



CHAPTER 14

Tracking Network Changes Using Change Audit

Change Audit tracks and reports changes made in the network. Change Audit allows other RME applications to log change information to a central repository. Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit.

RME applications write change records to Change Audit. Change Audit stores these records in the log tables (summary and details) for later use with reports.

For example, Software Management records a change for each completed device upgrade. If a job has ten devices, then Software Management writes ten entries to the Change Audit log, but the Change Audit report shows only one job with ten devices. You can then access individual device information.

Each application writes its own change records to Change Audit. For example, in Inventory you can set inventory change filters to filter out all kinds of information for different device types. Change Audit record maintenance is controlled by the Change Audit Delete Change History option.

You can convert change records into SNMP V1 traps and forward them to a destination of your choice. This allows system administrators to forward critical network change data to their own NMS.

You can define automated actions (e-mail and automated scripts) on creation of change audit record. The automated action gets triggered on creation of the change audit record.

How Does it Differ From Syslog?

Syslog clients or message suppliers are Cisco devices that have been configured to log messages to RME. Syslog Analyzer receives messages from routers and other Cisco devices configured to send messages to the syslog server in RME. The messages are sent either directly or through a remote syslog collector installed in the network. These messages originate from the device in response to some activity that affects it.

Change Audit clients are RME applications that record change information. Applications, such as Software Management, send messages to Change Audit when they make a change to the network, for example, uploading a new Cisco IOS image.

Often these changes and users who make changes from the command line interface also trigger syslog messages. The messages are logged in the RME syslog facility and are also passed on to other RME applications for processing.

For example, a device sends a syslog message about a device configuration change. This is passed on to Device Configuration, which determines the exact nature of the change and then writes a change record into the Change Audit log.

Performing Change Audit Tasks

Change Audit allows you to:

- Determine changes being made in the network during critical operations time

System administrators can define the start and end times during the day when network changes should not be made. Based on this selection you can quickly see, for a given day, whether changes were made when they should not be.

See [Defining Exception Periods](#) for defining the exception periods.
- Define automated actions on creation of change audit record

Automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are, E-mail, Traps, and Automated scripts

See [Defining Automated Actions](#) for defining the Change Audit automated actions.
- Monitor your software image distribution and download history for software changes made using the Software Management application.

Software Management automatically sends network change data to the Change Audit summary and details tables.

See [Generating 24 Hours and Standard Change Audit Reports](#) for generating the Change Audit reports.
- Track any configuration file changes

Device Configuration automatically sends data on configuration file changes to the Change Audit log.

See [Generating 24 Hours and Standard Change Audit Reports](#) for generating the Change Audit reports.
- Monitor inventory additions, deletions, or changes

Inventory tracks specific messages or monitors any and all changes in your network inventory. To set inventory filters, use the Inventory Change Filter option.

See [Generating 24 Hours and Standard Change Audit Reports](#) for generating the Change Audit reports.
- View all the latest changes that occurred in the network over the last 24 hours

24-Hour Reports provides a quick way to access the latest changes in the Change Audit log.

See [Generating 24 Hours and Standard Change Audit Reports](#) for generating the Change Audit reports.
- Purging the Change Audit records

Frees disk space and maintains your Change Audit records at a manageable size. You can either schedule for periodic purge or perform a forced purge of Change Audit data.

See [Performing Maintenance Tasks](#) for scheduling a periodic purge.
- Generating change audit data in XML format

`cwcli export changeaudit` is a command line tool that also provides servlet access to change audit data. This tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.

See [Overview: cwcli export Command](#) for generating the Change Audit data in XML format.

- Set the debug mode for Change Audit application
You can set the debug mode for Change Audit application in the Log Level Settings dialog box (**Resource Manager Essentials > Admin > System Preferences > Loglevel Settings**).
- Using Device Center you can perform the following Change Audit tasks:
 - Generate the 24-hour Change Audit Summary report for a selected device.
 - Generate the Change Audit Standard report for a selected device.
 See [RME Device Center](#) for further information.

