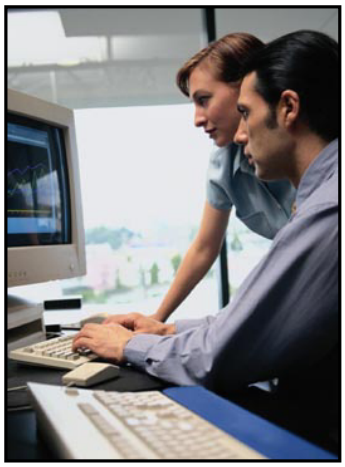
CiscoWorks Resource Manager Essentials

(RME) v4.0 Tutorial

About This Tutorial

Cisco.com

- **Identify the need for configuration management tools**
- **Describe the features and benefits of RME**
- **View various scenarios explaining how to use several RME functions**
- **Provide guidelines for System Administrators**
- **Provide links to documentation on CiscoWorks and RME**



About This Tutorial

The CiscoWorks Resource Monitor Essentials (RME) tutorial provides self-paced training focused on using RME to perform configuration management tasks. RME is a set of tools used to automate the collecting, monitoring, changing, and tracking of changes to device configuration information; saving both time and effort for the network administrator.

RME is available with the purchase of the CiscoWorks LAN Management Solution (LMS) bundle. The LMS bundle is a suite of network management applications used for configuring, administering, monitoring, and troubleshooting a Cisco-based network.

The tutorial is structured as a series of self-paced modules, or chapters, that conclude with self-administered exercises. The tutorial explores Resource Manager Essentials' architecture, features, and installation. Also included as part of the tutorial is a helpful reference section containing links to technical documents on component products, concepts, and terminology. The tutorial material is presented through text, illustrations, hypertext links, and typical scenarios.

This tutorial is not intended to teach you how to manage a network or what to use the collected data for, but rather to introduce you CiscoWorks RME and its rich set of time-saving tools that will simplify the process of managing a network.

How the Tutorial Is Organized

Cisco.com

Chapter 1 **Introduction to RME**	**Discuss the various challenges of performing configuration management and how RME can help**
Chapter 2 **RME Product Features**	**Learn about the rich set of features and time-saving tools in RME**
Chapter 3 **RME Scenarios**	**Using several examples, learn how to jump start RME and use it for various configuration management tasks**
Chapter 4 **System Administration Guidelines**	**Review important system requirements, installation guidelines, and RME administrative functions**
Chapter 5 **Helpful Links to Reference Material**	**A comprehensive set of links to information on CiscoWorks and RME**

How This Tutorial Is Organized

The tutorial is divided into five chapters:

Chapter 1: Introduction to RME

This chapter identifies the need for configuration management and the difficulties in collecting necessary data using traditional methods. RME is introduced as a set of tools to save time and effort to collect data and perform tasks associated with configuration management.

Chapter 2: RME Product Features

This chapter discusses the key features of RME through both discussions of the major functional components and screen shots of specific tasks.

Chapter 3: RME Scenarios

This chapter walks you through step-by-step examples to provide hands-on experience using RME. The case studies begin with steps on how to get started, followed by using various RME feature to achieve specific results.

Chapter 4: RME System Administration

This chapter provides information about RME client and server requirements, software installation guidelines, and additional administrative tasks not covered in the getting started scenario.

Chapter 5: References

This chapter contains a list of additional product information, such as links to related white papers and documentation.

Introduction to Resource Manager Essentials (RME)

Chapter 1

Chapter 1 Outline

Cisco.com

- **Managing Today's Network**
  - The proactive need
  - A closer look at the challenges
  - Solutions and pitfalls to network management
- **Cisco's Solution**
  - Resource Manager Essentials
  - CiscoWorks LAN Management Solution (LMS)

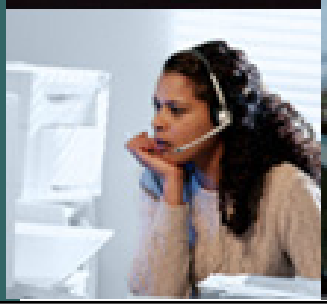
Chapter 1 Outline

Welcome to the CiscoWorks Resource Manager Essentials (RME) v4.0 tutorial! Before introducing RME, the first step is to acknowledge the importance of performing network management in today's environment. As will be discussed, there is a real need for managing the network proactively, however, the effort to collect and analyze the necessary data is often time-consuming, repetitive, and often error-prone. The most common traditional mechanism for performing network management will be discussed along with associated pitfalls.

This will set the stage to introduce the need for a tool to minimize effort and errors. RME is presented as Cisco's solution to performing network management to achieve all the benefits while minimizing the challenges. Chapter 2 will then focus on all the features of RME, followed by usage scenarios in Chapter 3. Finally, Chapter 4 will present further administrative information for using RME.

Managing Today's Network

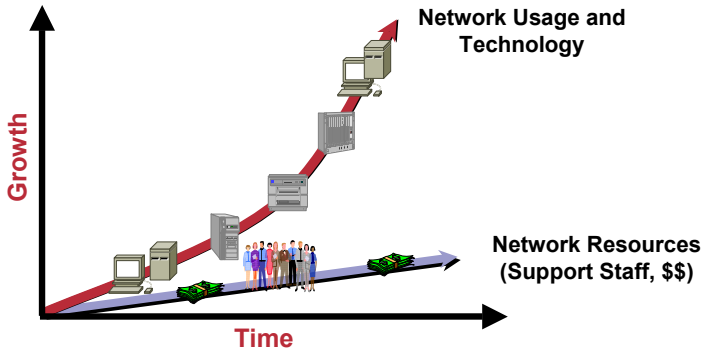
- **Managing Today's Network**
- Cisco's Solution



Managing Today's Network

The Proactive Need

Cisco.com



- **Operation of the network is crucial to the success of a business**
- **Many faults can be traced to incorrect configurations**
- **Use and complexity far outpacing staff resources**
- **Urgent need for current network configuration; Network assessments on large-scale networks are time consuming and prone to errors**

The Proactive Need to Managing Today's Network

There is no doubt that networks are the foundation that most organizations depend on for their day-to-day mission critical operations. Businesses today rely on their networks to provide reliable and responsive communications and services for departments and business partners located in every corner of the globe, enabling file and application sharing and providing portals for e-commerce services.

With the network being such a crucial element in the operation of a business, the management of the network is essential. In particular, the configuration of network infrastructure devices contain the very rules that determine how and what packets are forwarded, thus dictating the overall network behavior. However, managing the configuration of devices can be daunting; it includes every changeable aspect of the device, such as the individual modules, software images, and each line of the configuration file. Further complicating the task is the fact that the use and complexity of networks continues to increase exponentially, while the staff and other resource committed to its operation remain steady at best.

Managing your network's configuration is not optional; it is essential to the business that it supports. Help is needed to overcome the obstacles in managing the configuration of the network.

Types of Network Operations Failures

Failure Type	Reason for Failure Percentage
Configuration Errors	39%
Upgrade Errors	27%
Data Entry Errors	10%
Maintenance Errors	10%
Version Control Errors	7%
Other	7%

Source: Sage Research, Inc.

76% of network failures are attributed to configuration, upgrade, and entry errors!

Reasons for Network Failures

It can be argued that one of the most important aspects of a network is its configuration; after all, the configuration of devices contain the rules for forwarding packets and hence dictate the operation of the network. Therefore, configuration management, inventory reporting, and network change management tasks become an essential aspect of day to day operations. In fact, a survey of network managers revealed that roughly 75% of all network operations failures are directly related to tasks considered to be within the configuration management domain. Further, these presented failure categories point at human error…overworked, under trained, under funded?

Many readers may be thinking how hard can it be to change a configuration or update a device image? Or, what devices have changed over the past 24 hours? Sure, a few devices may not be a problem, but how about 20, 50, or 100 before heading home?

Managing Today's Network

A Closer Look at the Challenges

Cisco.com

- **Undesirable Network Behavior**
  - **What changed?**
  - **Who made the change?**
  - **When was the change made?**

- **Current Configuration Knowledge**
  - **What devices are running IOS v12.01?**
  - **How many switch slots are empty?**
  - **What devices are not yet configured for TACACS?**

- **Large Scale Upgrades**
  - **All devices need their community strings changed.**
  - **All 7200 routers need to be upgraded to IOS v 12.03(t).**

A Closer Look at the Challenges

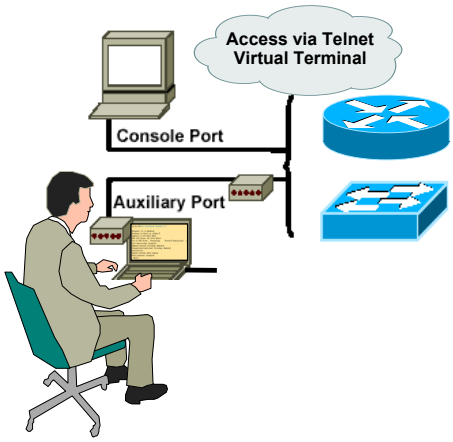
Let's now discuss some plausible day-to-day network management tasks faced by many network administrators. The previous page talks about the cause of failures, but doesn't begin to even mention how to fix them. Often times it is painfully obvious that the network is not running right (non-stop phone calls from angry users). The network administrator is now under the gun to determine what changed? Who made the change? and when was the change made? Far too often this exercise is akin to looking for a needle in a haystack. The network administrator can begin by using telnet to access devices and executing a 'show run'. But that assumes he is aware of how the configuration file is suppose to look.

There always seems to be someone that wants information about the current network, and of course needed the information yesterday. Questions like – What devices are running IOS v12.01? and How many switch slots are empty? Surely, any network administrator can find this information, but at what cost. Accessing every device to retrieve the information could take hours and is prone to human error (missing devices, bad tabulation, etc). Of course, this first assumes you have a list of devices readily handy. If the network administrator is thorough, this information will be available the next time someone asks the question…that is of course assuming the network doesn't change.

As discussed on the previous page, it may be easy to change a few devices, but what about thousands? How would you handle changing the SNMP community strings on all devices? Again telnet access to every device is time consuming and error-prone especially for the overworked network administrator who wanted to go home at 5 o'clock with all the other employees.

Managing Today's Network
Common Solutions and Pitfalls

Cisco.com



- **Command Line Interface CLI**
  - **Statistics (Show Commands)**
  - **Device Configuration (Config t)**

All management tasks can be handled using the CLI, but…

- **Potential Pitfalls**
  - **Need up-to-date list of devices and passwords**
  - **Human Error (fat finger, missing a device, etc.)**
  - **Correlating Statistics**
  - **Time Consuming**

RME v4.0 Tutorial Introduction 1-10

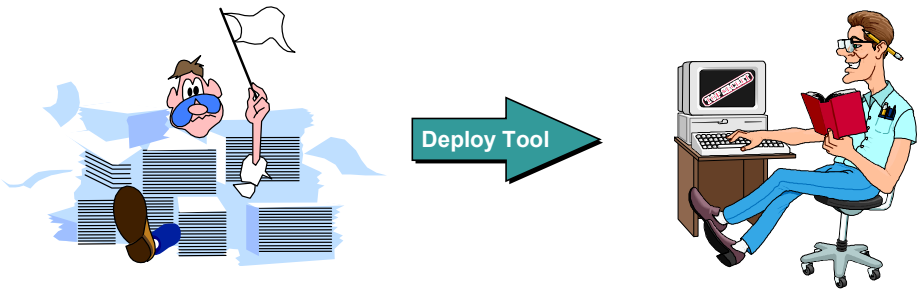
Common Solutions and Pitfalls

There is no real magic to performing configuration management tasks, all data is readily available through the Command Line Interface (CLI). The CLI provides direct access to the set-up, configuration, and statistics of a device. In fact, most skilled network administrators can quickly make necessary changes in this manner. So telnet, show commands, and 'config t' will always be important tools for configuration management tasks. This problem comes from when these tasks need to be performed for thousands of devices on an ever changing network. The biggest challenge being time! Cut and paste can help eliminate most errors, but even the most diligent can forget a device or two a couple hours into a task in the middle of the night. Plus, in the case of gathering data, the gathering part may be the easy portion of the task, the data still needs to be correlated and perhaps analysed before the goal of the task is achieved.

Managing Today's Network
Tool Requirement

Cisco.com

- **Network Management Tools Should…**
  - **Relieve Network Administrators from mundane repetitive tasks**
  - **Save time and prevent errors in performing large scale configurations and image upgrades**
  - **Quickly report up-to-date device information**



Tool Requirement

The past few pages should have clearly detailed the need for a tool to assist the network administrator in performing many network management tasks. The minimum goals of a network management tool should be to relieve the network administrator from mundane repetitive tasks, save time for configuration tasks, quickly provide up-to-date information, and to avoid configuration mistakes due to human errors.

Cisco’s Solution

- Managing Today’s Network
- ➢ **Cisco’s Solution**

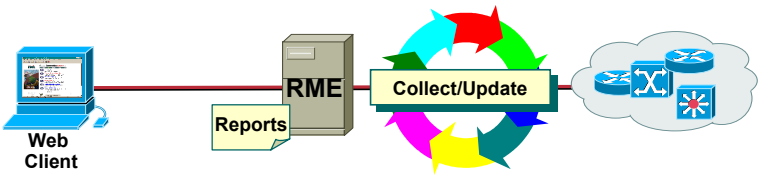
Cisco's Solution

Resource Manager Essentials (RME)

Cisco.com

CiscoWorks Resource Manager Essentials (RME)
provides the foundation for stable network operations reducing costly, error prone, repetitive processes used to configure, monitor, and troubleshoot the network

- **GUI-based Configuration Management tool**
- **Reduces errors and staff hours spent on network administration**
- **Automates tedious and difficult update tasks**
- **Offers powerful troubleshooting tools with fault and error detection**
- **Tracks all inventory, configuration, and software changes to devices**



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Introduction 1-13

CiscoWorks Resource Manager Essentials (RME)

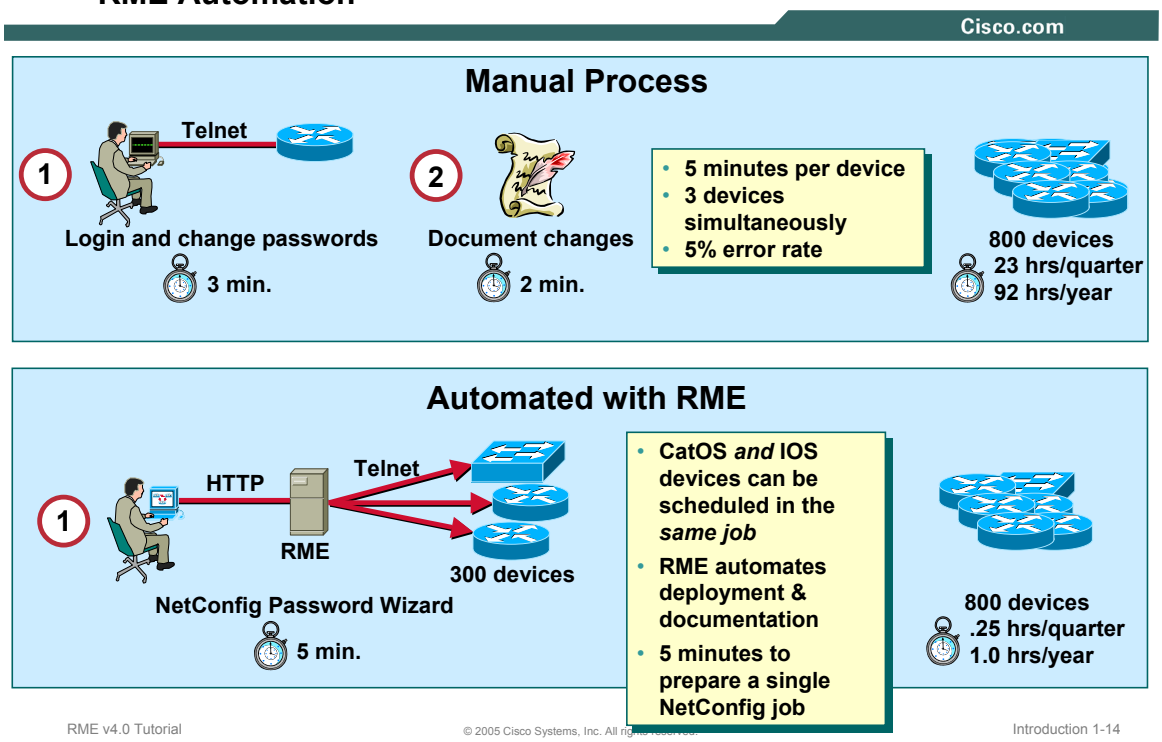
Cisco realizes that to efficiently maintain and troubleshoot a large network, network administrators need access to current network information and efficient tools to help in configuration and troubleshooting tasks. Since their time is at a premium, these tools need collect and process the information with little or no operator intervention.

CiscoWorks Resource Manager Essentials (RME) does exactly this, meeting the main goals of what a configuration management tool should do – automating mundane repetitive tasks, quickly providing up-to-date information, and simplifying large scale configuration and image deployments – minimizing complexity and saving time in the network administrator's busy day. RME achieves this by continuously collecting inventory and configuration information allowing the network administrator to quickly view up-to-date information and to determine if any changes occurred since the previous collection. Earlier it was mentioned that recognizing that a network is not functioning properly is easy, determining what changed is difficult; now RME handles that task automatically, minimizing down time and saving effort. Need to know what devices are running IOS 12.01, just a simple query of the inventory will provide the necessary data. Need to update those devices to IOS version 12.1, simply schedule a software management job to handle all the details. Again, saving time and effort, thus freeing up the network administrators time!

RME is an easy-to-use, intuitive resource for managing the network. The Web-based client interface with simple point-and-click tasks allows the network administrator to take advantage of the features of RME quickly and easily. After some minor setup, RME will continually collect device information and track any changes that may occur. No longer does the network administrator have to spend long hours gathering information or troubleshooting "what changed."

RME includes many time-saving features, including the ability to change many device configurations at one time or upgrading software images for multiple devices, all while the network administrator is at home asleep. The value of RME will quickly become apparent as it saves valuable time and effort and provides the answers to the "why" questions immediately!

Cisco's Solution
RME Automation



RME Automation

The figure above shows an example of automation using RME that will not only save time, but minimize errors as well. It has been stated before that network management tasks do not require special tools, however, the use of tools can certainly save a company time and money.

For example, if the task at hand is to change the passwords on 800 devices. Let's take a look at this task using both a traditional manual approach and using the NetConfig tool within RME.

Manual (Command Line Interface)

Assumption: Network administrator has a list of the devices and access to them.

Step 1: Access the device, login, and change the passwords – 3 minutes

Step 2: Update any documentation detailing this fact – 2 minutes

Job Completion: 5 minutes per device, working on 3 at the same time with a 5% error rate results in a total time of approximately 23 hours or nearly 3 days of one person's time!

RME (NetConfig)

Assumption: RME has been properly configured. Multiple jobs are created to break-up the project.

Step 1: Access RME, launch and configure NetConfig Password wizard (select devices, enter new passwords, schedule job) – 5 minutes

Step 2: NetConfig performs password change, updates RME database with new passwords, archives new configuration files, and produces a change record automatically! – No operator time required

Job Completion: 5 minutes per NetConfig job creation (300 devices/job, 3 jobs), 0% error rate results in a total time of approximately 15 minutes.

Analysis

The manual process takes 92 times longer than when using RME not to mention the automated documentation detailing the exact change made and when it was made by NetConfig. RME achieves multiple goals – saving time, automating mundane task, and simplifying large scale deployment!

Note: CatOS and IOS devices can be scheduled in the same job. Also, all 800 devices could be scheduled in one job if the job parameters are the same!

RME Time Savings!

	Manual	RME
Software Update	299 hrs/year	31 hrs/year
Gathering Configuration Info	89 hrs/year	.36 hrs/year
Device Configuration Change	92 hrs/year	1 hr/year
Total Time per Year	481 hrs/year	32 hrs/year

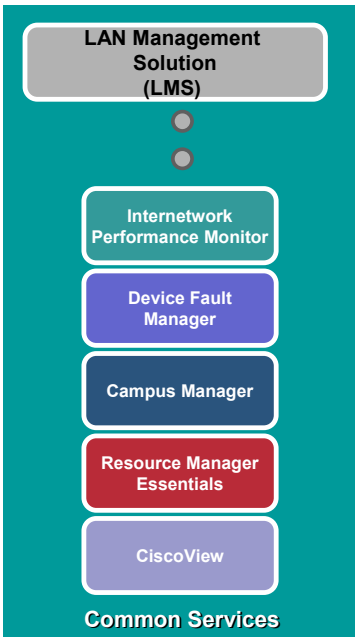
RME Time Savings

The network administrator is a busy person and time is a valuable commodity. Yet information is needed and configuration tasks need to be performed. RME provides a collection of tools to simply do what the network administrator doesn't have time to do, freeing time up so they can go about their business of providing a consistent, worry free network for the users.

Cisco's Solution

CiscoWorks LAN Management Solution (LMS)

Cisco.com



- **RME v4.0 is available in the CiscoWorks LAN Management Solution (LMS) bundle of applications**
- **All applications within a CiscoWorks bundle require the Common Services to be installed**

CiscoWorks LAN Management Solution (LMS)

So where does one find RME. RME v4.0 is available in the CiscoWorks LMS (LAN Management Solution) bundle of Cisco network management products. The applications within the CiscoWorks bundles all rely upon the Common Services (CS) software that is installed on the CiscoWorks server. These services provide the necessary background processes for accessing the database, web services, network discovery, process management, security, and more.

All applications share the same device database information, simplifying the use of all applications and speeding up the startup time. Other CiscoWorks applications included in the LMS bundle are:

- *CiscoView* — Graphical device-management providing real-time device status and operational and configuration functions.
- *Campus Manager* — Suite of applications designed for connectivity discovery, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, and Layer2/Layer 3 path-analysis.
- *Device Fault Manager (DFM)* — Provides real-time fault analysis for Cisco devices.
- *Internetwork Performance Monitor (IPM)* — Response time and availability troubleshooting application.

Note(s):

- *The CiscoWorks Small Network Management Solution (SNMS) bundle also contains a earlier and restricted version of RME.*

Thank You!

Continue on to Chapter 2 to discover the many features of RME used to maintain device information, manage software images, update configuration files, view Syslog messages, and track changes to the network.

<Intentionally Blank>

RME Features

Chapter 2

Chapter 2 Outline

Cisco.com

- **RME Overview**
- **RME Management Services**
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- **Device Center**

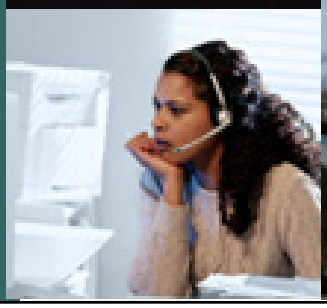
Chapter 2 Outline

Hopefully, Chapter 1 has excited you to the possibilities of Resource Manager Essentials (RME). This chapter discusses the key features of RME and how it can be used to help manage and troubleshoot problems on the network. In this chapter, RME is reintroduced and its main services are presented along with some of the key features in RME and a functional flow. In addition, each of the functional areas will be discussed in more detail – what they provide, their key features, how it works, and samples of the associated tasks. And lastly, the chapter briefly discusses the Device Center application which provides a collection of all CiscoWorks collected data for a specific device, and launch points for other CiscoWorks network management tasks.

By the conclusion of this chapter, the reader should have a good understanding of the components of RME and what is possible with them. Chapter 3 will then provide the jump start to using RME through a series of scenarios that takes you from getting started using RME, to managing the inventory, software images, and configuration archive.

RME Overview

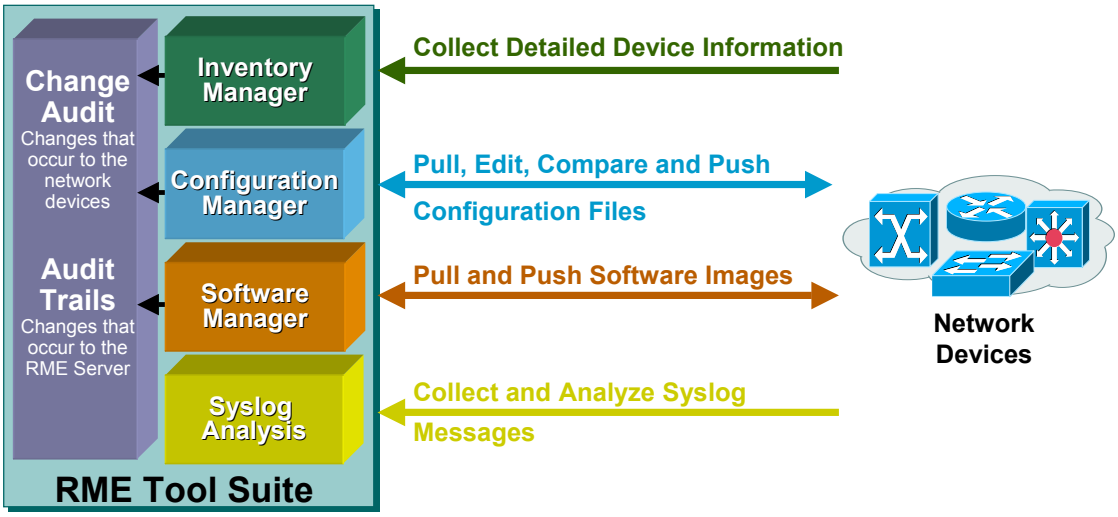
- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center



RME Overview

Cisco.com

Resource Manager Essentials is a suite of tools used to simplify management operations of a Cisco Network



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. RME Features 2-4

RME Overview

RME is the cornerstone application for the CiscoWorks LMS bundle of infrastructure management tools focusing primarily on configuration management tasks. It includes many automated features that simplify configuration management tasks, such as performing software image upgrades or changing configuration files on multiple devices. RME also includes some fault-management features, such as filtering of Syslog messages.

RME consists of the following major components:

- *Inventory Manager* - Builds and maintains an up-to-date hardware and software inventory providing reports on detailed inventory information.
- *Configuration Manager* – Maintains an active archive of multiple iterations of configuration files for every managed device and simplifies the deployment of configuration changes.
- *Software Manager* – Simplifies and speeds software image analysis and deployment.
- *Syslog Analysis* – Collects and analyzes Syslog messages to help isolate network error conditions.
- *Change Audit Services* – Continuously monitors incoming data versus stored data to provide comprehensive reports on software image, inventory, and configuration changes.
- *Audit Trails* - Continuously monitors and tracks changes made to the RME server by the system administrator

Each of these components will be examined in more detail in the next section.

RME Features

Cisco.com

Simplify and Automate Management Operations!

- **Builds a complete inventory of Cisco network devices**
  - Quickly create reports on detailed inventory information (device types, software versions, memory, flash characteristics, etc.)
- **Builds an archive of configuration files iterations**
  - Compare and search configurations
- **Builds a repository of software images**
- **Manages deployment of configuration changes and software image updates**
- **Simplifies monitoring of critical network resources**
- **Tracks changes to all devices and changes to the RME server**
- **Reduces chances of human error in data collection and change deployment**
- **Optional Job Approval requires certain jobs to be approved before they are run**

Saves Time & Minimizes Errors!

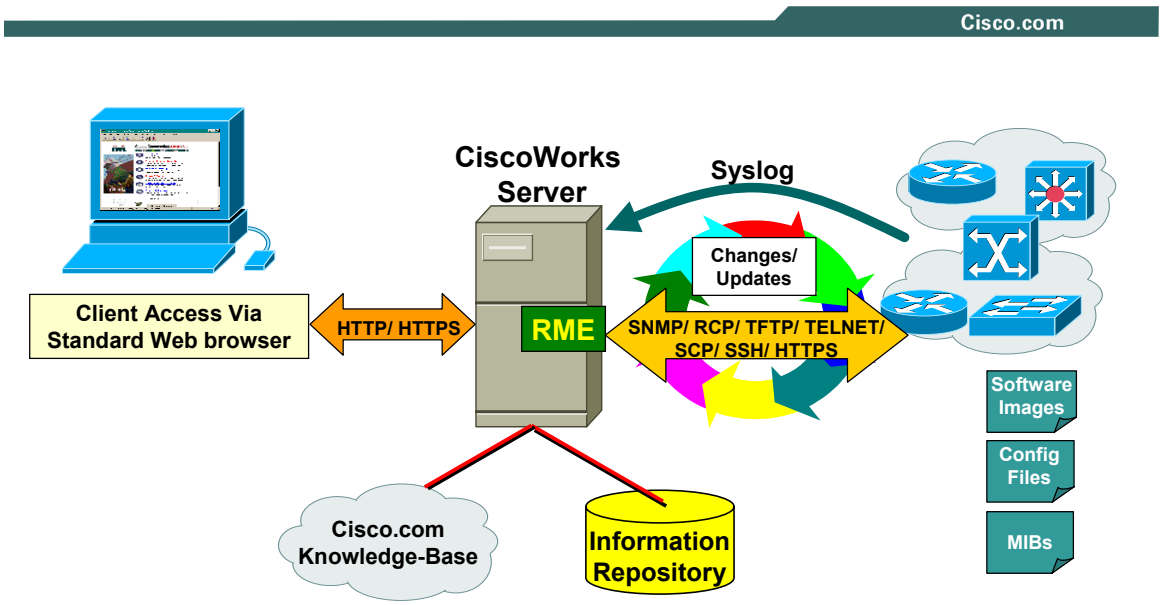
RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. RME Features 2-5

RME Features

Chapter 1 talked about goals of a configuration management tool. Plainly put, a good configuration management tool should make the life of a network manager simpler – saving time, simplifying, and automating. RME succeeds at all these goals. Chapter 1 mentioned that all needed configuration data can be retrieved using telnet and a lot of time and patience. RME automates all collection activities, and simplifies the device configuration modification tasks. The above list is the short version of the many features of RME and its associated components. The remainder of this chapter will highlight many of features of RME and how to use them in your daily tasks. The savvy reader will also certainly discover many additional uses for the tools.

Bottom line, RME saves time and reduces errors, resulting in better network operations.

RME Functional Flow



RME Functional Flow

The key to RME is its ability to keep the database up-to-date with all configuration information including device inventory, software images, and configuration files. A benefit of this activity is the ability for RME to detect and report changes. RME uses various transport protocols necessary (i.e. SNMP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), TFTP, Telnet, Secure Shell (SSH), and HTTPS) to access the devices and retrieve the necessary data.

Note:

- You can set the management protocol order for each of the management tasks using *RME > Administration*. The select the management tasks for which you would like to set the preferences for. For better performance, set *TFTP* as the first protocol. For unreliable WAN connections, use RCP.

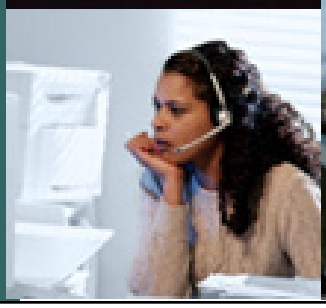
The best part about using RME for your network management needs is that many of its features are automatic, freeing the network administrator from mundane data collection activities. To start using RME, the administrator has to add the devices to be managed and provide the proper access credentials (SNMP community strings, passwords). Most of the collection activities already have a default schedule and begin collecting as soon as the devices are added.

User access to RME is through a standard web browser (refer to Chapter 4 for specific versions and client requirements). RME relies on the CiscoWorks server for common services. These services within CiscoWorks are call Common Services (CS), such as the database engine, online help, security, login, application launching, job and process management, and the Web server.

Now, let's take a look at RME and its components in more detail, starting with the RME Inventory.

RME Management Services Inventory

- RME Overview
- ➢ RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center



Inventory Management
What is it?

Cisco.com

- An up-to-date database about the details of the devices in the network:
  - ☑ Know the number, type, and capacity of all devices running on the network.
  - ☑ Keep track of additions, deletions, and changes to network devices.
  - ☑ Maintain detailed device information, such as chassis type, software version, memory characteristics, and interface settings.
- Starting point for other management functions

RME v4.0 Tutorial RME Features 2-8

What is Inventory Management?

Inventory Management is basically knowing what Cisco devices are actively deployed in the network and basic information about them - How many 7200 routers are there? What devices are running IOS v12.01? How many empty switch slots are there?

Inventory Management provides comprehensive device information, including hardware and software details. This information is crucial for network maintenance, upgrades, administration, troubleshooting, and basic asset tracking. The inventory information can also be leveraged by other applications needing access to this same information without the need for additional device queries. Network administrators must often be able to quickly provide information to management on the number and types of devices being used on the network. The more information network administrators have in one central place about all the devices, the easier it is to locate necessary information, resolve problems quickly, and provide detailed information to upper management.

Inventory Management is also the starting point for many other management activities. For example, to upgrade the software image of a device, information about the amount of RAM, the modules installed, and the current software version is needed. All this data is collected by RME Inventory Management!

Inventory Management
Key Features

Cisco.com

Cisco 2600 Series Multiservice Platforms

Device Name	Updated At	System Description	Location	Contact	Serial Number	Chassis Vendor Type	Total RAM Size (MB)	NVRAM Size (KB)	NVRAM Used (KB)	ROM Version	Total Flash Device Size (MB)
nmtg-cme-2651.cisco.com	Jan 03 2005 12:41:37	Cisco IOS Software, C2600 Software (C2600-IPBASE-M), Version 12.3(4)XD, RELEASE SOFTWARE (fc1) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2003 by Cisco Systems, Inc. Compiled Fri 07-Nov-03 18:39 by eaarmas			JAE073503YM (3192240085)	c2651XM	123.00	28.99	3.87	12.2(7r)	16.00

Cisco Systems

24 Hour Inventory Change Report

Generated on Jan 05 2005 10:10:04

Summary

Total number of submitted device(s):	29
Number of device(s) with data :	26
Device(s) with Change:	1

Changes for Device: nmtg-demo-6000-msfc.cisco.com

Memory Pool Identity: MemoryPoolID = 1

Attribute	Type of Change	Time Change Detected	Previous Value	Current Value
Used (MB)	Changed	2005-01-04 14:12:57.323	8422484	8435164
Free (MB)	Changed	2005-01-04 14:12:57.323	24086376	24073712

- **Automate the collection of detailed inventory information. This eliminates the chance of human error and allows tracking inventory changes**
- **Quickly create current reports on various details of the network device inventory**

RME v4.0 Tutorial RME Features 2-9

Inventory Management - Key Features

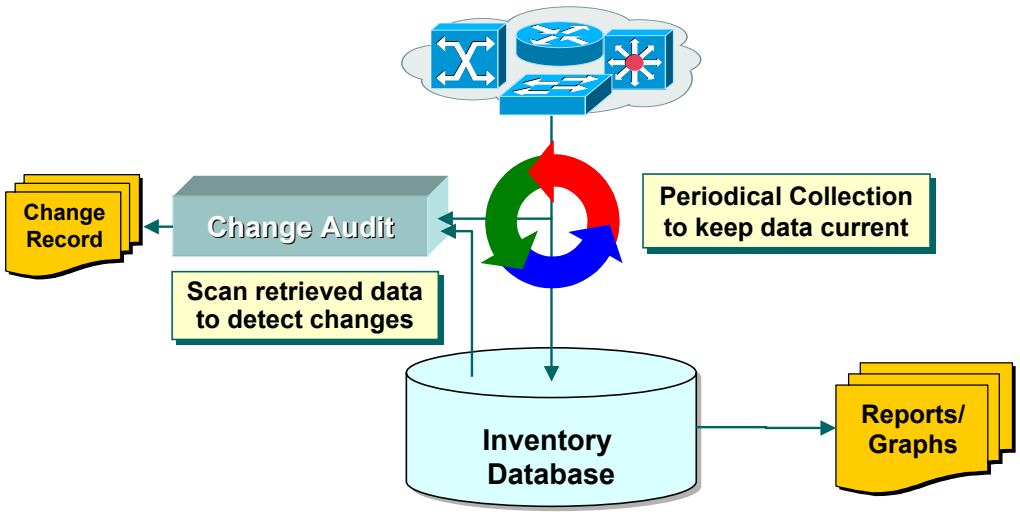
Since device inventory and component information is regularly collected and stored in the RME database, the Inventory Management function provides readily available up-to-date reports on hardware and software characteristics of Cisco devices.

RME contains numerous pre-defined inventory reports including detailed device reports which provides information on software versions, switch modules, and interfaces on each device. Chassis reports which contain information on available slots and slot capacity that can can assist in capacity planning activities. RME also allows the user to create custom reports which basically equates to performing a query on the database using user selected variables and conditions. For example, RME easily helps you answer the question, "*What devices have less than 32MB of RAM*?"

