



Troubleshooting Essentials

This appendix provides information on troubleshooting Essentials applications and Essentials-related CiscoWorks2000 Server problems.

- Change Audit
- Configuration Management
- Contract Connection
- Inventory
- Software Management
- Syslog Analysis
- CiscoWorks2000 Server

Change Audit

FAQs

Can I track every configuration change made to routers and switches in my network and who made them?

Yes, if the devices have been enabled for syslog. All changes made on a device are logged, including changes made by outside Telnet sessions.

You can enable Change Audit to listen to the syslog messages so that it can update the archive with the changed version of the configuration file and log the change. Select **Resource Manager Essentials > Administration > Configuration Management > General Setup**, then select the **Change Probe Setup** tab and enable **Listen to Syslog Messages**.

You can check for changes by selecting **Resource Manager Essentials > Change Audit > All Changes**. If the change was made by an outside Telnet session, Unknown is listed in the Connection Mode column of the report.

Configuration Management

FAQs

Where can I find out what devices are supported by Configuration Management?

Select **CiscoWorks2000 Server > About CiscoWorks2000 > Applications and Versions**. Under the CW2000 Installed Applications, click Configuration Archive to see a list of supported devices.

If I import devices from a remote NMS, can I compare the startup vs. running configurations?

Yes, but first you must:

-
- Step 1** Select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**.
 - Step 2** Select all the devices with the same passwords.
 - Step 3** Change the TACACS usernames and passwords.
-

Can I execute Network Show Command sets for more than 10 devices?

No. Only you can execute command sets for only 10 devices.

How many Network Show Command sets are allowed per user?

Each user is allowed a maximum of 6 command sets.

How many Network Show Commands are allowed per command set?

Each command set can contain a maximum of 6 router commands, 6 Catalyst commands and 6 FastSwitch commands.

Can I execute all device commands using Network Show Commands?

No, only show commands are supported. However, commands such as help, ?, debug, ping, traceroute, and where are also supported.

If I'm having problems with the Network Show Commands option, where can I check for error messages?

You can check for messages in these locations:

- The Java console available with your browser.
- In the Essentials server log files in /var/adm/CSCOPx/log for UNIX systems, and in NMSROOT/lib/jrun/jsm-cw2000/logs on Windows NT systems.
- In additional log files in /opt/CSCOPx/objects/jrun/jsm-cw2000/logs on UNIX systems, and in NMSROOT/log on Windows NT systems.
- In the Process Status dialog box. Select **CiscoWorks2000 Server > Administration > Process Management > Process Status**.

Troubleshooting

Use Table A-1 to help troubleshoot the Configuration Management application.

Table A-1 Configuration Management Troubleshooting Table

Symptom	Probable Cause	Possible Solution
The archive cannot retrieve the configuration module for Catalyst devices.	Incorrect password given when adding or importing the device.	Enter the correct Telnet and enable passwords for the Catalyst devices in the Essentials database. The configuration archive uses Telnet to gather module configurations for Catalyst devices.
The archive cannot retrieve the running configuration for a device.	Incorrect read and write community strings given when adding or importing the device.	Enter the correct read and write community strings in the Essentials database. You can also change the order of the protocols used to retrieve the configuration. (The configuration archive downloads configurations from devices using three different transport protocols in order: TFTP, Telnet, and rcp.)
The archive cannot retrieve the startup configuration for a device.	Incorrect password given when adding or importing the device.	Enter the correct Telnet and enable passwords for the device in the Essentials database. If the device is configured for TACACS authentication, add the TACACS username and password (not the Telnet password) in the Essentials database when you import the device. If the device is configured for local user authentication, add the local username and password in the Essentials database.
DNS hostname mismatch. The ip_address is unknown to DNS.	The device does not have the DNS server set up to resolve the hostname.	Make sure the DNS server can recognize the device hostname, or specify the IP address instead of the hostname.
SNMP timeout prevents TFTP from retrieving the running configuration for a device.	SNMP did not allow enough time for the operation.	Increase the SNMP timeout values.

