



Troubleshooting Essentials

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



Tip

For the latest technical tips, suggestions for troubleshooting common issues, and frequently asked questions (FAQs) on most Essentials applications, you can go to the following URL:

http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Software:Cisco_Resource_Manager_Essentials&s=Implementation_and_Configuration#Samples_and_Tips

- [Change Audit FAQs](#)
- [Configuration Management](#)
- [Contract Connection](#)
- [Inventory](#)
- [Software Management](#)
- [Syslog Analysis](#)
- [Data Extracting Engine](#)
- [CiscoWorks Server](#)

Change Audit FAQs

- Q.** Can I track every configuration change made to routers and switches in my network and who made them?
- A.** 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

Configuration Management FAQs

- Where can I find out what devices are supported by Configuration Management?
- If I import devices from a remote NMS, can I compare the startup vs. running configurations?
- Can I run Network Show Command sets for more than 10 devices?
- How many Network Show Commands are allowed per command set?
- Can I run all device commands using Network Show Commands?
- If I'm having problems with the Network Show Commands option, where can I check for error messages?
- I cannot unlock the device by the usual means. I need to go to CFG_ARCHIVE_LOCK. What is the procedure?
- Using RME, how do I configure Telnet credentials on a device by SNMP?

- Using RME, how do I configure SSH credentials on a device by SNMP?
- Q.** Where can I find out what devices are supported by Configuration Management?
- A.** Select **Server Configuration > About the Server > Applications and Versions**. Under the Applications Installed, click Configuration Archive to see a list of supported devices.
- Q.** If I import devices from a remote NMS, can I compare the startup vs. running configurations?
- A.** Yes, but first you must:

Step 1 Select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**.

You can select all the devices with the same passwords, or you can change the TACACS usernames and passwords.

Step 2 Update the device credentials for all the devices.

- Q.** Can I run Network Show Command sets for more than 10 devices?
- A.** Yes. You can run command sets for more than 10 devices if you:
 - Schedule a job with Batch Reports. You can schedule this job either from the Network Show GUI or from the Network Show CLI.
 - Run the command sets for immediate execution from the Network Show CLI. (The commands that you must use are:
`cwconfig netshow -device device list -execcmdset cmdsetlist -execcmd remotecmd list`).

However, if you run the Network Show command sets for immediate execution from the Network Show GUI, then you can run them only for a maximum of 10 devices.

- Q.** How many Network Show Commands are allowed per command set?
- A.** Each command set can contain a maximum of 6 commands from each device type. The supported device types are:
- IOS devices (Routers)
 - Catalyst switches
 - FastSwitch devices
 - Content Engine
 - Content Service switches
 - PIX Firewall devices.

- Q.** Can I run all device commands using Network Show Commands?

- A.** No. Network Show supports only these commands:

`show, ping, traceroute, help, where, ?, and version.`

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

- A.** You can check for messages in these locations:

- The Java console available with your browser.
- In the Process Status dialog box. Select **Server Configuration > Administration > Process Management > Process Status.**

- Q.** I cannot unlock the device by the usual means. I need to go to CFG_ARCHIVE_LOCK. What is the procedure?

- A.** A locked config file can only be unlocked through the application that has locked the config file.

For example, if you had checked out the config file using Config Editor, you should undo the check out of the config file using Config Editor, and not any other application. For example, if the config file has been checked out using Config Editor, then you cannot use cwconfig to unlock the file. The undo operation will fail.

Procedures to unlock the Config File and Device in different environments

- [Unlocking the Config File using Config Editor](#)
- [Unlocking the Config File using cwconfig](#)
- [Unlocking the Device](#)

Unlocking the Config File using Config Editor

To unlock the config file using Config Editor:

-
- Step 1** From the Config Editor screen of RME, choose **Tools > List Checkedout Files**.
A list of checked out files is displayed.
- Step 2** Select the config file to be unlocked from the list of checked out files.
- Step 3** Click **Undo Checkout**.
The Config file is unlocked.
-

Unlocking the Config File using cwconfig

Execute the following command to unlock a config file that has been locked by the cwconfig application:

```
cwconfig unlock
```

For more details on using cwconfig, see cwconfig manpages.

For more information on cwconfig command see the Resource Manager Essentials online help (**Resource Manager Essentials > Configuration Management > Using cwconfig**).

Example A-1 Example Usage of cwconfig on Solaris:

```
server# pwd  
/opt/CSCOpX/bin
```

```
server# ./cwconfig unlock -u <Username> -p <Password> -device  
10.76.38.141
```

```
* Warning * The -p option is highly insecure and *not* recommended.  
* Warning * See -u option for more details.
```

SUMMARY

Successful 10.76.38.141

Example A-2 Example Usage of cwconfig on Windows:

```
E:\RME>cwconfig unlock -u <Username> -p <Password> -device
10.76.38.140
```

```
* Warning * The -p option is highly insecure and *not* recommended.
* Warning * See -u option for more details.
```

SUMMARY

Successful 10.76.38.140

Unlocking the Device

To unlock the device:

Step 1 From the CiscoWorks desktop, select **Server Configuration > Administration > Job Management**.

The Job manager dialog box appears.

Step 2 In the lower panel of the dialog box, select the device that needs to be released.

Step 3 Click **Free Resource**.

The device will be released.

On your RME server, for more details, see the Server Configuration online help. (Select **Server Configuration > Administration > Job Management > Managing Jobs and Resources**.)

Q. Using RME, how do I configure Telnet credentials on a device by SNMP?

A. The procedure is to edit the config file of the device and push it back to the device using TFTP protocol.

Procedure

- Step 1** Export the config file from the archive using the following command on the RME server machine:

```
cwconfig export -u username -p password -device device -f filename
```

If you have set the CWCONFIGFILE Environment variable, then we do not need to give the -u and -p parameters.

For the description, let us say the exported archive is stored as “example”.

Example A-3 Running cwconfig export command

```
E:\Program Files\CSCOpX>cwconfig export -u username -p password  
-device 10.76.38.148 -f example
```

```
* Warning * The -p option is highly insecure and *not* recommended.
```

```
* Warning * See -u option for more details.
```

```
SUMMARY
```

```
Successful 10.76.38.148
```

```
E:\Program Files\CSCOpX>
```

- Step 2** Edit the “example” file to change the passwords to what you want.

Example A-4 Edit the following lines to change the password, if you are using simple authentication mechanism.

```
line vty 0 4
```

```
password password
```

```
enable password password
```

- Step 3** Save the file after editing.

- Step 4** Download this config file (“example”) to the device using the following command on the RME server machine.

```
cwconfig import -u username -p password -device device -f filename
```

Example A-5 Running cwconfig import command

```
E:\Program Files\CSCOpX>cwconfig import -u username -p password -device  
10.76.38.148 -f example
```

```
* Warning * The -p option is highly insecure and *not* recommended.
* Warning * See -u option for more details.
```

SUMMARY

```
Successful 10.76.38.148
E:\Program Files\CSCOp>
```

Important Points to Remember

- Using the import command merges the modified config file with the running-config file of the device.
- For more details on passwords refer to:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_command_reference_chapter09186a008010a7b8.html
- Instead of the import command, write2run command can also be used which will download only the modified lines. However, write2run command in cwconfig does not erase commands in the running-config of the device, and this is a known issue.

For example, if the running config has the following two commands:

```
cdp timer 125
cdp holdtime 125
```

And then you export the config from the archive using export command, remove these two lines from the file and use write2run to write into the running-config file. Even though the status reported is successful, the commands are still there in the running-config of the device.

The workaround for this is to edit the file and insert "no" in front of the commands that should be removed, instead of removing it.

- For more information on cwconfig command see the Resource Manager Essentials online help (**Resource Manager Essentials > Configuration Management > Using cwconfig> cwconfig Command Man Page**).

- Q.** Using RME, how do I configure SSH credentials on a device by SNMP?
- A.** The procedure is to edit the config file of the device and push it back to the device using TFTP protocol.