Again these questions can all be answered the traditional way by using telnet to access the device, running the appropriate show command, and recording the information. But how much easier is it when the data has already been collected?

Inventory Management
How it Works

Cisco.com



RME v4.0 Tutorial RME Features 2-10

How Inventory Management Works

The first order of business is adding devices to be managed by RME. The devices are added from the Device and Credentials Repository (DCR) which is a component of Common Services (briefly discussed next). RME can be configured to automatically import any device from the DCR into RME, or it can also be done in a more selective manner. The first scenario in Chapter 3 will have more details on this topic.

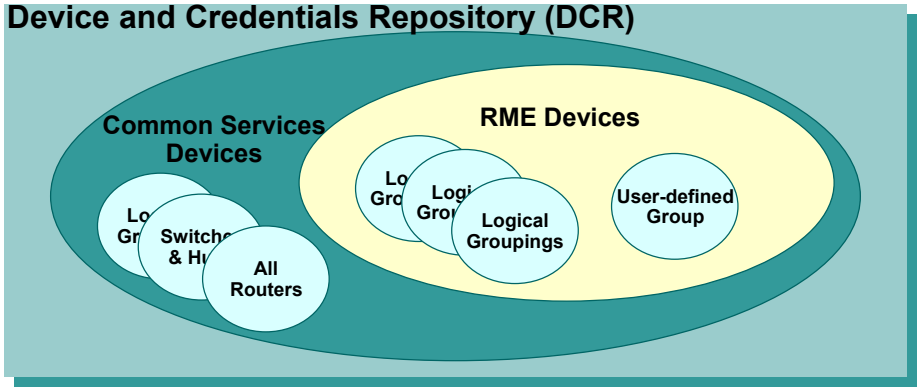
Once RME is informed of the devices to be managed (the SNMP read community string for the device must also be in the DCR), RME polls the MIB of the device and retrieves all necessary inventory information.

Inventory Management can now be configured to automatically re-retrieve the inventory information on a periodic basis in order to keep the database current and to detect any changes. (By default, a schedule exists.) If any changes are detected in hardware or software components, the inventory database will be updated and a change audit record will be created to inform the network administrator of the change and as a means to document the event. This helps to ensure that the information displayed in the inventory reports reflect the current state of network devices.

Inventory Management
Managed Devices

Cisco.com

- **Device and Credential Repository (DCR)**
  - Collection of devices to be managed and these credentials
    - IP Address
    - Community Strings
    - Passwords
- **RME subscribes to a subset of the devices in the DCR**
  - Users can create or use existing logical groupings of RME devices or CS devices to simplify performing RME tasks and generating reports



Inventory Management - Managed Devices

The previous page mentioned the Device and Credential Repository or DCR. The DCR is a component of the Common Services (CS) and all CiscoWorks applications use to access and manage the devices in CiscoWorks. The DCR allows for a common repository for device and credential information. No additional device data (software image, configuration file, etc.) is stored in the DCR. In this way, if credentials change (SNMP community strings, passwords, etc) on a device, the information only needs to be updated in one common place and all associated CiscoWorks applications will continue to work with the new credentials.

RME can subscribe to all or a subset of the devices in the DCR. RME keeps a local copy of the information which is continuously synchronized with the DCR. Therefore, if an RME application changes a device credential (i.e. NetConfig changing the SNMP community strings), the local data store is updated and immediately synchronized with the DCR so all other CiscoWorks applications are made aware of the change. The devices within the DCR and RME can also be grouped into logical groupings to assist in the selection of devices for various tasks.

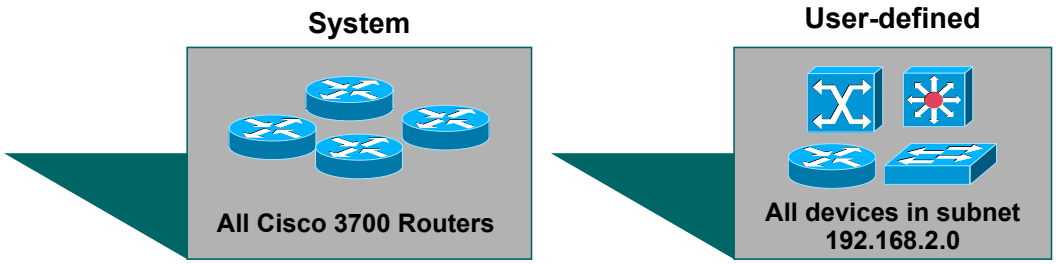
Note(s):

- *Groups created under the Common Service can also be used for RME tasks. A user is not restricted to using the groups only under RME.*
- *If other CiscoWorks applications are installed, such as Campus Manager, similar groups of devices are created for Campus Manager. The user can select from these devices as well when performing RME tasks.*
- *For more information on the DCR, its use, and the deployment of CiscoWorks, see the Common Services User Guide. A link to this guide can be found in Chapter 5 of this tutorial.*

Inventory Management
Grouping of Devices

Cisco.com

- **View is a Logical Grouping of Devices**
  - Simplify the selection of devices for various operations
- **System (pre-defined)**
  - Collection of devices based on device types
- **User-defined**
  - Membership based on set of rules
  - Groups can be private (available to creator only) or public (usable by all)



Grouping of Devices

Most every RME task is executed against a set of devices. When thousands of devices are being managed this will present some difficulties when trying to select specific devices for the task. For instance, a thousand devices are being managed and a detailed hardware report needs to be run for only the 7200 routers.

RME, and CiscoWorks in general, uses the concepts of groups to simplify the selection of devices. All CiscoWorks applications introduce default groupings. For example, Common Services has default system groups that categorize devices by type in a hierarchical manner (routers, 7200 router, etc). When selecting devices for an RME task, these groups can be used. A device can belong to multiple groups.

RME, and other CiscoWorks applications, also allow users to create their own groups. These groups are created using a set of rules and can be configured to be automatically populated or only with user intervention basically making for dynamic and static groups. Further, groups can be limited to only the original creator, or other CiscoWorks users.

This powerful feature further simplifies the use of RME if useful groups are created. Each device also has 4 user fields associated with it (stored in the DCR) that can be used to help define groups. For example, User Field 1 could be assigned to device location.

Inventory Management
Generating and Scheduling Reports

Cisco.com

24 Hour Inventory Change Report
Chassis Slot Details
Chassis Slot Summary
Chassis Summary Graph
Detailed Device Report
Hardware Report
Hardware Summary Graph
MultiService Port Report
Software Report
Software Version Graph

Report can be generated for one or more devices

Detailed Device Report

Generated on Jan 03 2005 15:55:46

Total number of devices:	1
Devices with Report Data:	1
Devices without Report Data:	None

Device Name : nmtg-hq-core-3725.cisco.com

System Information

Updated At	System Name	Domain Name	Description	Serial Numb
Jan 03 2005 12:41:37	nmtg-hq-core-3725		Cisco IOS Software, 3700 Software (C3725-IPBASE-M), Version 12.3(4)XD2, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2004 by Cisco Systems, Inc. Compiled Mon 12-Apr-04 02:33 by cmong	JMX0709L4

Chassis Information

Index	Description	Chassis Serial Number	Chassis Vendor Type	Chassis Model Name	Physical Entity Name	Slot Configuration	Manu
0	Two Network Module slot, three WIC slot, two Fast Ethernet port MARS router	JMX0709L4QR	c3725				

Bridge Information

Base Bridge Address	Number of Ports
00:0b:5f:30:40:18	0

Processor Information

Index	Parent Index	Parent Type	Slot Number	Description	Serial Number	Vendor Type	Model Name	Physical Entity Name	Slot Configuration	Manufacturer Name	Operational Status	RAM Size (MB)	NVRAM Size (KB)	NVRAM Used (KB)	Config Register Value	Reboot Config Register Value	HW Version	SW Version	FW Version	Number of Slots	Nu P
1	0	chassis	0	c3725 Motherboard with Fast Ethernet	0	cpu-c3725-2fe					OK	96.00	55.99	5.47	0x2102	0x2102	0.1				

RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. RME Features 2-13

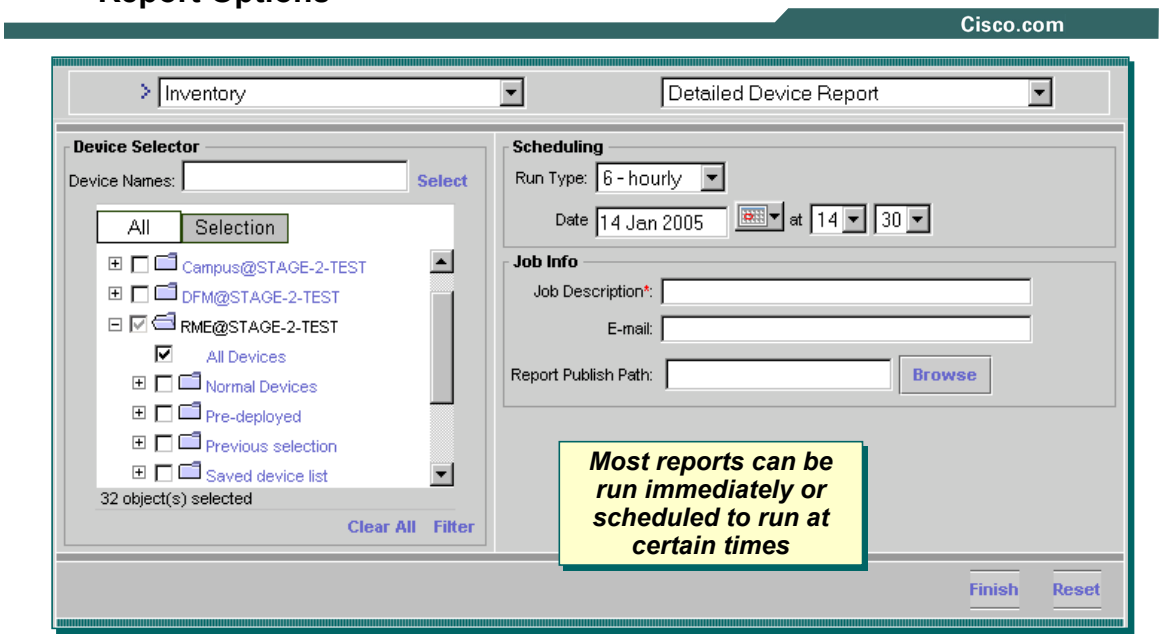
Inventory Management Sample Report - Detailed Device Report

The above picture is an example of the Detailed Device report. It includes system, chassis, bridge, processor, and module information presented in an easy to read format. This report was executed in a matter of seconds for a single device, but can also be run for a number of devices at one time. This provides a vivid example of the power of RME as the data in this report for even a single device using telnet and show commands would have taken quite some time to retrieve, and certainly would not be as well presented. Now multiply this by many devices, and the power of Inventory Management becomes even more evident.

Note(s):

- *The data field labeled 'Updated at' is a time stamp of when RME collected the data presented.*
- *The picture also shows a list of the other pre-defined system reports that can be quickly generated.*
- *RME also allows for the creation of custom inventory reports, as illustrated in Chapter 3.*

Inventory Management
Report Options



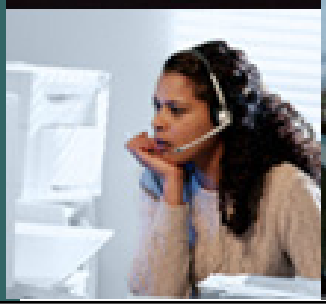
Report Options

RME is all about making network management easier and automating mundane tasks. This picture shows how the report generator can be used to schedule a report to be run on a periodic basis. This ability can assist in many troubleshooting activities and even allow for the automated reporting while safely at home.

Tip: It is important to remember that reports are based on the data in the database and do not directly contact the device. Therefore, a periodic inventory report only makes sense if an inventory collection occurs between the subsequent running of the report, else the data will be identical.

RME Management Services
Device Configuration

- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center



Device Configuration Management

What is it?

Cisco.com

- To be well informed about the configuration history of devices in the network:
  - ☑ Keep multiple iterations of device configurations (compare, download, etc.)
  - ☑ Simplify and control configuration changes to multiple devices
  - ☑ Track what changes were made, when the changes were made, and who made the changes
- Modify devices configurations with a variety of tools and templates to help create, compare, and deploy configuration files

What is Device Configuration Management?

Since network problems can often be traced to an incorrectly configured network device, device configuration management can be defined as the practice of being well informed about the configuration of devices in the network. Being “well informed” about the configuration of devices in the network means that in the event anything happens to a device, its configuration can be quickly restored. This would indicate that there should be some mechanism to record each version of configuration file for each device. This allows for the rapid restoration to a previous configuration and the ability to track changes between versions.

Device configuration management should also include mechanisms to simplify the actual configuration of devices. Although perfectly functional, using telnet to access multiple devices can be time consuming and possibly error prone if typing is not the forte of the administrator.

Device Configuration Management
Key Features

Cisco.com

- **Supports an up-to-date archive by automatically identifying and storing changes to configuration files**
- **Supports configuration file searching and comparing**
- **Config Editor tool allows for full screen editing and downloading of configuration files**
- **NetConfig tool uses templates to make the same change to multiple devices at one time**
- **Baseline Templates tool to create a set of commands containing placeholders for device-specific values to be substituted. Deploy to one or more devices or used to check for compliance.**
- **Supports one time passwords**

Device Configuration Management - Key Features

RME Configuration Manager includes several mechanisms to ensure that the configuration archive is populated with multiple versions of every device's configuration file. As new versions are retrieved, they are compared against the latest archived version and if any differences are noted a Change Audit record is created, acting as both documentation and possibly a heads up to why something is amiss. The existence of this archive makes performing several tasks much simpler for the network administrator including: searching to determine which device is configured with certain commands and comparing versions of configurations.

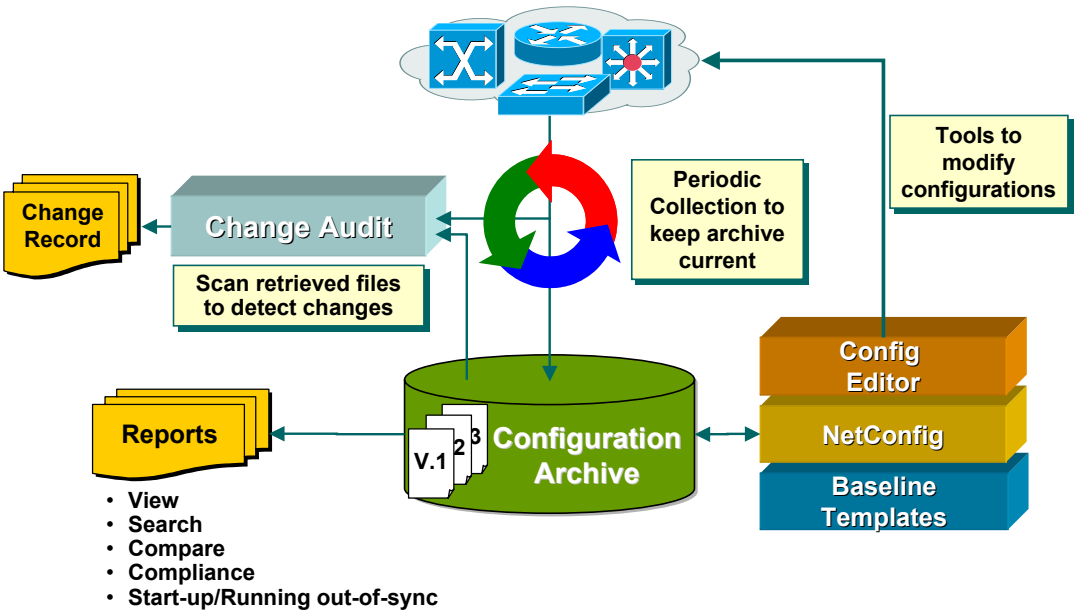
Configuration manager also has several tools useful in making changes to configurations, such as: Config Editor and Baseline Templates.

- The Config Editor tool allows the network administrator to make changes using a full screen editor and to then download those changes as part of a scheduled job.
- *Baseline Templates*, available in NetConfig, simplifies making the same change to many devices at once through the use of predefined command templates. For example, to change passwords on routers, the user would select the devices, select the password template, enter the new password, and schedule the download job; NetConfig would handle all the command syntax. The baseline template tool is similar to the NetConfig tool except all templates are created by the network administrator (NetConfig also allows for user created templates, but with hard-coded parameters). Uses for the Baseline Template tool are to create baseline configurations to assist in deploying new jobs. The templates would have all commands in the baseline and the network administrator would enter the proper parameters for each device and then schedule the download job. Further, using the baseline template, the network administrator can check to make sure deployed devices are conforming to the template by running a compliance report.

Device Configuration Management

How it Works

Cisco.com



How Device Configuration Management Works

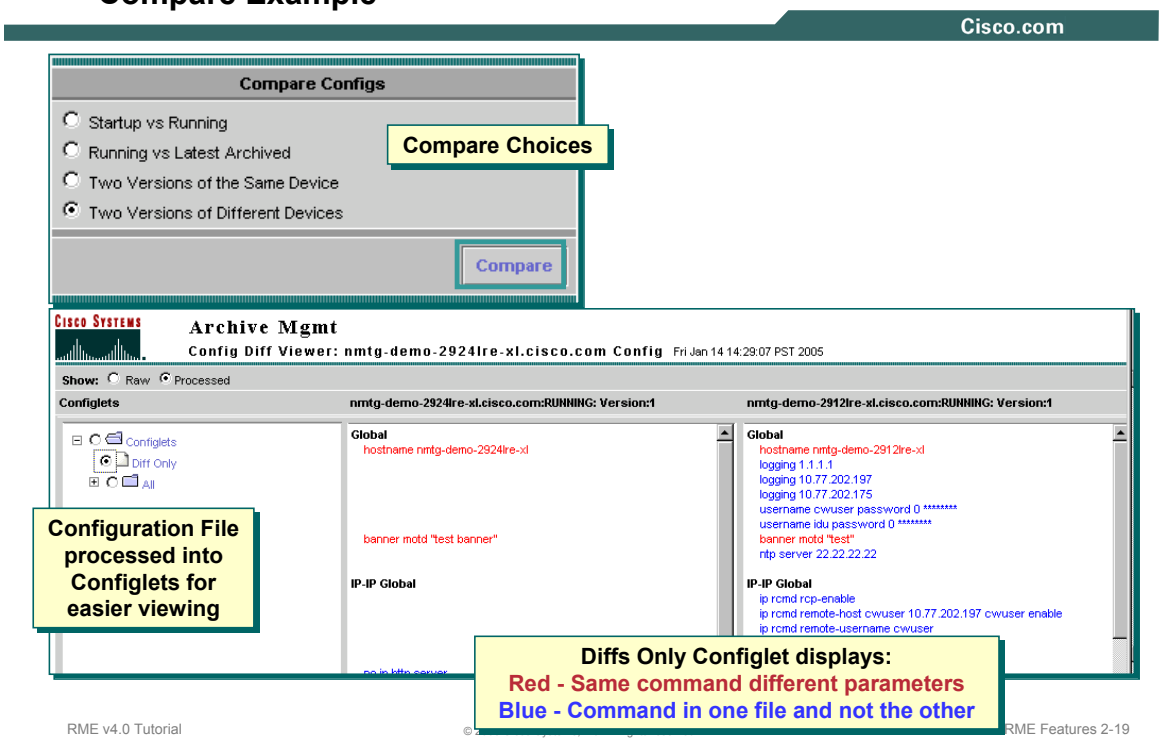
Configuration Manager is similar in operation as Inventory Manager. The first order of business is to create an archive of configurations and keep it up-to-date. The archive can be kept current using several mechanisms as described below.

- The first is to configure a schedule for retrieval. This method retrieves the configuration file and compares it with the latest version in the archive, if different, a Change Audit record is generated and the retrieved file becomes the latest in the archive.
- The second is to poll for the MIB variable indicating the time the configuration was last changed. If this is different then the value for the latest archived version, then the image is retrieved. Obviously, this method is not as resource intensive as the first.
- The third method is to configure the devices to send Syslog messages to RME. The Syslog Analysis function has an automated task that will retrieve and archive a configuration if a Syslog message is received indicating a change has occurred. Of course, the second and third method still makes sure the retrieved file is different than the latest in the archive to ensure that each archived version is different then the previous.

Once populated, the network administrator can search the archive, compare configurations, and use the archived versions as a starting point for using the several configuration tools.

Device Configuration Management

Compare Example



Compare Example

Comparing configurations files is an excellent way to see what changed or how close two different devices are. The Compare Config report (as well as any configuration report) allows you to view the configuration file in a *processed* format displaying Configlets or groups of like commands (i.e. all interface commands). The Compare Config report includes a special Configlet, 'Diffs Only', that allows the user to quickly see the differences between the two files. If both files have the same command, but with different parameters then the command will be displayed in red. If the command is in one configuration, but not the other, then it will be displayed in blue.

Four options are available for comparing configurations:

- *Startup vs. Running* - Compares the Start-Up configuration with the Running configuration. These configurations are fetched from the device.
- *Running vs. Latest Archived* - Compares the running configuration with the most recently archived configuration. The Running configuration is fetched from the device.
- *Two Versions of the Same Device* - Compares two archived configuration versions.
- *Two Versions of Different Devices* - Compares any two configurations in the configuration archive.

Device Configuration Management
Config Editor Example

Cisco.com

- **Config Editor**
  - ☑ Easy access to archived configurations
  - ☑ Full screen editor
  - ☑ Highly controllable download

Config Editor

The Config Editor tool included with RME Configuration Manager allows the network administrator to edit and download configuration files to devices using a GUI instead of the commonly used command-line interface. Use Config Editor to edit individual device configurations from the archive, and download them to a device. A copy of the updated configuration will automatically be stored in the configuration archive.

Note(s):

- *Config Editor is a full screen editor allowing for the user to modify, edit, or delete commands.*
- *No syntax checking is performed!*
- *Interactive commands are possible using the following syntax:*

  #INTERACTIVE

  command1<R>response1<R>response2

  command2<R>response1

  #ENDS_INTERACTIVE

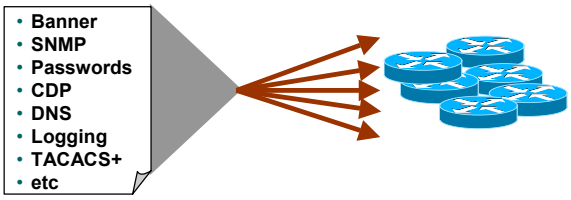
Device Configuration Management

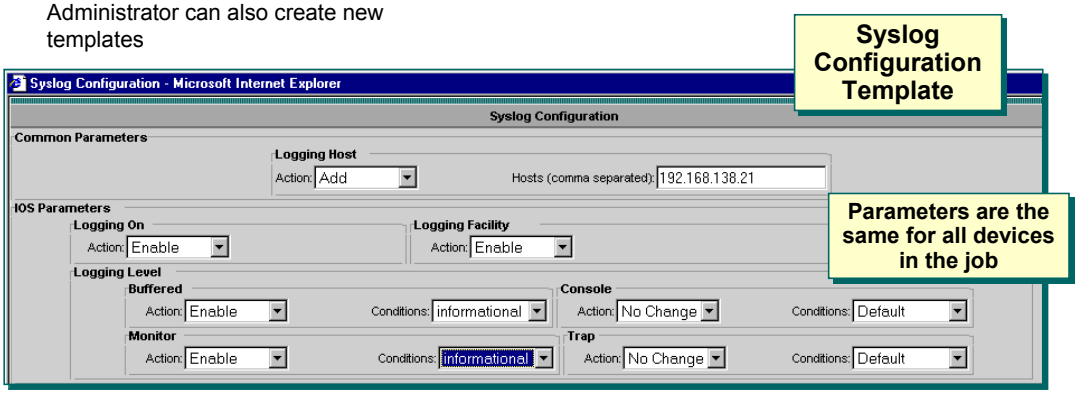
NetConfig Example

Cisco.com

➢ **NetConfig**

- ☑ Same change(s) to multiple devices in one highly controllable download job
- ☑ Template-based configuration changes to eliminate typos and the need to memorize syntax
- ☑ More than 30 pre-defined templates including an Adhoc (blank) template. Administrator can also create new templates





NetConfig

The NetConfig tool provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time. For example, if you want to change passwords on a regular basis to increase security on devices, you can use the appropriate password template to update passwords on all devices at once. A copy of all updated configurations will be automatically stored in the configuration archive.

NetConfig comes with many predefined templates that allow you to use a simple GUI to change many common device configuration parameters. These predefined templates include corresponding rollback commands. Therefore, if a job fails on a device, the configuration will be returned to its original state.

Note(s):

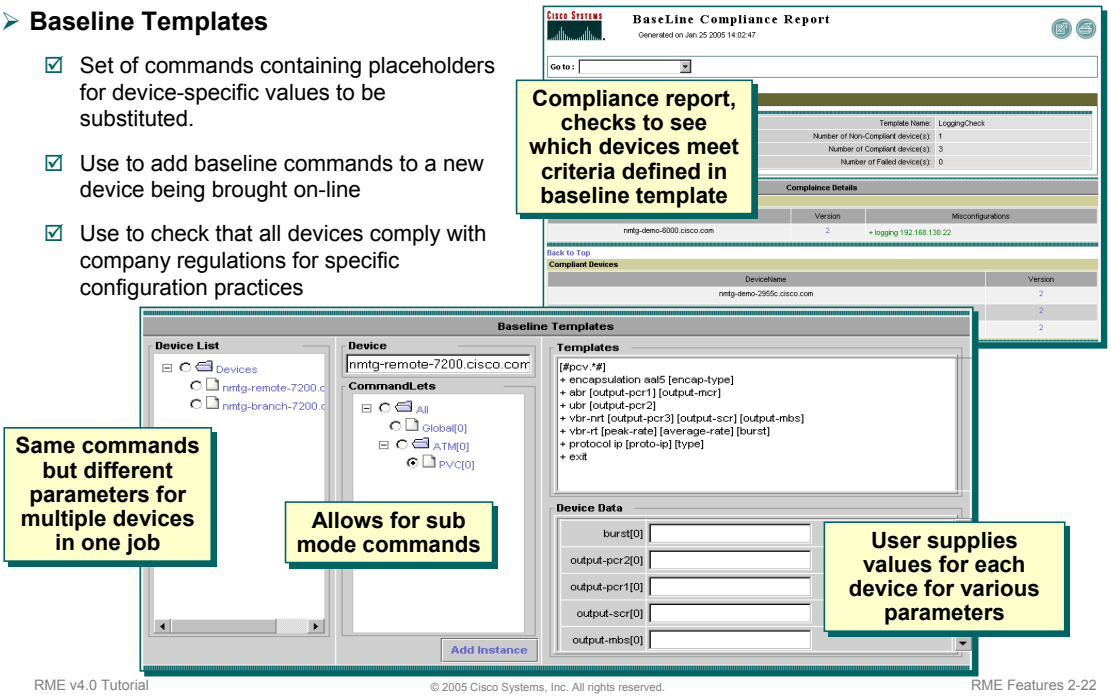
- *Network Administrators can also create new templates and assign CiscoWorks users without the Network Admin user role permission to run various templates. The assigned user must be a valid CiscoWorks user. If RME has been registered with a Cisco Secure ACS Server, then the user should be a valid ACS user. Also, the user must have the appropriate CiscoWorks privileges (Network Operator or Network Administrator) to use NetConfig. Use the Permission Report to check required privileges to perform task.*

Device Configuration Management

Baseline Templates Example

Cisco.com

- **Baseline Templates**
  - ☑ Set of commands containing placeholders for device-specific values to be substituted.
  - ☑ Use to add baseline commands to a new device being brought on-line
  - ☑ Use to check that all devices comply with company regulations for specific configuration practices



Baseline Templates

Baseline Templates allow for the creation of a set of commands containing placeholders for device-specific values to be substituted. These templates can now be run against a set of devices (of the same type or category) and the placeholders populated with the appropriate value for each device (with NetConfig templates, all devices included in the job get the same value for the command placeholders). Baseline Templates can be used to identify a set of standardized policy based commands that you would want to have on a set of like devices.

When a new device of the same type is added to the network, use a previously created Baseline Template to quickly bring the device into compliance with corporate policy. Baseline Templates can be created for any device or interface type.

Baseline Templates can also be used to compare existing device configurations against the templates to determine which devices are non-compliant to the baseline template. The non-compliant devices can also be brought into compliance as part of the same job.

RME Management Services Software Image

- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center

Software Image Management
What is it?

Cisco.com

- To control and simplify the routine deployment of software upgrades:
  - ☑ Keep current repository of images to quickly recover from failure or upgrade
  - ☑ Maintain history of software image upgrades
  - ☑ Distribute directly to device or use another device as a remote staging device

What is Software Image Management?

So far this chapter has discussed the management of both the hardware devices and their configuration files. The third piece to consider for overall configuration management of the devices in the network is the system software or operating system of the device. For complete coverage, it makes sense to have a repository of the software images being used on the network so that in the case of failure the image can be pushed back down to the device. Also, since improvements to the software are always being made, it would be nice to have a tool to help in the deployment of the new images that reduces the time and effort to upgrade devices to a new image.

Software Image Management
Key Features

Cisco.com

- Reliably distributes single or multiple images in a single deployment operation
- Automates the many time-consuming steps while reducing the error-prone complexities of the upgrade process
- Repository of current images allows for rapid recovery from failure
- Image can be deployed from repository or from another device flash
- Ability to identify critical bugs in software

Software Image Management - Key Features

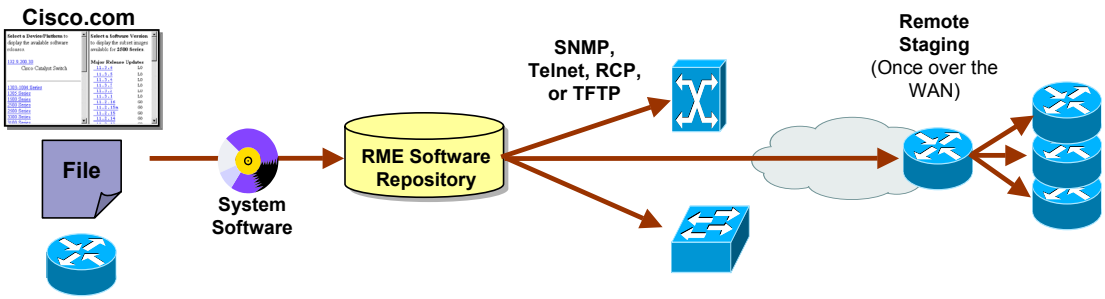
Perhaps the biggest feature of the Software Image Management function within RME is its ability to reduce the time and effort it takes to upgrade many devices in the network. Software Image Management allows for the creation of a single job that can upgrade multiple devices reliably and unattended.

Software Image Management is flexible enough to perform the upgrades from the server or by first deploying to a remote devices and then having the other devices retrieve the image from the remote device reducing WAN traffic. As the job is being created, Software Image Management will check to see if the device to be upgraded has enough resource for the image in the repository to be downloaded, thus reducing errors.

RME also has numerous reports that link to Cisco.com to help track the bugs reported for various images.

Software Image Management
How it Works

Cisco.com



How Software Image Management Works

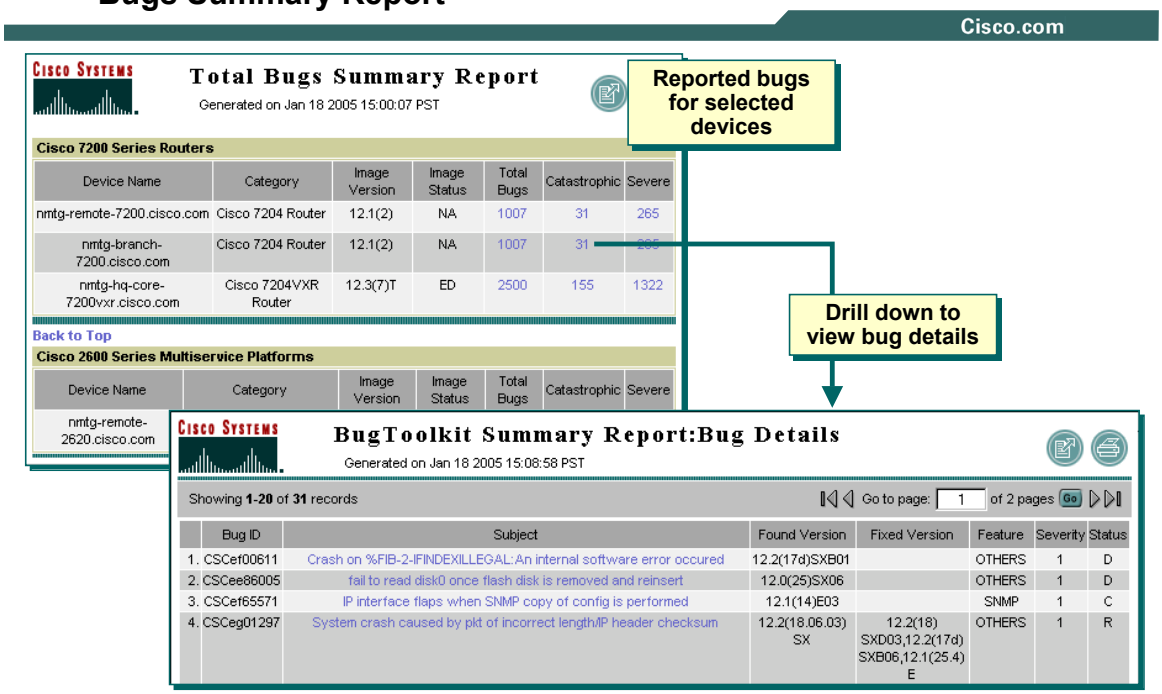
Before any images can be deployed to network devices, the software images must be first imported into RME to be maintained in the software repository. RME does include a mechanism to perform a baseline import from all devices on the network, and a job can be schedule to ensure that all unique images on the network are in the repository. In the case of failure, the proper image can now be deployed back to the device or its replacement.

To upgrade a device to a image not in the repository, it to must first be imported to the repository. This can be achieved from another device, a file, or most likely from Cisco.com. Prior to being imported from Cisco.com, the device to be upgraded can be analyzed to determine if it has the proper resources to run the proposed image.

Any image that is stored in the repository can now be distributed to one or more compatible devices on the network. Software distribution is performed in a reliable manner controlled by the network administrator. Each step of the deployment process is recorded, so if failure occurs, the network administrator will know exactly why. Once upgraded, Change Audit will generate a change record to document the event.

Software Image Management

Bugs Summary Report



Bugs Summary Report

The Bug Summary Report displays a summary of the software image bugs for selected devices. This list is retrieved from Cisco.com, hence a Cisco.com account is required to execute this report.

Software Image Management
Upgrade Analysis Report

Cisco.com

Cisco Systems — Resource Manager Essentials

Upgrade Analysis Report

Analysis Result for nmtg-branch-7200.cisco.com with image: c7200-jk9o3s-mz.122-26.bin

Device Information	FLASH	RAM	TELNET
Running Image Name: C7200-JK2O3S-M Running Image Version: 12.1(2) BootROM Version: 11.1(13)CA Running Image Feature: ENTERPRISE|FIREWALL 2 PLUS 3DES Device Family: C7200	Upgrade one of flash cards to 16 MB.	Upgrade from 68 MB to 128 MB	Telnet access not required for this device.

Use Upgrade Analysis to determine if the device to be upgraded has sufficient resources for the new image

- ☑ ***Does the device have sufficient RAM to hold the new software?***
- ☑ ***Have the minimum ROM version requirements been met?***
- ☑ ***Is the Flash memory large enough to hold the new software?***
- ☑ ***Do I need to add Telnet access information for the device to the Device and Credential Repository?***
- ☑ ***Have I performed an upgrade path and NVRAM analysis on my Catalyst devices?***
- ☑ ***Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?***

Upgrade Analysis Report

To avoid common resource related errors when upgrading the software image on a device, first use the Upgrade Analysis option to determine the impact to, and prerequisites for a new software deployment using images that reside in either Cisco.com or the image repository. An administrative task allows for the setting of certain criteria for an image to match in order to be analyzed against the device to be upgraded, to determine possible required hardware upgrades (boot ROM, Flash memory, RAM, and access).