Table A-1 Configuration Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Netsys error message: Error creating baseline.	Baseline creation on the Netsys server failed.	<ol style="list-style-type: none"> 1. Check the netsys_debug.log file on the CiscoWorks2000 server for error details. The file is located in the directory specified by the value of the environment variable PX_TMPDIR. 2. Check the -cb_run_ngs log file on the Netsys server for error details. The file is located in the directory specified by the value of the environment variable ECSP_TMPDIR.
Netsys error message: Error updating baseline.	Baseline updating on the Netsys server failed.	<ol style="list-style-type: none"> 1. Check the netsys_debug.log file on the CiscoWorks2000 server for error details. The file is located in the directory specified by the value of the environment variable PX_TMPDIR. 2. Check the -cr_run_ngs and -cb_run_ngs files on the Netsys server for error details. The files are located in the directory specified by the value of the environment variable ECSP_TMPDIR.
Netsys error message: Netsys report creation failed.	Netsys report creation on the Netsys server failed.	<ol style="list-style-type: none"> 1. Check the file netsys_debug.log on the CiscoWorks2000 server for error details. The file is located in the directory specified by the value of the environment variable PX_TMPDIR. 2. Check the files -cr_run_ngs and -cb_run_ngs on the Netsys server for error details. The files are located in the directory specified by the value of the environment variable ECSP_TMPDIR.

Table A-1 Configuration Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Netsys error message: Netsys report index creation failed.	Netsys report index creation on the Netsys server failed.	<ol style="list-style-type: none"> 1. Check the netsys_debug.log file on the CiscoWorks2000 server for error details. The file is located in the directory specified by the value of the environment variable PX_TMPDIR. 2. Check the -cr_run_ngs and -cb_run_ngs files on the Netsys server for error details. The files are located in the directory specified by the value of the environment variable ECSP_TMPDIR.
Network Show Commands execute command set error message: Sorry, no output for this command. Internal error.	The device is unreachable.	Enable the device.
	The device attributes have been changed.	Update the device attributes in the Inventory database by selecting Resource Manager Essentials > Administration > Inventory > Change Device Attributes .
Network Show Commands message: %Incomplete command.	Incomplete show command specified.	Instead of entering an abbreviated command, such as show ip , provide the complete command, for example show ip route .
Network Show Commands error message: The command you entered is not a valid command.	Used an invalid show command.	Enter a valid show command.

Table A-1 Configuration Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Network Show Commands error message: Failed to run show commands.	The wrong command has been entered for the device. For example, a switch command has been entered for a router.	Make sure you enter a command that is valid for the device.
Network Show Commands mail error message: SMTP not configured properly.	The SMTP server is not running on the mailer machine.	Make sure the SMTP server is running on the host.

Contract Connection

FAQs

What are the different types of serial numbers used in Contract Connection?

There are three types: two on the device and one in the inventory database:

- Shipment Serial Number, which is embedded on the chassis hardware.
- Electronic Serial Number, which you set using CLI when you introduce the device to the network.
- Managed Serial Number, which is the serial number reflected in the inventory database.

What do I do if the serial numbers are out of sync?

For Contract Connection to work properly, start with the Shipment Serial Number, because that is the serial number known to Cisco, and do the following:

-
- Step 1** Using the CLI, as described in the device configuration guide, make sure that the Electronic Serial Number matches the Shipment Serial Number.

- Step 2** Change the Managed Serial Number to match the other two using **Resource Manager Essentials > Inventory > Administration > Change Device Attributes**.
-

Why is the Electronic Serial Number field blank?

It is blank because it was not set in the device software when the device was introduced to the network. Update the number using the CLI, as described in the device configuration guide.

Inventory populates the Managed Serial Number using SNMP to get the MIB serial number information from the Electronic Serial Number setting. If the Managed Serial Number field is blank, the inventory collector could not collect the information for one of these reasons:

- The Electronic Serial Number field is not set. You can set this field by using the CLI as described in the device configuration guide, and update the inventory database by selecting **Resource Manager Essentials > Inventory > Administration > Change Device Attributes**.
- The device does not support MIBs for serial numbers. Select **Resource Manager Essentials > Inventory > Administration > Change Device Attributes** to enter the information in inventory.

Inventory

FAQs

Where can I find out what devices are supported by Inventory?

Select **CiscoWorks2000 Server > About CiscoWorks2000 > Applications and Versions**. Under CW2000 Installed Applications, click Inventory manager to see a list of the supported devices.

What main methods do I have for performing data collection?

You have the Schedule Collection option (**Resource Manager Essentials > Administration > Inventory**) or the Update Inventory option (**Resource Manager Essentials > Administration > Inventory**).

