



CHAPTER 22

Setting System-wide Parameters Using System Preferences

You can set system-wide parameters for RME, using the **RME > Admin > System Preferences** tab. Here you can set parameters for RME, such as log level settings, job purge preferences, device attributes and device credentials verification settings.

- [Application Log Level Settings](#)
- [Job Purge](#)
- [RME Device Attributes](#)
- [RME Secondary Credentials](#)
- [Collection Failure Notification](#)

Application Log Level Settings

You can use this option to set the logging levels for RME packages. You can set the log levels for all RME packages, or at a package (application) level.

Log files are stored at these locations:

- On Windows: *NMSROOT*/log, where *NMSROOT* is the CiscoWorks installation directory.
- On Solaris: /var/adm/CSCOpX/log

To set the log levels:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > Application Log level Settings**.
- The Set Application Logging Levels dialog box appears.
- Step 2** Select the Application from the drop-down list.
 - Step 3** Select the appropriate log level from the Logging Level drop-down list.

The fields in the Set Application Logging Levels dialog box are:

Application	Module	Log File Names	Description
All	-	-	Changes the logging level for the entire system.
ArchiveMgmt	• Archive Service	dcmaservice.log	Changes the logging level for Archive Management.
	• Archive Client	dcmaclient.log	
BugToolkit	Bug Toolkit	bugtoolkit.log	Changes the logging level for Bug Toolkit.
ChangeAudit	• Change Audit	ChangeAudit.log	Changes the logging level for Change Audit.
	• Change Audit User Interface	ChangeAuditUI.log	Changes the logging level for Change Audit UI.
CLIFramework	CLI Framework	cli.log	Changes the logging level for CLI Framework.
ConfigCLI	• Config CLI	ConfigCLI.log	Changes the logging level for Config CLI.
	• Netconfig CLI	netcfgcli.log	Changes the logging level for NetConfig CLI.
ConfigEditor	Config Editor	CfgEdit.log	Changes the logging level for Config Editor.
ConfigJob	Config Jobs	logs under %NMSROOT%\files\rme\jobs\NetConfigJob	Changes the logging level for Configuration Jobs.
ConfigJobManager	Config Job Manager	cjp.log	Changes the logging level for Configuration Job Browser. This log file is used for config purge jobs
ContractConnection	Contract Connection	contractcon.log	Changes the logging level for Contract Connections
CTMJrmServer	CTM Jrm Server	CTMJrmServer.log	Changes the logging level for CTM JRM Server.
CRI	CRI	<ul style="list-style-type: none"> • cri.log • criarvpurge.log • crijobpurge.log 	Changes the logging level for Common reporting Infrastructure.
DeviceManagement	• Device Management User Interface	• EssentialsDM.log	Changes the logging level for Device Management.
	• Check Device Attributes User Interface	• cda.log	Changes the logging level for Check Device Attributes User Interface
	• Device Credential Verification Jobs	• log files under %NMSROOT%\files\rme\jobs\cda\	Changes the logging level for Device Credential Verification jobs.
	• Device Management Operations	• EssentialsDM_Server.log	Changes the logging level for Device Management Operations.

Application	Module	Log File Names	Description
DeviceSelector	Device Selector	RMEDeviceSelector.log	Changes the logging level for Device Selector.
ICServer	• Inventory Collection Service	IC_Server.log	Changes the logging level for the IC Server.
	• Inventory Collection User Interface	ICServerUI.log	Changes the logging level for Inventory Collection User Interface.
	• Inventory Collection Jobs	Creates job logs under %NMSROOT%\files\rme\jobs\ICServer	Changes the logging level for Inventory Collection jobs.
Install	<ul style="list-style-type: none"> • Restore RME CCR • RME PSU Adapter • Migration 	CCRImport.log	Changes the logging level for the Installation modules.
InventoryPoller	Inventory Poller	Creates job logs under %NMSROOT%\files\rme\jobs\InvPoller	Changes the logging level for Inventory Poller.
InvReports	Inventory Reports	invreports.log	Changes the logging level for Inventory Reports.
MakerChecker	Maker Checker	MakerChecker.log	Changes the logging level for the Job Approval module.
NetConfig	Netconfig Client	netconfigclient.log	Changes the logging level for Netconfig client.
NetShow	NetShow Client	NetShowClient.log	Changes the logging level for NetShow client.
RME Portlets	RME Portlets	RMEPortlets.log	Changes the logging level for RME Portlets.
RMECommon	Common RME Functions	rme.log	Changes the logging level for the common RME functions such as, Job Management tasks, purge tasks, etc.
RMECSTMServer	RME CSTM Server	rme_ctm.log	Changes the logging level for RME CSTM Server.
SoftwareMgmt	• Software Management User Interface	swim_debug.log	Changes the logging level for the user interface of Software Management and the Software Management job creation workflows.
	• Software Management Jobs	swim_debug.log files under %NMSROOT%\files\rme\jobs\swim folder	Changes the logging level for Software Management jobs.