For the new features in this release, see [What's New in this Release](#).

Performing Maintenance Tasks

You can either schedule for periodic purge or perform a forced purge of Change Audit data. This frees disk space and maintains your Change Audit data at a manageable size.

You can perform these tasks using the **Resource Manager Essentials > Admin > Change Audit** tab:

- [Setting the Purge Policy](#)
- [Performing a Forced Purge](#)
- [Config Change Filter](#)

Setting the Purge Policy

You can specify a default policy for the periodic purging of Change Audit data.



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To set the Change Audit Purge Policy:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Set Purge Policy**.

The Purge Policy dialog box appears in the Periodic Purge Settings pane.

Step 2 Enter the following information:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged. The default is 180 days.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. The default is 180 days. See Tracking RME Server Changes Using Audit Trail for further information.

Field	Description
Scheduling	
Run Type	<p>You can specify when you want to run the purge job for Change Audit and Audit Trail records.</p> <p>To do this, select one of these options from the drop down menu:</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. <p>The subsequent instances of periodic 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	You can select the date and time (hours and minutes) to schedule.
at	Enter the start time, in the hh:mm:ss format (23:00:00).
Job Info	
Job Description	<p>The system default job description, <i>ChangeAudit Records - default purge job</i> is displayed.</p> <p>You cannot change this description.</p>
E-mail	<p>Enter e-mail addresses to which the job sends messages at the end of the job.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences).</p> <p>We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.</p>

**Caution**

You might delete data by changing these values. If you change the number of days to values lower than the current values, messages over the new limits will be deleted.

Step 3

Click either **Save** to save the purge policy that you have specified, or click **Reset** to reset the changes made to a Purge policy.

Performing a Forced Purge

You can perform a Forced Purge of Change Audit, as required.



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To perform a Change Audit Forced Purge:

Step 1 Select **Resource Manager Essentials > Admin > ChangeAudit > Force Purge**.

The Purge Policy dialog box appears.

Step 2 Enter the information required to perform a Forced Purge:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. See Tracking RME Server Changes Using Audit Trail for further information.
Scheduling	
Run Type	You can specify when you want to run the Force Purged job for Change Audit and Audit Trail records. To do this, select one of these options from the drop down menu: <ul style="list-style-type: none"> • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time.
Date	Enter the start date in the dd-mmm-yyyy format, for example, 02-Dec-2003, or click on the Calendar icon and select the date. The Date field is enabled only if you have selected Once as the Run Type.
at	Enter the start time, in the hh:mm:ss format (23:00:00). The At field is enabled only if you have selected Once as the Run Type

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	<p>Enter e-mail addresses to which the job sends messages at the end of the job.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences).</p> <p>We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.</p>

Step 3 Click **Submit** for the Forced Purge to become effective.

Config Change Filter

You can use this option to enable or disable VLAN Change audit filtering. When there is a change to the device configuration, a change record is created. By default, the VLAN change audit record is created for those devices that have a VLAN configuration.

To enable or disable the VLAN Change Audit Filter option:

Step 1 Select **Resource Manager Essentials > Admin > Change Audit > Config Change Filter**

The Config Change Filter dialog box appears.

Step 2 Check or uncheck the Enable VLAN Change Audit Filter option.

- Check **Enable VLAN Change Audit Filter**, if you do not want the change audit record to be created for devices that have a VLAN configuration.
- Uncheck **Enable VLAN Change Audit Filter**, if you want the change audit record to be created for devices that have VLAN configuration. By default, this option is unchecked.

Step 3 Click either **Apply** to apply the option or click **Cancel** to discard the changes.

Defining Exception Periods

An Exception period is a time you specify when no network changes should occur. This period does not prevent you from making any changes in your network. The set of Exception periods is known as an Exception profile.

You can have only one Exception period for a day.