Software Image Management

Add Images Example

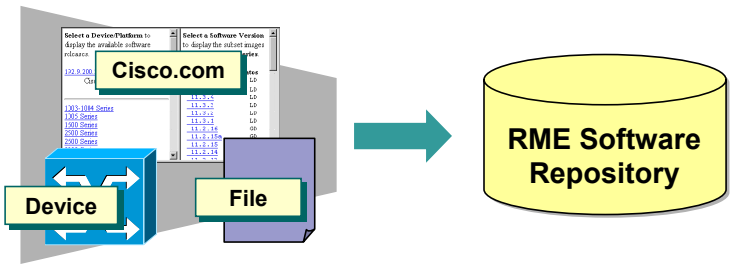
Cisco.com

Filter by: File Name Filter

Showing 6 records

		File Name	Image Family	Image Type	Version	Size	Status	Updated at	Comments
1.		c2900XL-c3h2-mz-112.8.5-SA6.bin	C2900XL	SYSTEM_SW	11.2(8.5)SA6	1.11 MB	Unknown	Jan 13 2005 12:32:50	Added as part of Job-1024
2.		c2900xl-c3h2l9s-mz.120-5.WC10.bin	C2900XLLRE	SYSTEM_SW	12.0(5)WC10	1.84 MB	Unknown	Jan 13 2005 12:32:19	Added as part of Job-1024
3.		c2900xl-c3h2l9s-mz.120-5.WC6.bin	C2900XLLRE	SYSTEM_SW	12.0(5)WC6	1.83 MB	Unknown	Jan 13 2005 12:32:51	Added as part of Job-1024
4.		c2950-i6q4l2-mz.121-9.EA1.bin	C2950	SYSTEM_SW	12.1(9)EA1	2.38 MB	Unknown	Jan 13 2005 12:32:52	Added as part of Job-1024

--Select an item to delete.--> Add Delete Update Status



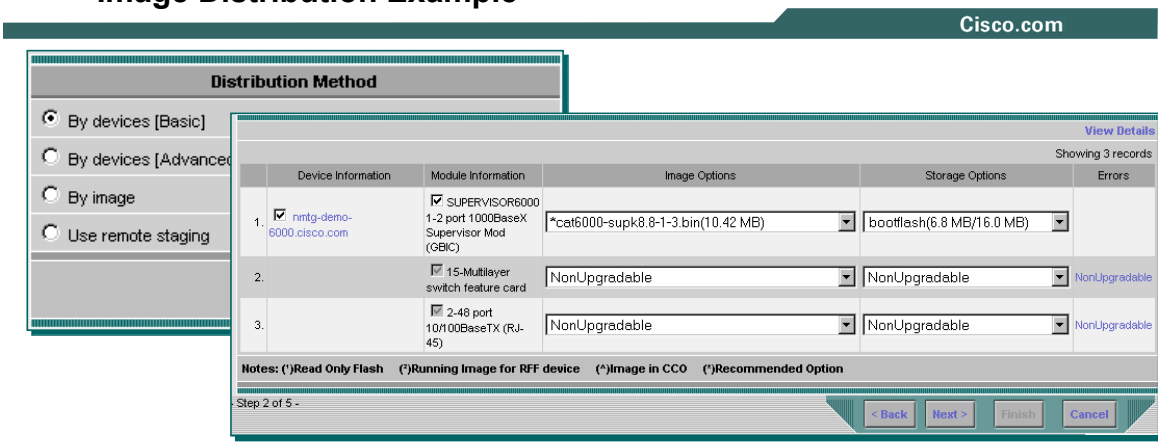
Add Images

RME allows for the importing of images into the repository from several different locations – another device, file, or Cisco.com. Images must be in the repository in order to be distributed to a device. The screen shot above shows the images currently in the repository.

A special import can be scheduled to import a baseline of images from the network. Similarly, a synchronization job can be schedule to ensure the repository contains all unique images of the network.

Software Image Management

Image Distribution Example



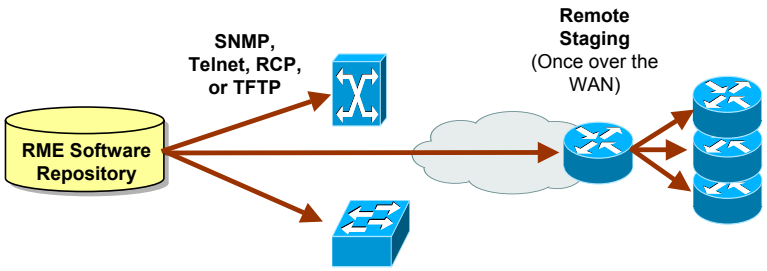
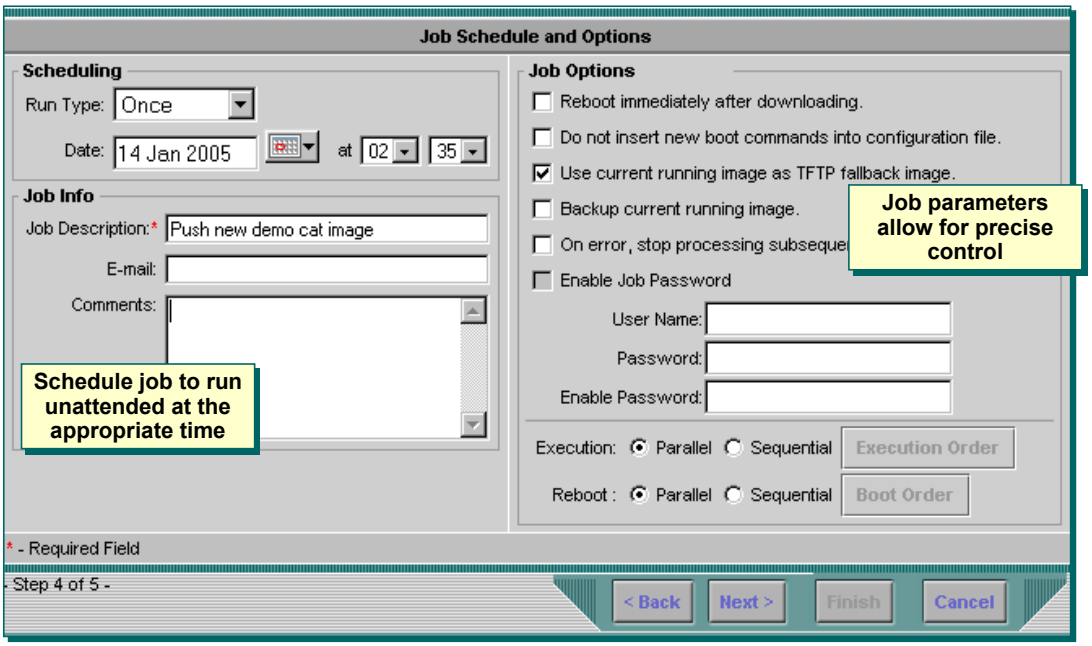


Image Distribution

RME allows the network administrator to schedule a job that will reliable distribute images to one or more devices. A software distribution job will record each step of the task so that if a failure occurs the network administrator will know exactly how to fix it. Images can be distributed directly from the server to the device, or by first distributing the image to a remote device and then have other devices retrieve it from there.

Software Image Management
Controlled Image Distribution



Controlled Image Distribution

Like most jobs in RME, the software distribution job allows the network administrator to closely control how the job is to be run. Not only can the job be scheduled to run at a specific time, but the administrator can also choose what to do to the device once the image is downloaded.

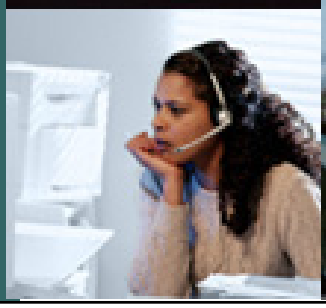
Additionally, you can enter the e-mail addresses to which the job will send status notices. (Separate multiple addresses with commas.) E-mail notification is sent when job is created, started, deleted, canceled, and completed.

The Job Options include:

- Reboot the device after downloading the software image
- Update the device configuration with new boot commands
- Failure policy – Specify what the job should do if it fails to run on the device.
- Enable Job Password – if job approval is enabled the user can the option to have RME ignore the username in the RME database and uses the newly entered username and passwords instead.
- Execution and Reboot order (parallel or sequential) - Based on your network topology and to minimize the impact on your network, you can schedule the upgrades job either sequentially or in parallel. For example, if devices A, B, and C are networked sequentially, then you must upgrade device C first, then device B, then device A. If you upgrade device B first, you might no longer have access to device C.

RME Management Services
Syslog Analysis

- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center



Syslog Analysis
What is it?

Cisco.com

- Track behavior of a device in the form of a message categorized by severity and function in real-time:
  - ☑ Messages sent by a device advertising a configuration change, error, or fault condition
  - ☑ Use filters to delete unnecessary messages and to execute a script in response to condition indicated in Syslog message
  - ☑ Identify and resolve problems quickly without having to decide what to monitor

Facility	Severity	Mnemonic	Description
LINK	3	UPDOWN	Interface E0 is down
SYS	2	MALLOCFAIL	Memory allocation of 28 bytes failed
RCMD	4	RSHPORTATTEMPT	Attempt to connect to RSHELL from 171.69.71.80
SYS	5	CONFIG I	Configured from 192.168.76.225 by snmp

What is Syslog Analysis?

One of the best forms of management is done by the device itself, and is communicated via Syslog messages. Syslog messages indicate some behavior or activity on a device. These can be strictly informational or can indicate a configuring change or even a failure. Imagine being informed of a network problem by the source and not by some irate user.

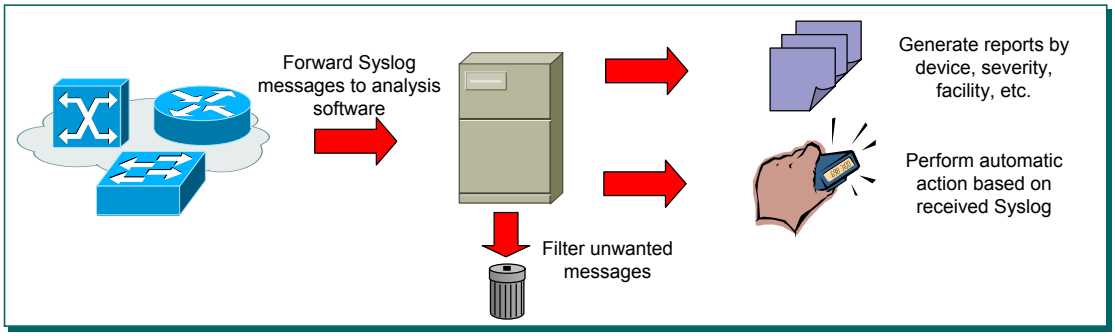
To leverage these useful messages, RME includes numerous reports to allow the user to view the received messages, and even allows for the configuration of an activity upon the receipt of select messages.

Of course to take advantage of this feature, devices must first be configured to forward Syslog messages to RME. This can be done easily using NetConfig!

Syslog Analysis
Key Features

Cisco.com

- Supports filtering of unwanted Syslog messages
- Can trigger user-defined scripts in response to specific Syslog messages
- Provides reports to quickly view Syslog events by severity, device, or message

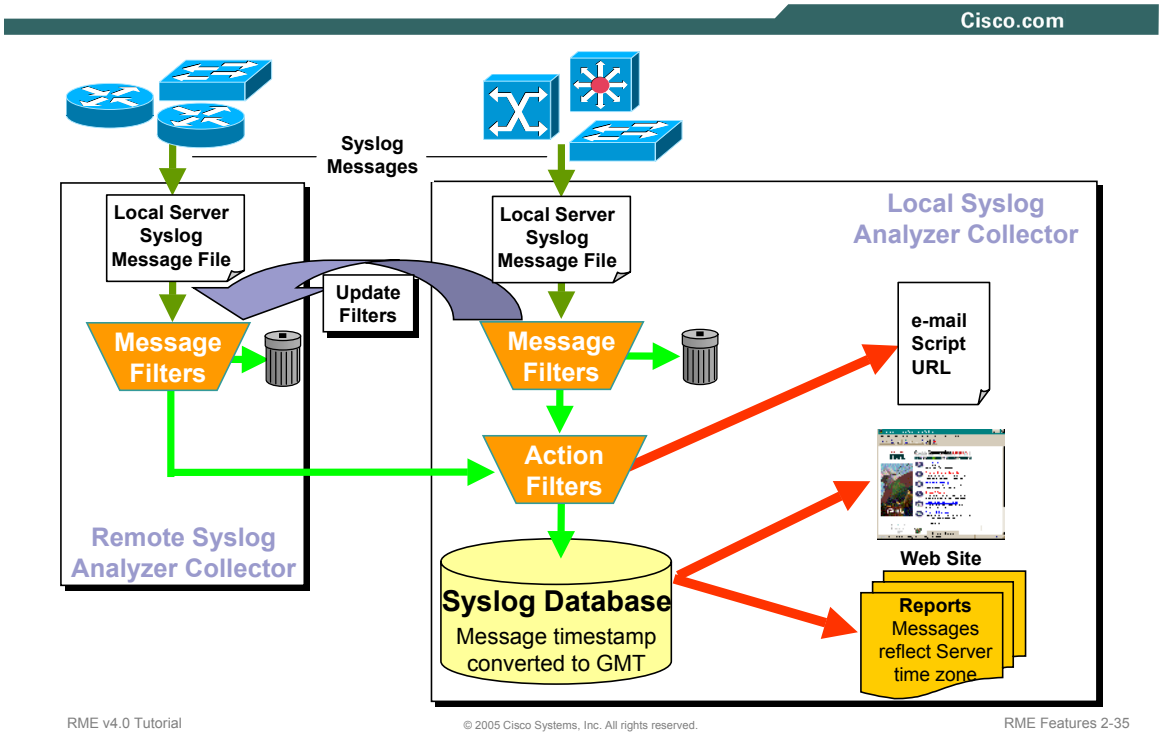


Syslog Analysis - Key Features

Since devices can send literally hundreds of messages a day, with many not being overly useful, RME allows for the creation of message filters to discard messages not critical to management activities. Conversely, some of the received messages may be so important that they need to be viewed and responded to prior to the next time someone happens to look at a Syslog report. In this case, a filter can be created to launch a task (email, URL, script) upon receipt of that message.

Finally, the available Syslog reports allow for their viewing by severity or by device, and includes the ability to create custom reports by message.

Syslog Analysis
How it Works



How Syslog Analysis Works

In order to utilize the Syslog Analysis features, devices must first be configured to forward Syslog messages to either the RME server or a remote Syslog Analysis Collection (SAC) server. The remote SACs are used to distribute Syslog message collection and processing in order to reduce Syslog traffic and processing on the RME server. All messages collected and processed by the remote SACs are periodically forwarded to the RME server, which maintains a central repository for all Syslog messages.

Syslog messages received by a collector are stored in the local Syslog facility on the server and are periodically read by the Syslog Analysis function for processing. Each message is compared against user-defined filters to determine if the message is considered important enough to keep. Messages not filtered are stored in the Syslog database (time stamp is converted to GMT) and checked against another set of user-defined filters to determine if the message should initiate a user-defined script (automated action). The database is then used to produce the various Syslog reports (messages displayed using the server time zone).

Any user-defined filters used for reducing the Syslog messages to be included in the Syslog database will be forwarded to any defined SAC.

Note(s):

- *Syslog Analysis has some message filters enabled by default. These include: Link Up/Down, PIX, Severity 7, and IOS Firewall Audit Trail messages are filtered out.*
- *PIX firewall devices generate a large number of Syslog messages. Thus, it has a tendency to lock the Syslog function on Windows servers due to the massive number of messages from the firewall.*
- *Creating your own filters or enabling/disabling filters is easy. Go to the tasks Resource Manager Essentials > Tools > Syslog > Message Filters.*

Syslog Analysis
Sample Report

Cisco.com

Resource Manager Essentials

Syslog Analyzer Severity Level Summary Report at Jan 14 2005 14:16:57 Pacific Standard Time(GMT -08:00:00)

Showing **1-7** of **7** records — Go to page: 1 of 1 pages

	Severity Level	Total number of records
1.	Severity Level 0	0
2.	Severity Level 1	0
3.	Severity Level 2	0
4.	Severity Level 3	276
5.	Severity Level 4	44
6.	Severity Level 5	3
7.	Severity Level 6	0

Rows per page: 20 — Go to page: 1 of 1 pages

Syslog messages by severity for a selected group of devices over a selected time period

Resource Manager Essentials

Syslog Analyzer Severity Level 5 at Jan 14 2005 14:17:01 Pacific Standard Time(GMT -08:00:00)

Showing **1-3** of **3** records — Go to page: 1 of 1 pages

	Interface	Timestamp	Facility[-Sub-facility]	Severity	Mnemonic	Description	Details
1.	192.168.159.106	Jan 12 2005 15:06:49	SYS	5	CONFIG	Configured from tftp://192.168.138.22/20050112150614296-192.168.140.1.cfg by console	*
2.	192.168.140.8	Jan 12 2005 16:29:59	SYS	5	CONFIG_I	Configured from tftp://192.168.138.22/200 192.168.140.8.cfg by console	
3.	192.168.140.8	Jan 12 2005 16:29:59	SYS	5	CONFIG_I	Configured from tftp://192.168.138.22/20050112162922906-192.168.140.8.cfg by console	*

Rows per page: 20 — Go to page: 1 of 1 pages

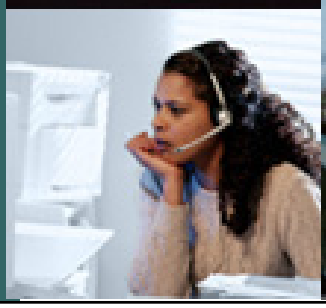
Syslog message details

Syslog Analysis Sample Report – Severity Level Summary

The Syslog Severity report lists the number of Syslog messages received (and not filtered) for each Syslog severity level for a selected time period and group of devices. Clicking on the number of received messages will show details of each individual Syslog message.

RME Management Services
Change Audit & Audit Trail

- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- Device Center



Tracking Changes

What is Change Audit and Audit Trail?

Cisco.com

- *Change Audit* is a record of all inventory, configuration, and software changes made in the managed network:
  - ☑ Know what change was made, when it was made, and who made it
  - ☑ Quickly identify network issues caused by changes
- *Audit Trail* is a record of all changes that are performed on the RME server by the RME administrator

What is Change Audit and Audit Trail?

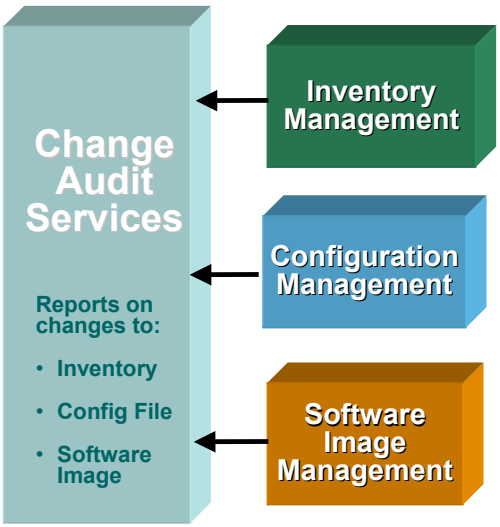
One of the most powerful features of RME is its ability to detect changes to the inventory, configuration files, and software images. Not only is this a great way to see what changed, when, and by who, but it is also an automatic way to document any changes made to the network.

Audit Trail tracks and reports changes that the RME administrator makes on the RME server. The list of changes that a system administrator can make to the RME server is huge and includes reports on changing preference settings, deleting devices, changing device attributes, changing policies or schedules, adding/editing Syslog filters, and more. For a complete list, refer to the RME User Guide.

Change Audit
Key Features

Cisco.com

- Comprehensive record of who changed what, when, and how
- Can trigger user-defined scripts in response to specific changes
- Integration with trap receivers

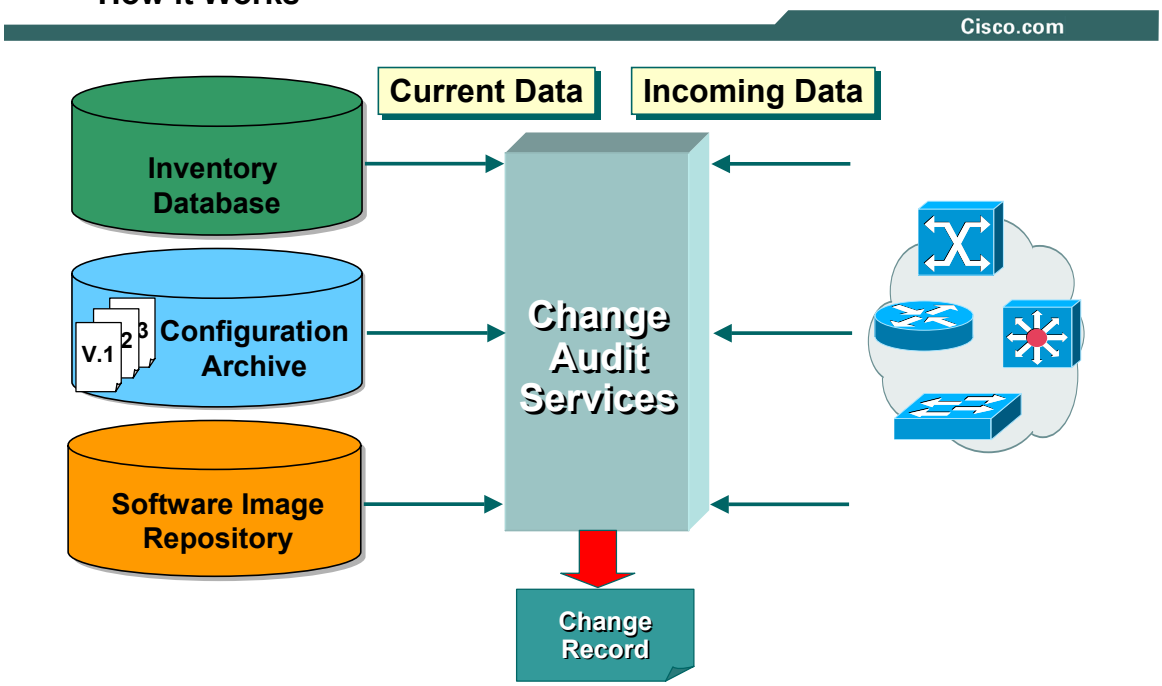


Change Audit - Key Features

The Change Audit feature within RME provides reports to make it easy to quickly view changes that have been made to a specific device, by a specific user, or during a specific time period. It provides a comprehensive record of who changed what, when, and how. This can help narrow down the source of problems when trying to troubleshoot a network error.

Similar to Syslog automated actions, Change Audit can also be configured to perform an automated action (Email, script, trap) when a specific change occurs.

Change Audit
How it Works

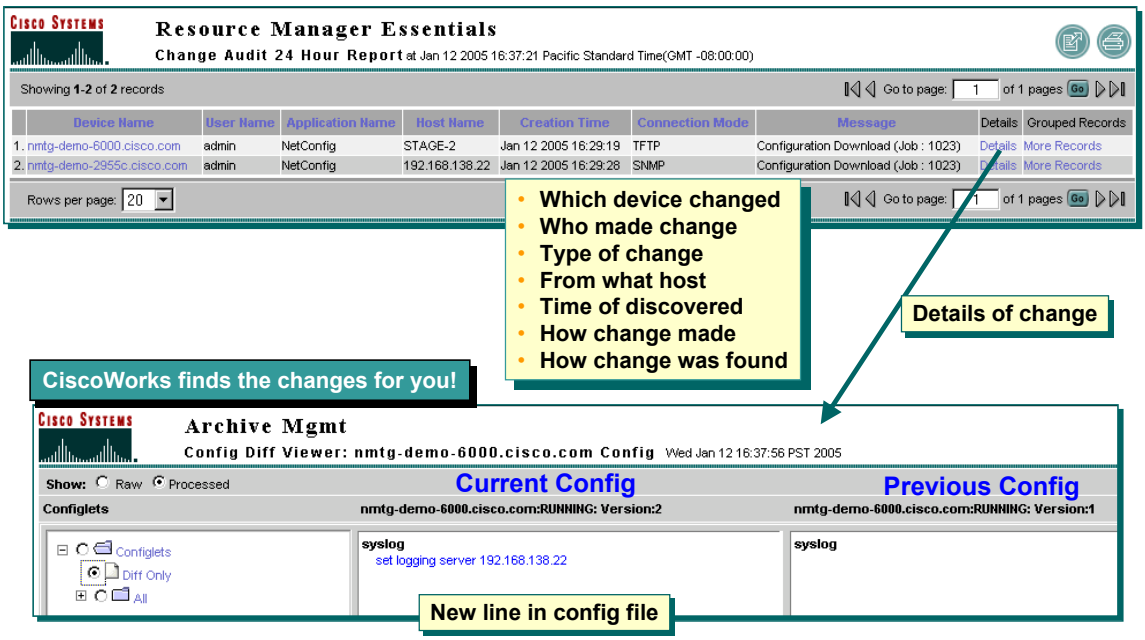


How Change Audit Works

Change Audit is pretty straight forward – the incoming data is compared against the most recent data in the database, if it is different then a change record is created to document the finding. The change record includes details of the change and how it was detected.

Change Audit
Sample Report

Cisco.com



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. RME Features 2-41

Change Audit Sample Report

Change Audit reports can be run against a selected group of devices and/or for a selected change type (software image change, inventory change, configuration change, etc.) over a selected period of time.

The above report was generated for the previous 24 hours and shows two changes that were detected by Change Audit. The listing shows that NetConfig job number 1023 was responsible for the change to the configuration files. Clicking on the *Details* link, it launches a *Configuration Diff Report* showing that the current configuration includes one additional command; the additional line "*set logging server 192.168.138.22*" was added to the new configuration line.

Using Change Audit services, the user quickly knows what change was made, who made the change, and when the change was made.

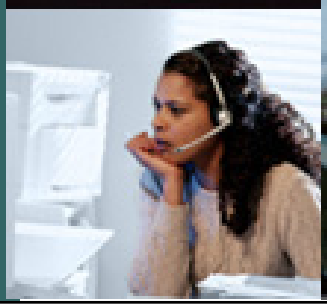
Note(s):

- *The Config Diff Viewer illustrates the changes in the current and previous configuration files. Use the legend below to understand the color-coded changes.*

Legend
Red = Same command, different parameters
Blue = Command in one file not in the other

Device Center

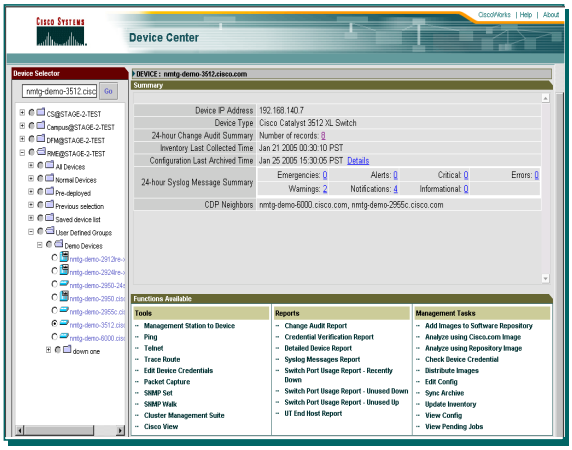
- RME Overview
- RME Management Services
  - Inventory
  - Device Configuration
  - Software Image
  - Syslog Analysis
  - Tracking Changes
- ➢ Device Center



Device Center
Overview

Cisco.com

- **Provides summary information about the device data collected by RME**
  - ☑ Device type
  - ☑ 24 hour change records
  - ☑ Summary of Syslog messages received
  - ☑ Configuration and Inventory archive time
  - ☑ CDP neighbors
- **Links to tools, reports, and valuable management tasks**
- **Can be launched by clicking on device name link in many RME reports**



Device Center - Overview

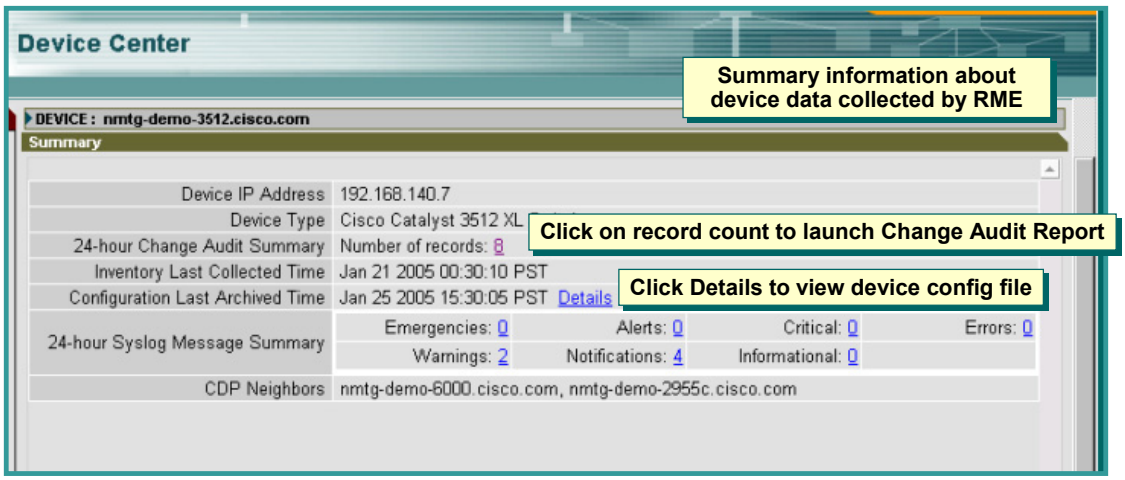
The Device Center provides information for a single device that includes both data and links from all CiscoWorks applications registered to Common Services. Device Center provides a central point from where you can see a summary and reports for the selected device, invoke various tools on the selected device, and perform the tasks that can be performed on the selected device.

After launching Device Center, you can perform device-centric activities, such as changing device attributes, updating inventory, Telnet etc. depending on the applications which are installed on the Common Services Server. You can also launch Element Management tools, reports, and management tasks from the Device Center.

The Device Center has a launch point from CiscoWorks Homepage, but is discussed here because it is easily launched by clicking on the hyper-linked device name in most RME reports.

Device Center
Device Summary Information

Cisco.com



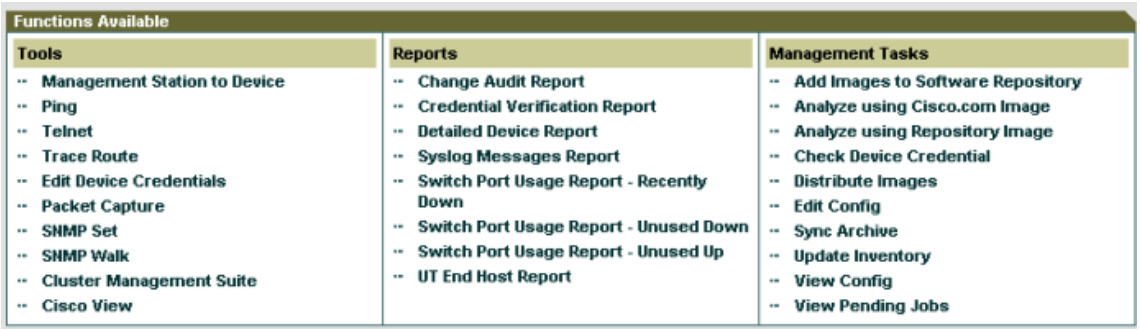
Device Summary Information

The summary window pane in the Device Center provides a quick look the the device name, type, and its CDP neighbors, but more importantly information on change records, Syslog messages received by RME, and a link to the configuration file for the device.

Device Center
Quick Links to Tools, Reports, and Tasks

Cisco.com

Quick links to tools, reports, and tasks for device
(Includes tasks for all registered CiscoWorks applications)



Quick Links to Tools, Reports, and Tasks

Once you have Device Center open for the device, you now have quick access to tools, command line utilities, common CiscoWorks reports and tasks. All these links are especially invaluable when trying to troubleshoot the device.

Thank You!

This concludes a brief look at many of the amazing features in RME. Chapter 3 will explore the use of many of these feature through a series of scenarios.

Scenarios Using RME

Chapter 3

RME Usage Scenarios

Cisco.com

- Getting Started
- Preparing RME for Use
- Reports
- Configuration Management
- Software Image Management
- Automated Actions

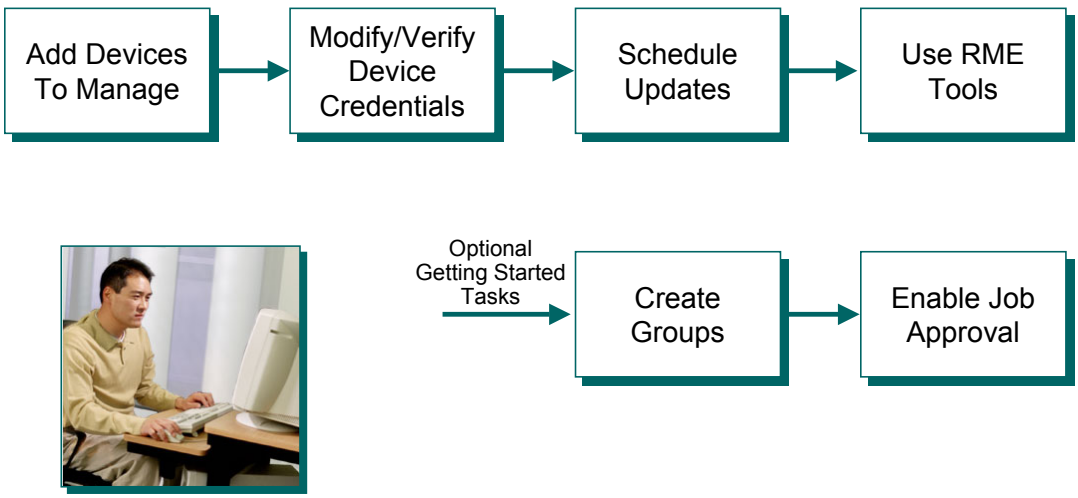
RME Usage Scenarios

As Chapter 2 demonstrated, RME is a collection of many useful, time-saving tools designed to make management of the network simpler and less susceptible to human error. In this chapter, we will demonstrate the use of RME though a number of common management tasks. The first two scenarios are directed at the system administrator in charge of getting RME ready for use. The remaining scenarios will highlight a number of RME features and their use in everyday situations.

To enhance the effectiveness of the chapter as a learning resource, the reader is encouraged to follow along on an operational system, and to explore the other function options not covered by this tutorial. It would also be wise to view the help screens associated with all functions to better understand the many different options available for most tasks. Launch help by selecting the Help link in the upper right-hand corner of the RME desktop. The help is content sensitive.

Basic RME Workflow

Cisco.com



Basic RME Workflow

Like most management products, RME requires some configuration work up front before it can begin to collect management information. Obviously, the first step is to tell RME which devices to manage and to associate the devices with their proper credentials (SNMP community strings and access passwords) so that RME can effectively collect all necessary information and perform all management functions. Because information reported by RME is only as good as the last time it collected it, it is important to schedule update tasks to ensure RME is reporting the most current information.

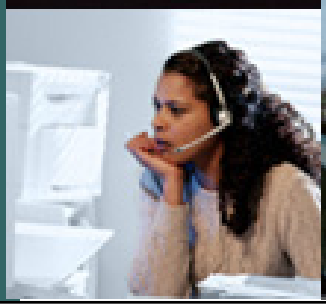
At this point RME is ready for use, however, the user may wish to logically group devices together to simplify the execution of RME tasks. For instance, if the boss wanted to know the memory on all data center devices, and RME was managing a thousand or more devices, it may take the user some effort and time to scroll thorough the list of managed devices to select all data center devices to run a report. To simplify the running of this report, a logical group of devices containing all data center devices could be created. Then when running this report the user would simply select this group as the devices to run the report for; both simplifying the execution and saving time!

Finally, since RME contains numerous tasks that can modify the configuration of a device (a critical endeavor that could change the behavior of the network), the administrator can choose to enable the feature “Job Approval.” When enabled, any critical job (a job that could potentially change the behavior of the network) must be “approved” prior to being executed.

The first two scenarios will look at the basic administrative tasks described here as well as the two optional ones mentioned (Device Groups and Job Approval).