Application	Module	Log File Names	Description
SyslogAnalyzer	<ul style="list-style-type: none"> Syslog Analyzer 	SyslogAnalyzer.log AnalyzerDebug.log	Changes the logging level for Syslog Analyzer. <ul style="list-style-type: none"> SyslogAnalyzer.log—for Windows AnalyzerDebug.log—for Solaris
	<ul style="list-style-type: none"> Syslog Analyzer User Interface 	SyslogAnalyzerUI.log	Changes the logging level for Syslog Analyzer User Interface.
Virtual Switching System	<ul style="list-style-type: none"> Virtual Switch Client 	VirtualSwitchClient.log	Changes the logging level for Virtual Switching System.

Step 4 Click **Reset** to apply the default logging levels.

Step 5 Click **Apply** after you set the log levels,

A message appears, that the log levels have been successfully updated.

Job Purge

The Job Purge option provides a centralized location for you to schedule Purge operations for the following RME jobs:

- Credential Verification Jobs—Purge all Credential Verification jobs. This also includes credential verification edit jobs.
- Software Management Jobs—Purge all Software Management jobs such as Image Import, Image Distribution, etc.
- Netconfig Jobs—Purge all NetConfig jobs.
- Archive Management Jobs—Purge Archive Management jobs such as Compliance Check, Deploy Compliance Results, etc.
- Archive Update Jobs—Purge Archive Management collection jobs, *Default config collection job*.
- Archive Poller Jobs—Purge Archive Management polling jobs, *Default config polling job*.
- Archive Purge Jobs—Purge Archive Management purge jobs, *Default archive purge job*.
- Config Editor Jobs—Purge all Config Editor jobs.
- CwConfig Jobs—Purge all cwcli config jobs such as Get Config, Put Config, etc.
- Inventory Collector Jobs—Purge Inventory collection jobs.
- Inventory Poller Jobs—Purge Inventory polling jobs.
- Reports Jobs—Purge all RME Reports jobs
- Reports Archive Jobs—All reports that are archived are purged. You can view all reports that are archived in the Archives window (**Resource Manager Essentials > Reports > Report Archives**).
- NetShow Jobs—Purge all RME NetShow jobs.

You cannot purge the jobs that are in the running state.

The Job Purge contains the following information:

Column	Description
Application	Lists the application for which the Purge is applicable.
Status	Whether a Purge job is enabled or disabled.
Policy	This value is in days. Data older than the specified value, will be purged. You can change value this as required. This is a mandatory field. The default is 180 days.
Job ID	Unique ID assigned to the job by the system, when the Purge job was created. This job ID does not change even when you disable or enable or change the schedule of the Purge job. For Purge Now task, job ID is not assigned. Also, if a Job ID already exist for that application, the job ID is not updated for Purge Now tasks. That is, the scheduled Purge job is not affected by Purge Now task.
Scheduled At	Date and time that the job was scheduled at. For example: Nov 17 2004 13:25:00.
Schedule Type	Specifies the type of schedule for the Purge job: <ul style="list-style-type: none"> • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. (A month comprises 30 days).

You can select the applications by checking the checkboxes next to the application to perform the following tasks using the Job Purge window:

Button	Description
Schedule	Schedules a Purge job.
Enable	After you schedule a job, you can enable Purge.
Disable	After you schedule a job, if you have enabled the Purge job, you can choose to disable it.
Purge Now	Perform Immediate Purge. You can select more than one application to purge in a single step. After selecting the applications, click on this button to purge jobs.

Scheduling a Purge Job

To schedule a Purge job:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.
The Job Purge dialog box appears.
To create a Purge job,
- Step 2** Select **Schedule**.

The Purge Schedule dialog box appears for the selected application.

Field	Description
Scheduling	
Run Type	<p>Specifies the type of schedule for the Purge job:</p> <ul style="list-style-type: none"> • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. (A month comprises 30 days). <p>For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete.</p> <p>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed. If the 10:00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.</p>
Date	<ol style="list-style-type: none"> 1. Click on the date picker icon and select the date, month and year. Your selection appears in the Date field in this format: dd Mmm yyyy (example: 14 Nov 2004). 2. Select the time (hh and mm) from the drop-down lists in the at fields.
Job Info	
Days	<p>The default setting for purging archived data is 180 days. That is, data older than 180 days will be purged. You can change this value as required. This is a mandatory field.</p> <p>You can enter non-negative full day only. You cannot enter fractions of days.</p>
Job Description	<p>Based on the option that you selected, you see a default job description.</p> <p>For example, for Software Management Purge jobs the default description is:</p> <p>Purge - Software Management Jobs.</p> <p>For Reports Archive Purge, the default description is: Purge - Reports Archive Purge.</p>

Step 3 Click **Done**.