Procedure

- Step 1** Export the config file from the archive using the following command on the RME server machine:

```
cwconfig export -u username -p password -device device -f filename
```

If you have set the CWCONFIGFILE Environment variable, then we do not need to give the -u and -p parameters.

For the description, let us say the exported archive is stored as “example”.

Example A-6 Running cwconfig export command

```
E:\Program Files\CSCOpX>cwconfig export -u username -p password  
-device 10.76.38.148 -f example
```

```
* Warning * The -p option is highly insecure and *not* recommended.
```

```
* Warning * See -u option for more details.
```

```
SUMMARY
```

```
Successful 10.76.38.148
```

```
E:\Program Files\CSCOpX>
```

- Step 2** Edit the “example” file to change the passwords to what you want.

Example A-7 Adit/Edit the following lines to change the password, if you are using simple authentication mechanism.

```
username username password 0 password
```

```
enable password password
```

- Step 3** Save the file after editing.

- Step 4** Download this config file (“example”) to the device using the following command on the RME server machine.

```
cwconfig import -u username -p password -device device -f filename
```

Example A-8 Running cwconfig import command

```
E:\Program Files\CSCOpX>cwconfig import -u username -p password -device  
10.76.38.148 -f example
```

```
* Warning * The -p option is highly insecure and *not* recommended.
```

* Warning * See -u option for more details.

SUMMARY

Successful 10.76.38.148

E:\Program Files\CSCOpX>

Important Points to Remember

- Using the import command merges the modified config file with the running-config file of the device.
- For more details on passwords refer to:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_command_reference_chapter09186a008010a7b8.html
- Instead of the import command, write2run command can also be used which will download only the modified lines. However, write2run command in cwconfig does not erase commands in the running-config of the device, and this is a known issue.

For example, if the running config has the following two commands:

```
cdp timer 125
cdp holdtime 125
```

And then you export the config from the archive using export command, remove these two lines from the file and use write2run to write into the running-config file. Even though the status reported is successful, the commands are still there in the running-config of the device.

The workaround for this is to edit the file and insert "no" in front of the commands that should be removed, instead of removing it.

- For more information on cwconfig command see the Resource Manager Essentials online help (**Resource Manager Essentials > Configuration Management > Using cwconfig> cwconfig Command Man Page**).

Troubleshooting Configuration Management

Use [Table A-1](#) to help troubleshoot the Configuration Management application.

Table A-1 Configuration Management Troubleshooting

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 hostname 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.

Table A-1 Configuration Management Troubleshooting (continued)

Symptom	Probable Cause	Possible Solution
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.
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.
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

Contract Connection FAQs

- [What are the different types of serial numbers used in Contract Connection?](#)
- [What do I do if the serial numbers are out of sync?](#)
- [Why is the Electronic Serial Number field blank?](#)

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

A. 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.

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

A. 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**.

- Q.** Why is the Electronic Serial Number field blank?
- A.** 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

Inventory FAQs

- [Where can I find out what devices are supported by Inventory?](#)
- [What main methods do I have for performing data collection?](#)
- [How often should I run Schedule Collection?](#)
- [What does the Inventory Poller do?](#)
- [How do I know when a schedule collection was last performed and how long it took?](#)
- [How can I see the most recent changes?](#)
- [Why is the Device Serial Number field blank in inventory?](#)
- [How can I make sure a device's serial number is correct, and fix it, if it is wrong?](#)

- Why am I receiving an error message, Write Community = INCORRECT although I have entered the correct Write Community String? This was done using the Inventory tasks, Add Devices or Change Device Attributes.
- Q.** Where can I find out what devices are supported by Inventory?
- A.** Select **Server Configuration > About the server > Applications and Versions**. Under Applications Installed, click Inventory Manager to see a list of the supported devices.
- Q.** What main methods do I have for performing data collection?
- A.** 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.
- Q.** How often should I run Schedule Collection?
- A.** 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.
- Q.** What does the Inventory Poller do?
- A.** 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.
- Q.** How do I know when a schedule collection was last performed and how long it took?
- A.** The Scan History option (**Resource Manager Essentials > Inventory > Scan History**) will give you this information.

- Q.** How can I see the most recent changes?
- A.** 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.
- Q.** Why is the Device Serial Number field blank in inventory?
- A.** 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.
- Q.** How can I make sure a device's serial number is correct, and fix it, if it is wrong?
- A.** 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**.
- Q.** Why am I receiving an error message, `Write Community = INCORRECT` although I have entered the correct Write Community String? This was done using the Inventory tasks, Add Devices or Change Device Attributes.
- A.** Check if you have dropped the system group from the view (read-view and write-view). The system group must be available for read and write operation. In MIB-II, the system group is available as the default.

Troubleshooting Inventory

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.
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.	See these troubleshooting FAQs: <ul style="list-style-type: none"> • How do I re-initialize the Essentials database on a Solaris system, if the Essentials database is corrupted and the database restore operation has failed? • How do I re-initialize the Essentials database on a Windows system, if the Essentials database is corrupted and the database restore operation has failed?
	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.	Suspend the device. Run the address validation tool on the device by selecting Server Configuration > Diagnostics > Connectivity Tools > Validate Device Addresses to ensure that a broadcast address or network address is not being used.
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

Software Management FAQs

- Can an option be provided during Software Management installation to update the `/etc/inetd.conf` file?
- How does Software Management handle proxy environments?
- Does Software Management support proxy with user authentication environments?
- When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an automatic backup performed?
- Can I set up a periodic download of Software Management images from Cisco.com?
- Is browser timeout something I should consider when downloading?
- Do bug reports work for both Cisco IOS and switches? How is the filtering done? Does Software Management document how much we can filter at a granular level?
- What are crypto images?
- When does Software Management use the RCP protocol to transfer images?
- Are there DNS dependencies for RCP to work properly for a device?
- Why does Software Management sometimes leave behind image files in the `tftpboot` directory after an upgrade?
- How much temporary space is required during image distribution?
- What is the maximum recommended number of devices per upgrade job?
- What is the default SNMP timeout used by Software Management? Can I configure it?
- At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
- Which Cisco IOS devices support bootldr images?
- Should I use special images with SWIM for 2900XL/3500XL devices?
- How can I speed up Image Recommendation?

- When a job is rejected, can it be edited or should I resubmit?
 - Can different group members edit jobs? What are the restrictions?
 - What is the role of the registry files in RME?
 - How do I upgrade Network Analysis Module (NAM) using Software Image Management (SWIM)?
 - The image imported from Cisco.com (CCO) or from the device, is staged into a temporary staging area. However, the status of the import job is Pending for Import. Why is this so?
 - Is the SNMP read-write community string needed for Software Management to work?
- Q.** Can an option be provided during Software Management installation to update the */etc/inetd.conf* file?
- A.** No. The Software Management installation automatically adds an entry in the */etc/inetd.conf* file to start the *in.tftpd* process.

**Note**

This process may not work in all environments. After installing, the administrator must ensure that the system is setup correctly to run the TFTP/RCP server.

- Q.** How does Software Management handle proxy environments?
- A.** Software management uses http protocol to communicate with Cisco.com for downloading images and their attributes. If you use http proxy for Internet connectivity, configure proxy URL information by selecting **Resource Manager Essentials > Administration > System Configuration**.
- Q.** Does Software Management support proxy with user authentication environments?
- A.** No.
- Q.** When a Software Management job is scheduled, how is the baseline determined? When I distribute a job, is an *automatic backup* performed?
- A.** There are two operations that import images from the network to the software library:
- Baseline tasks

- Synchronization

The baseline task (**Resource Manager Essentials > Software Management > Add Image to Library > Network**) should be done only once as a part of the initial setup. This imports the images running on the network to your library.

To keep the library synchronized with any new images and changes caused by upgrades from sources other than Software Management, schedule a synchronization job to run periodically at appropriate intervals.

When this synchronization job runs, it looks for differences between the library and the network and allows any new images to be imported. During job distribution, Software Management backs up the current running image only if the option to *backup current running image* or *TFTP fallback* was selected when the job was created.