Getting Started

- Getting Started
- Preparing RME for Use
- Reports
- Configuration Management
- Software Image Management
- Automated Actions



Getting Started

Cisco.com

- Server Access
- Permissions Review
- Navigation
- Device Management
  - Add Devices to RME from DCR
  - Modify/Verify Credentials

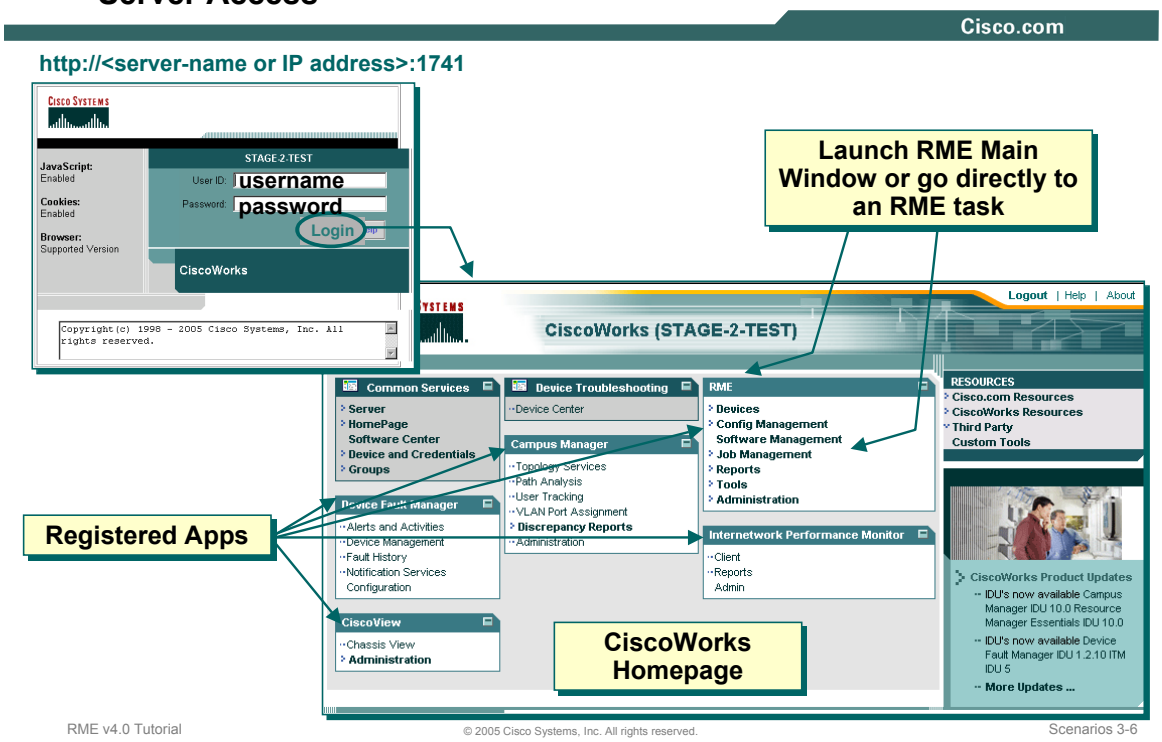
Getting Started

In this first scenario, the user will first learn how to access the server. This will be followed by a review on CiscoWorks user permissions and how they affect the look and use of RME.

Note: More information on user permissions and security in general can be found in the Common Services User Guide and the Permissions Report, discussed in Chapter 2.

Before actually beginning to use RME, the navigation and layout of RME will be discussed. Finally, this chapter will show the reader how to add devices from the Device Central Repository (DCR) to the RME list of devices to be managed, and to associate those devices with their proper credentials so that various RME tasks can properly access the device.

Getting Started
Server Access



Server Access

Accessing the CiscoWorks server is easy, simply enter the server's DNS name or IP address followed by the http port being used (port 1741 is used by default during installation) as a URL in a standard browser (see Chapter 4 for complete client requirements):

http://<server-name or IP address>:1741

The CiscoWorks login banner will be displayed. The left-hand side of the banner will display the results of a requirements check against the browser being used.

To access the CiscoWorks home-page, enter your User ID and password provided by the CiscoWorks administrator and click **Login**. The CiscoWorks home-page will be displayed. The home-page will display the different CiscoWorks applications registered for use. Find the RME listing and click on the RME header to take you to RME in general, or selected one of the RME tasks listed to launch RME to the screen for the selected task. Before looking at the RME desktop, let's briefly review CiscoWorks user permissions.

Note: For more information on the CiscoWorks homepage layout and configuration see the "Common Services" User Guide.

Getting Started

Permissions Review – User Roles

Cisco.com

- **User Roles determine tasks that can be performed by user**
- **User can be assigned more than one user role**

System Administrator	**Server configuration and user accounts**
Network Administrator	**Device configuration**
Network Operator	**Backup for most configuration management tasks**
Approver	**Approve jobs that change device software or configuration**
Help Desk	**View reports (Default User Role – assigned to all users)**

- **Tasks displayed change depending on user's assigned roles**

User Roles

RME, and CiscoWorks in general, contain many critical tasks that can modify the behavior of a network, as well as, many totally benign tasks that simply display information. Obviously, it would not be wise to allow all types of users access to the critical functions, but at the same time it would be beneficial to allow all types of users access to the basic information. To allow for proper access to all types of users, CiscoWorks employs the concept of User Roles (also known as user privileges or permissions). Use of the various functions or tasks within all CiscoWorks applications is based upon the "roles" assigned to user accounts. In fact, if a task is not permitted to the user role assigned to the logged in user, then that task will not be selectable in the navigation tree of the application.

CiscoWorks uses five user roles; users can be assigned more than one user role, and all are assigned the basic user role of Help Desk. The five user roles and their basic access ability are:

System Administrator – Server configuration and user accounts

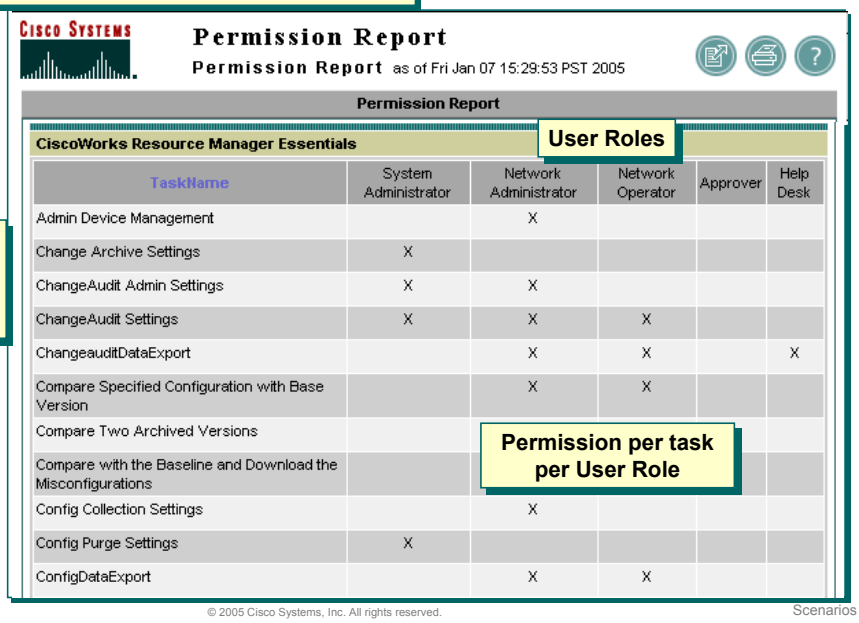
Network Administrator – Device configuration

Network Operator – Backup to most configuration management tasks

Approver – Approves jobs that modify a device (Used when Job Approval is enabled)

Help Desk – Basic user role assigned to all users, allows for viewing of all reports

Launch Permission Report from:
Common Services > Server > Reports > Permission Report



TaskName	System Administrator	Network Administrator	Network Operator	Approver	Help Desk
Admin Device Management		X			
Change Archive Settings	X				
ChangeAudit Admin Settings	X	X			
ChangeAudit Settings	X	X	X		
ChangeauditDataExport		X	X		X
Compare Specified Configuration with Base Version		X	X		
Compare Two Archived Versions					
Compare with the Baseline and Download the Misconfigurations					
Config Collection Settings		X			
Config Purge Settings	X				
ConfigDataExport		X	X		

Permission to perform tasks are based on User Roles

RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-8

Permissions Report

To determine which applications and functions are available for each user role, view the *Permissions Report*. To launch the Permissions Report:

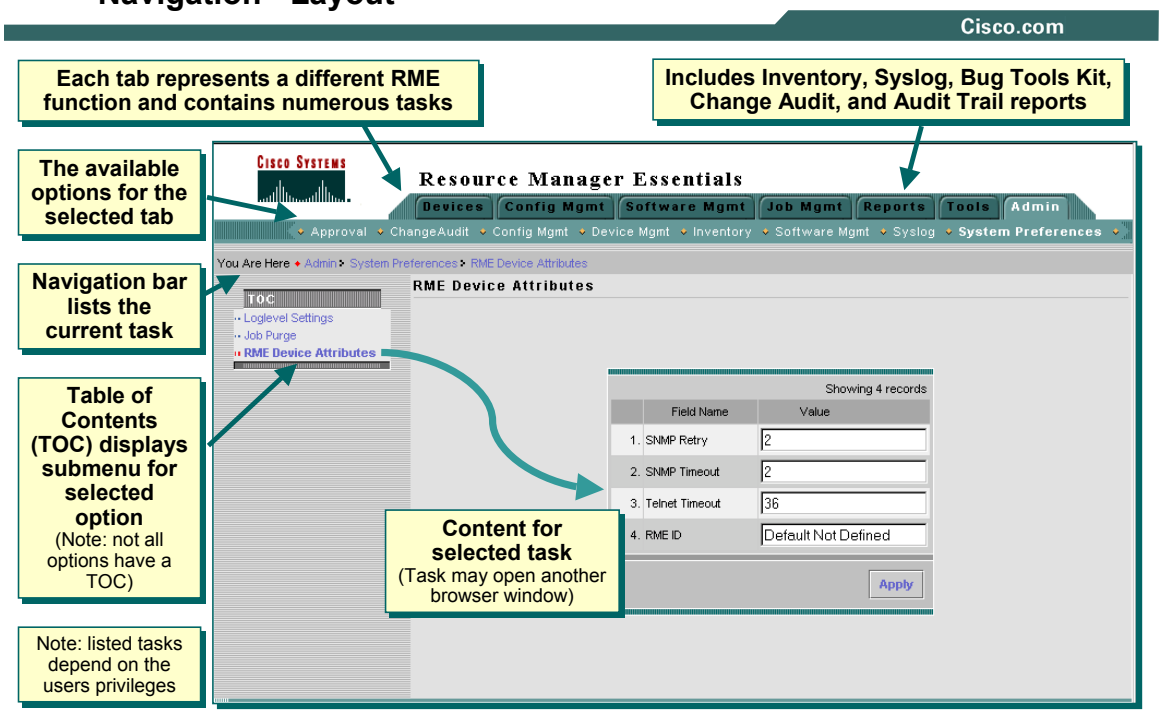
1. From the **CiscoWorks Home Page,** Click on the **Common Services** application

   The Common Services Desktop is displayed
2. Click on the **Server** tab
3. From the listed options for the tab, click on the **Reports** option
4. From the displayed dialog box select **Permissions Report** and then click **Generate Report**

The Permissions Report lists every CiscoWorks application and the tasks for that application and indicates which user role is capable of executing it. To determine the user role(s) assigned to your user account, review your account by selecting **Common Services > Server > Security > Single Server Management > Local User Setup**.

Note: For more information on CiscoWorks users and permissions see the “Common Services” User Guide.

Getting Started
Navigation - Layout



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-9

Navigation - Layout

Prior to the brief tangent to discuss user roles and privileges, the RME desktop was launched from the CiscoWorks Home Page. Before actually using RME, it would be beneficial to discuss the basic layout to help you understand how to navigate through RME.

All CiscoWorks applications employ identical user interfaces and layouts to minimize the burden of learning a different interface for each application within the suite of tools. The RME desktop appears as a series of folders representing the major task categories within RME. The contents of these folders are accessible by selecting the appropriate folder tab. The currently selected folder is identifiable by the different color of the tab and it's text. Immediately under the tabs are the options associated with the selected major task category. Notice that this bar is the same color as the selected tab helping to further identify which tab is selected. To select one of these options, simply click on it. The selected option will be in bold text. At this point, the selected option my have a dialog box associated with it, which will be displayed in the content area. The selected option may also have sub-tasks associated with it. These will be listed in a table of content dialog on the left-hand side of the screen. Again, to select one of the sub tasks, simply click it and it's text will now become bold to identify it as the selected task.

When the selected task has no further sub-tasks, a dialog box with further instruction or simply displaying the requested information will be shown in the content display area. To determine where the user currently is, the display line (appropriately titled "You Are Here") under the tab options indicates the path currently selected.

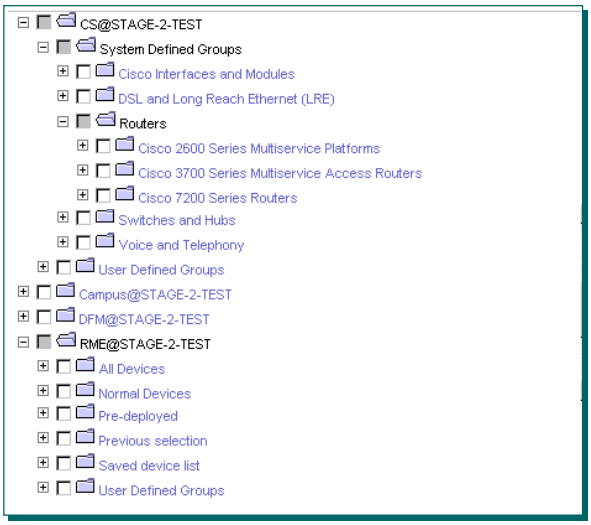
Note: The RME major functions discussed in Chapter 2 (Inventory, Configuration Management, Software Management, Syslog Analysis, and Change Audit) do not correspond to the tabs. Rather the tabs represent major task categories. So in the Reports task category, Inventory, Software Bugs, Change Audit, and Syslog functions can be executed in the form of reports.

Note: To help reduce the number of pages in this tutorial, the entire desktop is not always shown. To facilitate the user in understanding what task is being displayed, the following notation is used to represent the options clicked: application > option > task > sub-task. For example to access the report generator, the user would be in the RME application, click the Reports tab and then click the Report Generator option or RME > Reports > Report Generator.

Getting Started
Navigation – Device Selector

Cisco.com

Device Selector



To select devices for various RME operations, select the devices or groups of devices from the device selector

All CiscoWorks applications have predefined groups as well as allow for user-created groups

Expand tree to see device groups, and devices within a group

RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-10

Navigation – Device Selector

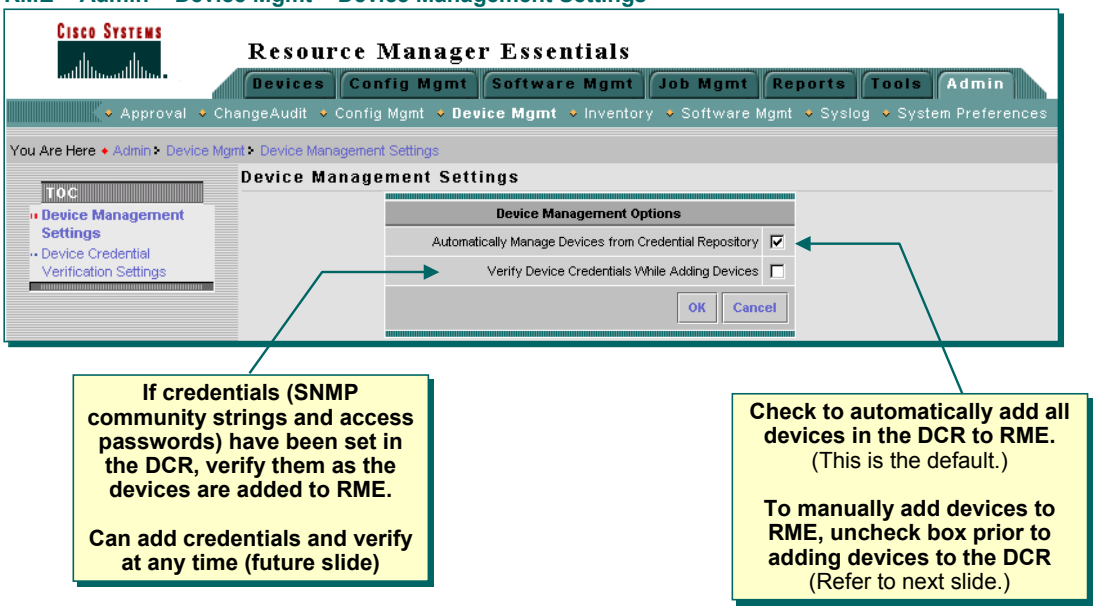
Other than the navigation through the RME desktop, the other major navigation related piece that should be discussed is the device selector. Many of the RME tasks require the user to select the device or devices to execute the selected task against. The Device Selector is the mechanism used for that step and will be used so often that is best described in detail here.

When displayed, the Device Selector presents the user with a listing of all CiscoWorks applications registered with the instance of CiscoWorks (applications listed on the Home Page). Each application can have its own subset of devices in the DCR (Common Service will have all devices since this is the owner of the DCR). Each application also has it's own set of pre-defined groups of devices, for instance Common Services has pre-defined groups associated with each device class and type. As mentioned before, these groups of devices can simplify the selecting of devices to execute a task against. Opening the expand button next to the application will list the various groups under it. Continually expanding groups will eventually lead to the actual devices.

When executing a task, the Device Selector is used to select which device(s) are to be used. Being familiar with the structure of the device selector will simplify and speed up this task. Though not shown in the picture above, the device selector will always allow you to select devices by simply entering the IP address or name of the device. With out this structure of devices, could you imagine going through a list of 2000 or more devices to pick out the five 7200 routers you want to run a report for!

Hopefully, this further clarifies the importance of device groups and why you would want to create your own (a task we will look at in the next scenario).

RME > Admin > Device Mgmt > Device Management Settings



If credentials (SNMP community strings and access passwords) have been set in the DCR, verify them as the devices are added to RME.

Can add credentials and verify at any time (future slide)

Check to automatically add all devices in the DCR to RME.
(This is the default.)

To manually add devices to RME, uncheck box prior to adding devices to the DCR
(Refer to next slide.)

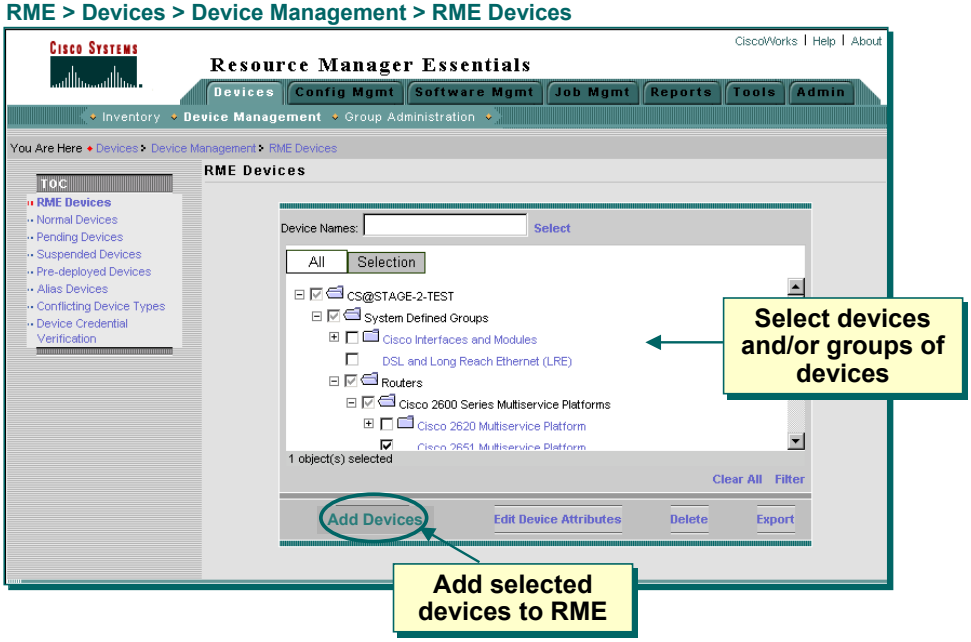
Adding Devices Automatically

Now it is time to look at how to add devices from the DCR to RME in order for RME to manage them. By default, when devices are added to the DCR, the devices are automatically added to RME. But this feature can be disabled if the user does not need to have all devices in the DCR managed by the local RME.

To view this setting, select **RME > Admin > Device Mgmt > Device Management Settings** as shown in the figure above. Full RME functionality requires RME have the ability to access the devices both through SNMP and normal telnet type access. This is the reason device credentials (SNMP community strings and access passwords) need to be associated with a device in the DCR. Selecting the "Verify Device Credentials While Adding Devices" option will cause RME to attempt to access each device with the credentials found for it in the DCR as the device is added. A report, illustrated later, will provide the results of this test.

Though this is a nice feature to have all devices added to RME, you may want to have more control; for example, having multiple copies of RME, one for each region, the regional RME should only manage a single region and not the whole network. In this case you want to control which devices are sent to each instance of RME. To change this feature, you need to un-check the automatic feature "*Automatically Manage Devices from the Credentials Repository*" *prior* to adding devices to the DCR.

RME > Devices > Device Management > RME Devices



Adding Devices Manually

If the automatic add feature was disabled, let's explore how to add devices manually to RME.

1. From the **RME** desktop, select the **Devices** tab
2. From the listed options for the tab, click on the **Device Management** option
3. From the TOC menu, select the **RME Devices** sub-task

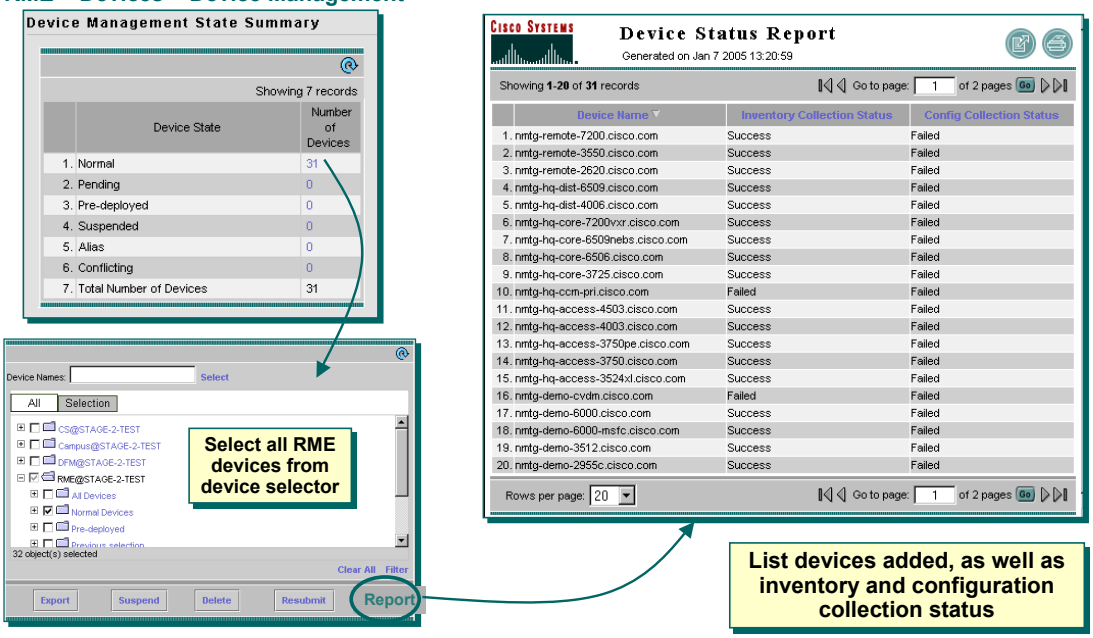
   T he Device Selector is displayed.
4. Using the expand buttons, locate the groups of devices or individual devices to add to RME, select them (a check mark will appear in the box to the left of the group or device)
5. Click **Add Devices** to add these devices to RME

Getting Started

Device Management – Adding Devices Result

Cisco.com

RME > Devices > Device Management



Result of Adding Devices

To see the results of the device adding operation whether the devices are automatically or manually added:

1. Select **RME > Devices > Device Management** (application > tab > option)

   The *Device Management State Summary* is displayed. This list indicates the state each device is in as a result of the device add operation. Ideally all devices should eventually be in the **Normal State** meaning RME was at least able to contact them using an SNMP read operation. The **Pending State** would indicate the add operation is still in progress.

2. From here click on the number of normal devices to view membership.
3. Expand the RME application button and select the **Normal Devices** group
4. Click on **Report**

   The *Device Status Report* is displayed showing the devices added to the RME managed list and the results of the inventory and configuration collection. At this point there may be many failures due to incorrect credentials, which we will explore how to change next.

Additional RME State definitions:

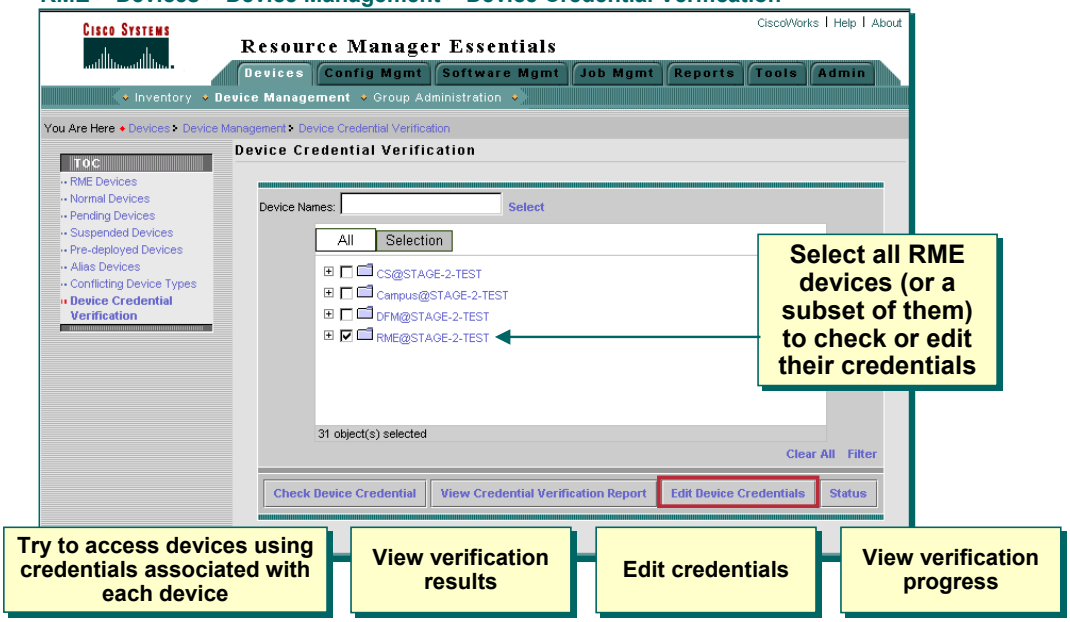
- **Pre-deployed** - The device has never been contacted by RME
- **Alias** - This device may already exist in RME, but with another hostname or IP address
- **Conflicting** - Occurs if the sysObjectID in the device and that in the DCR do not match.
- **Suspended -** State of a device by virtue of explicit user action wherein a device cannot participate in any application flows but all historical data pertaining to the device will continue to be maintained by RME. You can re-submit the devices in this state for participation in RME workflows.

Getting Started

Device Management – Device Credentials

Cisco.com

RME > Devices > Device Management > Device Credential Verification



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-14

Device Credentials

Chances are that when the devices were originally added to the DCR, only the SNMP read community string was added to the DCR. RME, however, requires additional credentials to perform all of its functions. The next few pages will look at how to add/modify the device credentials in the DCR and how to verify that they are correctly set. All these tasks start from the same subtask:

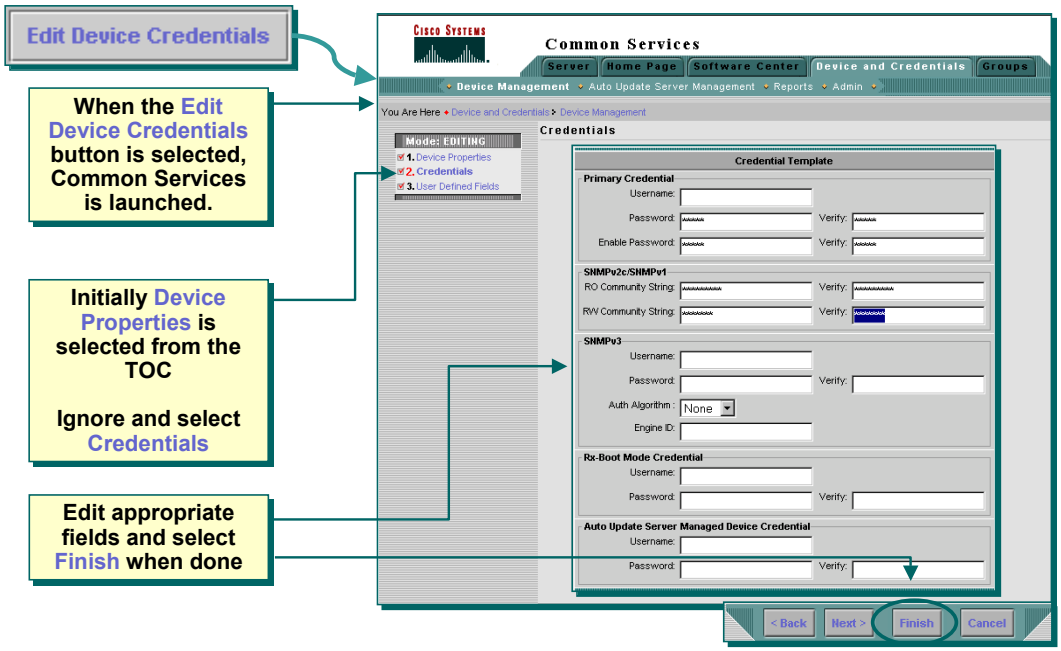
1. Select **RME > Devices > Device Management > Device Credential Verification**

   The content area will display a *Device Selector* along with four options. Use the device selector to select the appropriate devices for the task. In this case let's assume that all devices in RME use the same credentials so that we can change them all at once.

2. Select the box to the left of the RME application to select all RME devices
3. Click the **Edit Device Credentials** task button.

Getting Started

Device Management – Edit Device Credentials



Edit Device Credentials

4. What happens after selecting the **Edit Device Credentials** button in RME is tricky. The Common Services Desktop is opened to **Common Service > Device and Credentials > Device Management > Mode: Editing** after first displaying a pop-up dialog box informing "Application 'RME' is performing 'Edit Device' operation on the following devices…' Click **OK** to proceed with the edit operation.
5. The edit operation is a three stage wizard: Device Properties, Credentials, and User Fields. In this case we are only changing the credentials so click **step 2** in the TOC area.
6. The *Credentials Template* is displayed. Enter the appropriate information and click **Finish**

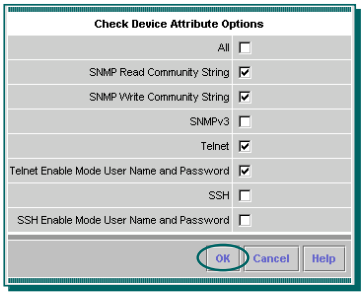
Note: We have discussed how beneficial creating logical groups can be to simplifying the use of RME and we will demonstrate their creation in the next scenario. As an additional credential or attribute, each device has User Fields. The administrator can decide what each user field represents, for example User Field #1 might be device location. The contents of the user field can then be used to create a group. This feature is mentioned now because the third step of the above wizard is how you would populate these fields.

Getting Started

Device Management – Verify Credentials

Cisco.com

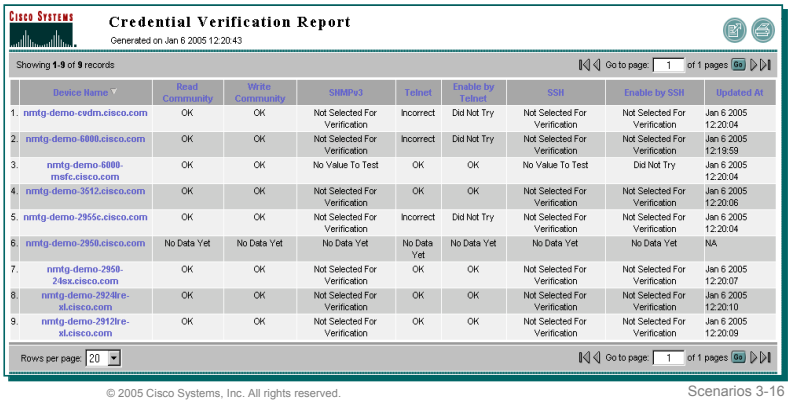
Check Device Credential



Select the device attributes to check for

Click OK. RME then begins to contact all devices to verify their attributes

View Credential Verification Report



	Device Name	Read Community	Write Community	SNMPv3	Telnet	Enable by Telnet	SSH	Enable by SSH	Updated At
1.	nmtg-demo-cvdm.cisco.com	OK	OK	Not Selected For Verification	Incorrect	Did Not Try	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:04
2.	nmtg-demo-6000.cisco.com	OK	OK	Not Selected For Verification	Incorrect	Did Not Try	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:19:59
3.	nmtg-demo-6000-msfc.cisco.com	OK	OK	No Value To Test	OK	OK	No Value To Test	Did Not Try	Jan 6 2005 12:20:04
4.	nmtg-demo-3512.cisco.com	OK	OK	Not Selected For Verification	OK	OK	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:06
5.	nmtg-demo-2955c.cisco.com	OK	OK	Not Selected For Verification	Incorrect	Did Not Try	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:04
6.	nmtg-demo-2950.cisco.com	No Data Yet	No Data Yet	No Data Yet	No Data Yet	No Data Yet	No Data Yet	No Data Yet	NA
7.	nmtg-demo-2950-24sx.cisco.com	OK	OK	Not Selected For Verification	OK	OK	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:07
8.	nmtg-demo-2924lre-xl.cisco.com	OK	OK	Not Selected For Verification	OK	OK	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:10
9.	nmtg-demo-2912lre-xl.cisco.com	OK	OK	Not Selected For Verification	OK	OK	Not Selected For Verification	Not Selected For Verification	Jan 6 2005 12:20:09

For all RME functions to operate properly, each device must have correct SNMP community strings and access passwords

RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-16

Verify Credentials

After editing the device credentials, the next step is to verify that they are correct by having RME attempt to contact each device using these credentials.

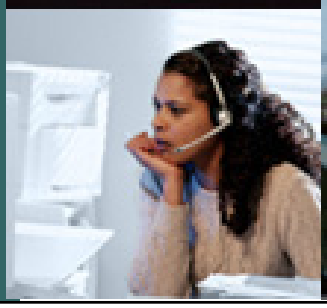
1. From the previous RME point **RME > Devices > Device Management > Device Credential Verification** (which should still be displayed on the RME desktop with all RME devices selected – remember the edit operation opened the Common Services desktop. Select the **Check Device Credential** button.
2. A list of what attributes to be checked will be displayed. In this case, select both SNMP community strings and telnet and enable access to be checked and click **OK**.
3. At this point you can either click the **Status** button to see the current progress of the operation, or wait awhile and then select the **View Credential Verification Report**.

   This report displays the device and the results for all potential access methods and the time the check occurred. The database will store the results of the latest credential verification and display them whenever the **View Credential Verification Report** is selected. The desire here is to ensure RME can access each device with SNMP and CLI access to the enable mode so that all RME operations can be performed. If not, re-edit the devices that are incorrect.

At this point RME is fully operational, the next scenario will look at additional administrative functions to enhance the use of RME.