Schedule Collection is the “heavyweight” collection method. It collects on all managed devices at a scheduled time and updates the database.

Update Inventory collects information only on the devices you specify, and it collects the information right away. Update Inventory uses the same collection mechanism as Schedule Collection.

How often should I run Schedule Collection?

You should run the Schedule Collection option at least once a week. If your system has more than 100 devices, you might not want to run Schedule Collection that often because it could place too heavy a load on your network. To detect changes in managed devices with the least impact on your network, use the Inventory Poller option.

What does the Inventory Poller do?

The Inventory Poller uses a “lightweight” mechanism to determine whether database information is out-of-date. Although the Inventory Poller itself does not perform an actual collection, it determines whether any device information is out-of-date. If information is outdated, the Inventory Poller initiates a full collection on the pertinent devices.

How do I know when a schedule collection was last performed and how long it took?

The Scan History option (**Resource Manager Essentials > Inventory > Scan History**) will give you this information.

How can I see the most recent changes?

To view inventory changes made in the last 24 hours, use the Inventory Change Report option (**Resource Manager Essentials > 24-Hours Reports**).

To view changes made since the last scheduled collection, use the Change Audit application.

Why is the Device Serial Number field blank in inventory?

The field is blank because inventory could not obtain the information from the device. This is due to one of these reasons:

- The serial number was not set in the device software when the device was introduced to the network. This should have been done using CLI, as described in the device configuration guide.
- The device does not support MIBs for serial numbers.

In either case you can set the serial number in the inventory database by selecting **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**, and setting the field to the serial number printed on the device chassis.

How can I make sure a device's serial number is correct, and fix it if it is wrong?

The serial number in inventory should always match the number printed on the chassis. If the serial number does not match the number on the chassis, change it using **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**.

Troubleshooting

Use Table A-2 to troubleshoot the Inventory application.

Table A-2 *Inventory Troubleshooting Table*

Symptom	Probable Cause	Possible Solution
Device import from local database fails. (Solaris only.)	The user casuser is not a member of the CiscoWorks groups.	Add group membership before starting Essentials.
	The name resolution is incorrect.	Correct the name resolution. If that is not possible, then apply remote import rules; add .rhosts to the casuser home directory.
Device import from remote NMS fails.	Essentials and the remote NMS reside in different DNS domains.	Set up Essentials and the remote NMS stations in the same DNS domains.

Table A-2 *Inventory Troubleshooting Table (continued)*

Symptom	Probable Cause	Possible Solution
The device serial numbers or the router chassis numbers differ from those on outside labels.	Hardware reports get data from the user-defined optional serial number field when the device or router is added to Essentials (or through Change Device Attributes), not from the SNMP variable chassis serial number. The user-defined serial number takes precedence over the outside label number.	No action is required. However, you might want to change the serial number so that it matches the outside label number by selecting Resource Manager Essentials > Inventory > Change Device Attributes .

Table A-2 Inventory Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
The device stays in a pending state.	The database is corrupt.	<p>Stop Essentials. Install a backup database, if you have one; otherwise, install the basic database, px.db, over the corrupt database.</p> <ol style="list-style-type: none"> Back up or rename the corrupted database files: <ul style="list-style-type: none"> CSCOpX/databases/rme/rme.db CSCOpX/databases/rme/syslog.db Install the basic database files: <ul style="list-style-type: none"> From CSCOpX/databases/rme/orig/rme.dborig to CSCOpX/databases/rme/rm.db From CSCOpX/databases/rme/orig/syslog.dborig to CSCOpX/databases/rme/syslog.db <p>Both files must be copied into the database location and must be owned by user casuser and group casusers on both Windows NT and UNIX systems.</p>
	The DIServer is not running.	Check the process status. If the DIServer is not running, restart it.
	A broadcast address has been imported and is being used for an SNMP write.	<p>Suspend the device. Run the address validation tool on the device by selecting</p> <p>CiscoWorks2000 Server > Diagnostics > Connectivity Tools > Validate Device Addresses to ensure that a broadcast address or network address is not being used.</p>

Table A-2 *Inventory Troubleshooting Table (continued)*

Symptom	Probable Cause	Possible Solution
Devices are not importing.	The access list is applied to the SNMP-server community configurations.	Add the permissions to the access lists on all routers.
	There has been an SNMP timeout.	Increase the SNMP slow timeout and slow retry values.
	Reverse DNS lookup failed.	Add a device entry to the localhost file.
	The device name is not configured in the DNS or localhost file.	Add a device entry to DNS or localhost file.
Cannot add a device to the database.	The HPOV/SNMP has an old version of wsnmp.dll files.	Remove or rename HP OpenView version of the wsnmp.dll files.