- Q.** Can I set up a periodic download of Software Management images from Cisco.com?
- A.** No. However, you can schedule a one-time import from Cisco.com to occur at a later time. Software Management does not allow you to automatically import images from Cisco.com to the library based upon your preferences.
- Q.** Is browser timeout something I should consider when downloading?
- A.** The image import operation from Cisco.com and other devices can be done on a scheduled basis. Since this process runs as a background task on the server, the browser is not involved. However, when an immediate import operation is done, it is performed as a foreground task, and the browser can still timeout.
- Q.** Do bug reports work for both Cisco IOS and switches? How is the filtering done? Does Software Management document how much we can filter at a granular level?
- A.** Yes, bug reports are supported for both the Cisco IOS software and Catalyst switches. The filtering is done only on the basis of the software version and the platform. This means that a Cisco 2503 running IOS 11.3(2) will produce the same report as a Cisco 2511 access server running IOS 11.3(2).

In Software Management, the features and protocols enabled on the device are not taken into account. This can result in a large number of bugs being reported against a device, not all of which may be applicable to your environment. You must manually review the bugs to find those which may be important to you.

- Q.** What are crypto images?
- A.** Crypto images are software images that use 56-bit Data Encryption Standard (DES) (or higher) encryption, and are subjected to export regulations. You must be a registered Cisco.com user, and be eligible and authorized to download such images.
- Q.** When does Software Management use the RCP protocol to transfer images?
- A.** If you select the remote copy protocol (RCP) preference under **Resource Manager Essentials > Administration > Software Management > Edit Preferences**, Software Management uses the RCP protocol to transfer images (upload and download) to Cisco IOS software devices that support CISCO-FLASH-MIB.

Cisco Catalyst 5000 switches and Cisco 700 Series devices do not support RCP. Cisco IOS devices that do not support RCP include Cisco 7000 Series (RP-based 7000 only) and MC3810. All other Cisco IOS devices support the RCP protocol. Software Management always uses the TFTP protocol for config file updates on Cisco IOS devices.

- Q.** Are there DNS dependencies for RCP to work properly for a device?
- A.** Yes. If there are multiple IP addresses configured on the device, all IP addresses on the device must be configured using Domain Name System (DNS). Examples of devices with multiple IP addresses are those having many interfaces, with each interface configured with its own IP address, or a device that interfaces configured with primary and secondary IP addresses.

Configure the DNS so all IP addresses are resolved to the same host name. The host name in the DNS should match the hostname in the RME Inventory.
- Q.** Why does Software Management sometimes leave behind image files in the tftboot directory after an upgrade?

- A.** Software Management removes the image files from the tftpboot directory after the upgrade unless the *tftp fallback* job option is set. If the *tftp fallback* option is set, Software Management uploads the image from the device and leaves it in the tftpboot directory for fallback.

Software Management also modifies the boot system commands on the device to add a fallback command to boot from the original image on the Essentials TFTP server if the upgraded image does not boot.

- Q.** How much temporary space is required during image distribution?
- A.** The amount of free space that is required depends upon the image file size and the number of devices that are being upgraded simultaneously. If the tftp fallback option is set, additional free disk space is required to keep the current image in the tftpboot directory. Disk space is used both in the tftpboot and temp directories.
- Q.** What is the maximum recommended number of devices per upgrade job?
- A.** Each job upgrades devices sequentially. The duration of the upgrade varies depending on the network bandwidth and the type of devices being upgraded. The recommended maximum number of devices per job is 12.
- Q.** What is the default SNMP timeout used by Software Management? Can I configure it?
- A.** Software Management makes three attempts to connect to the device using SNMP. The first retry timeout interval of 10 seconds is not configurable. Subsequent retry timeout intervals are configurable and are based on the value in the slow timeout variable. To verify the timeout value, select **Resource Manager Essentials > Administration > System Configuration**.

If the initial attempt to connect to the device fails, Software Management waits three minutes before it attempts to connect again. The three minute wait enables routing protocol or spanning tree convergence to occur, which could have been initiated because another device was rebooted during the software upgrade.

The number of retries is not configurable. The underlying Software Management stack also tries three times to connect to the device. All the secondary addresses configured in DNS for the device are tried during each attempt.

- Q.** At what time will the images directory get created during the process of obtaining images from a device? Does this happen during the initial step?
- A.** The software images directory gets created at the time of importing an image to the library; however, this should be transparent to you.
- Q.** Which Cisco IOS devices support bootldr images?
- A.** The following Cisco IOS device families support bootldr images:
- Cisco 4500, 4700
 - Cisco 7500, RSP-based 7000
 - Cisco 7200
 - Access Servers 5200, 5300, 5800
 - Route Switch Module (RSM) on Catalyst 5000

Q. Should I use special images with SWIM for 2900XL/3500XL devices?

A. 2900XL/3500XL devices consist of the following images:

- Regular Cisco IOS Software Image.
- A TAR format HTML image that contains files for Visual Switch Manager.
- A TAR format image that contains both the above mentioned images.

Software Management uses the TAR format image as well as the Cisco IOS image. These images are posted on Cisco.com. When Add Image to Library from CCO/Slam Dunk is used, only these images are displayed.

The location for the 2900XL and 3500XL images on Cisco.com is as follows:
Cisco.com > Technical Support > Software Center > Cisco IOS Software.

- Q.** How can I speed up Image Recommendation?
- A.** If you include Cisco.com for Image Recommendation, try to limit the images by filtering (**Resource Manager Essentials > Administration > Software Management > Edit Preferences**).
- Q.** When a job is rejected, can it be edited or should I resubmit?
- A.** No. You cannot edit or retry the rejected job. You should schedule a new job.
- Q.** Can different group members edit jobs? What are the restrictions?

- A.** The only job attribute that can be edited is the schedule time for non maker-checker jobs. Any user who has the *netadmin* role defined can edit jobs or create new jobs; however, in the maker-checker model, the jobs can only be approved by users who are in the approver list specified during the creation of the job.
- Q.** What is the role of the registry files in RME?
- A.** Software Management manipulates the Windows registry to automatically manage remote authentication during the **rcp** transfers on Windows. The following registry parameters are important for **rcp** service on Windows:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\DEBUG
Dictates the amount of debug information written in the Windows event log. (Default = 0, Maximum = 0xff)
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rhosts
Contains the list of authenticated hosts that can run remote commands on this machine. This list is automatically managed by Software Management.
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\rusers
Contains the list of authenticated remote users that can run remote commands on this machine. This list is automatically managed by Software Management.
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crmrsh\Parameters\NoUserCheck
If set to 1, the remote user authentication is skipped or, in other words, any remote user from authenticated hosts can run commands on this machine. (Default = 0)

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cmrsh\Parameters\NoRhostCheck

If set to 1, the remote host authentication is skipped or, in other words, commands can be run on this machine from any remote machine. (Default = 0)

Q. How do I upgrade Network Analysis Module (NAM) using Software Image Management (SWIM)?

A. To upgrade NAM using using Software Image Management (SWIM):

- Ensure that the passwords for NAM's application and maintenance modes are the same.

This is because SWIM takes the password information from Inventory. However, Inventory requires the application mode password to manage the device, and SWIM requires the maintenance mode password to upgrade the device. Therefore, the passwords for NAM's application and maintenance modes should be the same.

- For a NAM card present in a Catalyst 6000 device running CatOS , ensure that you set auto logout to a value that is high enough to allow the copying of the new image.

This is because a NAM image is usually very large (nearly 65 MB), and it may take between 1 to 2 hours to copy this image during SWIM upgrade. We recommend that you set the auto logout to 0 to ensure that there is no auto logout while the image is being copied.

To set the auto logout value, use the CLI command, `set logout 0`.

For a NAM card present in a Catalyst 6000 device running IOS, ensure that you set exec timeout to a value that is high enough to allow the copying of the new image. We recommend that you set the exec timeout value to 0 (`exec-timeout 0 0`) on all the vty lines.

- Ensure that the htdocs directory under CSCOpX has enough space to stage the NAM image.

During the NAM upgrade, SWIM first copies the NAM image from the NMSROOT/CSCOpX/files/sw_images directory, to the NMSROOT/CSCOpX/htdocs/swimtemp directory and then copies the NAM image to the NAM card, using HTTP.