You perform the following tasks for Exception profiles:

Tasks	Description
Creating an Exception Period	Creating an exception profile.
Enabling and Disabling an Exception Period	Enabling and disabling a set of exception profiles.
Editing an Exception Period	Editing an exception profile.
Deleting an Exception Period	Deleting a set of exception profiles.

Creating an Exception Period

To create an Exception profile:



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select:

- Days of the week from the Day drop-down list box
- Start and end times from the Start Time and the End Time drop-down list box.

Step 3 Click **Add**.

The defined exception profile appears in the List of Defined Exception Periods pane.

To enable the exception period, see [Enabling and Disabling an Exception Period](#).

Enabling and Disabling an Exception Period

To enable and disable a set of exceptions periods:



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

-
- Step 1** Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.
The Define Exception Period dialog box appears.
- Step 2** Select one or more exception profiles in the List of Defined Exception Periods pane.
- Step 3** Click **Enable/Disable**.
- If you have selected Enabled, then the exception period report is generated for that specified time frame.
 - If you have selected Disabled, then the exception period report is not generated for that whole day.
- For example: If you have disabled exception period for Monday from 10:00 am to 12:30 pm, then there will not be any exception period report generated for Monday.
-

Editing an Exception Period

To edit an exception profile:



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

-
- Step 1** Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.
The Define Exception Period dialog box appears.
- Step 2** Select a day from the Day drop-down list box for which you want to change the exception period.
- Step 3** Change the start and end times in the Start Time and the End Time drop-down list box.
If required you can also enable or disable the status for the exception period.
- Step 4** Click **Add**.
- The edited exception profile appears in the List of Defined Exception Period dialog box. This will overwrite the existing exception profile for that day.
-

Deleting an Exception Period

To delete a set of Exceptions Periods:



Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

- Step 1** Select **Resource Manager Essentials > Tools > Change Audit > Exception Periods**.
The Define Exception Period dialog box appears.
- Step 2** Select one or more exception profiles in the List of defined Exception Periods pane.
- Step 3** Click **Delete**.

Defining Automated Actions

You can define automated actions on creation of change audit record. This automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are:

- E-mail
- Traps
- Automated scripts

Understanding the Automated Action Window

This window contains the following entries:

Field	Description
Name	Name of the automated action.
Status	Status of the automated action—Enabled, or disabled.
Type	Type of automated action—Email, Script or Trap.

You perform the following tasks from this window:

Tasks	Description
Creating an Automated Action	Creating an automated action.
Enabling and Disabling an Automated Action	Enabling and disabling a set of automated actions. This button gets activated only after selecting an automated action.

Tasks	Description
Editing an Automated Action	Editing an automated action. This button gets activated only after selecting an automated action.
Exporting and Importing an Automated Action	Exporting and importing a set of automated actions.
Deleting an Automated Action	Deleting a set of automated actions. This button gets activated only after selecting an automated action.

Creating an Automated Action

To create an automated action:



Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Click **Create**.

The Define Automated Action dialog box appears.

Step 3 Enter the following:

Field	Description
Name	Name for the automated action.
Status	Select either Enabled or Disabled For the automated action to trigger.
Application	Select the name of the application on which the automated action has to be triggered.
Category	Select the types of the changes, for example, configuration, inventory, or software on which the automated action has to be triggered.
Mode	Select the connection mode on connection modes on which the automated action has to be triggered.
User	Select the user name on which the automated action has to be triggered.

Step 4 Click **Next**.

The Automated Action Type dialog box appears.

Step 5 Select either **E-mail** or **Trap** or **Script**. Based on your selection, enter the following data:

If you have selected E-mail, enter...

Field	Description
Send To	<p>Enter the E-mail ID for which the trigger has to be notified.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences).</p> <p>We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). You will receive the e-mail with the CiscoWorks E-mail ID as the sender's address.</p>
Subject	Enter the subject of the e-mail.
Content	Enter the content of the e-mail.

If you have selected Trap, perform...

Enables configuration of a single or dual destination port numbers and hostnames for the traps generated by Change Audit.

