu, select **Deployment** and then **Delete Objects**. You see the Deployment Wizard dialog box with the message, “Ready to delete 1 object.”
 - Step 3** Click **Finish**. You get a message that the object has been deleted.
 - Step 4** Click **OK**.
 - Step 5** Redeploy the device following the instructions in [Chapter 5, “Deploying Your Network in Cisco MGC Node Manager,” “Manual Deployment” section on page 5-10](#).

- Step 6** After deployment, rediscover the device as described in the “Rediscovering a Device After a Problem” section on page C-6.
-

Rediscovering a Device After a Problem

Follow these steps to rediscover a device after correcting a problem that interfered with discovery. This synchronizes the Cisco MNM network object model with the real-world network.

-
- Step 1** In the Map Viewer, select the object and right-click.
- Step 2** Choose **States**. You see the States dialog box.
- Step 3** On the States tab, click **Rediscover**. You are asked if you want to rediscover the device.
- Step 4** Click **Yes**. Cisco MGC Node Manager rediscovers the device. During discovery, Current State is discovering. When the discovery is complete, Current State changes to active.
- Step 5** Close the dialog box.
-

Troubleshooting SSH-Related Errors

If you suspect an SSH, security-policy error, such as a mismatch between the security policy defined for a component at deployment and its actual security policy, you can do one of two things:

- Check SSH-related alarms in the Event Browser. You can see SSH-related alarms, such as a mismatched security policy or an incorrect password, for the BAMS, Cisco PGW, and HSI server, in the Event Browser. These are Warning alarms. For a description of Cisco PGW 2200, BAMS, and HSI alarms caused by login failures related to SSH problems, refer to *Cisco PGW 2200 Security Enhancements*, “Alarms and Messages” at http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_installation_and_configuration_guide_chapter09186a00801bde43.html#wp1095818.
- For an IOS device, check the ssh protocol version or configuration with this command:

show ip ssh

```
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

To see ssh users logged on

show ssh

```
Connection  Version Encryption      State      Username
1           1.5      DES           Session started      lab
```

Troubleshooting Other Issues

Table 0-3 lists common problems you may encounter and suggested corrective actions. Other troubleshooting information is provided in the Installation Guide, Chapter 2, Troubleshooting Common Installation Problems.

Table 0-3 *Troubleshooting Symptoms and Suggested Steps*

| Problem | Action |
|--|--|
| Alarms are not being received from a device. | <p>Check that SNMP trap forwarding has been configured. If not, configure it (see Chapter 2, “Configuring Network Devices for Management”).</p> <p>If trap forwarding has been configured, check the snmpd.cnf file (Cisco MGC host or BAMS) against the instructions in Chapter 2 for possible typing errors.</p> |