- Ensure that NAM is added with the correct Local User (root) and its password.
 - Ensure that NAM is added with the correct SNMP read/write community strings.
 - Ensure that the switch, which contains NAM, is added with the correct attributes.
- Q.** The image imported from Cisco.com (CCO) or from the device, is staged into a temporary staging area. However, the status of the import job is `Pending for Import`. Why is this so?
- A.** This is because information about some of the image requirements such as `minRAM`, `minFlash`, `minBootRom` etc., cannot be obtained from the image headers imported from Cisco.com (CCO) or from the device.

Therefore, you must enter this information before the check-in of these images into the Software Management library. To do this, click on the URL in the Import Job Results page.

- Q.** Is the SNMP read-write community string needed for Software Management to work?
- A.** 1900, 2820, VPN, 700, PIX, NAM devices do not need SNMP read-write community strings for Software Management upgrades.

However, devices such as 2900XL, 3500XL, 2950, 3550, 2500, 1600, 800, need SNMP read-write strings, for config update even though the Software Management upgrade is through Telnet.

For all other devices, read-write community strings are mandatory for Software Management upgrade.

Troubleshooting Software Management

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 Cisco.com 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 system, select Start > Programs > Administrative Tools > 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.	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 system:</p> <ol style="list-style-type: none"> 1. Verify that the CRMrsh service is running correctly using Start > Programs > Administrative Tools > 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.	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 Cisco.com from the Essentials server is slow.	Configure Cisco.com filters or select fewer numbers of devices and then retry the operation.
	The Cisco.com 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 Cisco.com 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

Syslog Analysis FAQs

[Why am I not getting syslog messages for my devices?](#)

[Why does the syslog window appear to lock up when daily syslog messages are being retrieved?](#)

[Where does Essentials keep syslog messages?](#)

[Where can I get the description of the error messages?](#)

Q. Why am I not getting syslog messages for my devices?

A. 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 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.
- Q.** Why does the syslog window appear to lock up when daily syslog messages are being retrieved?
- A.** 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.
- Q.** Where does Essentials keep syslog messages?
- A.** For the location of the log file that contains syslog information, check the Message Source field in the Change Storage Options dialog box. (To invoke the Change Storage Options dialog box select **Resource Manager Essentials > Administration > syslog Analysis > Change Storage Options.**) Essentials uses only the syslog file for local7 to get information for the network devices.
- Q.** Where can I get the description of the error messages?
- A.** 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 Syslog Analysis

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 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 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 systems, view the file in <i>NMSROOT</i>\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 <code>/usr/ucb/ps -aux grep syslogd</code> • On Windows, 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 only.)	Installation failure.	Install a remote collector on a Windows system by entering <code>SacNTService/install</code> . 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 only.)	Configuration failure.	<ol style="list-style-type: none"> 1. Configure the remote collector. Select Start > Programs > Administrative Tools > Services. 2. Select Cisco Syslog_Collector. 3. In the Startup Parameters field, enter the location of your SAenvProperties.ini file, for example: <code>-pr c:\\temp\\SAenvProperties.ini</code> 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 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 systems, check using Start > Programs > Administrative Tools > 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 Start > Programs > Administrative Tools > Services dialog box. Remember to specify the properties file using the <code>-pr</code> 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 systems to NMSROOT\log\syslog.log.	Processes are not running properly.	<ol style="list-style-type: none"> 1. Select Server Configuration > 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 systems, view the syslog.log file in <i>NMSROOT</i>\log. On Solaris systems, view the syslog_info file in /var/log. Note the source of the messages (hostname appears immediately after the timestamp). 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.

Data Extracting Engine

Data Extracting Engine FAQs

Data Extracting Engine FAQs

The following is the list of frequently asked questions asked about DEE:

- The Inventory Schema shows a number of elements. I am not able to see many of them in the output. Why?
- What is ComputerSystemPackage Class?
- Where does DEE collect the configuration information from?
- Do we have the schema for the running configuration output?
- Is the containment hierarchy in inventory schema exactly the same as that in CIM?
- What is an XSD file?
- What is the AdditionalInformation tag in the inventory schema used for?
- How do I know what fields come under AdditionalInformation?
- Where can I find information specific to a particular node which I can see in detailed device information but not in DEE?
- How can I make use of the servlet interface?
- How can I get data for some particular entity from devices which are managed by different Essentials servers?
- While using the -m option, can I use more than one email id?
- I do not want to give the password in the command line as it is insecure. Is there a way to give the password in a secure way?
- I am using -view or -input options which has the list of devices. The command fails saying that some devices are not in managed state. Is there a way to run the command for devices other than the devices that fail?
- Where will the XML output file be stored?
- Where can I get the descriptions of each node in the schema?
- Why am I getting parse error when trying to parse some of the output files?

- Q.** The Inventory Schema shows a number of elements. I am not able to see many of them in the output. Why?
- A.** Only those elements which are collected in the database and have data in them are included in the output. The data missing for some of the classes, may be present for some other class.
- Q.** What is ComputerSystemPackage Class?
- A.** It is the class that contains the InstanceID of chassis and the Network Element, and relates the two.
- Q.** Where does DEE collect the configuration information from?
- A.** DEE collects the running configuration data from the latest configuration in the Essentials Config Archive.
- Q.** Do we have the schema for the running configuration output?
- A.** No. There is no schema for running configuration output. The running configuration data is collected from Essentials Config Archive and presented in XML format. See the topic, Exporting Running Configuration from Essentials, in the Essentials Online Help.
- Q.** Is the containment hierarchy in inventory schema exactly the same as that in CIM?
- A.** No. Although the containment hierarchy in inventory schema is based on Common Information Model (CIM), it does not follow the exact containment hierarchy because of the limitations in the Essentials database schema.
- Q.** What is an XSD file?
- A.** XSD file is an XML based alternative to Document Type Definition (DTD). It is based on XML schema language which describes the structure of an XML document. An XML schema defines the legal building blocks of an XML document, just like a DTD.

An XML Schema:

- Defines elements that can appear in a document.
- Defines attributes that can appear in a document.
- Defines which elements are child elements.
- Defines the order of child elements.

- Defines the number of child elements.
 - Defines whether an element is empty or can include text.
 - Defines data types for elements and attributes.
 - Defines default and fixed values for elements and attributes.
- Q.** What is the AdditionalInformation tag in the inventory schema used for?
- A.** The AdditionalInformation tag is provided to define information that is specific to a device. The inventory schema may not contain information for all the elements in all the devices supported by DEE. The AdditionalInformation tag addresses scenarios where the inventory schema does not have tags to define information that you want to collect for some of the elements in a particular device.
- Q.** How do I know what fields come under AdditionalInformation?
- A.** For this information, see the topic, Additional Information Table, in the Essentials Online Help.
- Q.** Where can I find information specific to a particular node which I can see in detailed device information but not in DEE?
- A.** For this information, see the topic, Additional Information Table, in the Essentials Online Help.
- Q.** How can I make use of the servlet interface?
- A.** You must write customized scripts which could connect to the servlet. The arguments and options have to be specified in XML format.
For more details, see the topic, Using the Servlet to Export Data from Essentials, in the Essentials Online Help.
- Q.** How can I get data for some particular entity from devices which are managed by different Essentials servers?
- A.** You have to write a script to connect to different Essentials servers and aggregate all data into a single file. After you get the aggregated data, you can parse it and get the data for any required entity.