Ensure that you have copied these files:

- CISCO-ENCASE-MIB.my
- CISCO-ENCASE-APP-NAME-MIB.my

into the destination system to receive the traps.

These files are available in the following directories on RME server:

On UNIX:

/opt/CSCOpX/objects/share/mibs

On Windows:

NMSROOT\objects\share\mibs. Where *NMSROOT* is the root directory of the CiscoWorks Server.

- Enter the Server and Port details in the Define Trap field.
- Click **Add**.

The server and port information appears in the List of Destinations text box.

If you want delete, the server and port information, select the server and port information from the List of Destinations text box and click **Delete**.

If you have selected Script, enter...

You can run only shell scripts (*.sh) on Unix and batch files (*.bat) on Windows. The shell script or batch file should have only write/execute permissions for casuser:casusers in solaris and casuser/Administrator in Windows. The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the casuser account.

The script files must be available at this location:

On UNIX:

/var/adm/CSCOpX/files/scripts/changeaudit

On Windows:

NMSROOT/files/scripts/changeaudit

To select the script file:

- a. Click **Browse**.

The Server Side File Browser dialog box appears with the predefined location.

- b. Select the script file (*.sh on Unix and *.bat on Windows)

- c. Click **OK**.

- Step 6** Click **Finish**.

The Automated Action window appears with the defined automated action.

Editing an Automated Action

To edit an automated action:


Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

- Step 1** Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

- Step 2** Select an Automated Action.

- Step 3** Click **Edit**. (See step 3 to step 5 in [Creating an Automated Action](#).)

- Step 4** Click **Finish**.

The Automated Action window appears with the updated data.

Enabling and Disabling an Automated Action

To enable or disable a set of automated actions:

**Note**

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Select a or a set of Automated actions.

Step 3 Click **Enable/Disable**.

The Automated Action window appears with the updated data.

Exporting and Importing an Automated Action

To export or import an automated action:

**Note**

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 If you want to export an Automated action, then select the automated actions else go to next step.

Step 3 Click **Export/Import**.

The Export/Import dialog box appears.

Step 4 Select the task to be performed—**Export** or **Import**.

Step 5 Either:

- Enter the filename along with the absolute path.

Or

- Click **Browse**,

The Server Side File Browser dialog box appears.

a. Select a folder.

b. Click **OK**.

c. Enter the filename.

Step 6 Click **OK**.

Deleting an Automated Action

To delete a set of automated actions:


Note

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Resource Manager Essentials > Tools > Change Audit > Automated Action**.

The Automated Action dialog box appears.

Step 2 Select a or a set of Automated actions.

Step 3 Click **Delete**.

The Automated Action window appears with the updated data.

Using Change Audit Reports

You can generate the following reports based on Change Audit data:

- [Generating an Exception Period Report](#)
- [Generating 24 Hours and Standard Change Audit Reports](#)

You can generate change audit data in XML format using the `cwcli export changeaudit` command line tool. This tool also provides servlet access to change audit data.

See [Overview: cwcli export Command](#) for generating the Change Audit data in XML format.

You can perform the following actions using these icons on the Change Audit reports:

Button	Description
Export to File (Icon)	You can export this report in either PDF or CSV format.
Print (Icon)	Generates a format that can be printed.

Generating an Exception Period Report

This option lets you compile a report on changes that occurred in the network during a specific time period. This report is based on the Exceptions profiles you set up to occur as often as each day for a week.