Software Management

FAQs

A comprehensive list of Software Management FAQs can be found at:

<http://www.cisco.com/warp/public/477/31.html>

Troubleshooting

Use Table A-3 to troubleshoot the Software Management application.

Table A-3 Software Management Troubleshooting Table

Symptom	Probable Cause	Possible Solution
The approver cannot change the scheduled time for the Distribute Images job using Software Management.	Job Approval is enforced on the Distribute Images jobs.	Create a new job and submit it for approval. When the Distribute Images job requires approval, Software Management does not allow you to change the scheduled time for the job from the Browse Jobs screen.
Cannot undo an upgrade on Microcom firmware and Catalyst devices.	Undoing a software upgrade is not supported on the devices.	Check the Supported Device Matrix in online help for the supported devices and software releases.
Distribute Images and Image Import jobs fail on a device.	Defective software is running on the device.	Go to CCO and examine the software image. If it is deferred, contact your TAC representative. If the software image is not deferred: <ol style="list-style-type: none"> 1. Select Resource Manager Essentials > Administration > Software Management > Edit Preferences. 2. Select Enable Debugging. 3. Rerun the job and then use the Mail or Copy Log File option to extract Software Management debugging information. 4. Send the information and a complete description of the problem to your TAC representative.
A job is in a pending state after the scheduled time.	The Essentials server is not functioning correctly, has been powered off, or has been rebooted before the scheduled time.	Software Management moves the job to an error state 1 hour after the scheduled time. Do not change the job while it is pending; the system will take care of it. If necessary, create another job.

Table A-3 Software Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
A job is running, but the Job Details report shows no progress.	The Essentials server is not functioning correctly, has been powered off, or was rebooted while the job was running, causing the job to stop.	Software Management moves the job to an error state 1 hour after the scheduled time. Do not change the job while it is pending; the system will take care of it. If necessary, create another job.
While modem or CIP microcode images are being added to the Software Management library, the image type is displayed as Unknown. Software Management cannot retrieve attributes from images.	Images for the 3640 digital modems are not imported in an AS5300 format file.	Download a supported version of the software or firmware from http://www.cisco.com . Check the Supported Device Matrix in online help for the supported devices and software releases.
	The Microcode firmware image is not combined firmware/DSP code.	
	The CIP Microcode version is older than 22.0	
Cannot schedule Distribute Images and Image Add jobs.	The at service is not running or is configured incorrectly.	If Essentials is running on a Windows NT system, select Control Panel > Services and check that the service is running. If it is not, start it manually. If Essentials is running on a Solaris system, make sure the /usr/bin/at command is present. Also make sure that the at.deny file in the /usr/lib/cron directory does not contain the casuser username.
Essentials cannot upload images from a device.	Essentials needs read-write SNMP access to the device.	Configure the read-write SNMP string on the device.
The Mail or Copy Log File function does not mail log files. (Windows NT only.)	The e-mail address is incorrect.	Enter the correct e-mail address in the Mail or Copy Log File options.

Table A-3 Software Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Software Management does not recognize the Mica/Microcom/CIP cards on an AS5x00 or 7x00 device.	The devices are running an unsupported version of IOS system software.	Check the Supported Device Matrix in online help for supported devices and software releases.
Rcp is not being used to transfer software images between the Essentials server and devices.	The device does not support rcp protocol. (Only Cisco IOS devices support rcp.) Or Rcp is not properly configured on the Essentials server.	<ol style="list-style-type: none"> 1. Make sure your device is IOS-based. 2. Make sure that rcp is defined as the preferred protocol. 3. Select Resource Manager Essentials > Administration Inventory > System Configuration to make sure that an rcp username is configured. <hr/> <p>If Essentials is running on a Windows NT system:</p> <ol style="list-style-type: none"> 1. Verify that the CRMrsh service is running correctly using Control Panel > Services. 2. If the service is stopped, start it manually. 3. Launch the Event Viewer from the Administrative Tools group to make sure that the service has started properly. <hr/> <p>If Essentials is running on a Solaris system, make sure that the home directory for the rcp user account has an .rhosts file in it and that the user casuser has write privileges.</p>