- Q.** While using the `-m` option, can I use more than one email id?
- A.** No. You can use only one email address at a time, when you use the `-m` option of the `cxexport` command.
- Q.** I do not want to give the password in the command line as it is insecure. Is there a way to give the password in a secure way?
- A.** Yes. You can create an environment variable called `CWEXPORTFILE` which points to a text file that has the username and password list separated by a space.
- Q.** I am using `-view` or `-input` options which has the list of devices. The command fails saying that some devices are not in managed state. Is there a way to run the command for devices other than the devices that fail?
- A.** You can run the command with `-continue` option to run it for devices that have not failed. You can use the command with this option for exporting inventory data as follows:
- ```
cxexport inventory -u username -p password -device dev1,dev2 -continue
```
- Q.** Where will the XML output file be stored?
- A.** The default location for storing the XML output file is `PX_DATADIR/archive/cxexport/dateconfig/inventory.xml`. You can use the `-f` option to specify an alternative location.
- Q.** Where can I get the descriptions of each node in the schema?
- A.** You can find the descriptions in the Essential Online help topic, About Inventory Schema.
- Q.** Why am I getting parse error when trying to parse some of the output files?
- A.** Some of the classes in IDU and Optical switches contains some special characters with ASCII code larger than 160. Most of the XML parsers does not support these characters and hence fails to parse these characters. To overcome this, you have to manually search for those elements with special characters and append CDATA as given in the example below:  
If there is an element,  
`checksum <?> /checksum`  
you must change it to  
`checksum <![CDATA[?> ]> /checksum`

# CiscoWorks Server

## CiscoWorks Server FAQs

- What kind of directory structure does CiscoWorks use when backing up Resource Manager Essentials data?
- How do I re-initialize the Essentials database on a Solaris system, if the Essentials database is corrupted and the database restore operation has failed?
- How do I re-initialize the Essentials database on a Windows system, if the Essentials database is corrupted and the database restore operation has failed?
- How do I change the IP Address of the CiscoWorks Server after installing it, or after running it for a while?
- How do I change the Hostname of the CiscoWorks Server after installing it, or after running it for a while?
- Can I back up the database for a single application?
- How do I find out which devices are supported by a particular application?
- How do I enable or disable Java plug-in?
- How to verify if SSH is enabled or disabled on my device using CiscoWorks Server?
- How to verify which version of SSH is running on my system?
- I modified the date and time on the CiscoWorks Server, but Essentials does not reflect the change. What should I do?
- I am not able to add some of my devices to Essentials server. What could be the reason?
- Can I use the CiscoWorks TFTP server for downloading or uploading files from unmanaged devices?
- How can I migrate data between identical versions of RME, from one server to another server?

- Q.** What kind of directory structure does CiscoWorks use when backing up Resource Manager Essentials data?
- A.** CiscoWorks uses a standard database structure for backing up all suites and applications.
- A sample directory structure for the CiscoWorks server (represented by the rme acronym) follows. The Essentials directory has two databases: rme and syslog.
- Q.** How do I re-initialize the Essentials database on a Solaris system, if the Essentials database is corrupted and the database restore operation has failed?
- A.** You can use the dbRestoreOrig.pl utility to re-initialize the Essentials database. To reinitialize the database, follow this procedure:

---

**Step 1** Stop the daemon manager by entering:

```
/etc/init.d/dmgttd stop
```

**Step 2** At the prompt, run the PERL script dbRestoreOrig.pl:

```
/opt/CSCOpX/bin/perl /opt/CSCOpX/bin/dbRestoreOrig.pl
```

The usage details for dbRestoreOrig.pl appear.

Enter the required variable parameters and the corresponding values based on your application (see “[Variable Parameters](#)” table).



**Caution**

All the user configurable variable parameters are case-sensitive. Ensure that you enter the exact value as mentioned in the table below— if not, the database will get corrupted.

We recommended that you reinitialize the database for both the applications—Common Services and Essentials. You can follow any order for reinitialization. Else, the database may become inconsistent.

**Table A-5** Variable Parameters

| Variable Parameter | For Common Services enter | For Essentials enter |
|--------------------|---------------------------|----------------------|
| dsn                | cmf                       | rme                  |

Table A-5 Variable Parameters

| Variable Parameter                                                                                                                                                | For Common Services enter | For Essentials enter     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|--------------------------|
| <code>dmprefix</code>                                                                                                                                             | <code>Cmf</code>          | <code>Essentials</code>  |
| <p><code>npwd</code></p> <p>It is optional to enter a new password for this variable. Enter a new password only if you want to change your database password.</p> | <i>Your new password</i>  | <i>Your new password</i> |

You will see a message that the initialization is complete.

**Step 3** Restart the daemon manager by entering:

```
/etc/init.d/dmgttd start
```

- Q.** How do I re-initialize the Essentials database on a Windows system, if the Essentials database is corrupted and the database restore operation has failed?
- A.** You can use the `dbRestoreOrig.pl` utility to re-initialize the Essentials database.

To re-initialize the Essentials database follow this procedure:

**Step 1** Open a command prompt window, and stop the daemon manager by entering:

```
net stop crmdmgttd
```

**Step 2** At the prompt, run the PERL script, `dbRestoreOrig.pl`:

```
NMSROOT\bin\perl NMSROOT\bin\dbRestoreOrig.pl
```

where `NMSROOT` is the directory in which CiscoWorks is installed.

The usage details for `dbRestoreOrig.pl` are displayed.

Enter the required variable parameters and the corresponding values based on your application (see “[Variable Parameters](#)” table).

**Caution**

All the user configurable variable parameters are case-sensitive. Ensure that you enter the exact value as mentioned in the table below— if not, the database will get corrupted.

It is recommended that you reinitialize the database for both the applications—Common Services and Essentials. You can follow any order for reinitialization. Else, the database may become inconsistent.

**Table A-6 Variable Parameters**

| Variable Parameter                                                                                                                            | For Common Services enter | For Essentials enter     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|--------------------------|
| <code>dsn</code>                                                                                                                              | <code>cmf</code>          | <code>rme</code>         |
| <code>dmpprefix</code>                                                                                                                        | <code>Cmf</code>          | <code>Essentials</code>  |
| <code>npwd</code>                                                                                                                             | <i>Your new password</i>  | <i>Your new password</i> |
| <b>Note</b> It is optional to enter a new password for this variable. Enter a new password only if you want to change your database password. |                           |                          |

You will see a message that the initialization is complete.

**Step 3** Restart the daemon manager by entering:

```
net start crmdmgt
```

**Q.** How do I change the IP Address of the CiscoWorks Server after installing it, or after running it for a while?

**A.** You can change the IP address on the server, and then access it using the new IP address.

To change the IP address on Windows:

**Step 1** On the machine that is your server, click **Start > Settings > Network and Dial-up Connections > Local Area Connection**.

The Local Area Connection Status dialog box appears.

- Step 2** Click **Properties**.  
The Local Area Connection Properties dialog box appears.
- Step 3** Select Internet Protocol (TCP/IP) and click **Properties**.  
The Internet Protocol (TCP/IP) Properties dialog box appears.
- Step 4** Select the radio button Use the following IP address.
- Step 5** Change the IP address as required, in the IP Address field.  
For the subnet mask and default gateway values, use the command `ifconfig` at the command prompt.  
The subnet mask and default gateway values will be displayed.
- Step 6** Enter these values in the Subnet mask and default gateway fields.
- Step 7** Click **OK**.
- Step 8** Restart the server.
- 

To change the IP address on Solaris, use the command `ifconfig` at the command prompt to change the IP address of the required interface.

For example, at the command prompt, you can enter:

```
ifconfig interfacename inet ipv4address
```

where the variable *interfacename* represents the name of the interface and *ipv4address* represents the new IP address.