Preparing RME for Use

- Getting Started
- ➢ Preparing RME for Use
- Reports
- Configuration Management
- Software Image Management
- Automated Actions



Preparing RME for Use

Cisco.com

- **Schedule Updates**
  - Inventory
  - Configuration Archive
- **Create Groups**
- **Job Approval**

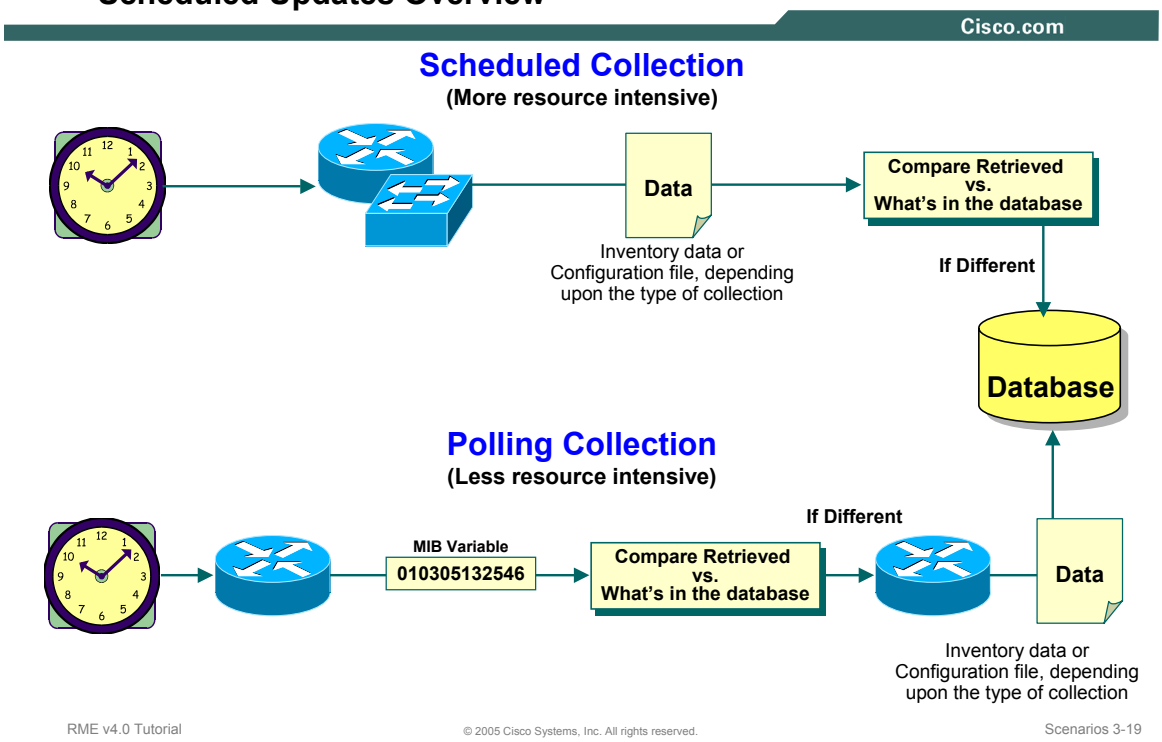
Preparing RME for Use

Even though RME was ready for use after the previous scenario was completed, this scenario looks at additional administration type functions to perform in order to help keep RME up-to-date, thus, making it more effective to use.

The first portion of the scenario will look at keeping both the inventory information and the configuration archive up-to-date. This procedure is important because it is one of the ways how RME identifies any change that has occurred. This is followed by the creation of a group to help simplify report generation and task execution. Finally, since modifying a device (either its configuration or system software) can cause many problems, if not done correctly, the Job Approval process is discussed along with an example.

Preparing RME for Use

Scheduled Updates Overview



Scheduled Updates Overview

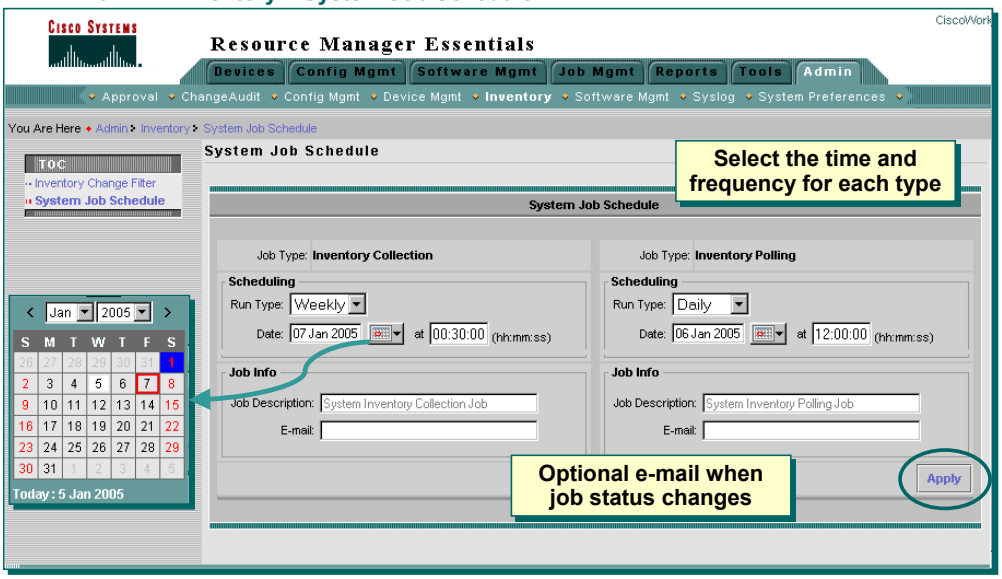
Reports and information provided by RME is only as good as the last time the data was collected. Therefore, it is important to make sure the information in RME stays up to date. The two major systems that trigger data collection are the inventory and configuration archive. Though they collect different data using different methods, the setup of the retrieval mechanisms are similar.

RME uses two different types of collections: Polling and Scheduled. The polling collection is typically much less intrusive then the scheduled method so can be run more often. In the polling mechanism, the administrator selects a reoccurring time for RME to poll each device for changes. During the poll, a single MIB variable is returned that contains a time stamp indicating the time of the last change. If this time is different than the one saved in the database for this device, then a collection is initiated for the device. If not, the poller moves on to the next device.

In the case of the scheduled collection, the administrator defines a time and frequency; and then at those scheduled times, RME retrieves all information for the type of collection being performed regardless if they have changed or not. When the information is returned to RME, it is compared with the information in the database, if different it is put into the database, otherwise it is discarded.

Now let's look at how to set up the schedules for these types of collection.

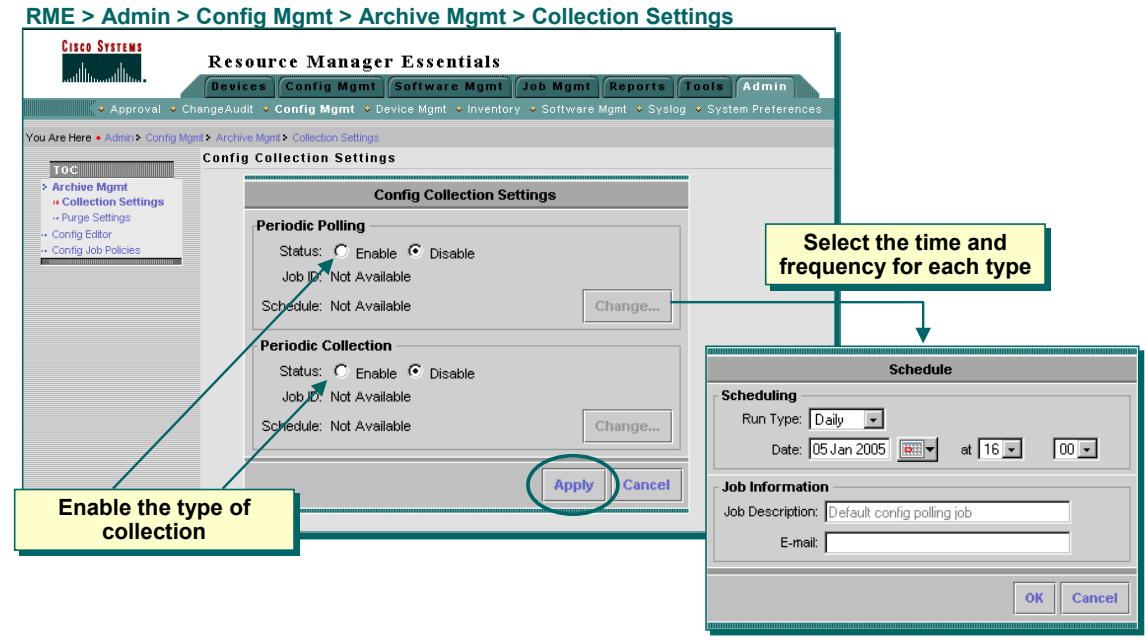
RME > Admin > Inventory > System Job Schedule



Inventory Updates

To schedule both the inventory scheduled collection and polled collection use the following steps:

1. Select **RME > Admin > Inventory > System Job Schedule**
2. The dialog displayed contains two parts, one for each type of collection mechanism. Select the frequency, start date and time for each method. Note that the Job Description cannot be changed. E-mail addresses can also be added to inform the recipients when the collection has completed. Select **Apply** when finished.



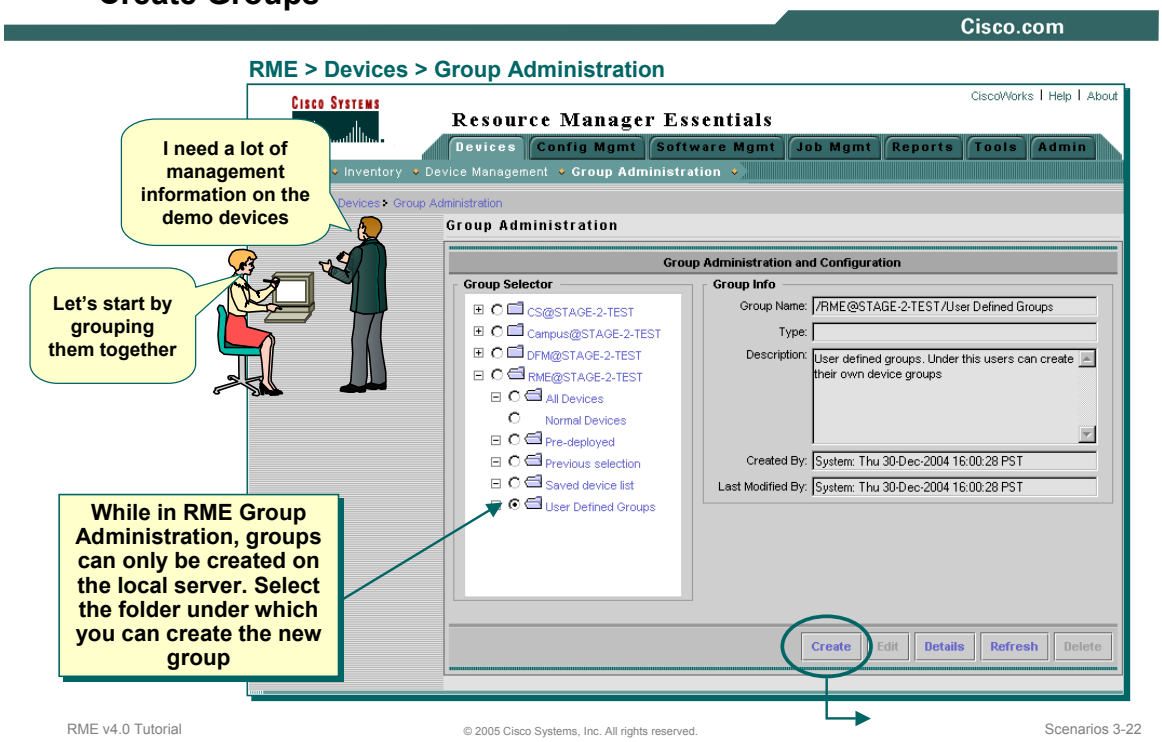
Configuration Archive Updates

Though the basic scheduling philosophy is the same, the configuration archive collection can also be disabled (default) if desired. Use the following steps to enable and configure configuration archive collection:

1. Select **RME > Admin > Config Mgmt > Archive Mgmt > Collection Settings**
2. The dialog displayed in the content area has two portions one for each type of collection. The first step would be to click **Enable** radio button for each collection type. This will now activate the **Change** button.
3. Click the **Change** button to bring up the scheduling information. Select the frequency and enter the start date and time for the operation. Again you cannot change the Job Description and you can add a list of e-mail recipients to receive an e-mail when the job is completed. Click **OK** to accept the schedule changes.
4. Click **Apply** to have the new jobs and times take effect

Preparing RME for Use

Create Groups



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-22

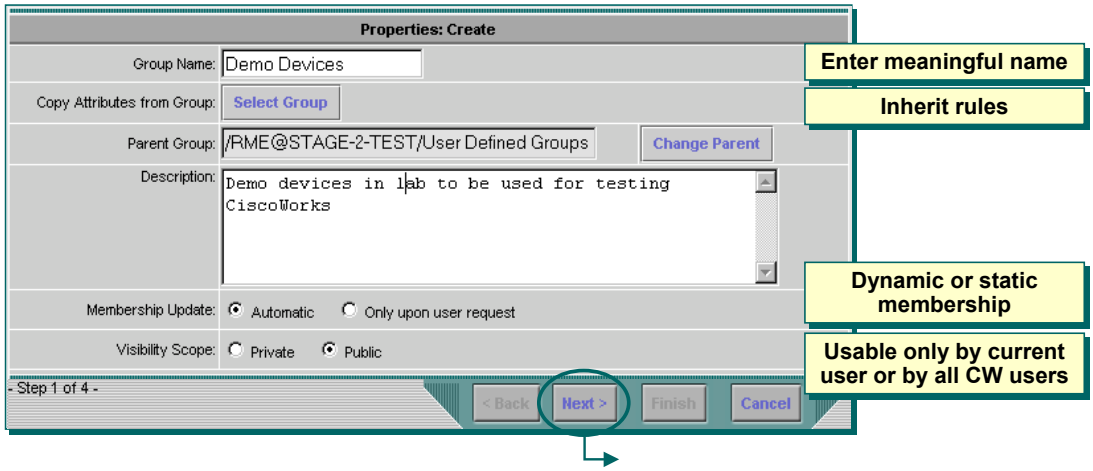
Creating Device Groups

For the remainder of this chapter, we introduce Ted, the IT manager for East coast operations of a large firm and one of his brightest engineers Sally. The company was always in a reactive mode when it came to management of the network and Sally convinced Ted to purchase and install CiscoWorks to help them work more efficiently. As part of the CiscoWorks roll out, Ted wants to test the features of RME against the set of demo devices they are evaluating prior to introducing them into the live network. Sally has previously populated the DCR with a number of devices, and in the previous scenario added the devices to RME and associated the credentials (SNMP community strings and passwords) with the devices.

The first order of business is to make the use of RME simpler by creating a group of the demo devices to quickly select when running reports and performing other RME tasks.

Sally uses the following steps to create a group of the demo devices:

1. Select **RME > Devices > Group Administration**. The Group Administration dialog is displayed.
2. The dialog contains a Group Selector which closely resembles the device selector except no actual device is ever displayed when the groups are expanded. Sally expands the RME entry to revel the group categories for RME. When using RME to create groups, the groups must be created under the **User Defined Groups** category, so Sally selects it. If groups were already defined under this category, Sally could have selected one of them if the Demo Group was a subset of it. In other words, you can create a hierarchy of groups. The right side of the dialog displays information about the selected group.
3. Click **Create** to perform the next step



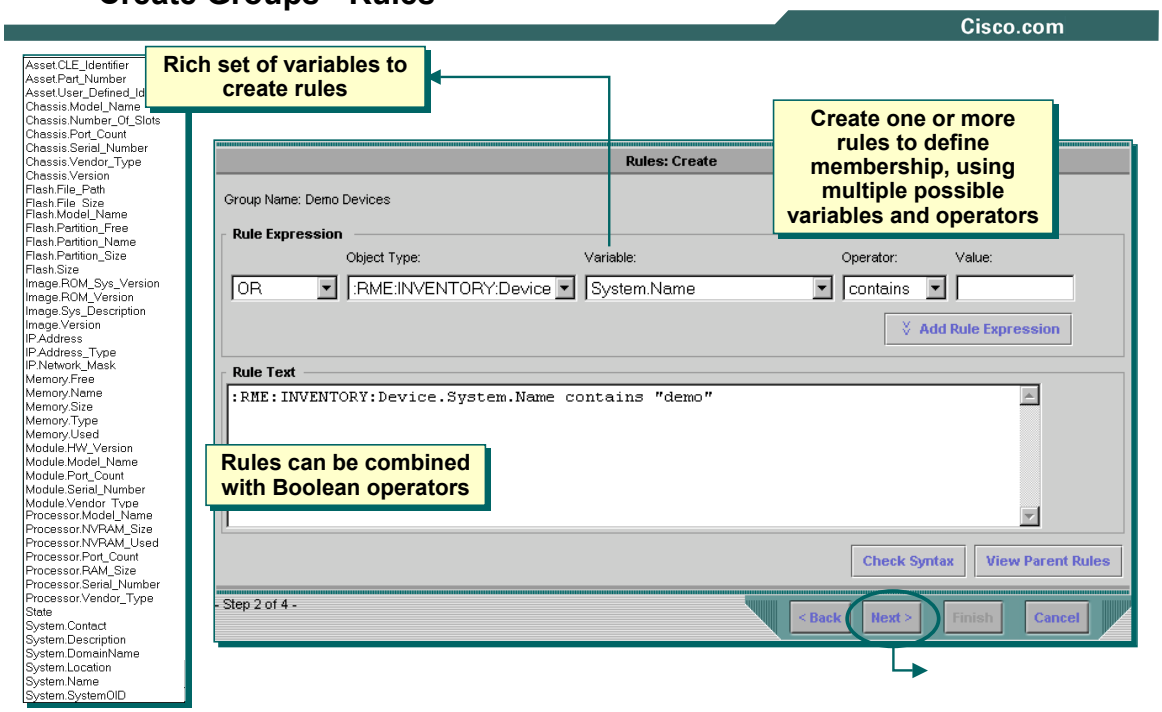
Group Properties

When clicking Create on the Group Administration dialog, the 4-step Create Group wizard is launched. The first step is to set the group properties:

4. Enter a meaningful name for the group
5. If attributes are to be selected from an existing RME system or user-defined group use the **Select Group** button
6. Use the **Change Parent** button to change the group parent. Note: the display will always show RME/User Defined Groups/ as the parent selecting the *Change Parent* button will display the actual parent. The parent must be in the User Defined Groups hierarchy.
7. Membership updates can be **Automatic** meaning that if a device meets the rules of membership at any time, then it becomes a member, or loses membership if it no longer matches the membership rules. This is known as a dynamic group. Conversely, selecting **Only Upon User Request** effectively makes a static group whose membership is only changed by the group creator regardless if a device meets or no longer meets the membership rules after the group was created.
8. The **Visibility Scope** defines who will see this group in the device selector. If Sally were to select Private, then Ted would not be able to use this group when he logged into CiscoWorks unless he also created a similar group.
9. Click **Next** to go to the next step in the Create Group wizard

Preparing RME for Use

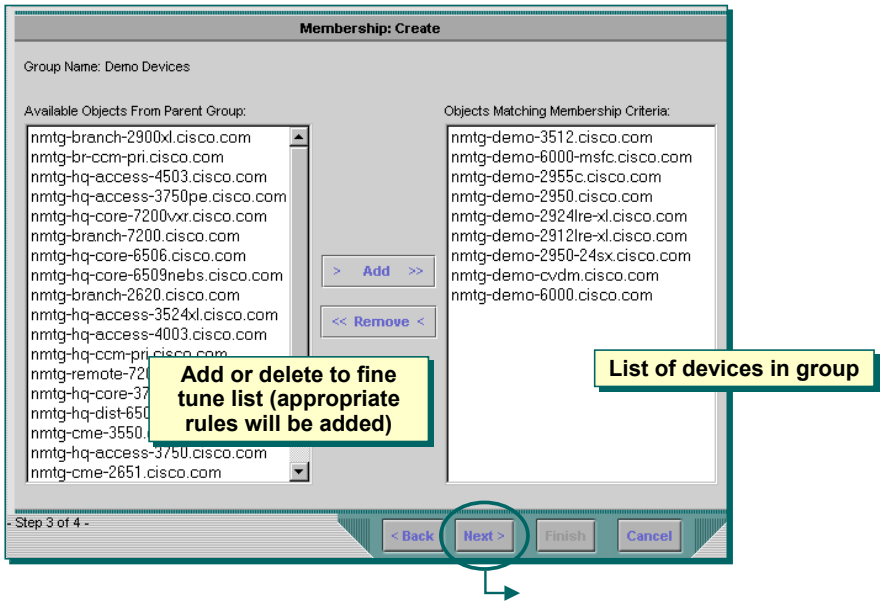
Create Groups - Rules



Group Membership rules

The next step of the Create Group wizard is to define the rules that determine membership in the group. Rules can be created using just about every variable in the RME inventory using multiple operators including equals, contains, etc. Rules can be combined with Boolean operators to create very detailed membership rules.

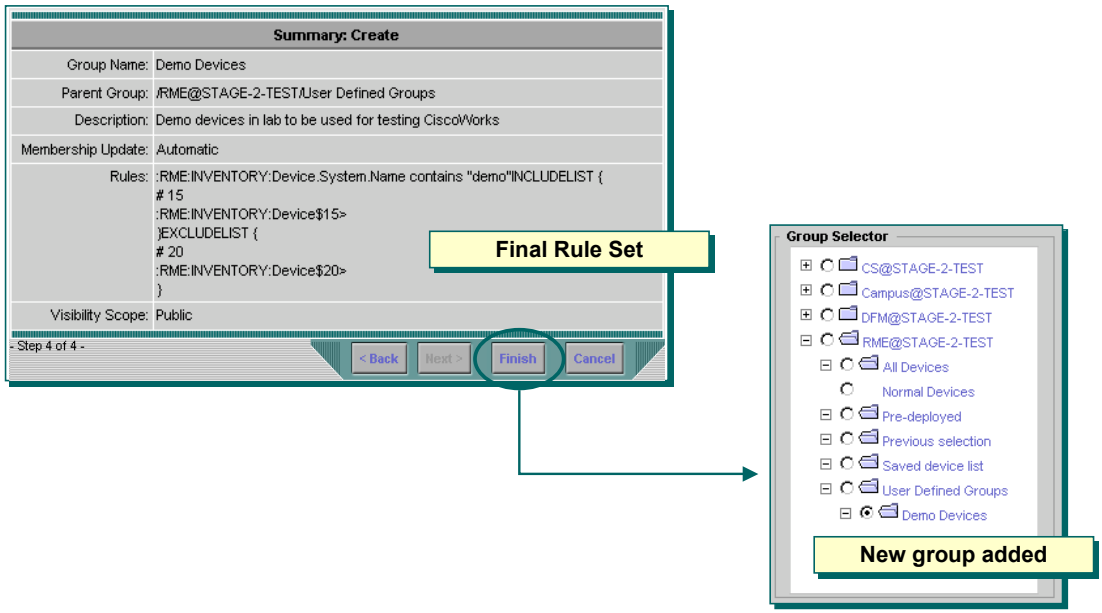
10. From the variable pull down list, Sally selects **System.Name**
11. From the Operator Pull down list select **contains**
12. In the value field enter **demo** (all demo devices in their network are suppose to include the word demo in the sysName)
13. Click **Add Rule Expression** to add membership rule
14. Click **Next** to go to the next step in the Create Group wizard



Initial Group Membership

Step 3 of the 4-step Create Group wizard displays the membership of the group on the right side of the dialog box based on the membership rules just created. The left side of the dialog box is a list of the remaining available objects in the parent group. This step can be used to fine tune membership in the group by adding and/or removing devices. Devices added or removed will cause the appropriate membership rules to be generated. Viewing the list, it looks like Sally needs to add one device and remove another to perfect her list. The new membership rules will be seen in the final wizard step.

15. Click **Next** to go to the next step in the Create Group wizard.



Create Group Summary

The final wizard step shows a summary of the group just created. Notice in the Rules, there was a rule added to include a device and to remove a device.

16. Click **Finish** to create the group. The device selector now displays the Demo Devices group as a child group to the User Defined Groups entry.

Preparing RME for Use

Job Approval - Overview

Cisco.com

Why

- Changing software or the configuration file on a device is a critical function

How

- Network Administrator configures job to change device
- Approver must OK job before job is executed

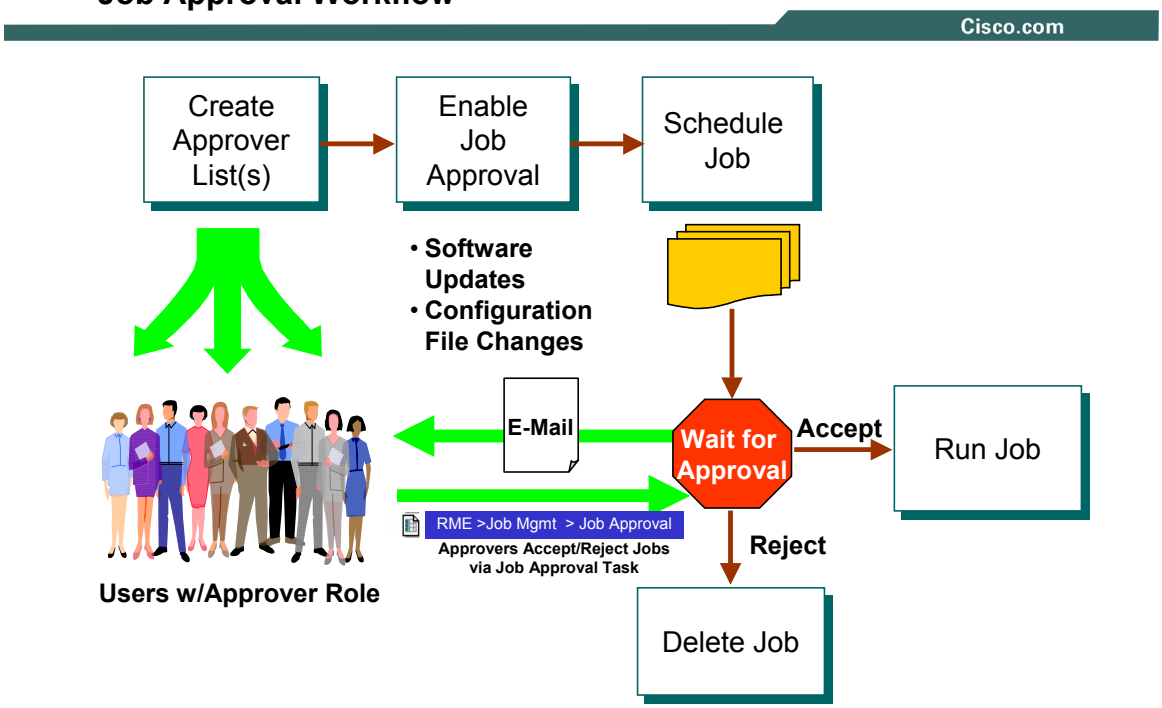
Can have a different set of Approvers for each job

Job Approval Overview

CiscoWorks allows for users with the user role of *Network Administrator* to configure and schedule jobs that can change the configuration of a device, and thus alter the way the network behaves. As an added security measure, CiscoWorks can be configured so that no job that changes a device's configuration will execute until it has been approved. Users with the *Approver* user role assigned are responsible for checking and verifying these jobs prior to approving them for execution. Lists of approvers can be created for each type of job, but only one needs to approve the job to have the job executed.

Preparing RME for Use

Job Approval Workflow



Job Approval Workflow

To help increase the security on your network and minimize the potential for destructive device configuration, job approval forces a second set of eyes to “approve” a job prior to it modifying the device configuration or system software.

Job approval is a 4-step process. First, in addition to having the *Approver* user role, the users must be further identified within RME as an approver. Second, one or more lists of approvers are created and populated with the members identified in step one. The third step is to assign an approver list to each of the approvable tasks (NetConfig, Config Editor, Software Distribution, and Archive Management). An approver list can be assigned to more than one type of task. Finally, those tasks are enabled for job approval.

When job approval is enabled for a job requiring job approval, a user with the *Network Administrator* user role would first create the change job. Then during the scheduling phase, they would select a future time to execute the job to allow enough time for the job to be first approved. The job would then be placed in a waiting state. Each approver in the task’s associated approver list is sent an e-mail notification about the pending job. One of these approvers must go to the Job Approval task (RME > Job Mgmt > Job Approval) to review the job details and accept or reject the job before it is schedule to run. Accepted jobs are placed into the run queue an executed at the scheduled time. Jobs that are not approved before the scheduled execution time or that are rejected are deleted from the job execution queue.

Note: If job approval is not enabled the job can be scheduled to run at any time, including immediately, with no further checks.

Preparing RME for Use

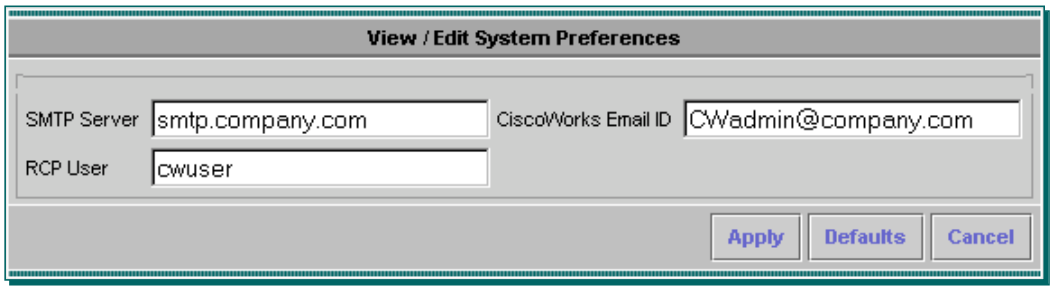
Job Approval - E-Mail Configuration

Cisco.com

RME jobs can be configured with an e-mail address to inform user when job has completed.

E-mail is also necessary for the Job Approval process.

Common Services > Server > Admin > System Preferences



E-mail Configuration

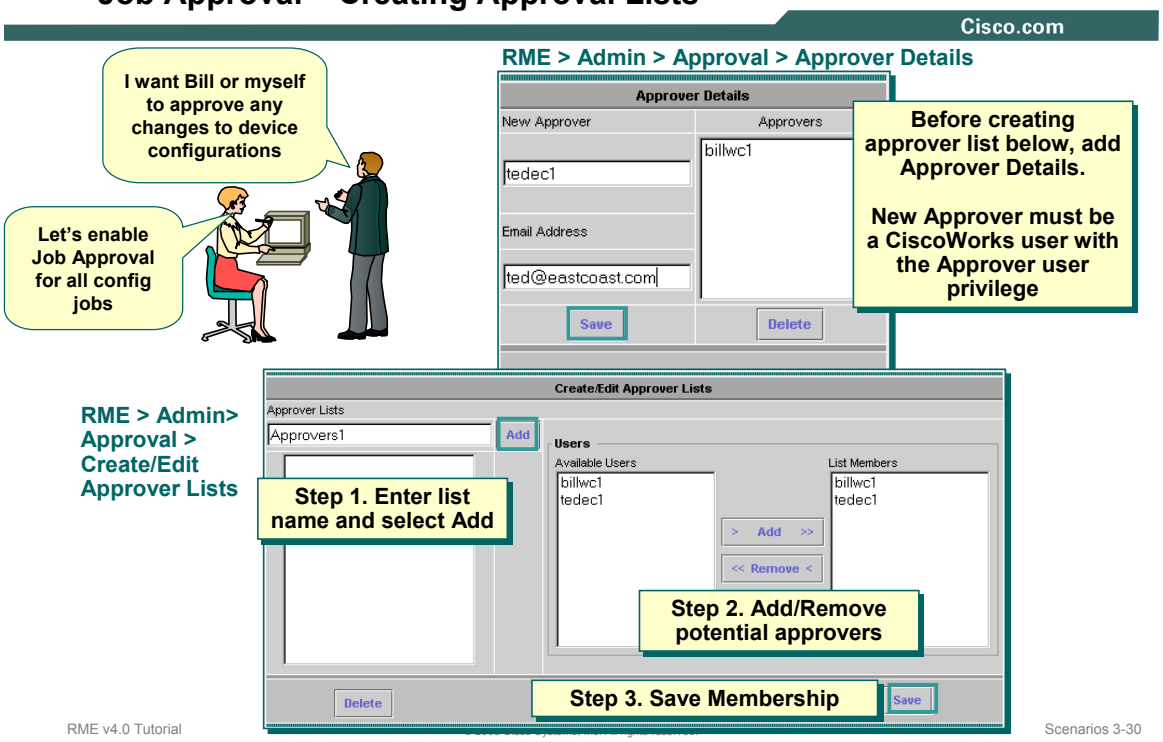
As shown in the workflow on the previous page, the sending of e-mail to 'Approvers' is an essential task in the job approval process, as well as, useful in other RME tasks to inform a user of job completion. So before beginning the actual job approval configuration, the CiscoWorks server needs to be configured with information about the e-mail server to be used.

Note: E-mail configuration is a Common Services task and is common to all CiscoWorks applications

1. Select **Common Services > Server > Admin > System Preferences.** The View/Edit System Preferences dialog box is displayed.
2. Enter the host name or IP address of the e-mail server in the SMTP Server entry box. **Note**: when CiscoWorks is installed on a Solaris platform, this value is typically set to localhost.
3. Enter the CiscoWorks e-mail ID. This is the e-mail ID from which CiscoWorks applications sends e-mail.
4. Click **Apply** for the changes to take effect.

Preparing RME for Use

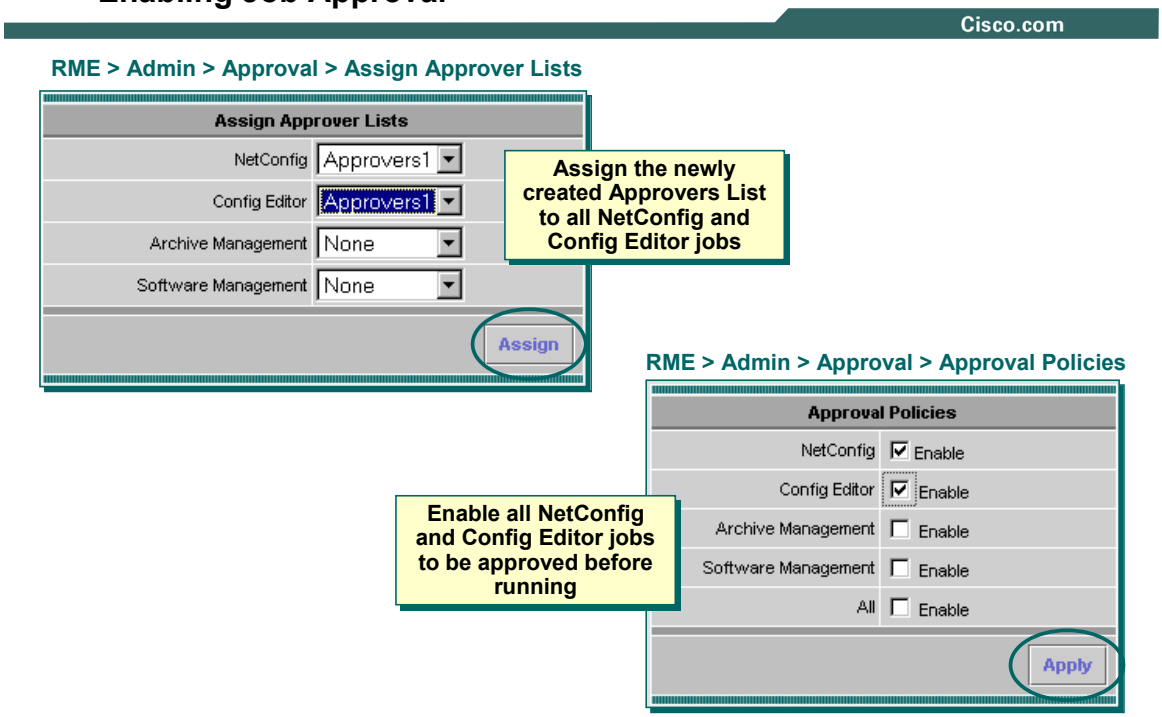
Job Approval – Creating Approval Lists



Approver Lists

Before testing some of RME features, Ted wants to make sure he or his counterpart on the West coast, Bill, are involved in any RME job that will modify a device's configuration. Sally will first need to tell RME that Bill and Ted are acceptable approvers (their CiscoWorks accounts must already have the Approver user role) and will then create a list with both of them as members.

1. Select **RME > Admin > Approval > Approver Details.** The Approvers dialog box is displayed.
2. Sally enters Bill's CiscoWorks user name and e-mail address and clicks **Save.**
3. Ted's information is entered in the same manner. These two users are now capable of being placed in RME approver lists.
4. Select **RME > Admin > Approval > Create/Edit Approver Lists**. The Create/Edit Approver Lists dialog box is displayed.
5. Enter a name for the approver list being created.
6. From the left side of the Users dialog select the members of the approvers list and click **Add** to make them a member (only approvers assigned in steps 2 and 3 will be listed).
7. Click **Save** when finish to create the list.



Enabling Job Approval

The final two steps are to assign approver lists to the tasks and enable the tasks to use job approval.

1. Select **RME > Admin > Approval > Assign Approver List**. The Assign Approver Lists dialog box is displayed.
2. For the NetConfig job select the approvers list just created from the pull down list of approver lists.
3. Repeat step 2 for Config Editor jobs (these are the two tasks which will modify a device's configuration).
4. Click **Assign** for the assignments to take effect.
5. Select **RME > Admin > Approval > Approval Policies**. The Approval Policies dialog box is displayed.
6. Enable Job Approval for NetConfig and Config Editor
7. Click **Apply** to enable Job Approval for those two tasks.