Note View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate a Exception Period Report:

- Step 1** Select **Resource Manager Essentials > Reports > Report Generator**.
The Report Generator dialog box appears.
- Step 2** Select **Change Audit** from the first drop-down list box.
- Step 3** Select **Exception Period Report** from the second drop-down list box.
- Step 4** Select the required devices using the Device Selector. (See [Using RME Device Selector](#) for more information.)
- Step 5** Enter the information required to generate the required report:

Field	Description
Date Range	
From	Click on the calendar icon and select the start date.
To	Click on the calendar icon and select the end date.
Exception Period	
Select Days	Select the days for the week. If the exception profiles are defined, then the exception periods are displayed in this box. If the exception profiles are not defined, then this box will be blank. You can define your exceptions profiles in the Exception Period Definition dialog box (Resource Manager Essentials > Tools > Change Audit > Exception Periods).
Scheduling	
Run Type	You can specify when you want to run the Exception Report job. To do this, select one of these options from the drop down menu: Immediate—Runs the report immediately. Once—Runs the report once at the specified date and time.
Date	Click on the calendar icon and select the start date. The Date field is enabled only if you have selected an option other than Immediate in the Run Type field.
at	Select the hours and minutes from the drop-down lists.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. The Job Description field is enabled only if you have selected an option other than Immediate in the Run Type field.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.

Step 6 Click **Finish**.

- If you have selected the Run Type as Immediate, the report appears in a separate browser window.
If you have selected the Run Type as Once, a message is displayed:

`Job ID created successfully.`

Go to Reports->Report Jobs to view the job status.

Where *ID* is a unique Job number.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Generating 24 Hours and Standard Change Audit Reports

This option lets you compile a report on all changes that occurred in the network during a specific time period. You can compile a report based on the selection criteria, such as application, users, connection mode.

You can also generate these report using Device Center (from CiscoWorks LMS Portal home page, select **Device Troubleshooting > Device Center** to launch Device Center).

**Note**

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

To generate the 24 Hour and Standard Reports:

Step 1 Select **Resource Manager Essentials > Reports > Report Generator**.

The Report Generator dialog box appears.

Step 2 Select **Change Audit** from the first drop-down list box.**Step 3** Select **Standard Report** from the second drop-down list box.

- Step 4** Select the required devices using the Device Selector. (See [Using RME Device Selector](#) for more information.)
- Step 5** Enter the information required to generate the required report:

Field	Description
Date Range	
Last X	Select this option, if you want to generate a report for the last <i>X</i> days or weeks or months or years. Where <i>X</i> represents the number of days or weeks or months or years. Let us say, you want to generate a 24 Hour Change Audit report for the last 4 weeks. You can enter 4 in the textbox and select weeks from the listbox. The generated report will contain the Change Audit data gathered during the last 4 weeks. This option is applicable only for 24 Hour Change Audit Reports.
24 Hours	Select this option, only if you want to generate a 24 hours report. This report will contain all the Change Audit data gathered during the last 24 hours.
From	Click on the calendar icon and select the start date. The From field is enabled only if you have de-selected the 24 Hours check box.
To	Click on the calendar icon and select the end date. The To field is enabled only if you have de-selected the 24 Hours check box.
Selection Criteria	
User Name	Select the user name. This report will be filtered on user names.
Mode	Select the connection mode through which the change was made. This report will be filtered on connection modes.
Category	Select the types of the changes. The supported categories are: <ul style="list-style-type: none"> • CONFIG_CHANGE—Configuration changes on the device. • INVENTORY_CHANGE—Hardware changes on the device. • SOFTWARE_CHANGE—Software changes on the device.
Application	Select the name of the application. This report will be filtered on application names.

Field	Description
Scheduling	
Run Type	<p>You can specify when you want to run the Standard Report job.</p> <p>To do this, select one of these options from the drop down menu:</p> <ul style="list-style-type: none"> • Immediate—Runs the report immediately. • 6 - hourly—Runs the report every 6 hours, starting from the specified time. • 12 - hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • 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. <p>The subsequent instances of periodic 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	<p>Click on the calendar icon and select the start date.</p> <p>The Date field is enabled only if you have selected an option other than Immediate, in the Run Type field.</p>
At	Select the hours and minutes from the drop-down lists.
Job Info	
Job Description	<p>Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.</p> <p>The Job Description field is enabled only if you have selected an option other than Immediate, in the Run Type field.</p>
E-mail	<p>Enter e-mail addresses to which the job sends messages at the end of the job.</p> <p>The E-mail field is enabled only if you have selected an option other than Immediate, in the Run Type field.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences).</p> <p>We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.</p>

Step 6 Click **Finish**.