- Q.** How do I change the Hostname of the CiscoWorks Server after installing it, or after running it for a while?
- A.** To change the hostname of the CiscoWorks Server, you need to update several files, and reboot the server:

**Step 1** Change the hostname in all the following files:

| <b>Bundle</b>        | <b>Solaris</b>                                                                                                                                                                                               | <b>Windows</b>                                                                                                                                                                                                             |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LMS Bundle           | <ul style="list-style-type: none"> <li>• hosts</li> <li>• hostname.hm0</li> <li>• nodename</li> <li>• md.properties</li> <li>• ANIServer.properties</li> <li>• pkginfo</li> </ul>                            | <ul style="list-style-type: none"> <li>• Identification tab in the Network window</li> <li>• md.properties file</li> <li>• Windows registry key</li> <li>• ANIServer.properties</li> </ul>                                 |
| RWAN Bundle          | <ul style="list-style-type: none"> <li>• hosts</li> <li>• hostname.hm0</li> <li>• nodename</li> <li>• md.properties</li> <li>• aclm.properties</li> <li>• pkginfo</li> </ul>                                 | <ul style="list-style-type: none"> <li>• Identification tab in the Network window</li> <li>• md.properties file</li> <li>• Windows registry key</li> <li>• aclm.properties file</li> </ul>                                 |
| LMS and RWAN Bundles | <ul style="list-style-type: none"> <li>• hosts</li> <li>• hostname.hm0</li> <li>• nodename</li> <li>• md.properties</li> <li>• aclm.properties</li> <li>• ANIServer.properties</li> <li>• pkginfo</li> </ul> | <ul style="list-style-type: none"> <li>• md.properties file</li> <li>• Windows registry key</li> <li>• Identification tab in the Network window</li> <li>• aclm.properties file</li> <li>• ANIServer.properties</li> </ul> |




---

**Note** For Solaris, the `sys-unconfig` command erases the hostname and IP addresses pertaining to the Solaris system (not the LMS or SMS software) and guides you through the server-renaming process. You also do this when you change the hostname in the `hosts`, `hostname.hm0`, and `nodename` files in the `/etc` directory.

---

For the detailed procedure to change each of the files, see these URLs:

For Solaris,

[http://www.cisco.com/warp/customer/477/RME/sol\\_hostname.html#files](http://www.cisco.com/warp/customer/477/RME/sol_hostname.html#files)

For Windows,

[http://www.cisco.com/warp/customer/477/RME/winnt\\_hostname.html#idtab](http://www.cisco.com/warp/customer/477/RME/winnt_hostname.html#idtab)

**Step 2** Stop and restart the ANI server.

For Solaris:

- a. Type `/etc/init.d/dmgt d stop` to stop the server.
- b. Delete `gatekeep.ior` file under `/opt/CSCOpX/www/classpath` directory.
- c. Type `/etc/init.d/dmgt d start` to start the server.

For Windows:

- a. On the Windows desktop, select **Start >Run**.
- b. Type `cmd`, and then click **OK**. This will open up a DOS Window.
- c. At the prompt, type `net stop crmdmgt d` to stop the server.
- d. Delete the `gatekeeper.ior` file under `NMSROOT\www\classpath` directory, the default install location for CiscoWorks.
- e. At the prompt, type `net start crmdmgt d` to start the server.




---

**Note** You must have Administrator privileges to execute these commands.

---

**Table A-7 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 CiscoWorks 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"> <li>• xxx_DbVersion.txt</li> <li>• xxx.db database files</li> <li>• xxx.log database log files</li> <li>• xxx.txt database backup manifest file</li> </ul> |

- Q.** Can I back up the database for a single application?
- A.** No. You cannot back up the database for individual applications or suites (if you have more than one installed). CiscoWorks 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.
- Q.** How do I find out which devices are supported by a particular application?
- A.** Select **Server Configuration > About the Server > Applications and Versions**. Under Applications Installed, click the application name to see a list of the supported devices.

- Q.** How do I enable or disable Java plug-in?
- A.** 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**.

---

**Q.** How to verify if SSH is enabled or disabled on my device using CiscoWorks Server?

**A.** You can verify whether SSH is enabled or disabled using the CiscoWorks Server.

---

**Step 1** Select **Server Configuration > Diagnostics > Connectivity Tools > Management Station to Device**.

**Step 2** In the Check Connectivity dialog box, enter the device name and select the SSH check box.

If SSH enabled on the device, you will see:

**SSH OK.**

If SSH is not enabled on the device, you will see:

**SSH failed.**

---

- Q.** How to verify which version of SSH is running on my system?
- A.** You can verify the SSH version that is running on your system using the commands:
- ```
show ip ssh
```
- or
- ```
show ssh
```
- Q.** I modified the date and time on the CiscoWorks Server, but Essentials does not reflect the change. What should I do?
- A.** You will need to stop and restart the CiscoWorks Daemon Manager for Essentials to reflect the changes in date, time or timezone.
- On Solaris,
- Stop the daemon manager by entering:
- ```
/etc/init.d/dmgttd stop
```
- Restart the daemon manager by entering:
- ```
/etc/init.d/dmgttd start
```
- On Windows,
- Open a command prompt window, and stop the daemon manager by entering:
- ```
net stop crmdmgttd
```
- Restart the daemon manager by entering:
- ```
net start crmdmgttd
```
- Q.** I am not able to add some of my devices to Essentials server. What could be the reason?
- A.** If your devices are running on a slow link that is less than 2 Mbps, you may encounter this problem. DIServer sends SNMP GETNEXT requests fast, and slower interfaces need queuing so that the packets are not lost.
- It is recommended that you enable any one of the types of queuing (for example, fair queuing) to avoid the packets being lost.

To configure fair queueing on an interface, use one of the following commands in interface configuration mode after specifying the interface:

| Command                                                                                                 | Purpose                                                                                    |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <b>fair-queue</b><br><i>[congestive-discard-threshold<br/>[dynamic-queues<br/>[reservable-queues]]]</i> | Configure an interface to use fair queueing.                                               |
| or                                                                                                      | or                                                                                         |
| <b>fair-queue</b>                                                                                       | Configure an interface to use fair queueing on a Cisco router using a VIP-based interface. |

- Q.** Can I use the CiscoWorks TFTP server for downloading or uploading files from unmanaged devices?
- A.** TFTP works on a client-server architecture and therefore, the RME server acts as the TFTP server, and the device as the TFTP client. This means that you cannot access any data from the device using the command line of the RME server.

To access the files, you should use the push/pull model from the device that acts as the client. There is no security in-built into TFTP.

Assumptions:

- /etc/inetd.conf on the server will give you the TFTP root directory. By default it will be /tftpboot and will be used in all the examples below.
- *NMSROOT*/tftpboot will be the TFTP root directory on the Windows RME server.

### For Solaris

To copy a file (a.txt) from the RME server to an IOS device, on a Solaris server:

- 
- Step 1** Copy the required file to the /tftpboot directory on the RME server. Ensure that the file has read permissions for all.
- Step 2** On the device, use the following command if you have the copy the file to slot0:

```
copy tftp://RME Server IP /file name slot0:
```

**Example 0-9 Usage on Solaris**

```
7200_1#copy tftp: slot0:
Address or name of remote host []? 10.104.138.50
Source filename []? a.txt
Destination filename []? a.txt
Accessing tftp://10.104.138.50/a.txt...
Loading a.txt from 10.104.138.50 (via FastEthernet1/0):
!!!!!!!!!!!! [OK
- 51640 bytes]
51640 bytes copied in 2.536 secs (20363 bytes/sec)
```

Or enter:

```
7200_1#copy tftp://10.104.138.50/a.txt slot0:a.txt
Destination filename [a.txt]?
Accessing tftp://10.104.138.50/a.txt...
Loading a.txt from 10.104.138.50 (via FastEthernet1/0):
!!!!!!!!!!!! [OK - 51640 bytes]
C 51640 bytes copied in 2.512 secs (20557 bytes/sec)
```

---

To copy a file (a.txt) to the RME server from an IOS device, on a Solaris server:

---

- Step 1** Create a file of zero bytes by using the following command in the /tftpboot directory:
- ```
Solaris-u10#touch a.txt
```
- Step 2** Give the write privilege to the file:
- ```
Solaris-u10# chmod 662 a.txt
```
- Step 3** In the enable mode, on the device, use the following command to copy the file from the device to server:
- ```
7200_1#copy slot0:a.txt tftp://10.104.138.50/a.txt
```
- Step 4** After ensuring the address of the remote host is correct, press **Enter**.
- Step 5** After ensuring the filename that was created on the remote host is the same as what is displayed, press **Enter**.