The RME basics have now been configured and it is time to start using some of the features of RME.

Note: Job Approval was disabled later by Sally to speed up the testing of RME functions since Bill or Ted were usually looking over her shoulder anyway. They will be re-enable when RME is deployed into operations.

Reports

- Getting Started
- Preparing RME for Use
- ➢ Reports
- Configuration Management
- Software Image Management
- Automated Actions

Reports

Cisco.com

- **Types of Reports**
- **Generating Reports**
  - Immediate
  - Scheduled
    - Report Archives
- **Custom Templates**

Reports

RME collects a tremendous amount of valuable management information. This scenario looks at how to view RME information in the form of reports. The reports can be generated and viewed immediately, or scheduled to run at a later time and on a reoccurring basis for maximum flexibility and time saving. This scenario will also see how to create custom templates to get the exact data required.

Reports
Types

Cisco.com

Types

- **Standard**
  - Inventory
  - Change Audit
  - Syslog
  - Bug Toolkit
  - Audit Trail
- **Custom**
  - Inventory
    - Attributes
  - Syslog
    - Facility
    - Severity
    - Mnemonic

Execution

- **Immediate**
- **Scheduled**

Report Types

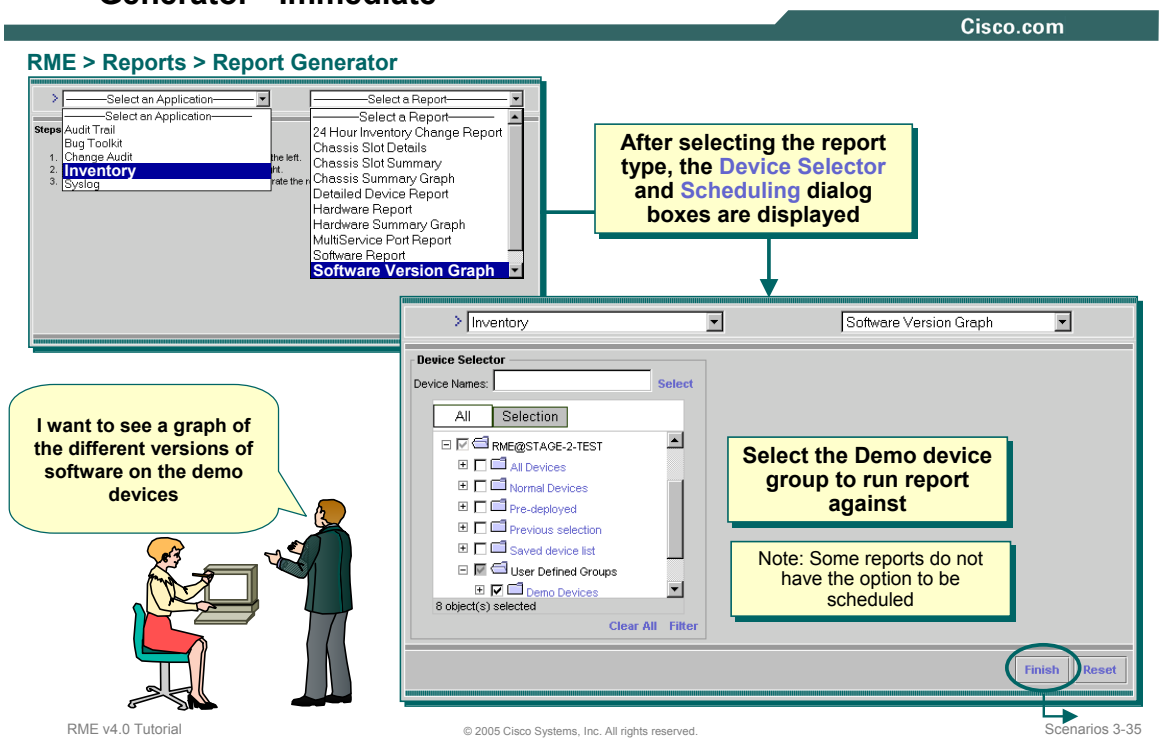
As briefly mentioned, there are two basic types of reports: Standard Reports –included with CiscoWorks that simply require you to select the devices to run the report for and an execution schedule, and Custom Reports – reports that require you to first create a template or query into the database for the desired data prior to selecting the devices and execution schedule.

Standard reports are included for many different RME functions – Inventory, Change Audit, Syslog, Bug Toolkit (requires connection to Cisco.com), and Audit Trail which details user activities of RME functions. Whereas, the custom reports are limited to queries into the inventory and Syslog databases.

Some of the reports are only available to be executed immediately, whereas others can be scheduled to run at a later time and with a reoccurring frequency.

Report generation follows a simple workflow: Select the report application, select the report, select the devices to run the report again, select the scheduling, run the report.

Reports
Generator - Immediate



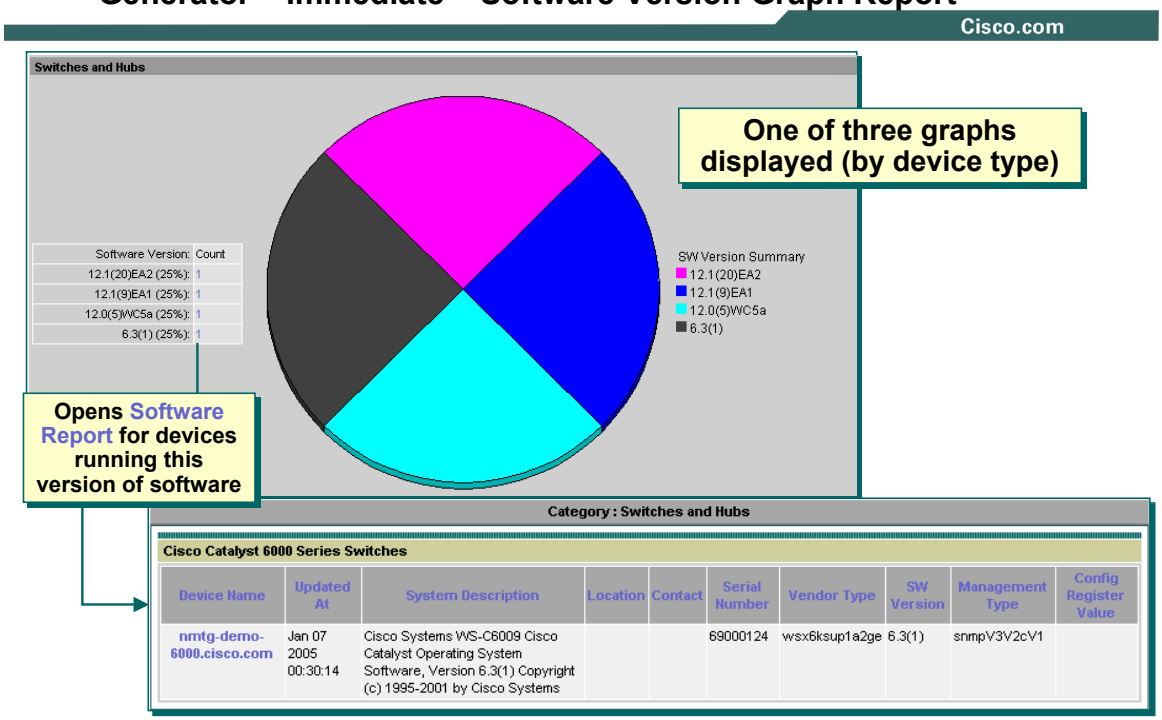
Immediate Report Generation

Ted is excited to start seeing the power and versatility of CiscoWorks and RME. However, earlier in the day he was given a priority job to provide a list of the software versions being run on the demo devices to the operation folks. He first started to look for a list of the devices so he could telnet to them and run the appropriate show command. He created a spreadsheet to enter the data into. As he tried to get into the first device he realized he no longer knew the frequently changed password. He called Sally and told her what he needed, she laughed at him and said this is one of the exact reasons they are implementing CiscoWorks – to avoid the set backs he was running into. She said she could give him the data in just a couple of clicks of the mouse.

1. Select **RME > Reports > Report Generator**. The Report Generator dialog is displayed.
2. From the pull down list of report applications, select **Inventory**.
3. From the pull down lists of reports, select **Software Version Graph**. The dialog changes to show the parameters for the selected report.
4. The left side of the dialog is the Device Selector, expand the RME entry, expand the User Define Groups entry, and select the **Demo Devices** group.
5. This type of report has no scheduling options, so simply click **Finish** to run the report.

Reports

Generator – Immediate – Software Version Graph Report



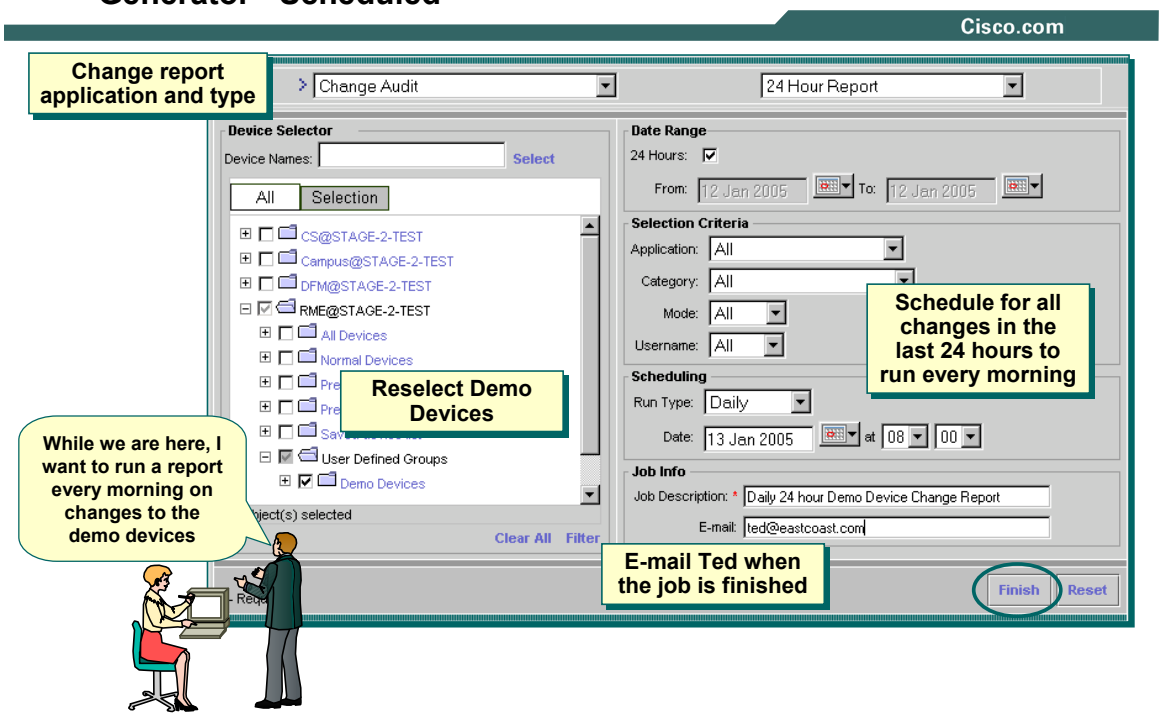
RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-36

Software Version Graph Report

Sally was right, with just a few simple clicks Ted has the information that was requested. Devices in the demo group are broken down into device types and then a graph shows the number of devices running each version of software. Ted also discovers that by clicking on the number of devices he gets additional information about those devices.

Ted quickly sees a time savings in a simple request for information, and he realizes that as easy as it was to get the information, he just needs to give the operation folks Help Desk access to the CiscoWorks server and they can get the information themselves freeing up more of his and his peoples time!

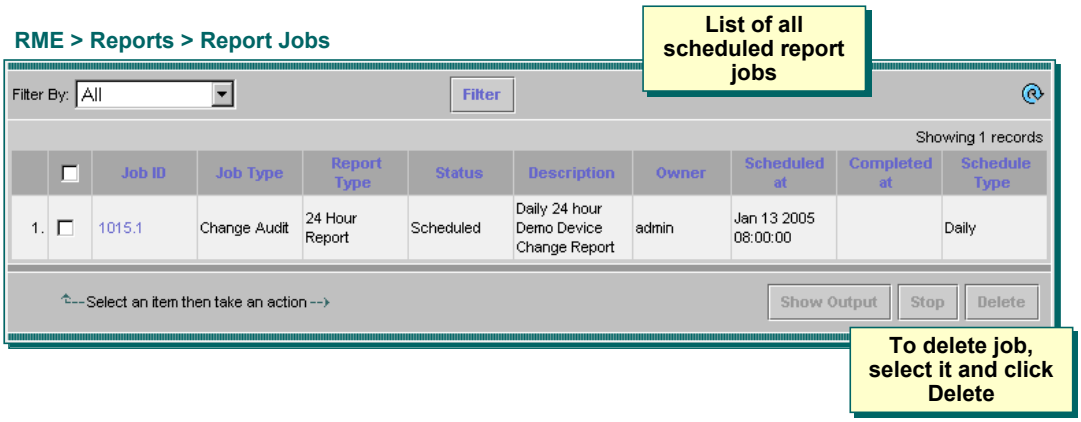
Reports
Generator - Scheduled



Scheduled Report Generation

The first use of RME turned out to be a huge success for Ted, both in time-savings and accuracy. Now he wants to see a report detailing the changes to the demo devices everyday. He's worried that this will be a bit of a pain to have to remember to run each morning. Sally lays his fears to rest informing him that she can simply schedule the job to run every morning.

1. RME should still display the Report Generation dialog, if not select **RME > Reports > Report Generator.**
2. From the Report Application pull down menu select **Change Audit**.
3. From the Report Type pull down menu select **24 Hour Report**.
4. Select the **Demo Devices** group from the Device Selector on the left side of the dialog.
5. Enter the following parameters: *Data Range*: check the **24 Hours** entry, *Selection Criteria*: Select **All** for every category, Scheduling: select *Run Type* = **Daily** and set appropriate start date and time, *Job Info*: enter meaningful job description and enter an e-mail address of a person to inform when the job is complete.
6. Click **Finish**.



Report Jobs

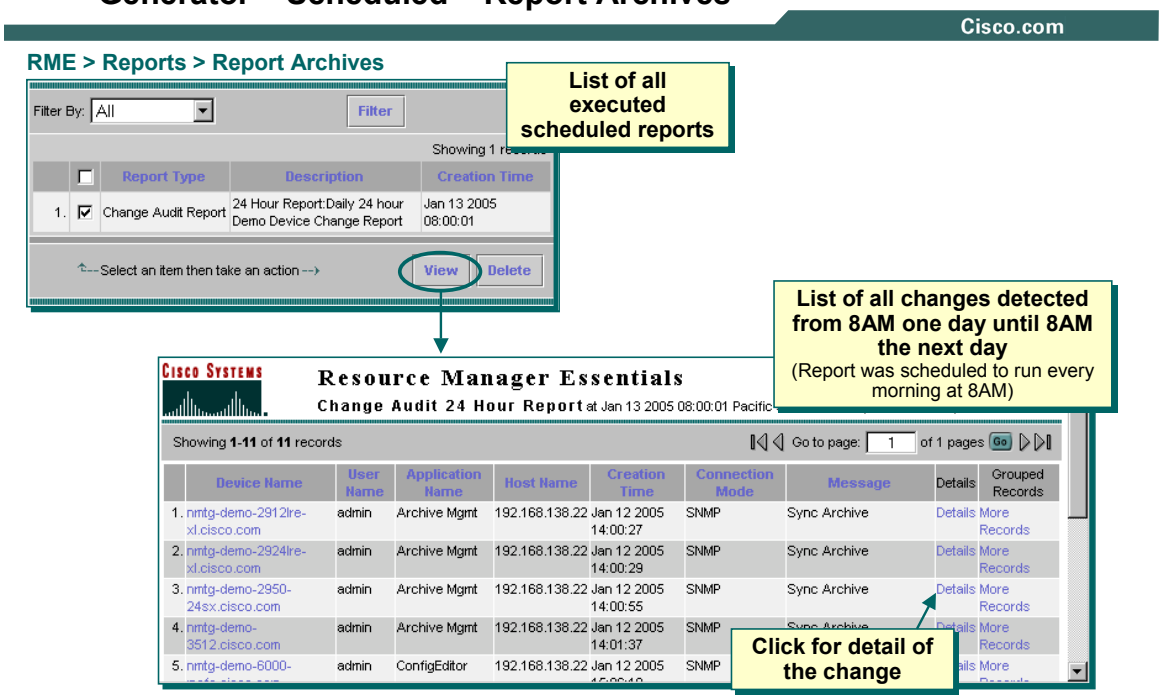
To verify the creation of the scheduled job or to check it's status:

1. Select **RME > Reports > Report Jobs**. The Report Job Browser dialog box is displayed.

   A list of all scheduled and completed scheduled jobs is displayed. Upon completion, the job can be selected and the **Show Output** button can be selected to view the report. Alternatively, as shown on the next page, the output can be viewed using the Report Archives screen.

   Note: Deleting an entry for a completed job will also remove the output from the Report Archive.

Reports
Generator – Scheduled – Report Archives



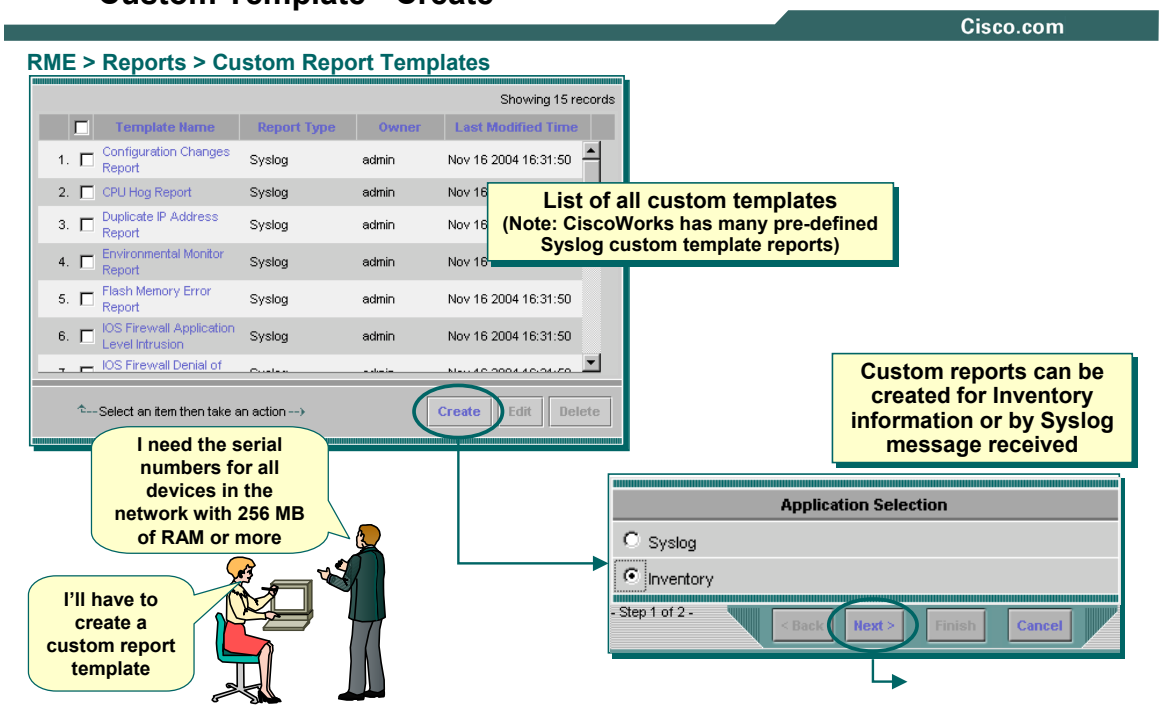
Report Archives

The next morning Ted receives an e-mail stating that the report was successfully created and containing a link into the Report Job Browser. To view the report if an e-mail is not sent:

1. Select **RME > Reports > Report Archive**. The Archives dialog is displayed showing a listing of all completed scheduled reports.
2. Click the box on the row of the report to be viewed and click the **View** button. In this case the Change Audit 24 Hour Report is displayed in a separate window detailing the changes to demo devices in the last 24 hours.

Reports

Custom Template - Create



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-40

Creating Custom Report Templates

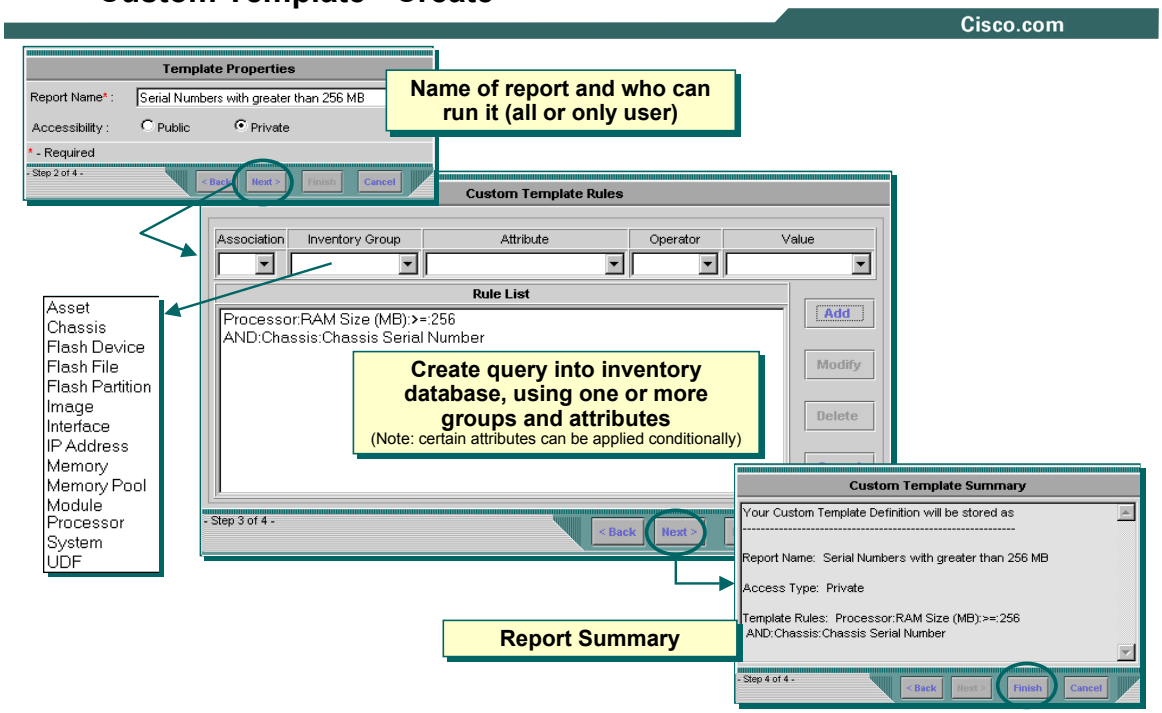
Ted is loving the data that RME easily provides him, but he's afraid the operations manager's latest request won't prove to be as easy to provide. The operations manager wants to know the serial numbers for all devices in the network with 256 MB or more of RAM. Ted sees that the information is available when he runs an Inventory Hardware Report but it means he will have to go though each entry (potentially thousands of devices in some networks) to find the devices meeting the desired criteria. Sally stops him and assures him there is an easier way. She informs Ted that RME provides a mechanism for basically creating a custom query into the database referred to as a Custom Template. Custom templates can be created to query either the Inventory or Syslog databases. In fact, RME comes pre-loaded with several custom templates for Syslog messages.

Use the following steps to create Ted's report:

1. Select **RME > Reports > Custom Report Templates**. The Custom Templates dialog box is displayed showing all currently defined custom templates (RME comes preloaded with several Syslog custom templates to query the database for specific message types)
2. Click **Create** to begin the Custom Template wizard (the actual number of steps is determined by the choice in the first step). The Application Selection dialog is displayed.
3. Select **Inventory**.
4. Click **Next**.

Reports

Custom Template - Create

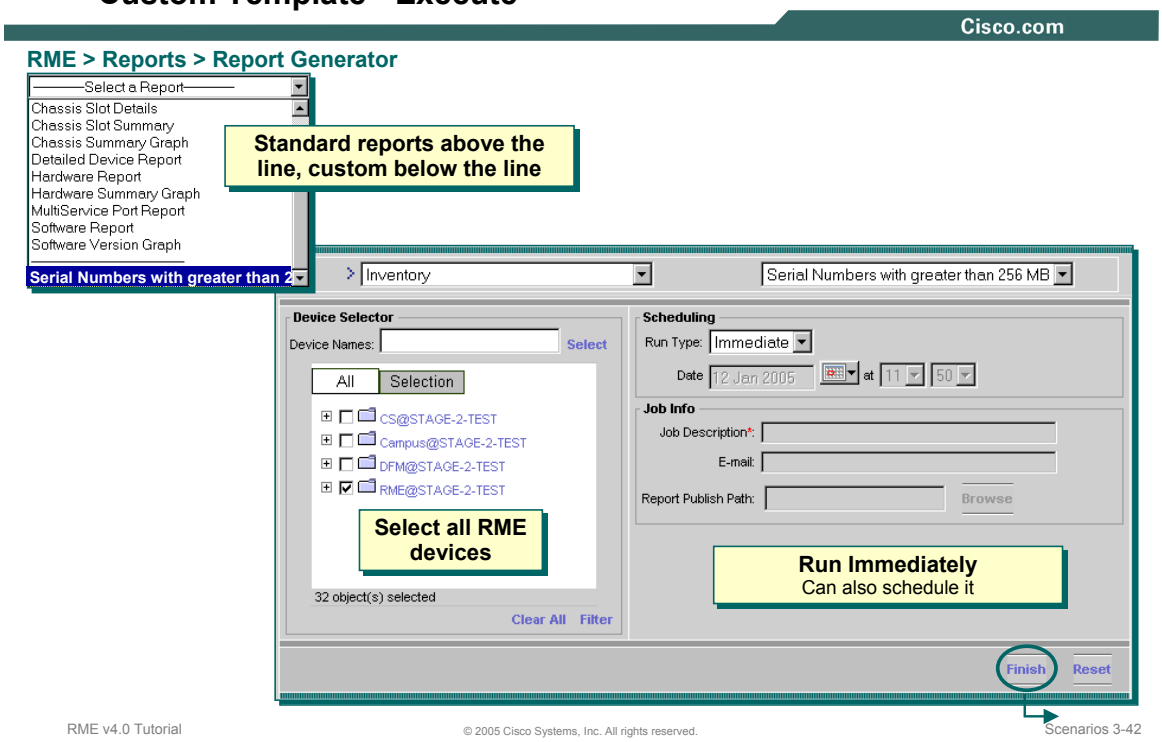


Creating Custom Report Templates

5. The Template Properties dialog is displayed (Step 2 of 4). Enter a Meaningful name for the template and select the access type (private to current user or public for everyone to use)
6. Click **Next**. The Custom Template Rules dialog is displayed.
7. Adding rules is basically creating the query into the database. Each rule is based on a relationship with different Inventory group variables. In this case Sally selects the Inventory group **Processor**, the attribute **Ram Size**, the operator **>=**, and enters a value of **256** to create the first part of the query. For the second part of the query she selects the Association to be **AND**, the Inventory group **Chassis**, the attribute **Chassis Serial Number**, this query portion does not need an operator or value.
8. Click **Next**. The Custom Template Summary is displayed.
9. If all looks OK click **Finish**.

Reports

Custom Template - Execute



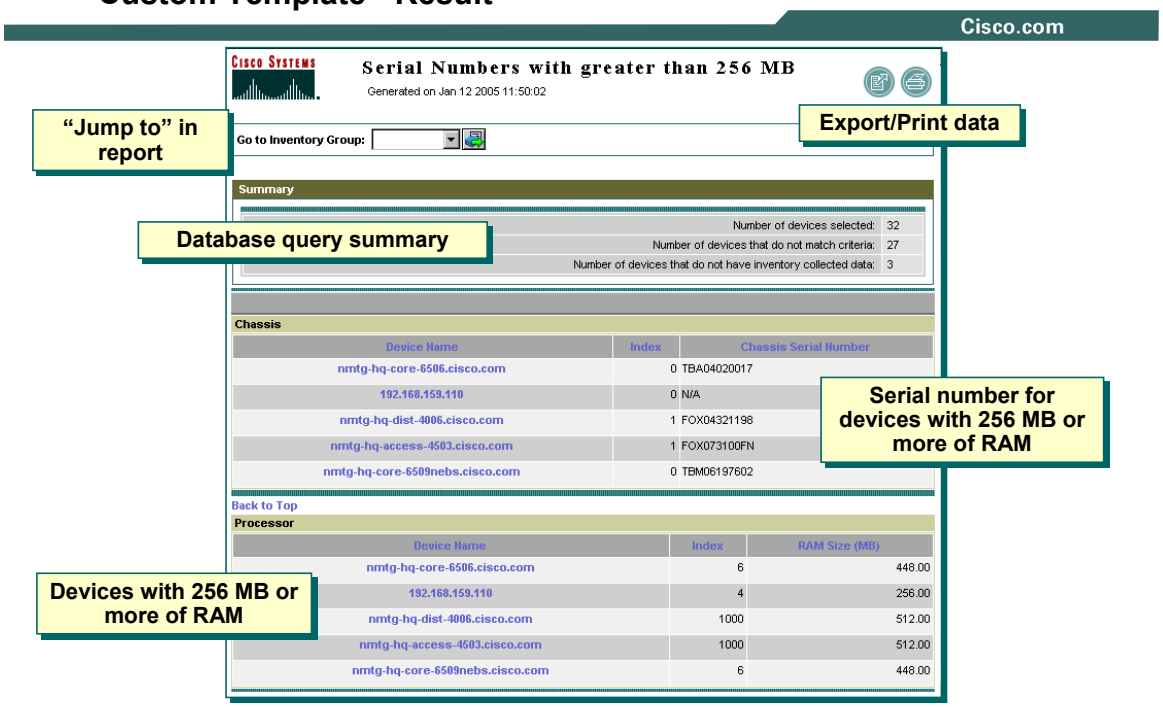
Generating a Custom Report Template

At this point the template has been created, the next step would be to generate a report to get the data. This procedure is identical to the discussion earlier on report generation where reports can be generated immediately or scheduled.

1. Select **RME > Reports > Report Generator**. The Report Generator dialog is displayed.
2. From the pull down list of report applications, select **Inventory**.
3. From the pull down lists of reports, select **Serial Numbers with Greater than 256 MB** (The template just created). Notice that there is a line separating the reports into two categories: above the line are system (pre-defined) reports and below the line is a listing of any Custom Templates.The dialog changes to show the parameters for the selected report.
4. Select **All RME Devices** using the Device Selector on the left side of the dialog.
5. Select the Run Type to be **Immediate**, no further parameters are necessary.
6. Click **Finish** to run the report.

Reports

Custom Template - Result



Custom Report

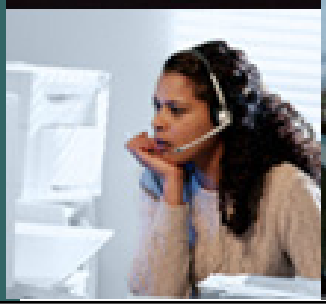
The Custom Report is displayed in a separate window. It contains two sections, one showing the amount of RAM for the devices with 256 MB or more, and the other section showing the serial numbers for these devices.

Ted is ecstatic! RME has made the collection and presentation of data a snap. Ted is simply amazed at how easy it was to get data that would have taken hours to get before having RME installed.

Ted is ready to see how RME can help him manage the device configurations.

Configuration Management

- Getting Started
- Preparing RME for Use
- Reports
- ➢ Configuration Management
- Software Image Management
- Automated Actions



Configuration Management

Cisco.com

- Search
- Config Editor
- NetConfig
- Change Audit

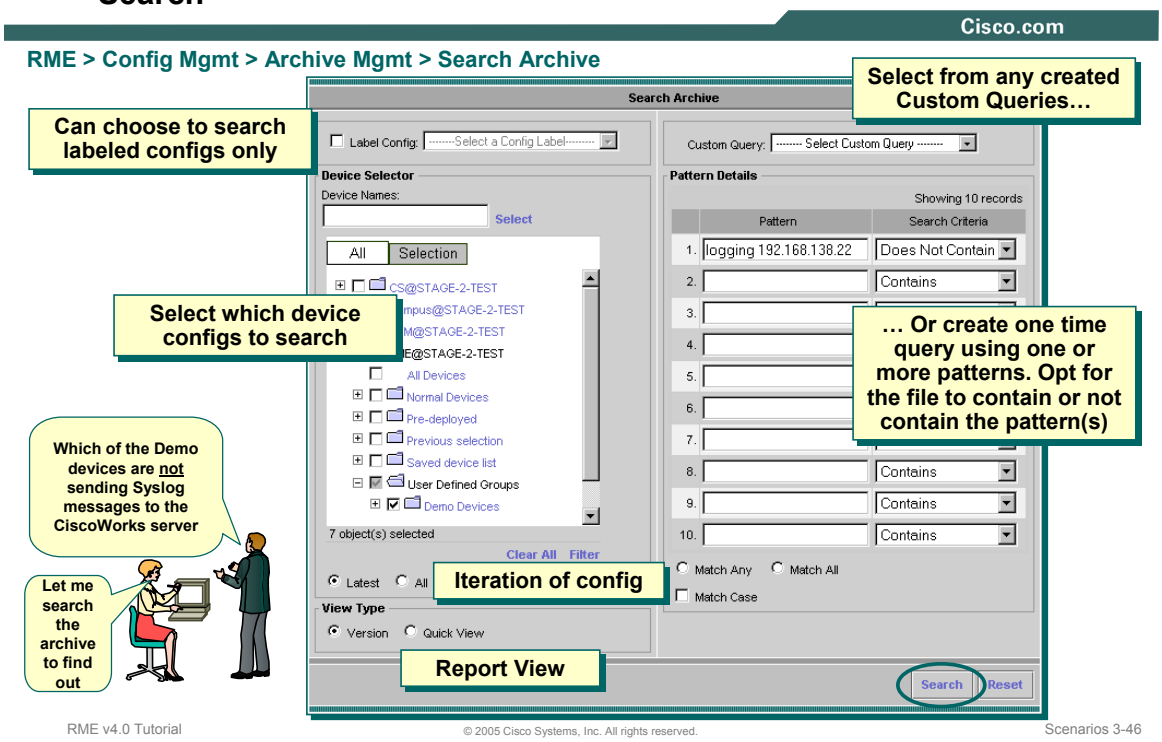
Configuration Management

Most businesses can no longer survive without their networks. Perhaps the most critical piece of the network are the set of instructions detailing how each device should handle the forwarding of each and every packet. Hence it stands to reason that managing the devices' configuration files is an extremely important endeavor.

In the second scenario, we looked at how to do basic configuration to continuously check configuration files to create an archive of different versions for each device. Many times network troubles begin when someone made what they thought was a benign change to a configuration file. Finding this change is often like looking for a needle in a haystack. This is one area were RME Configuration Management excels - by automatically detecting the change, and providing a simple and straight forward way of viewing the change.

This scenario examines many of the RME tools useful for Configuration Management. The user is encouraged to think beyond these simplistic examples to fully appreciate the true power of these tools and how they can benefit them in their own environments.