The Purge job appears in the Job Purge dialog box.

**Note**

You cannot purge the jobs that are in the running state.

Enabling a Purge Job

You can enable only a scheduled Purge job.

To schedule a Purge job, see [Scheduling a Purge Job](#).

To enable a Purge job:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.
The Job Purge dialog box appears.
- Step 2** Click **Enable**.
A confirmation message appears:
There is a purge schedule and it is enabled.
- Step 3** Click **OK**.
The Status column in the Job Purge window displays `Enabled` for the selected application Purge job.
-

Disabling a Purge Job

You can only disable a Purge job that is scheduled and enabled.

To schedule a Purge job, see [Scheduling a Purge Job](#) and to enable a Purge job, see [Enabling a Purge Job](#).

To disable a Purge job:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.
The Job Purge dialog box appears.
- Step 2** Click **Disable**.
A confirmation message appears:
There is a purge schedule and it is disabled.
- Step 3** Click **OK**.
The Status column in the Job Purge window displays `Enabled` for the selected application Purge job.
-

Performing an Immediate Purge

Using this option you can purge application jobs immediately. That is, you can purge RME jobs without scheduling and enabling the Purge job.

For the Purge Now task, the Job ID is not assigned. Also, if a Job ID already exist for that application, the Job ID is not updated for Purge Now tasks. That is, the scheduled Purge job is not affected by Purge Now task.

To perform an immediate purge:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > Job Purge**.

The Job Purge dialog box appears.

Step 2 Click **Purge Now**.

The Explorer User Prompt dialog box appears.

Step 3 Enter the number of days jobs that have to be purged.

The default setting for purging archived data is 180 days. That is, data older than 180 days will be purged. You can change value this as required.

You can enter non-negative full day values only. You cannot enter fractions of days.

Step 4 Click **OK**.

The Purge Job Details window appears displaying the purged job details.



Note

You cannot purge the jobs that are in the running state.

RME Device Attributes

This option enables you to set the default values for device attributes. These values are applicable to all devices in RME. The RME device attributes are:

- **SNMP Retry**—Number of times that the system should try to access devices with SNMP options.
The default value is 2. The minimum value is zero and the maximum value is 6.
- **SNMP Timeout**—Amount of time that the system should wait for a device to respond before it tries to access it again. It refers to the total transaction time of SNMP Packets.
The default value is 2 seconds and the minimum value is zero seconds. There is no maximum value limit. Changing the SNMP timeout value affects inventory collection.
- **Telnet Timeout**—Amount of time that the system should wait for a device to respond before it tries to access it again. It refers to the initial response time required to create a socket.
The default value is 36 seconds and the minimum value is zero seconds. There is no maximum value limit.
Changing the telnet timeout value affects inventory collection.

- Natted RME IP Address—The RME server ID. This is the translated address of RME server as seen from the network where the device resides.

You need to enable support for NAT, in a scenario where RME tries to contact devices outside the NAT boundary.

The default value is Not Available.

- TFTP Timeout—Amount of time that the system should wait to get the result status of the copy operation. Changing the TFTP timeout value affects Config collection.

The default value is 5 and the minimum value is 0 seconds. There is no maximum value limit.

To edit the RME device attributes:

Step 1 Select **Resource Manager Essentials > Admin > System Preferences > RME Device Attributes**.

The RME Device Attributes dialog box appears.

Step 2 Enter the default values for:

- SNMP Retry
- SNMP Timeout
- Telnet Timeout
- Natted RME IP Address
- TFTP Timeout

The value you enter here will be applicable for all RME devices. You can change the value for individual devices and also enter the device serial number information using the Edit Devices Attributes option on RME Devices window. (see [To set or edit the RME device attributes for a single RME device.](#))

Step 3 Click **Apply**.

A confirmation message appears:

Default settings are updated successfully.

Step 4 Click **OK**.

RME Secondary Credentials

The RME server polls and receives two types of credentials from each device and populates the Device Credential Repository (DCR). These credentials are:

- Primary Credentials
- Secondary Credentials

RME uses either the primary or secondary credentials to access the devices using the following protocols:

- Telnet
- SSH

The RME server first uses the Primary Credentials to access the device. The Primary Credentials is tried out three times and on failure the Secondary Credentials is tried out three times. Secondary Credentials is used as a fallback mechanism in RME 4.2 for connecting to devices.

For instance, if the AAA Server is down, accessing devices using their primary credentials will lead to failure.

You can add or edit the Secondary Credentials information through the DCR page available in CiscoWorks Common Services if the Secondary Credential information is not available for a device.

**Note**

The use of Secondary Credentials fallback is applicable for both Login and Enable connectivity.