Table A-3 Software Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
The options to Browse Bugs by Device and Locate Devices by Bugs result in the internal error: Can't resolve address for proxy.	The proxy or DNS configuration is incorrect.	<ol style="list-style-type: none"> 1. Make sure the proxy URL is set up correctly. Select Resource Manager Essentials > Administration > Inventory > System Configuration. 2. If you configure a hostname for the proxy URL, check for the DNS configuration on the Essentials server. 3. Make sure that you are not required to enter a login each time you access the system. Multiple logins are not supported. <p>If none of the previous steps correct the error:</p> <ol style="list-style-type: none"> 1. Run your Internet browser on the server where Essentials is installed. 2. Configure the proxy in the browser. 3. Check to see if you can access www.cisco.com. 4. Call TAC and tell them the actions you have taken to troubleshoot the error and the results.
The Schedule Synchronization Job report is not mailed. (Windows NT only.)	Incorrect e-mail address.	Correct the e-mail address in the Schedule Synchronization Job option.
	The SMTP server is not configured.	Configure the SMTP server by selecting Resource Manager Essentials > Administration > Inventory > System Configuration .
Unable to download IOS (error 4151).	The /var/tmp file has insufficient space to accommodate the IOS image.	Increase the /var/tmp space.

Table A-3 Software Management Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
The CCO Upgrade Analysis screen and the Recommend Image Upgrade screen time out.	The connection to CCO from the Essentials server is slow.	Configure CCO filters or select fewer numbers of devices and then retry the operation.
	The CCO server is down.	If these actions do not work, follow the instructions specified for the symptom: The Browse Bugs by Device and Locate Devices by Bugs options result in the internal error: Can't resolve address for proxy.
	The CCO filters are not configured correctly.	
The upgrade failed.	Software Management does not allow an upgrade from version 4.0 software to version 4.2 X.25 software on the Cisco 700 series.	Upgrade the device to version 4.1 (any feature set), and then upgrade to version 4.2 X.25 software image.

Syslog Analysis

FAQs

Why am I not getting syslog messages for my devices?

You might not be getting syslog messages for one of the following reasons:

- The device is not managed by Essentials.
- The syslog parameters are not enabled correctly on the device.
- Too many messages are being received by the syslog program. On Windows NT systems, logging for the PIX firewall has a tendency to lock the syslog function due to the massive number of messages from the firewall.
- Filters might be applied to incoming syslog messages. By default, Link Up/Down, PIX, Severity 7, and IOS Firewall Audit Trail messages are filtered out.

Why does the syslog window appear to lock up when daily syslog messages are being retrieved?

The query program used by syslog generates large (1.5 MB and greater) HTML pages in table format, and some HTML programs have problems viewing pages this large. It might take a little longer to display large syslog reports.

Where does Essentials keep syslog messages?

Look in /etc/syslog.conf to see in which files the syslog information is logged. Essentials uses only the syslog file for local7 to get information for the network devices and then writes the information to the /var/adm/CSCOpX/log/dmgt.d.log file.

Where can I get the description of the error messages?

To get the description of the error messages follow either of these procedures:

Procedure 1

-
- Step 1** Select **Resource Manager Essentials > Syslog Analysis > Standard Reports**.
 - Step 2** Select the views and devices of the report you want then click **Next**. The Select Dates and Report Type dialog box appears.
 - Step 3** Select the report type and the dates for the report.
 - Step 4** Click **Finish**.
 - Step 5** Click on * in the details column for the respective device name.
-

Procedure 2

-
- Step 1** Select **Resource Manager Essentials > Syslog Analysis > Unexpected Device Report**.
 - Step 2** Select the dates for the report.
 - Step 3** Click **Finish**.
 - Step 4** Click on * in the details column for the respective device name.
-

Troubleshooting

Use Table A-4 to troubleshoot the Syslog application.