Configuration Management
Search

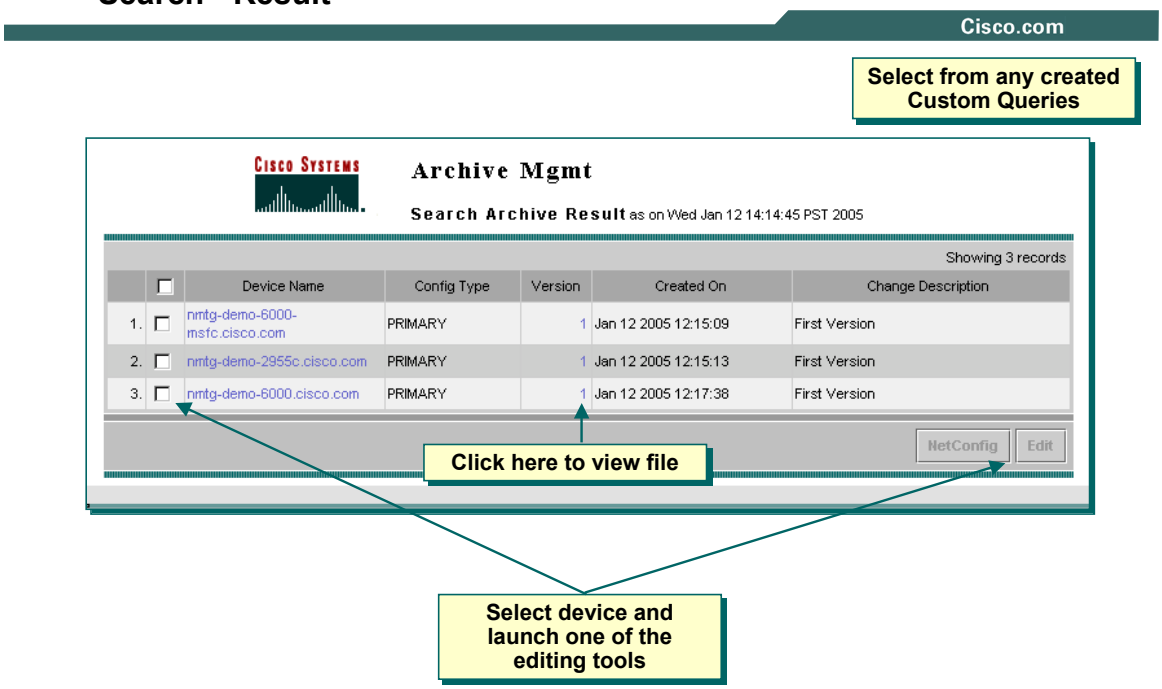


Search Configuration Archive

Ted noticed that RME included lots of reports for Syslog messages, which if used wisely are extremely beneficial for detecting faults and other network anomalies. To have RME report on Syslog messages, they must be forwarded from the device to RME. Ted also figures this is an excellent way to test the RME configuration tools. Ted informs Sally of his desire to have all demo devices forwarding Syslog messages to RME, so he can run the RME Syslog reports. Ted figures the first step is to figure out which of the demo devices are not currently forwarding messages to RME. He could certainly telnet to each device and look at their configurations to ascertain this, but he already knows this would be time consuming. Sally suggest simply searching the configuration archive since it is kept up to date with all the latest files.

1. Select **RME > Config Mgmt > Archive Mgmt > Search Archive**. The search Archives dialog is displayed.
2. The dialog consists of two halves: the left side is used to select the device(s) configs to search (this includes the latest or all versions as well as searching labeled configs only. A labeled config remains in the archive regardless of the archive purge policy. Config files can be labeled using the RME > Config Mgmt > Archive Mgmt > Label Configs task.) The right side allows you to either select a saved custom query (another Archive Mgmt sub-task) or create a new query. In this case, Sally selects the **Demo Devices** group from the device selector, the Latest button, and the View Type as Version. On the query side enters 'logging 192.168.138.22 (the Syslog command on a device to send Syslog messages to the server) and selects **'Does Not Contain'** as the search criteria.
3. Click **Search** to begin the archive search.

Configuration Management
Search - Result



Search Result

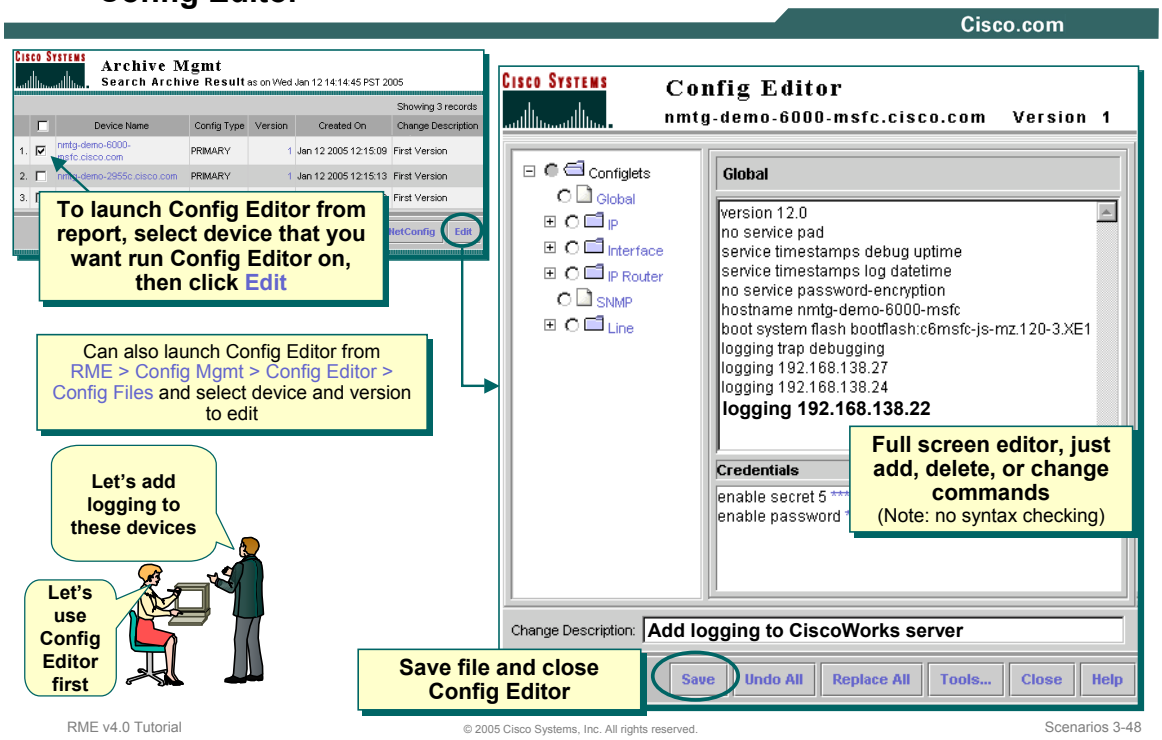
An Archive Mgmt Search Archive Result report is opened in a new window. It lists all devices whose current configuration in the archive does not contain the string ‘logging 192.168.138.22’. That means these three devices need to have their configuration files modified to add Syslog logging.

To view the configuration, click the version number. Notice in this case it is the first version for each device meaning that RME has not found a change to these configuration files since the first version was archived. As we will see later that in addition to archiving configuration files based on the schedule, RME will also archive a new version if a Syslog message is received indicating that the configuration has changed.

This report also has hooks into two configuration tools of RME: *Config Editor* and *NetConfig*. Sally and Ted are going to use this report to launch both of those tools to modify the files.

Note: All three files could be modified with a single NetConfig job, but then Sally and Ted would not learn how to use Config Editor.

Configuration Management
Config Editor

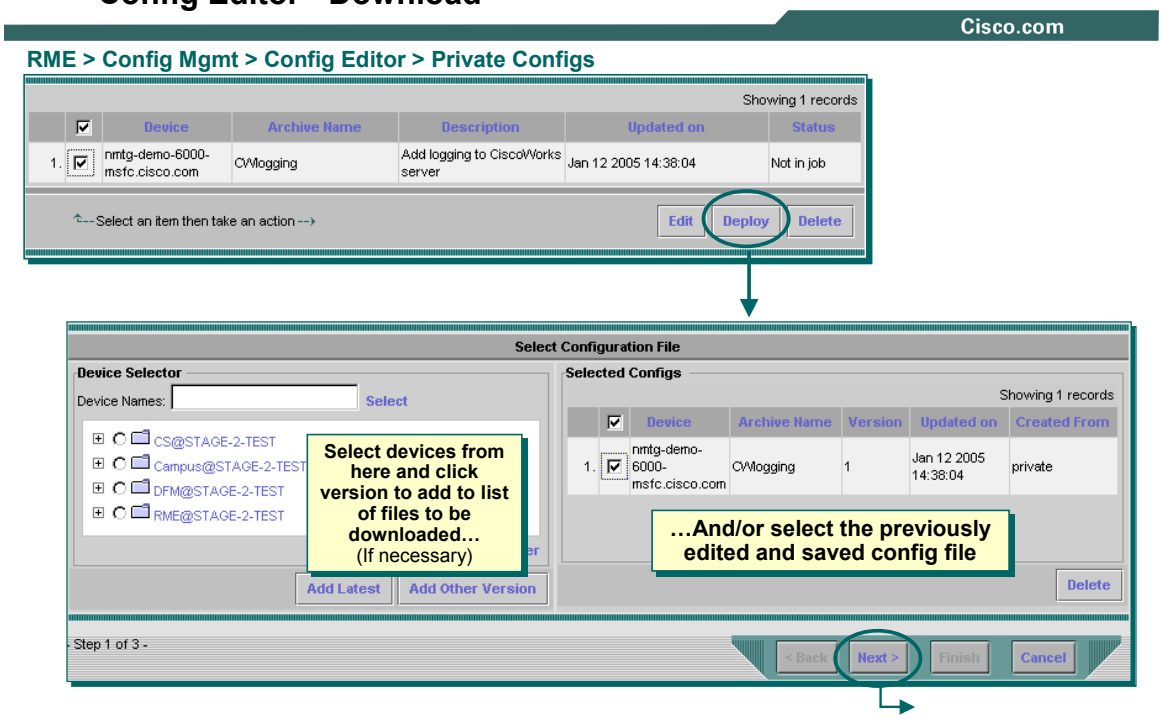


Config Editor

The following steps illustrate how Sally and Ted use the report to launch and use Config Editor for the first device in the list.

1. Highlight the first device in the list. Both the NetConfig and Config Editor buttons are enabled. Click the **Config Editor** button to launch Config Editor with the configuration File version 1 in the archive for this device. (Config Editor can also be launched directly from the RME desktop by selecting RME > Config Mgmt > Config Editor > Config Files and then using the displayed device selector to select the device and configuration file version.)
2. The Config Editor processes the raw configuration file and breaks it into configlets to ease in the viewing and modifying of the file. Open the global configlet. Config Editor is a full screen editor. Since some logging commands already exist, Sally just needs to add the command 'logging 192.168.138.22' to the list.
3. Add a meaningful change description.
4. Click **Save** to save the file and changes to the logged in user's private storage.

Configuration Management
Config Editor - Download



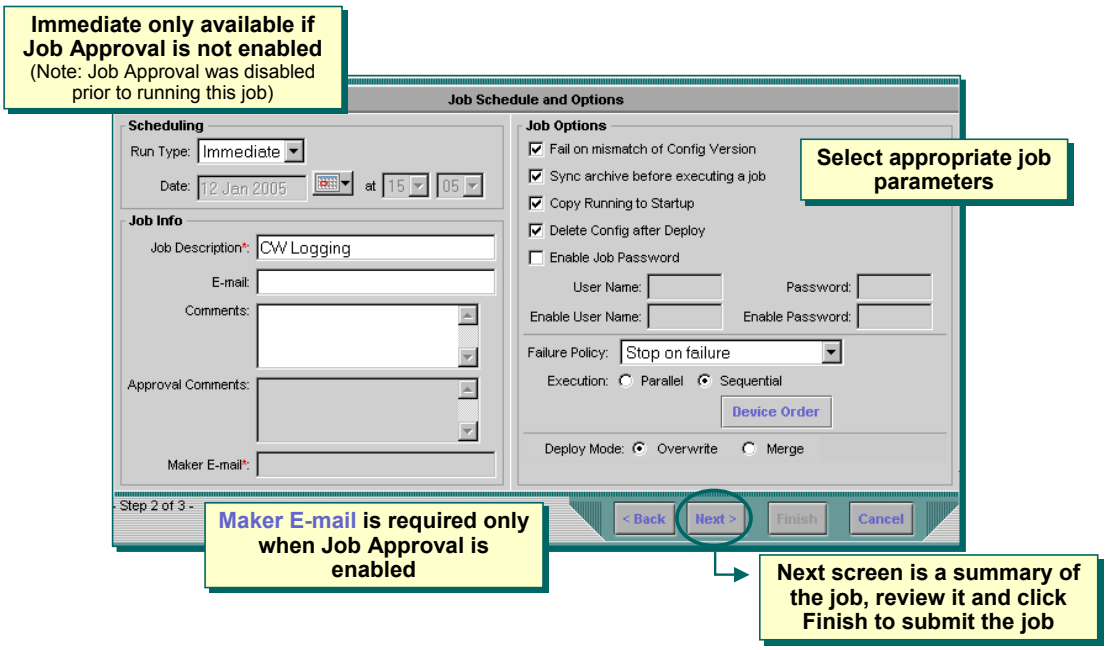
Download Config Editor Modified File

The next step is to actually download the file just modified and saved.

1. Select **RME > Config Mgmt > Config Editor > Private Configs**. The Private Configs dialog is displayed listing all files modified by this user with Config Editor.
2. Highlight the file just modified and click **Deploy**. The Deployment 3 step wizard is displayed.
3. The left side includes a device selector that would allow you to select a device and version of configuration file to deploy essentially allowing for a roll-back operation. In this case the file we wish to deploy is already listed on the right side of the dialog, simply highlight it and click **Next** to go to step two of the deployment wizard.

Configuration Management
Config Editor - Download

Cisco.com



RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-50

Download Config Editor Modified File

4. The Job Scheduling and Options dialog is displayed. The left side of this display will differ depending on whether or not Job Approval is enabled. Sally disabled Job Approval earlier since Ted is looking over her shoulder. Since Job Approval is Disabled, Sally can select the Run Type to be **Immediate**. Enter a meaningful Job Description. If desired enter e-mail addresses for those to be notified when the job is complete, and any comments. If Job Approval was enabled, Immediate would not be an option and the job would have to be scheduled. Remember to leave enough time for the approvers to get the e-mail and approve the job.
5. The right side allows you to control the job download. Config Editor only protects multiple users of RME from making changes at the same time, it does not prevent user from making changes using telnet. The first option 'Fail on Mismatch of Config Version' prevents this by first uploading the current version and comparing it against the version being modified by Config Editor. Selecting this option also turns on 'Sync archive before executing a job'. If you did not select the first but selected the second option, and someone had made a telnet change, at least you will archive it. The remaining options are self-explanatory. If downloading multiple files, set a failure policy and processing order to minimize the possibility of effecting reachability of device not yet modified. Finally select whether to overwrite the file with the one being deployed or to simply merge the two.
6. After selecting all parameters, select **Next** to view the job work order detailing what will be done.

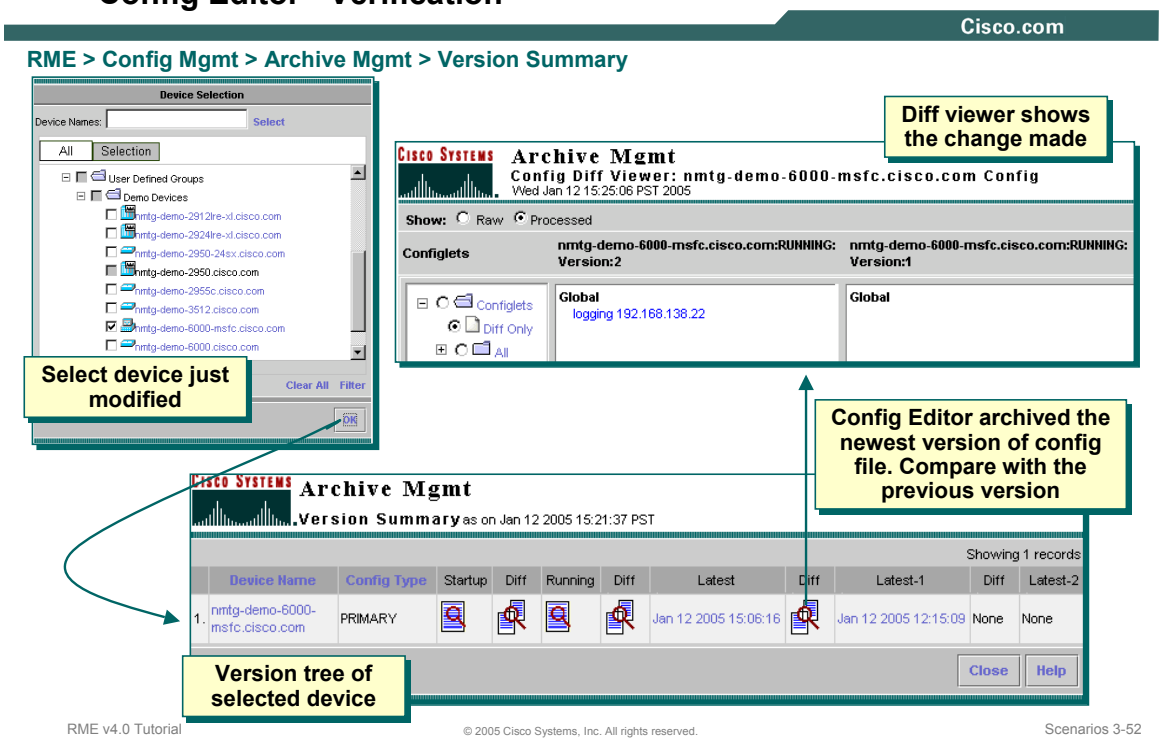
Configuration Management
Config Editor – Job Results

Config Editor Deployment Results

The job has been place on the job queue and since the run type was Immediate, it has already begun to execute. To see the status of any Config Editor job, follow these steps.

1. Select **RME > Config Mgmt > Config Editor > Config Editor Jobs**. The Config Deploy Job Browser is displayed listing the Config Editor deploy jobs and there status.
2. Click the **Refresh Icon** in the upper right-hand corner until the deployment job currently running shows Successful or Error.
3. When the job is completed, click the Job ID to see the details of the job. In the event of an error the details will show the exact step that caused the error allowing you to correct the problem and resubmit the job.

Configuration Management
Config Editor - Verification



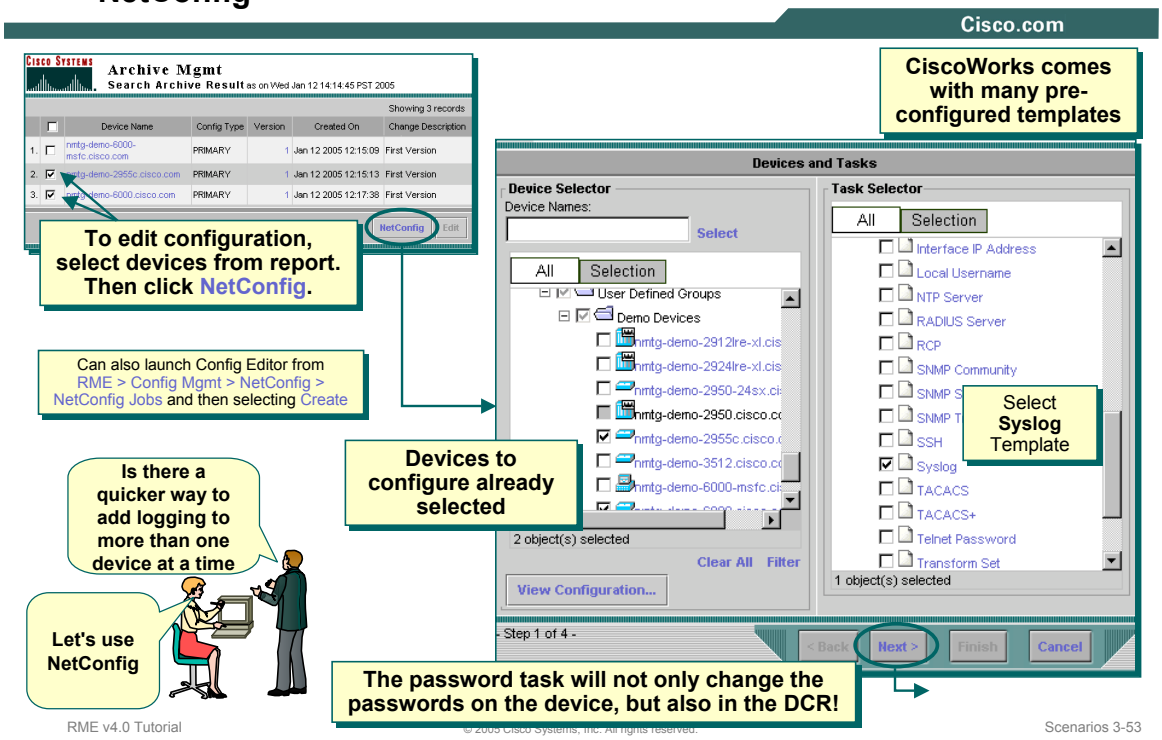
Did the Change Really Happen?

Ted doesn't quite fully trust RME yet and wants to double check that the change actually took place. Rather than using telnet to view the running config, Sally at least convinces Ted to look into the archive to see if there is a new version and what the difference is between the old version and the latest. (After adding the logging command, it should have caused the device to send a Syslog message to RME saying the configuration had changed, which is suppose to trigger RME to fetch and archive the new version.)

1. Select **RME > Config Mgmt > Archive Mgmt > Version Summary**. A Device Selector is displayed as the Version Summary dialog.
2. Expand RME,User Defined Groups, and Demo Devices to get a list of the devices in the Demo Devices group. Select the device that was just modified.
3. Click **OK**. The Archive Mgmt Version Summary Report is displayed showing the different versions for the selected device in the archive.
4. In this case, the list shows two archived versions. Select the **Diff Icon** located between the two archived versions to see the difference.
5. The Archive Mgmt Config Diff Viewer is displayed showing the two config files parsed into configlets. One special configlet is Diff Only. Select this and only the differences between the two files are displayed. Blue text indicates a command in one file but not the other, red text indicates the same command but with different parameters.

Since the difference between the latest version and previous is the logging command, it stands to reason RME worked as advertised complete with a record of the change activity!

Configuration Management
NetConfig



NetConfig

Ted is impressed at the reliability of Config Editor and how easy it was to use, but he realizes it would be burdensome to use Config Editor on lots of devices especially if the same changes were being made to all. This is exactly where NetConfig excels. Ted and Sally decide to use NetConfig to modify the remaining two config files that are not logging to RME.

1. From the *Archive Mgmt Search Archive Report* run earlier, select the two devices that were not previously configured with Config Editor. The NetConfig button is now enabled (the Config Editor button is not enabled at this time because more than one device was selected). Select the **NetConfig** button. The first step of the four part NetConfig wizard is displayed – Devices and Tasks.

   NetConfig can also be opened by selecting *RME* > *Config Mgmt* > *NetConfig* > *NetConfig Jobs*, then selecting *Create* in the NetConfig Job Browser dialog box.

2. The Devices and Tasks dialog consists of two parts: the left side to select the devices (in this case the devices are already selected based on input from the report), and the right side which allows for the selection of one or more templates to configure to modify the configuration files.

   Note(s):

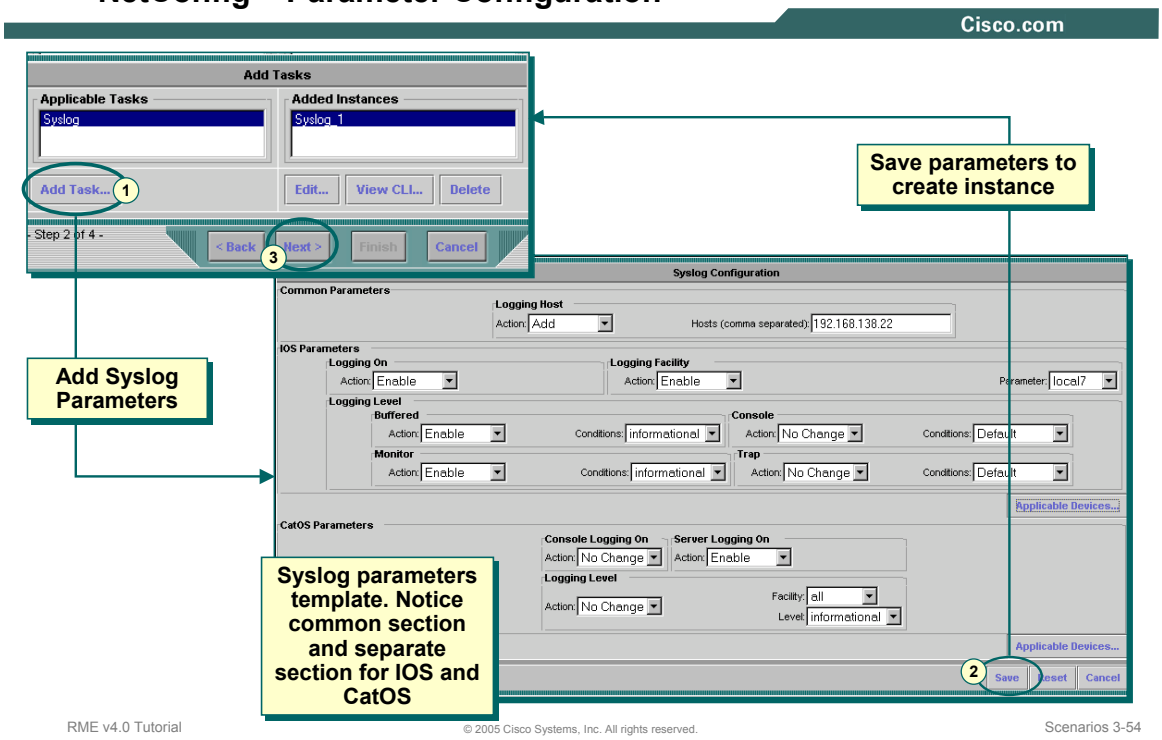
   - A user with Network Administrator rights can create new tasks or templates (*RME> Config Mgmt> NetConfig> User-defined Tasks*) and can also assign other users permission to use existing templates (*RME> Config Mgmt> NetConfig> Assigning Tasks*).
   - The assigned user must be a valid CiscoWorks user. If RME has been registered with a Cisco Secure ACS Server, then the user should be a valid ACS user. Also, the user must have the appropriate CiscoWorks privileges (Network Operator or Network Administrator) to use NetConfig. View the Permission Report (*Common Services* > *Server* > *Reports*) to check required privileges to perform task.

3. Scroll down the list to select the **Syslog** task. If warranted, more than one task can be selected for a given NetConfig job.

4. Click **Next**.

Configuration Management

NetConfig – Parameter Configuration

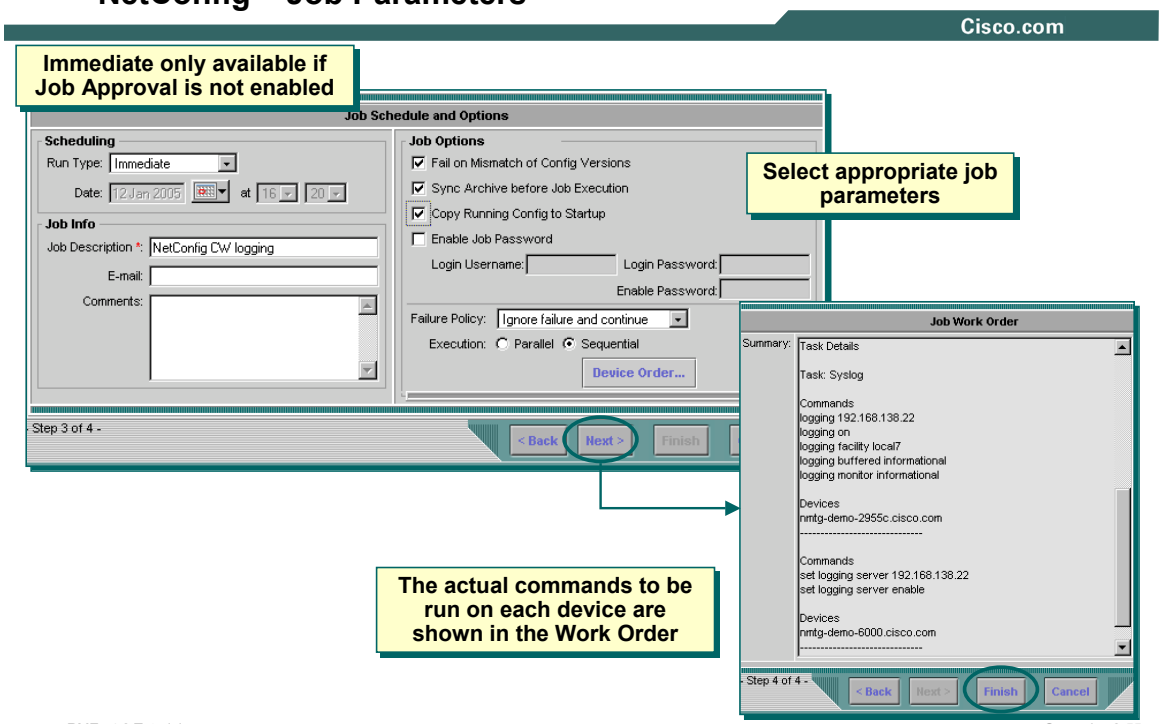


NetConfig – Parameter Configuration

5. The Add Tasks dialog box (step 2 of 4) is displayed. The left side of the dialog will consist of the list of tasks selected in the previous wizard step. To configure the task, highlight the task and click **Add Task**.
6. The configuration screen appears for the selected task. Depending on the devices and task selected, the configuration screen can have multiple parts. In this case there are three sections: Common Parameters, IOS Parameters, and CatOS parameters since the two devices selected are of different types. Sections will only appear if necessary for the selected devices. Configure this screen as appropriate and click **Save**.
7. The task configuration screen closes and the Add Tasks dialog now shows an instance of the selected task in the right hand portion of the dialog box (implying that some tasks may need to have multiple instances to fully configure). Click **Next** when done configuring tasks.

Configuration Management

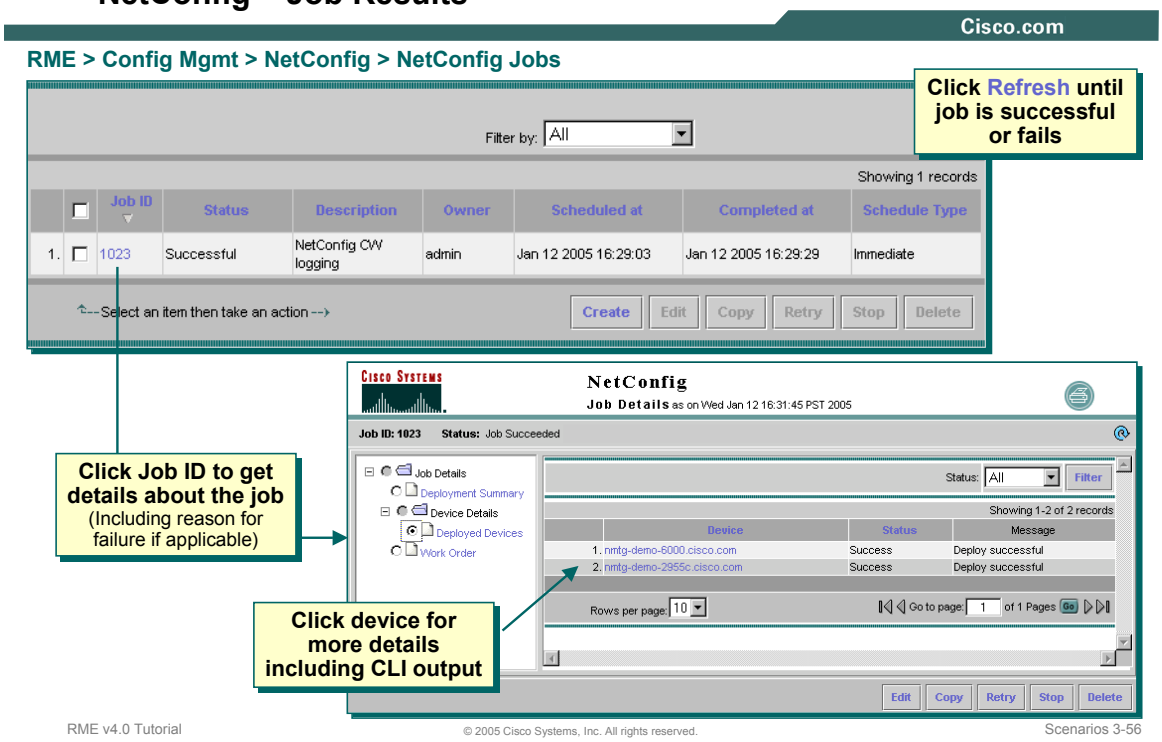
NetConfig – Job Parameters



NetConfig – Job Parameters

8. The Job Schedule and Options dialog (step 3 of 4) is displayed. Again the option for this dialog will differ if Job Approval is enabled. Sally chooses to run the job Immediately and ensure that nobody has changed the configs of these devices with telnet since the last archiving.
9. Click **Next** when finish with the job options and the work order is displayed. Scrolling though this the reader will notice the work order includes the commands to be executed on each device.
10. Click **Finish** to place the job in the job queue.

Configuration Management
NetConfig – Job Results

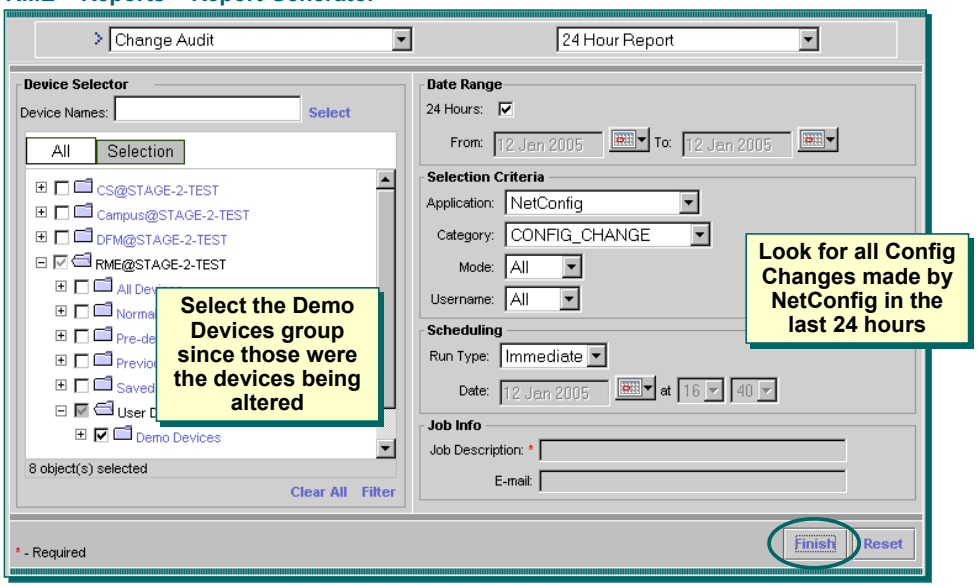


NetConfig Job Results

Looking at the status of NetConfig jobs is similar to the steps for looking at the status of the Config Editor, except using a different starting task. To see the status of any NetConfig job, follow these steps.

1. Select **RME > Config Mgmt > NetConfig > NetConfig Jobs**. The NetConfig Job Browser is displayed listing the NetConfig jobs and there status.
2. Click the **Refresh Icon** in the upper right-hand corner until the job currently running shows Successful or Error.
3. When the job is completed, click the Job ID to see the details of the job. In the event of an error the details will show the exact step that caused the error allowing you to correct the problem and resubmit the job.

RME > Reports > Report Generator



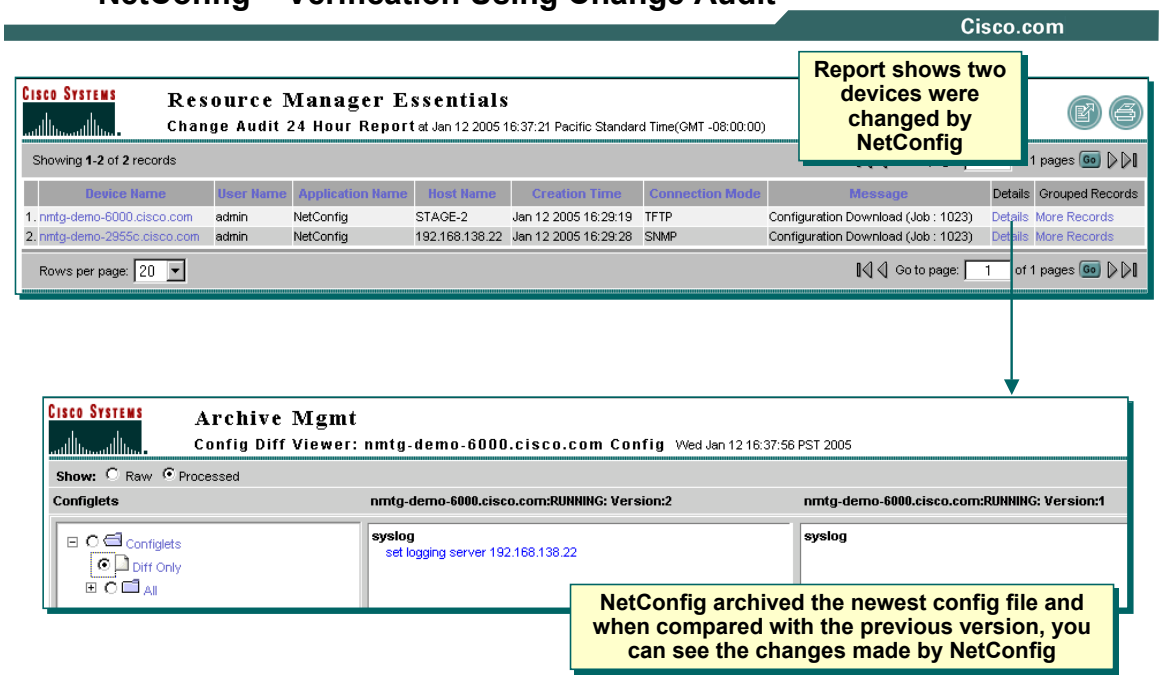
NetConfig Job Verification

Ted again wants to verify that NetConfig did its job as efficiently as Config Editor. Sally again reasons that since turning on Syslog logging back to RME should have caused RME to receive a Syslog message from each device, triggering RME to fetch the new configuration files, compare them to the previous version in the Archive, recognize the change, and thus create a Change Audit record; that looking at a Change Audit report should detail the change and satisfy Ted.