You can use the RME Secondary Credential dialog box to enable or disable Secondary Credentials fallback when the Primary Credentials for a device fails. This is a global option which you can use to enable or disable the use of Secondary Credential fallback for all RME applications.

To enable or disable the Secondary Credentials fallback:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > RME Secondary Credentials**
- The RME Secondary Credentials dialog box appears.
- Step 2** Do either of the following:
- Check **Fallback to Secondary Credentials** checkbox if you want to enable the Secondary Credential fallback.
- Or
- Uncheck **Fallback to Secondary Credentials** checkbox if you want to disable the Secondary Credential fallback.
- Step 3** Click either **Apply** to apply the option or click **Cancel** to discard the changes.
-

Collection Failure Notification

You can use the Collection Failure Notification option to configure the destination Server and Port to receive trap notification on Inventory Collection or Config Fetch failure. This failure trap is sent per device from the RME server whenever the collection does not happen. Other network management stations can use this trap to know about RME Inventory or Config collection failure status. You can check or uncheck the options available in this page to enable or disable the sending of trap notifications to other servers on Inventory Collection or Config Fetch failure.

[Table 22-1](#) lists the various fields and buttons available in the Notification on Failure Window:

Table 22-1 **Collection Failure Notification**

Field	Description
All	<p>Check this option, if you require both the Config Fetch Failure and Inventory Collection Failure trap notification to be sent to the listed servers.</p> <p>The listed servers are those servers that you have configured to receive trap notifications. See the description for List of Destination field for more information.</p>

Field	Description
Config Collection	<p>Check this option, if you require the Config Fetch Failure trap notification to be sent to the listed servers.</p> <p>Uncheck this option if you do not want the Config Fetch Failure trap notification to be sent to the listed servers.</p> <p>The listed servers are those servers that you have configured to receive trap notifications. See the description for List of Destination field for more information.</p>
Inventory Collection	<p>Check this option, if you require the Inventory Collection Failure trap notification to be sent to the listed servers.</p> <p>Uncheck this option if you do not want the Inventory Collection Failure trap notification to be sent to the listed servers.</p> <p>The listed servers are those servers that you have configured to receive trap notifications. See the description for List of Destination field for more information.</p>
Trap Destination Information	
Server	The name or IP address of the destination server.
Port	The port number of the destination server.
List of Destinations	The names of the destination servers along with their ports which are configured to receive the trap notifications.
Buttons	
Add	Use the Add button to add the destination server and port information. On clicking Add, the server and port information get reflected in the List of Destinations list.
Delete	Use the Delete button to remove server and port information from the List of Destinations. To do so, select one or more server and port entry from the list of Destinations list and click on Delete to remove the entries from the list.
Apply	Click to accept the changes made.

Configuring Trap Notification Messages

To configure the distribution of trap notification messages from RME to the connected hosts:

-
- Step 1** Select **Resource Manager Essentials > Admin > System Preferences > Collection Failure Notification**
- The Notification on Failure dialog box appears. Refer to to further complete the selection in this dialog box.
- Step 2** Click **Apply** to accept the changes made.
-

Examples for Collection Failure Notification

Example for Config Fetch Failure

You are providing the following information in the Collection Failure Notification screen:

Destination Server: 10.77.153.47

Destination Port: 162

You are also enabling the Send Notification on Config Fetch Failure option. By enabling this option you are allowing trap notifications to be sent to the specified destination server on Config Fetch Failure using the specified port.

After that you add few new devices to RME and schedule a job to fetch the configurations for all the devices. There is a Config Fetch Failure as the scheduled job is unable to fetch the configurations for the new devices. The server 10.77.153.47 receives trap notifications for each Config Fetch Failure per device.

Example for Inventory Collection Failure

You are providing the following information in the Collection Failure Notification screen:

Destination Server: 10.77.153.47

Destination Port: 162

You are also enabling the Inventory Collection option. By enabling this option you are allowing trap notifications to be sent to the specified destination server on Inventory Collection Failure using the specified port.

After that you add few new devices to RME and schedule a job to fetch the inventory information for all devices. There is a Inventory Collection Failure as the scheduled job is unable to fetch the inventory details for the new devices. The server 10.77.153.47 receives trap notifications for each Inventory Collection Failure per device.

Fields in a Trap Notification Message

[Table 22-2](#) lists the various fields that constitute a Configuration Fetch or Inventory Collection Failure trap notification message.

Table 22-2 Fields in a Trap Notification Message

Field	Description
Application Name	RME application that caused this change or identified the change and generated the notification.
Device Display Name	Network device for which the inventory or configuration collection has failed.
Collection Failure Time	Time at which the inventory or configuration collection job failed.
Error Message	The message that describes the reason for the collection failure. Some examples of trap error messages: Inventory Collection Failed due to SNMP TimeOut Exception. Config Collection Failed due to authentication failure.