Table A-4 Syslog Troubleshooting Table

Symptom	Probable Cause	Possible Solution
Filters are not taking effect.	It takes about 5 minutes for filters to propagate to process.	If you need the filters to take effect immediately, restart the remote Syslog Analyzer Collector.
Message source is given as ??? (Solaris only.)	The syslogd is unable to resolve the source address of the network device sending the message.	Add a name resolution for the device to DNS, /etc/host, and similar items. Install Solaris patch 103291-02. This will change the ??? to an octal IP address in brackets [171.69.219.72]. This allows the format to be parsed by the syslog analyzer.
New messages are not appearing in reports after changing syslog message file using Syslog Analysis > Change Storage Options.	A new filename needs to be defined in the configuration information.	On Windows NT systems, run the registry editor, regedit. Then set the parameters to the name of the file for logging the syslog messages on HKEY_LOCAL_SYSTEM > System > CurrentControlSet > Services > crmlog. On Solaris systems, modify the /etc/syslog.conf file. (For more information, refer to the Solaris man pages.)

Table A-4 Syslog Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Logging is enabled in the IOS/Catalyst device to send messages to Essentials, but it is not working.	<p>The syslog daemons are not running properly.</p> <p>Messages sent to the Essentials server by network devices are logged by a process independent of the Syslog Analyzer.</p> <p>On Solaris systems, this process is syslogd and on Windows NT systems, this process is the Essentials syslog service.</p>	<ol style="list-style-type: none"> 1. Telnet to the device and log in. 2. Enter enable and the enable password. 3. Enter configure terminal. 4. Enter logging on. 5. Enter the IP address of the Essentials server to receive router messages. 6. Enter End. 7. On Solaris systems, view the file named in the local7.info line (default is /var/log/syslog_info) in the /etc/syslog.conf file. If this file does not exist, create one and make sure it can be accessed by syslogd. 8. On Windows NT systems, view the file in C:\Program Files\CSCOPx\log\syslog.log. 9. Send an HUP signal to syslogd (kill -HUP 'cat/etc/syslog.pid'). <p>If the syslog message from the device is not in the syslog file, check device configuration.</p> <p>If the syslog message is in the syslog file, make sure that the syslog daemons are running properly:</p> <ul style="list-style-type: none"> • On Solaris systems, enter /usr/ucb/ps -aux grep syslogd • On Windows NT, go to the Control Panel and make sure the Essentials syslog service is running.
	The device is configured incorrectly.	Make sure the device is logging to the correct Essentials server. (Refer to the device documentation for details on enabling syslog.)

Table A-4 Syslog Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
No messages appear on any generated syslog report.	Network devices are not sending messages to the Essentials server.	Select Resource Manager Essentials > Administration > Syslog Analysis > Collector Status to examine the Syslog Analyzer Collector status. If the numbers are all zeros, make sure that network devices are sending messages to the Essentials server. (Refer to procedures for setting up an IOS/Catalyst device.)
Remote collector error message: Could not start the Syslog collector service on the server_name ERROR 0002: The system cannot find the file specified. (Windows NT only.)	Installation failure.	Install a remote collector on a Windows NT system by entering sacNTService/install1 . Do not add an .exe extension to the file name.
Remote collector error messages: Could not start the Syslog collector service on the server_name ERROR 1067: The process terminated unexpectedly” and “SacNTService: The service cannot be started without the properties file specified, please specify the properties file you want to use.” (Windows NT only.)	Configuration failure.	<ol style="list-style-type: none"> 1. Configure the remote collector. Select Control Panel > Services. 2. Select Cisco Syslog_Collector. 3. In the Startup Parameters field, enter the location of your SAenvProperties.ini file, for example: <pre>-pr c:\\temp\\SAenvProperties.ini.</pre> Remember to use \\ to separate the directory paths.

Table A-4 Syslog Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
The remote collector is not running properly when it is installed and started on a non-Essentials machine.	Incorrect configuration parameters.	<ol style="list-style-type: none"> 1. Check the remote collector table for the name and status of the remote collector. 2. Make sure that the parameter SAC_SERVER is set to the hostname of the Essentials server. 3. On Solaris systems, view the SAEnvProperties.ini file located in the following directory: <code>/opt/CSCOsac/lib/classpath/com/cisco/nm/sysloga/sac</code> 4. On Windows NT systems, view the SAEnvProperties.ini file and ensure that the parameter SAC_PORT is set to 514. 5. Perform the ping command using the hostname to ensure that the remote collector can be reached.
Remote collector messages in syslog file, but not in reports.	Running incorrect version of Java.	Install Java 1.1.6 or later.
	Remote collector has stopped.	<p>On Solaris systems, check if the remote collector has stopped by entering:</p> <pre><code>/usr/bin/ps -f grep java.</code></pre> <p>Restart the remote collector by entering:</p> <pre><code>sh /opt/CSCOsac/lib/sacStart.sh.</code></pre>
	Remote collector is not installed correctly.	<p>On Windows NT systems, check using Control Panel > Services. If Syslog_Collector is not listed, reinstall the remote collector by entering:</p> <pre><code>SacNTService.exe /install.</code></pre> <p>If the collector is installed but not running, start the remote collector from the Control Panel > Services dialog box. Remember to specify the properties file using the -pr option.</p>