- If you have selected the Run Type as Immediate, then the report appears in a separate browser window.
- If you have selected an option other than Immediate, in the Run Type field, then a message is displayed:

```
Job ID created successfully.
Go to Reports->Report Jobs to view the job status.
```

Where *ID* is a unique Job number.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Understanding Change Audit Report

Change Audit report provides a summary and, when available, detailed record information.

**Note**

When an application is unable to obtain information for Change Audit, N/A is used on the Change Audit report.

The Change Audit report contains all change information provided by RME applications based on your filter criteria.

It contains the following fields.

Table 14-1 Change Audit Report

Field	Description
Device Name	Device Display Name as entered in Device and Credential Repository. Click on the device name to launch the Device Center.
User Name	Name of the user who performed the change. This is the name entered when the user logged in. It can be the name under which the RME application is running, or the name using which the change was performed on the device. The User Name field may not always reflect the user name. The User Name is reflected only when: <ul style="list-style-type: none"> • Config change was performed using RME. • Config change was performed outside of RME, but the network has username based AAA security model, wherein authentication is performed by a AAA server which could be TACACS/RADIUS or local.
Application Name	Name of the RME application involved in the network change. For example, Archive Mgmt, ConfigEditor, CwConfig, etc.
Host Name	Host name of the machine from which the user accessed the device or the host name of the RME server. The Host name can contain IP address if the address does not resolve to a name.
Creation Time	Date and time at which the application communicated the network change or when Change Audit saw the change record.
Connection Mode	Connection mode through which the change was made. For example, Telnet, SNMP, or console. The mode is obtained by querying the device and if the query fails, <code>default</code> or <code>NA</code> is shown.

Table 14-1 Change Audit Report (continued)

Field	Description
Message	Brief summary of the network change.
Details	<p>Application details for a particular device displayed in a separate browser window.</p> <p>Select the highlighted Details text to view application details in a separate browser window.</p> <p>Applications that make or detect changes in the network log a change record in Change Audit log and provide a means for getting to the detailed data.</p> <p>The following information is displayed when you click on the Details link for:</p> <ul style="list-style-type: none"> • Archive Mgmt, ConfigEditor, CwConfig, and NetConfig—The Config Diff Viewer window is displayed. This window shows the differences between the configurations. See Understanding the Config Diff Viewer Window for further information. • ICServer—The Inventory Change report is displayed. This window shows the changed values (previous and current value) of different Inventory entities such as FlashDevice, FlashPartition, FlashFile. • Software Management—The Software Modification History report is displayed. This window shows the changed software image details.
Grouped Records	<p>Similar change details grouped by the same job ID and the same function ID (for example: inventory collection) displayed in a separate summary window.</p> <p>Select the highlighted More Records text in the Grouped Records column to view similar change details in a frame below the summary window.</p> <p>For example, you have completed a software update on five devices. The Change Audit report shows the Software Management summary information about who performed the job, when, and so on.</p> <p>To display all devices affected by this upgrade, click More Records to display the summary information related to the five devices. From here you can look at details of the individual device upgrades.</p>

ChangeAudit Process

The change audit process consists of the following Java programs, which provide the back-end functionality of Device Configuration:

- CasServer
- ConfigArchive
- InvChangeProbe
- Scheduler

This process depends on the following:

- RMEDbMonitor
- CTMJrmServer
- jrm

Stopping and Restarting the Change Audit Process

The following procedure describes the steps to stop and restart the ChangeAudit Process:

**Note**

View Permission Report (**Common Services > Server > Reports**) to check if you have the required privileges to perform this task.

Step 1 Select **Common Services > Server Configuration > Admin > Processes**.

The Process Management dialog box appears.

Step 2 Select the ChangeAudit process.

Step 3 Click either **Stop** to stop the process or **Start** to Restart the process.