Example 0-10 Usage on Solaris

```
7200_1#copy slot0:a.txt tftp://10.104.138.50/a.txt
Address or name of remote host [10.104.138.50]?
Destination filename [a.txt]?
!!!!!!!!!!!!!! 51640 bytes copied in 0.508 secs (101654
bytes/sec)
7200_1#
```

You will see the following error if the created file does not have adequate privileges:

```
7200_1#copy slot0:a.txt tftp://10.104.138.50/a.txt
Address or name of remote host [10.104.138.50]?
Destination filename [z.txt]?
TFTP: error code 2 received - Access violation
%Error opening tftp://10.104.138.50/a.txt (Permission denied)
7200_1#
bill-u10# touch z.txt
bill-u10# ls -al z.txt
-rw-r--r-- 1 nobody4 nogroup 0 Oct 10 22:40 z.txt
```

On Windows

To copy a file (a.txt) from the RME server to an IOS device, on a Windows server:

-
- Step 1** Copy the required file (a.txt) to the *NMSROOT*\tftpboot directory on the RME server.
- Step 2** On the device use any one of the following commands if you have to copy the file to slot0:

```
7200_1#copy tftp://RME Server IP/file name slot0:
```

or

```
7200_1#copy tftp: slot0:
Address or name of remote host []? 10.104.137.125
Source filename []? a.txt
Destination filename []? a.txt
```

Example 0-11 Usage on Windows

```

E:\Program Files\CSCOpX\tftpboot>dir
Volume in drive E is Extra
Volume Serial Number is 5820-6992
Directory of E:\Program Files\CSCOpX\tftpboot
10/11/2003 12:30p <DIR> .
10/11/2003 12:30p <DIR> ..
10/11/2003 12:18p 51,640 a.txt
04/14/2003 03:24p 60 README.txt
2 File(s) 51,700 bytes
2 Dir(s) 18,727,092,224 bytes free

7200_1#copy tftp: slot0:
Address or name of remote host [10.104.137.125]?
Source filename [a.txt]?
Destination filename [a.txt]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://10.104.137.125/a.txt...
Loading a.txt from 10.104.137.125 (via FastEthernet1/0):
!!!!!!!!!!!!!!
[OK - 51640 bytes]
51640 bytes copied in 2.544 secs (20299 bytes/sec)

```

To copy a file (a.txt) to the RME server from an IOS device, on a Windows server:

-
- Step 1** Create a file of zero bytes in the *NMSROOT*\tftpboot directory. One of the ways could be:
- ```
E:\Program Files\CSCOpX\tftpboot>more > a.txt Press Enter, ^C <-- <CTRL + C>
```
- After you do this, you will create a file called a.txt of size zero bytes.
- Step 2** In the enable mode, on the device, use the following command to copy the file from the device to server
- ```
7200_1#copy slot0:a.txt tftp://10.104.137.125/a.txt
```
- Step 3** After ensuring that the address of the remote host is correct, press **Enter**.

- Step 4** After ensuring that the filename that was created on the remote host is the same as what is displayed, press **Enter**.

Example 0-12 Usage on Windows

TFTPBOOT directory before the copy:

```
E:\Program Files\CSCOpX\tftpboot>dir
Volume in drive E is Extra
Volume Serial Number is 5820-6992
Directory of E:\Program Files\CSCOpX\tftpboot
10/11/2003 12:30p <DIR> .
10/11/2003 12:30p <DIR> ..
10/11/2003 12:30p 0 a.txt
04/14/2003 03:24p 60 README.txt
2 File(s) 60 bytes
2 Dir(s) 18,727,145,472 bytes free
```

At the command prompt, enter:

```
7200_1#copy slot0:a.txt tftp://10.104.137.125/a.txt
Address or name of remote host [10.104.137.125]?
Destination filename [a.txt]?
!!!!!!!!!!!!!!
51640 bytes copied in 0.500 secs (103280 bytes/sec)
```

TFTPBOOT directory after the copy:

```
E:\Program Files\CSCOpX\tftpboot>dir
Volume in drive E is Extra
Volume Serial Number is 5820-6992
Directory of E:\Program Files\CSCOpX\tftpboot
10/11/2003 12:30p <DIR> .
10/11/2003 12:30p <DIR> ..
10/11/2003 12:33p 51,640 a.txt
04/14/2003 03:24p 60 README.txt
2 File(s) 51,700 bytes
2 Dir(s) 18,727,092,224 bytes free
```

-
- Q.** How can I migrate data between identical versions of RME, from one server to another server?
- A.** For this example, let us assume that we have the following two machines:
- SrcA

- DstA

SrcA has RME installed, and also has the RME data. We need to replicate the data that is present on SrcA to DstA.

**Caution**

You cannot migrate data from a Solaris server to a Windows server, or vice versa. You should migrate data only between identical versions of RME. For example, RME 3.5 data can only be migrated on another RME 3.5 machine, it should not be migrated on RME 3.5 IDU X releases.

For Solaris**Important Points to Remember:**

- Restoring data which has changed Config Archive location on Solaris does not work.

For example, if you have changed the Config Archive location to let's say, /NewPartition/config on the SrcA machine, the same partition should exist on the DstA machine also, with adequate space. Files will be copied to the DstA machine but the Config Archive location will still continue to be the default location (/var/adm/CSCOpX/files).

- After restoring, Software Management jobs will not run and you cannot reschedule them either. You will see the following error in Job Results:

Job Results:

```
Error Message: System Error: Cannot cancel schedule. Error message is at: 1195281600.e: No such file or directory .
```

```
Error Action: Probable Cause: The job was deleted from CRON by the system administrator.
```

```
Recommended Action: Select Resource Manager Essentials->Software Management->Job Management->Browse Jobs to delete the job.
```

You have to recreate the jobs afresh.

- The following procedure is applicable when only RME and CiscoWorks Common Services are present. It has not been tested when other applications are also present.

Procedure

-
- Step 1** Back up the data in SrcA machine under any directory.
- Step 2** Copy the backed up data from SrcA machine to DstA machine. Then:
- a. Tar the contents of the backup directory.
 - b. Transfer the .tar file of backup directory to the DstA machine. If you are using FTP to transfer the file, then ensure that you transfer in the ASCII mode.
 - c. Untar the .tar file to get the backup contents.
- Step 3** Stop the Daemon Manager.
- Step 4** Restore the data on DstA machine using the following command, assuming the data is copied to the location /backup/initial and RME is installed in /opt/CSCOpX.
- Step 5** Start the Daemon Manager.
-

Example 0-13

```
RME-SERVER-DST# tar -xvf backupexample.tar
RME-SERVER-DST# ./restorebackup.pl -d <Directory where the files are
untarred> -f
avail=34945887
*****
Restore from backup '/backup/initial/' started at:2003/11/17 01:04:22
Please see '/var/adm/CSCOpX/log/restorebackup.log' for status.
```

```
Restoring generation '0' of group(s) 'All' from back up directory
'/backup/initial/'. The 'force' parameter is TRUE. This will force a
restore even if version or data file do not match.
```

```
INFO:If you are restoring cmf data and if the CiscoWorks server is/was
SSL enabled, the backed up Server Certificate and Private Key will also
be restored. Your existing Certificate and Private Key will be over-
written.
```

```
Do you want to continue (y-continue or n-quit, y/n)?[n] y
Files /opt/CSCOpX/backup/manifest/rme/database/rme_DbVersion.txt and
```

```
/backup/initial//0/rme/database/rme_DbVersion.txt are not the same.  
Files /opt/CSCOpX/backup/manifest/cmf/database/cmf_DbVersion.txt and  
/backup/initial//0/cmf/database/cmf_DbVersion.txt are not the same.  
The above files do not match. Since 'force' parameter is TRUE, this  
will force a restore even if version or data file do not match.  
Restoring from /backup/initial//0/rme/filebackup.tar.  
Restoring from /backup/initial//0/cmf/filebackup.tar.  
Restored generation 0 of All Database(s) and related files from backup  
'/backup/initial/'.
```

For Windows

Important Points to Remember:

- On DstA, install in the same location as you have installed RME in SrcA machine. For example, if you have installed in E:\CSCOpX in SrcA, you have to install in E:\CSCOpX itself in DstA machine also. This is mandatory, without this requirement being met, data cannot be replicated across the machines. Also, see the defect CSCds74983 using the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> (You will be prompted to log into Cisco.com.).
- Changing Config Archive location is fine, but the destination machine(DstA) should also have that drive, otherwise replication will fail. For example, if you have installed RME in "E:\CSCOpX" and the Config Archive location is changed to "H:\Config\archive", DstA machine should also have "H:\\" with adequate space.
- Changing the message source file(syslog.log) for Syslog messages on the source(SrcA) is fine, but additional steps needs to be done to ensure that the data gets replicated correctly.
- The following procedure is applicable when only RME and CiscoWorks Common Services are present. It has not been tested when other applications are also present.