Table A-4 Syslog Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Reports are empty even though messages on Solaris systems are appended to /var/log/syslog_info and on Windows NT systems to C:\Program Files\CSCOpX\log\syslog.log.	Processes are not running properly.	<ol style="list-style-type: none"> 1. Select CiscoWorks2000 Server > Administration > Process Management > Process Status and make sure the syslog analyzer is running properly. If it is not, restart it. 2. Make sure the CMLogger, RmeOrb, and DBServer processes are running. If they are not, restart the system.
	Timestamp problem.	<p>If the Messages Processed counter is not zero, check the timestamp for a message in the syslog file. If there are two timestamps, and the second timestamp is current, the syslog analyzer uses the second. If it is older than 7 days, the reports will not display it.</p> <p>If the Messages Processed counter is zero and the Messages Filtered counter is not zero, change the filters.</p> <p>If the Messages Processed and the Messages Filtered counters are zero, but the Invalid Messages counter is not zero, contact your TAC representative.</p>

Table A-4 Syslog Troubleshooting Table (continued)

Symptom	Probable Cause	Possible Solution
Unexpected Device report contains syslog messages that should not be in the standard report.	The messages are from a managed device but there is a name resolution problem.	<p>Syslog analyzer uses all IP addresses associated with the device name to try to map it to a device managed by Inventory Manager. Verify the device-name-to-IP-address mapping:</p> <ol style="list-style-type: none"> 1. On Windows NT systems, view the syslog.log file in C:\Program Files\CSCOPx\log. On Solaris systems, view the syslog_info file in /var/log. <p>Note the source of the messages (hostname appears immediately after the timestamp).</p> <ol style="list-style-type: none"> 2. Obtain a list of IP addresses (perform nslookup on the device name at the command prompt). 3. Select Resource Manager Essentials > Inventory > Detailed Device Report to generate a report. 4. In the Network Address column, verify that the IP addresses returned from nslookup appear on the list. If any IP addresses are not on the list, the mapping is incorrect. 5. Update the naming services (DNS,/etc/hosts, etc.) with the missing IP addresses.

CiscoWorks2000 Server

FAQs

What kind of directory structure does CiscoWorks2000 use when backing up Resource Manager Essentials data?

CiscoWorks uses a standard database structure for backing up all suites and applications.

A sample directory structure for the CiscoWorks2000 server (represented by the rme acronym) follows. The Essentials directory has two databases: rme and syslog.

Table A-5 Sample Essentials Backup Directory

Directory Path	Description	Usage Notes
/tmp/1	Number of backups	1, 2, 3, ...
/tmp/2/rme	Application or suite	Essentials backs up all application data, including images, configuration files, and other data.
/tmp/1/rme/filebackup.tar	All CiscoWorks2000 server application tar files	Application data is stored in datafiles.txt and is compiled into tar file.
/tmp/1/rme/database	Essentials database directory, which includes both Essentials and syslog databases	Files for each database: <ul style="list-style-type: none"> • xxx_DbVersion.txt • xxx.db database files • xxx.log database log files • xxx.txt database backup manifest file

Can I back up the database for a single application?

No. You cannot back up the database for individual applications or suites (if you have more than one installed). CiscoWorks2000 backs up all suite databases using the Back Up or Schedule Back Up options. You can restore or move suite-specific pieces when required. To restore only the Essentials database, specify the rme.db.

How do I find out which devices are supported by a particular application?

Select **CiscoWorks2000 Server > About CiscoWorks2000 > Applications and Versions**. Under CW2000 Installed Applications, click the application name to see a list of the supported devices.

How do I enable or disable Java plug-in?

For applications for which the plug-in is optional, you can either enable or disable Java plug-in.

To enable or disable Java Plug-in:

-
- Step 1** Select **Server Configuration > Setup > Java Plug-in Use**.
- Step 2** Click **Enable** or **Disable**.
- Step 3** Click **Finish**.
-