Procedure

-
- Step 1** Install RME in the same location as installed in SrcA on DstA machine.
 - Step 2** Backup the data in SrcA machine under any directory.
 - Step 3** Copy the backed up data from SrcA machine to DstA machine.

- Step 4** Stop the Daemon Manager.
- Step 5** Restore the data on DstA machine using the following command, assuming the data is copied to "E:\backup" and RME is installed in "E:\Program Files\CSCOpX". If the Config Archive location is changed in SrcA, the location will also be changed to that location in the new machine(DstA).
- Step 6** Start the Daemon Manager.
-

Example A-14 If you have not changed any file locations

```
E:\Program Files\CSCOpX\bin>restorebackup.pl -f -d e:\backup
Restore from backup 'e:\backup' started at:2003/11/12 15:08:29
Please see 'E:\PROGRA~1\CSCOpX\log\restorebackup.log' for status.
Restoring generation '0' of group(s) 'All' from back up directory
'e:\backup'. The 'force' parameter is TRUE. This will force a restore
even if version or data file do not match.
INFO:If you are restoring cmf data and if the CiscoWorks server is/was
SSL enabled, the backed up Server Certificate and Private Key will
also be restored. Your existing Certificate and Private Key will be
overwritten.
Do you want to continue (y-continue or n-quit, y/n)?[n] y
Files
E:\PROGRA~1\CSCOpX\backup\manifest\rme\database\rme_DbVersion.txt
and e:\backup\0\rme\database\rme_DbVersion.txt are not the same.
Files
E:\PROGRA~1\CSCOpX\backup\manifest\cmf\database\cmf_DbVersion.txt
and e:\backup\0\cmf\database\cmf_DbVersion.txt are not the same.
The above files do not match. Since 'force' parameter is TRUE, this
will force a restore even if version or data file do not match.
Restoring from e:\backup\0\rme\filebackup.tar.
Restoring from e:\backup\0\cmf\filebackup.tar.
Restored generation 0 of All Database(s) and related files from backup
'e:\backup'.
```

Example 0-15 When you have changed the Config Archive location

```
E:\PROGRA~1\CSCOpX\bin>restorebackup.pl -f -d e:\backup
Restore from backup 'e:\backup' started at:2003/11/12 18:48:14
Please see 'E:\PROGRA~1\CSCOpX\log\restorebackup.log' for status.
```

```
Restoring generation '0' of group(s) 'All' from back up directory  
'e:\backup'. The 'force' parameter is TRUE. This will force a restore  
even if version or data file do not match.
```

```
INFO:If you are restoring cmf data and if the CiscoWorks server is/was  
SSL enabled, the backed up Server Certificate and Private Key will  
also be restored. Your existing Certificate and Private Key will be  
overwritten.
```

```
Do you want to continue (y-continue or n-quit, y/n)?[n] y
```

```
Files E:\PROGRA~1\CSCOPx\backup\manifest\rme\config\datafiles.txt  
and e:\backup\0\rme\config\datafiles.txt are not the same.
```

```
The above files do not match. Since 'force' parameter is TRUE, this  
will force a restore even if version or data file do not match.
```

```
Restoring from e:\backup\0\rme\filebackup.tar.
```

```
Restoring from e:\backup\0\cmf\filebackup.tar.
```

```
Restored generation 0 of All Database(s) and related files from backup  
'e:\backup'.
```

Additional Points

- If the message source file (syslog.log) location is changed in SrcA machine, then after step 6 that is, after restoring the data, the CWCS Syslog Service should be updated with location that was in SrcA machine.

For more details, see Resource Manager Essentials Online help (**Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Changing Storage Options**).

- If the message source file (syslog.log) location is changed in DstA machine, then after step 6 that is, after restoring the data, change the location of message source file to what it was in the SrcA machine, because the DB contains this absolute path.

Essentials Process Description Table

The following table lists each Essential's process in alphabetical order, describes its function, and names other processes that must be running before the process can start. The CiscoWorks Server also controls other processes that are not Essentials-specific.

Table A-8 *Essentials Process Description Table*

Name	Description	Dependency
AvIcmpPoller	Polls devices using ICMP and provides information about whether a device is accessible.	AvInputGen
AvInputGen	Retrieves polling information from the database and provides AvIcmpPoller and AvSnmpPoller with a list of devices to poll and the frequency with which to poll them.	EssentialsDbMonitor
AvLoader	Moves data from AvIcmpPoller and AvSnmpPoller to the Essentials database.	EssentialsDbMonitor
AvSnmpPoller	Polls devices using SNMP and provides protocol distribution and reload information.	AvInputGen
AvTrimmer	Transient process that runs on a regular schedule to trim expired availability data from the Essentials database.	EssentialsDbMonitor
CasServer	Change Audit program that provides back-end database services for applications that want to log network changes and for Change Audit reports.	EssentialsDbMonitor

Table A-8 Essentials Process Description Table (continued)

Name	Description	Dependency
ChangeAudit	Consists of the following Java programs, which provide the back-end functionality of Device Configuration: <ul style="list-style-type: none"> • CasServer • ConfigArchive • InvChangeProbe • Scheduler 	<ul style="list-style-type: none"> • CMLogger • EDS • EssentialsDbMonitor
CMLogger	Used by Java back-end processes and clients to get error messages from Essentials message catalogs.	RmeOrb
ConfigArchive	Change Audit program that gets configuration files from devices and archives them.	<ul style="list-style-type: none"> • CMLogger • EssentialsDbMonitor • EDS
ConfigChangeDetector	Detects configuration changes in the network.	<ul style="list-style-type: none"> • CMLogger • EssentialsDbMonitor • EDS
ConfigPurge	Deletes expired configuration files from the archive.	<ul style="list-style-type: none"> • CMLogger • EssentialsDbMonitor
ConfigUpdate	Sweeps managed devices looking for configuration changes.	<ul style="list-style-type: none"> • CMLogger • EssentialsDbMonitor
DIServer	Imports and adds devices to the inventory.	EssentialsDbMonitor
EssentialsDbEngine	System service: the database engine for Resource Manager applications.	None
EssentialsDbMonitor	System service that monitors the accessibility of the Resource Manager database engine, which helps to ensure that the system is not started until the database engine is ready.	<ul style="list-style-type: none"> • CMLogger • EssentialsOSG

Table A-8 Essentials Process Description Table (continued)

Name	Description	Dependency
IcServer	Routinely collects inventory updates from managed devices. Inventory updates are acquired through SNMP queries on MIBs in the devices that maintain inventory information.	EssentialsDbMonitor
InvChangeDetector	Detects inventory changes in the network and causes the device database to be updated.	<ul style="list-style-type: none"> • CMLogger • EDS • EssentialsDbMonitor
InvChangeProbe	Change Audit program that sends notifications when new devices are managed by DIServer or when managed devices are deleted from inventory.	<ul style="list-style-type: none"> • CMLogger • EDS • EssentialsDbMonitor
Proxy	Used only on Windows NT systems. A system service that allows back-end processes to perform privileged operations on Windows NT systems that they normally would not be permitted to perform, for example, scheduling jobs on a Windows NT system for Software Management. Without Proxy, the application's Perl code would not allow the scheduling.	None
Scheduler	Change Audit program that schedules repeating jobs for the Inventory and Device Configuration back-end processes.	<ul style="list-style-type: none"> • CMLogger • EssentialsDbMonitor
SyslogAnalyzer	Filters and forwards messages from routers and switches to the central Essentials server.	<ul style="list-style-type: none"> • CMLogger • EDS • EssentialsDbMonitor