1. Select **RME > Reports > Report Generator**. The Report Generator dialog is displayed.
2. From the pull down list of report applications, select **Change Audit**.
3. From the pull down lists of reports, select **24 Hour Report**. The dialog changes to show the parameters for the selected report.
4. The left side of the dialog is the Device Selector, expand the RME entry, expand the User Define Groups entry, and select the **Demo Devices** group.
5. Select Application to be **NetConfig**, Category to **CONFIG_CHANGE**, and Run Type to be **Immediate**. Click **Finish** to run the report.

Configuration Management

NetConfig – Verification Using Change Audit



NetConfig – Verification Using Change Audit

The Change Audit 24 Hour Report is displayed showing two devices that had their configurations changed by the same NetConfig job. Clicking on the details for one of the entries launches the Archive Mgmt Config Diff Viewer report showing that the difference between the two most recent versions of configuration files for the device in the archive is the addition of the logging command.

Ted is thrilled with the power and flexibility of RME and especially its ease of use. Ted was able to change a number of device configurations reliable and easily with complete confidence. Time to see how RME handles Software Image downloads. Ted is now convinced that this task will be a smooth as those up to this point.

Software Image Management

- Getting Started
- Preparing RME for Use
- Reports
- Configuration Management
- ➢ Software Image Management
- Automated Actions

Software Image Management

Cisco.com

- **Version Analysis**
- **Add Software Image to CiscoWorks archive**
- **Distribution of Image**

Software Image Management

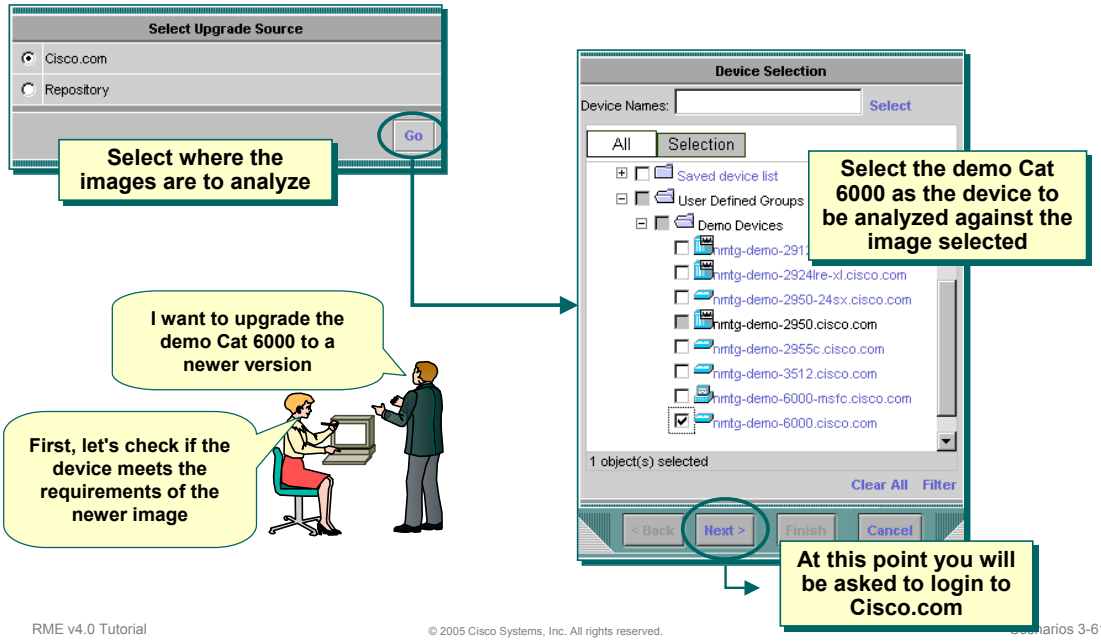
Upgrading the software images on devices has traditionally been a royal pain for many IT folks. They usually have to perform them in the middle of the night and if something goes wrong they know there is no sleep for them. Software Image Manager attempts to take much of the pain out of upgrading images by first analyzing the device to see if it has enough resources to run the new image. This is done automatically to ease the burden. The deploy job, like the configuration jobs, is highly configurable with parameters to schedule to run while your asleep, have a fall back rule, as well as, instructions on what to do if a failure occurs. The details of the job can then be reviewed to see exactly why the job failed.

This scenario looks at the available features through a simple analysis, download of image from Cisco.com, and deployment of the image to the device.

Software Image Management
Analysis

Cisco.com

RME > Software Mgmt > Software Distribution > Upgrade Analysis



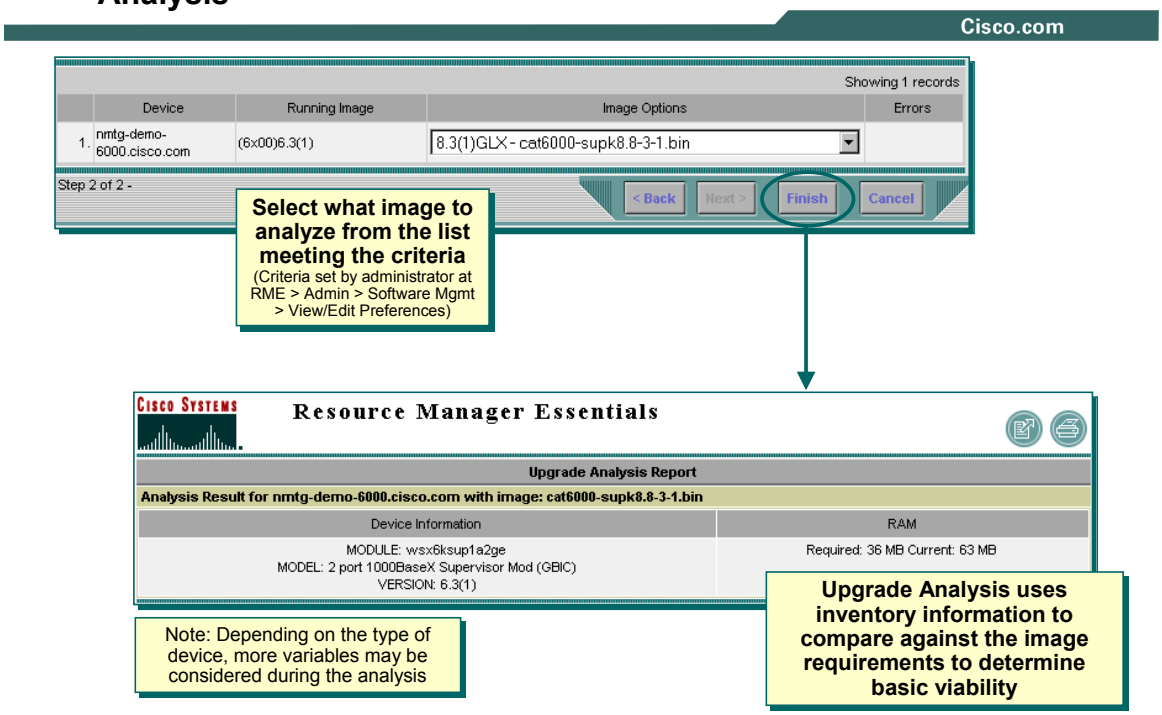
RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-61

Software Image Analysis

Ted wants to upgrade the demo Cat6000 to a newer version of software requested by the operations manager. Having been burned in the past putting an image on a device that didn't have enough memory to support it, Ted wants to avoid that mistake and do his homework upfront. He gets ready to start searching Cisco.com for the image and its requirements and to run a hardware report for the demo Cat6000 to see what its resources are. Sally stops him and suggests using the software analysis feature of RME instead. Ted is all for that since RME has come through so brilliantly in the past. To analyze a device against a potential upgrade software image, follow these steps:

1. Select **RME > Software Mgmt > Software Distribution > Upgrade Analysis**. The Upgrade Analysis dialog is displayed. Images from either Cisco.com or the RME library (user populated) can be used.
2. Select **Cisco.com** and then the **Go** button to begin the analysis
3. A Device Selector is displayed, expand the RME, User Defined Groups, and Demo Devices. Select the demo Cat6000 device and click **Next**. At this point you may be prompted for Cisco.com login information. Usually the entering Cisco.com login information on any RME task will remain in effect until the end of the RME session.

Software Image Management
Analysis



Software Image Analysis

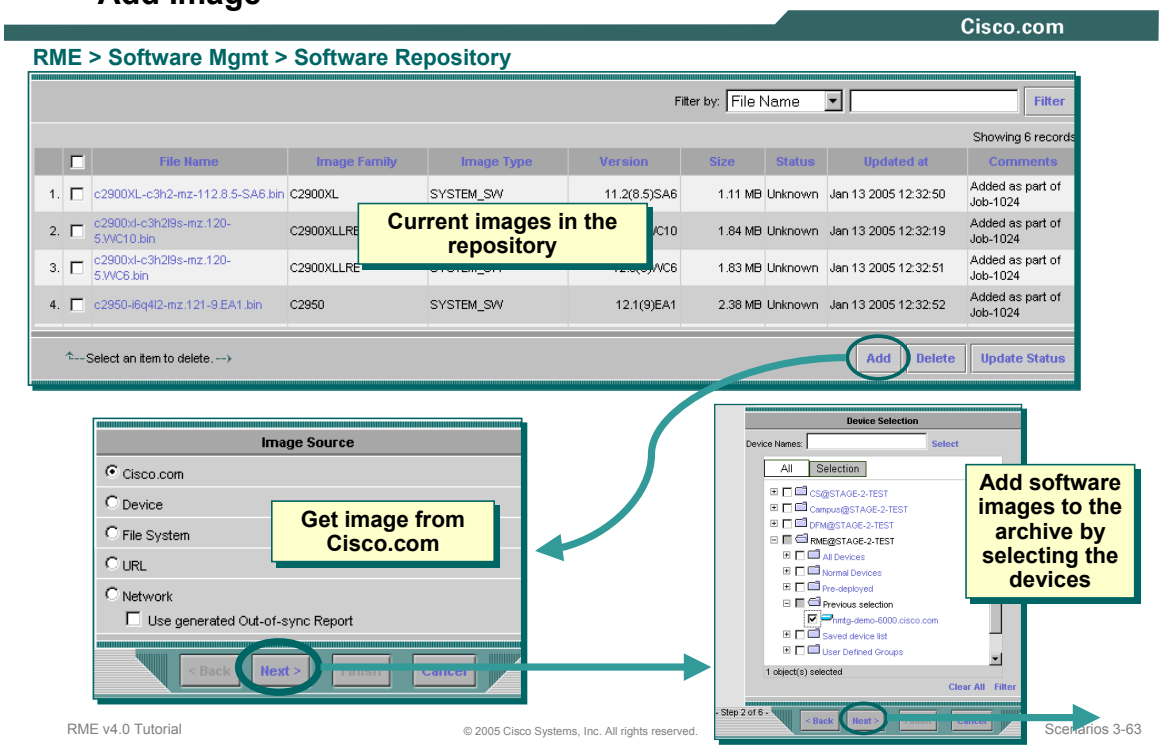
4. After some processing time the Cisco.com Upgrade Analysis dialog box will be displayed listing all selected devices with image recommendations for each based on criteria set by the administrator using the RME > Admin > Software Mgmt > View/Edit Preferences task (see chapter 4 for more information on this task). From the pull down list of image options, select the image to be analyzed for potential upgrade on the selected device.
5. Click **Finish** to perform the analysis.

The Upgrade Analysis Report is displayed in a separate window detailing specific requirements for the software and whether or not the device meets them.

Note: The number and type of variables analyzed depends on the device type and software version selected. The knowledge base used for analysis can be upgraded by selecting RME > Admin > Software Mgmt > Update Upgrade Analysis.

Software Image Management

Add Image



Adding Image to Software Repository

For an image to be deployed using RME Software Manager, the image must be in the image repository. An early on administrative task would have been to populated the repository with every unique image on the network. This would allow for easy re-deployment in the event of a major failure. This same task that Sally and Ted are about to use to download an image from Cisco.com to the repository can also be used to create the baseline of images on the network by simply selecting 'Network" as the image source.

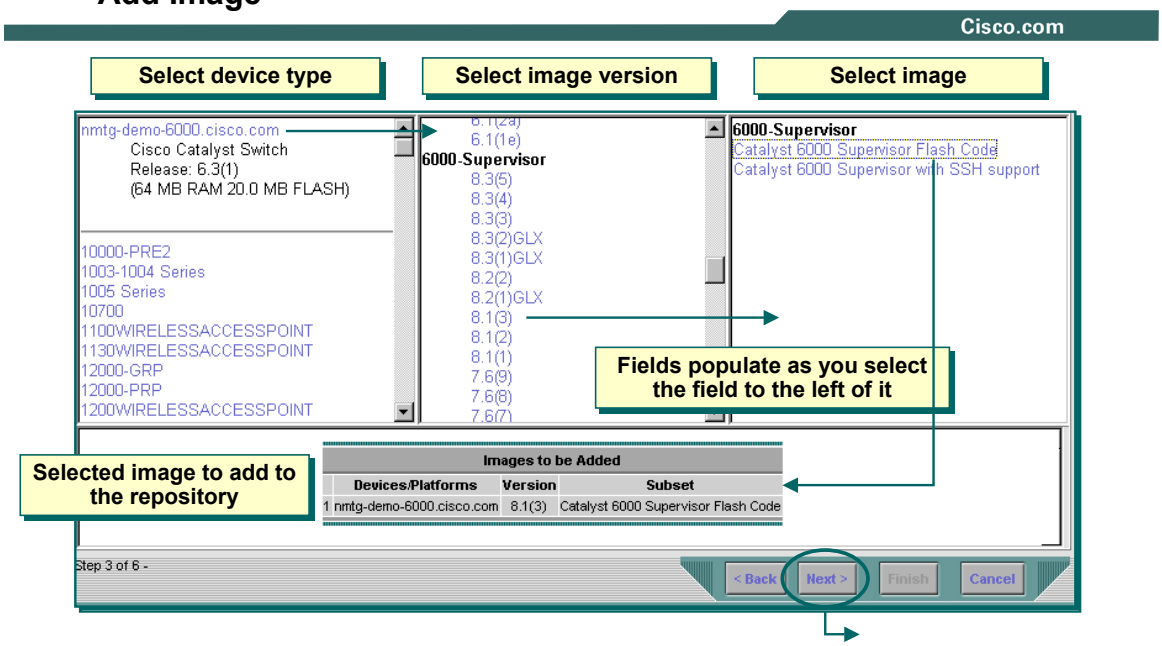
In this case, Ted is ready to upgrade the demo Cat6000 with the image previous analyzed since the device meets it's resource pre-requisites.

Note: Upgrade Analysis only verifies resource requirements. It is up to the user to use other Cisco.com tools to ensure the image is compatible with the model and configuration of the device.

Sally uses the following steps to add the image from Cisco.com to the image repository:

1. Select **RME >Software Mgmt > Software Repository**. A dialog is displayed listing the current images in the repository.
2. Click Add to begin the Image Add wizard.
3. The first step is to select the image source. In this case, **Cisco.com** is selected.
4. Click **Next**. A device Selector is displayed. Select the device(s) in which images will be downloaded for.
5. Click **Next** to proceeded with the Add Image wizard.

Software Image Management
Add Image

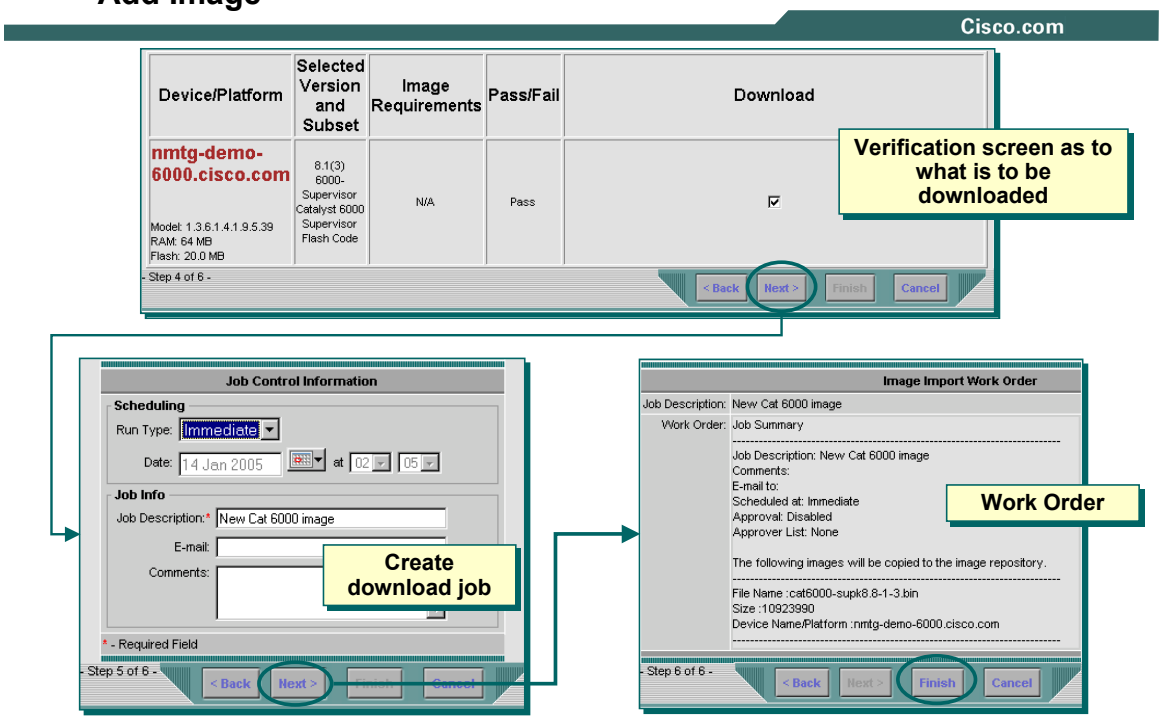


Adding Image to Software Repository

6. The third step in the wizard is to select the images to download. The displayed dialog is divided into four parts. When first displayed, only the upper left section is populated. At the top of this section will be entries for each device selected in the previous step. Below them is a listing for all device types. Select the image type to download. In this example Sally simply selects the demo Cat6000 listing.
7. Selecting a device type in the first portion will populate the second portion of the dialog box which lists available image versions. Select the appropriate image version.
8. The third portion of the dialog is now populated with image types for the selected version. Selecting one of these will populated the forth section of the dialog with the actual image to be downloaded.
9. Repeat steps 6-8 for any additional images to be downloaded at this time. When done selecting images to download, click **Next**.

Software Image Management

Add Image



Adding Image to Software Repository

10. The forth step of the wizard displays a dialog box listing the images for download with any image requirements if available. This step also verifies if the selected images will run on the selected devices. At this step, the user can opt out of downloading one or more of the previously selected images. Click **Next**.
11. The Job Control dialog is displayed. Select the Run Type – **Immediate** or Once with a scheduled date and time. Enter a job description and the e-mail addresses of any individuals who should be contacted when the job is complete. Click **Next**.
12. The work order is displayed detailing what images are to be downloaded and when. Click **Finish** to place the job on the job queue for execution.

Software Image Management
Add Image

Cisco.com

Click Refresh until job is successful or fails

RME > Software Mgmt > Software Mgmt Jobs

Filter by: All | Filter

Showing 3 records

		Job ID	Job Type	Status	Description	Owner	Scheduled at	Completed at	Schedule Type
1.		1025	Image Import	Successful	New Cat 6000 image	admin	Jan 13 2005 17:17:44	Jan 13 2005 17:18:13	Immediate
2.		1024	Image Import	Successful	Demo device baseline	admin	Jan 13 2005 12:30:40	Jan 13 2005 12:35:56	Immediate
3.		1001	Image Out Of Synch Report	Successful	SoftwareImages Out Of Synch Report.	admin	Jan 14 2005 00:00:00	Jan 13 2005 00:00:10	Daily

Select an item and perform a task --> Edit | Retry | Undo | Stop | Delete

Click Job ID to get details about the job (Including reason for failure if applicable)

Adding Image to Software Repository

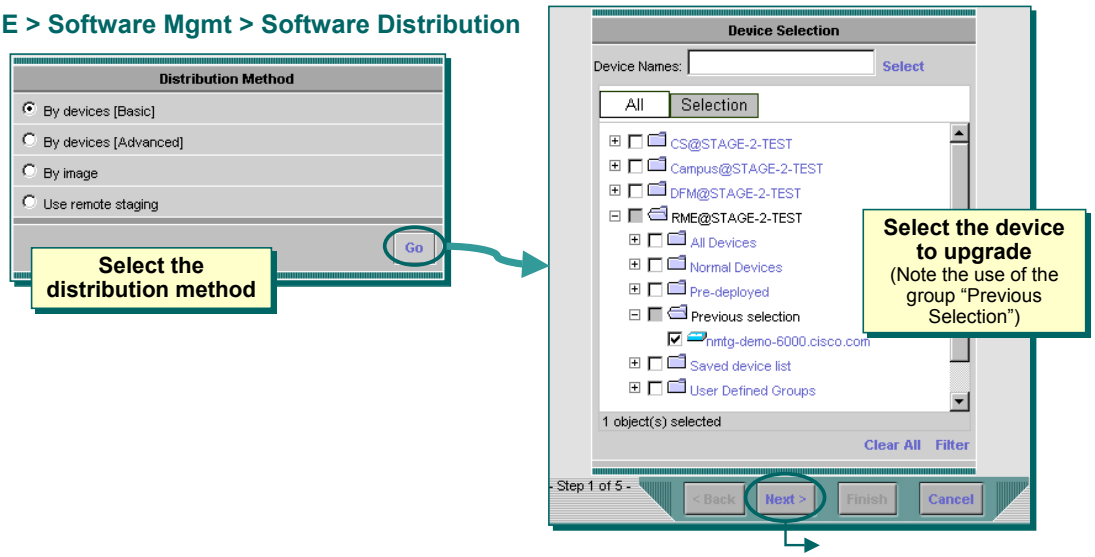
As seen with the configuration jobs, Software Manager also has a job browser listing pending and completed job. Launch the job browser to see the status of the download job.

1. Select **RME > Software Mgmt > Software Mgmt Jobs**. The Software Management Job Browser is displayed listing any completed jobs not purged from the system and all pending jobs either executing or waiting for execution.
2. If the status of the job of interest does not indicated Error or Successful, click on the Refresh Icon in the upper right corner until the job completes.
3. Select the job ID to see all details about the job (Work Order and Job Results). If the job had errors, use the job details to determine what they were.

Software Image Management
Distribution

Cisco.com

RME > Software Mgmt > Software Distribution



Software Image Distribution

Now that the desired image for upgrading the demo Cat 6000 is in the image repository, Sally can create a job to download it to the device using the following steps:

1. Select **RME > Software Mgmt > Software Distribution**. The Distribution Method dialog box is displayed.
2. The methods of distribution include:

   Basic - This option enables you to select devices and then perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image for distribution.

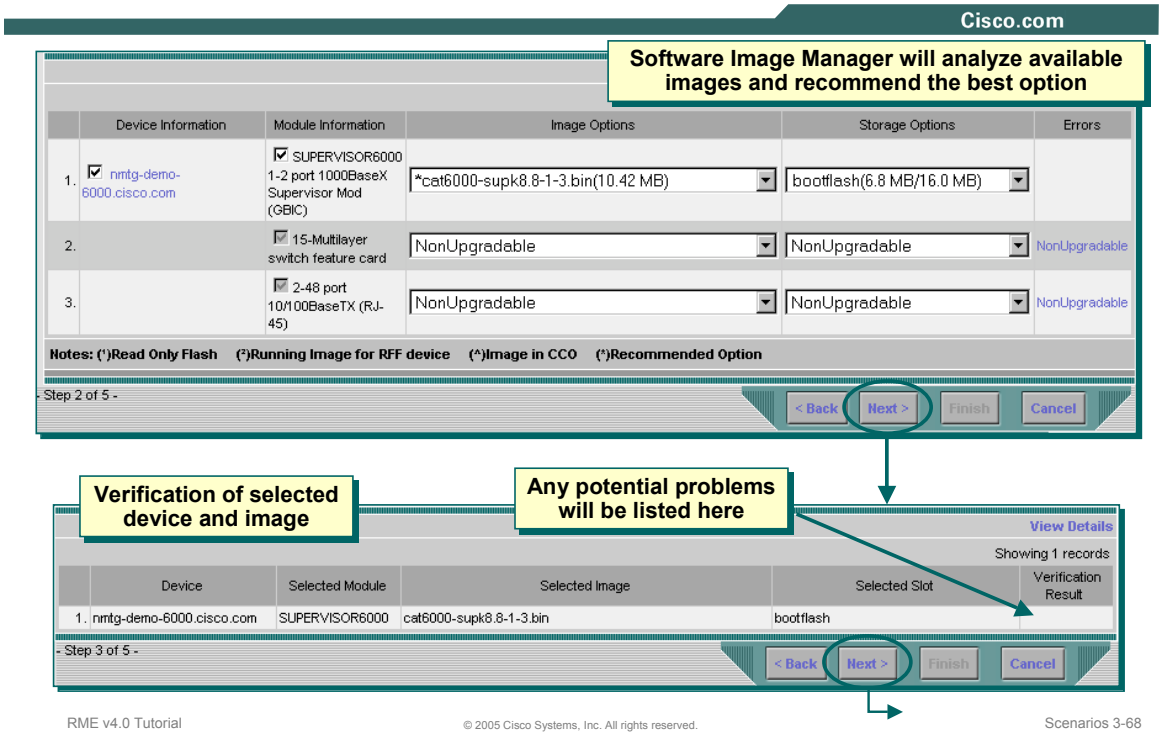
   By devices [Advanced] - This option enables you to enter the software image and storage media for the device that you want to upgrade. The selected image and storage media is validated and verified for dependencies and requirements.

   By images - This option enables you to select a software image from the software image repository and then use it to perform an image upgrade on suitable devices in your network.

   Use Remote Staging - This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This is helpful when the Resource Manager Essentials server and the devices (including the remote stage device) are distributed across a WAN.

   In this case select **Basic** and click **Go**.
3. The Device Selector is displayed as the first step in the deployment wizard. Select the demo Cat6000 device and click **Next**.

Software Image Management
Distribution

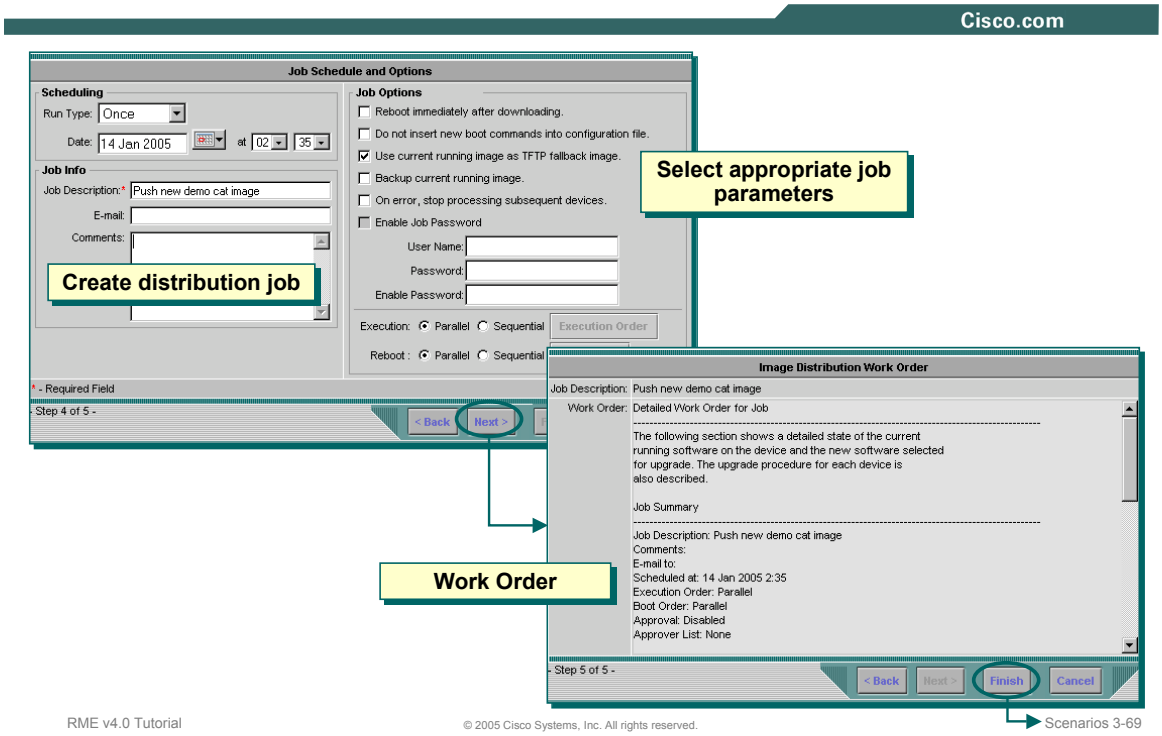


RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. Scenarios 3-68

Software Image Distribution

4. The next dialog displayed by the deployment wizard lists the selected device(s) and any modules associated with the device and the recommended image to upgrade to. From the pull-down list select the image to use for upgrade. **Note**: if enabled (RME > Admin > Software Mgmt > View/Edit Preferences) the list of possible and recommended images will include images at Cisco.com. Click **Next**.
5. The Distribute By Devices dialog is displayed detailing information about the selected device and image. Software Manager does a further verification check and will present any findings. After reviewing the information click **Next**.

Software Image Management
Distribution



Software Image Distribution

6. The Job Schedule and Options step of the wizard is displayed. Sally decides to run this job at night when the network is less busy. She selects *Run Type* to be **Once** and selects the appropriate date and time.
7. The right side of the dialog contains Job Option parameters to control various aspects of the upgrade job including the execution and reboot order. **Note**: to reboot a device after upgrade, the device must be configured to allow this via SNMP. Click **Next** when finished with the job parameters.
8. The final dialog in the Distribution wizard is the work order detailing the specifics of the job as just configured. Review the information to ensure it is correct and click **Finish** to place the job on the job queue for execution.

Software Image Management
Distribution

Cisco.com

Click Refresh until job is successful or fails

RME > Software Mgmt > Software Mgmt Jobs

Filter by: All | Filter

Showing 4 records

		Job ID	Job Type	Status	Description	Owner	Scheduled at	Completed at	Schedule Type
1.		1026	Image Distribution	Successful	Push new demo cat image	admin	Jan 14 2005 02:35:00	Jan 14 2005 02:51:29	Once
2.		1025	Image Import	Successful	New Cat 6000 image	admin	Jan 13 2005 17:17:44	Jan 13 2005 17:18:13	Immediate
3.		1024	Image Import	Successful	Demo device baseline	admin	Jan 13 2005 12:30:40	Jan 13 2005 12:35:56	Immediate
4.		1001	Image Out Of Synch Report	Successful	SoftwareImages Out Of Synch Report.	admin	Jan 14 2005 00:00:00	Jan 13 2005 00:00:10	Daily

--Select an item and perform a task--> Edit | Retry | Undo | Stop | Delete

Click Job ID to get details about the job
(Including reason for failure if applicable)

Software Image Distribution – Job Results

The next morning when Sally arrives at work she want to check the results of the distribution job.

1. Select **RME > Software Mgmt > Software Mgmt Jobs**. The Software Management Job Browser is displayed listing any completed jobs not purged from the system and all pending jobs either executing or waiting for execution.

   Sally notes that the Job was completed successfully and notes the time it took to assist her planning for the next upgrade job. If the job had failed, Sally could click on the Job ID to view the step by step actions software Manager used to determine the exact step and reason for failure.

Automated Actions

- Getting Started
- Preparing RME for Use
- Reports
- Configuration Management
- Software Image Management
- ➢ Automated Actions

Automated Actions

Cisco.com

- **Syslog**
- **Change Audit**

Automated Actions

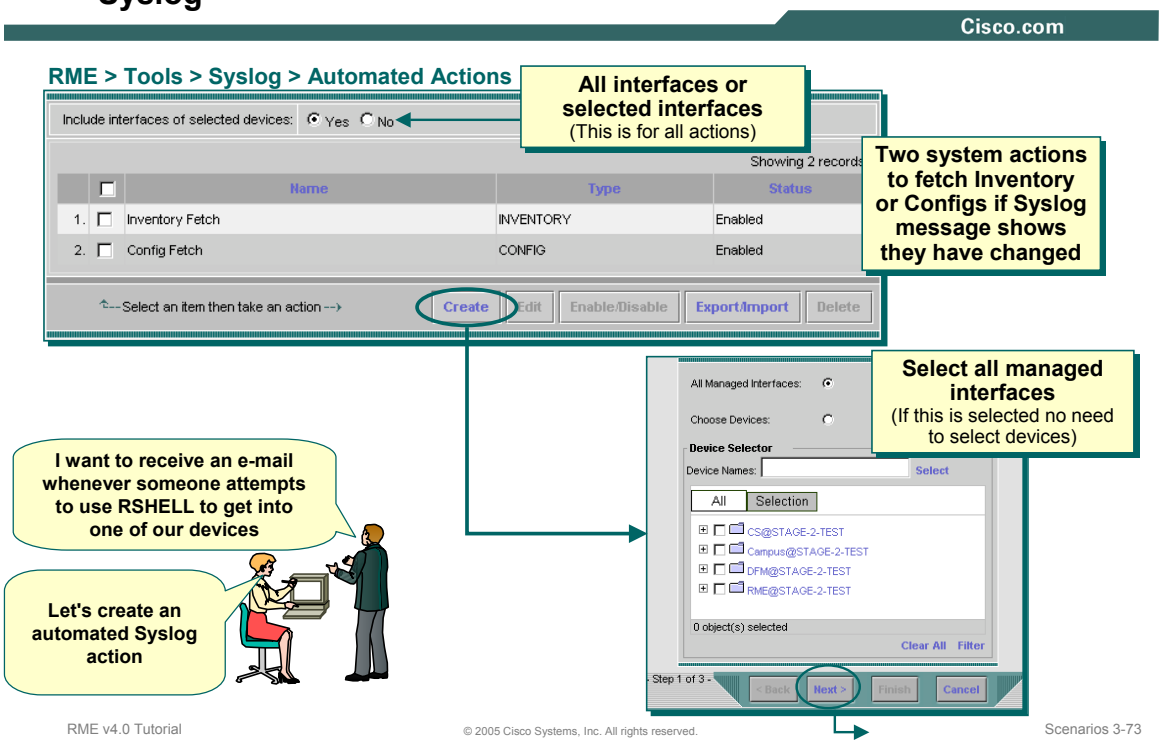
RME easily collects and displays data that traditionally has been time consuming to gather and analyze. Up to this point, the scenarios have shown how to run the reports to view the data. But what if something occurs that you need to know about right away? By the time you run a report it might be too late to fix before disrupting the overall performance and behavior of the network.

This is one of the key points in Ted's network management strategy - to be less reactive and more proactive. Certainly with the data collected by RME, Ted is better off than before, but now he just needs to have data in a more automated fashion. The scheduling of reports on a continuous basis with e-mail notification upon completion is a great start, but is still not real-time.

To address this need, RME allows the creation of automated actions for certain real-time events. Specifically, Ted can be notified immediately via e-mail, script, or URL invoking upon the receipt of a defined subset of Syslog messages (single or category wide – for example any Emergency level Syslog message). Ted can also be notified of a general or specific change via e-mail, trap, or script based on the detection of the change by Change Audit.

This scenario looks at the configuration of both these types of Automated Actions.

Automated Actions
Syslog

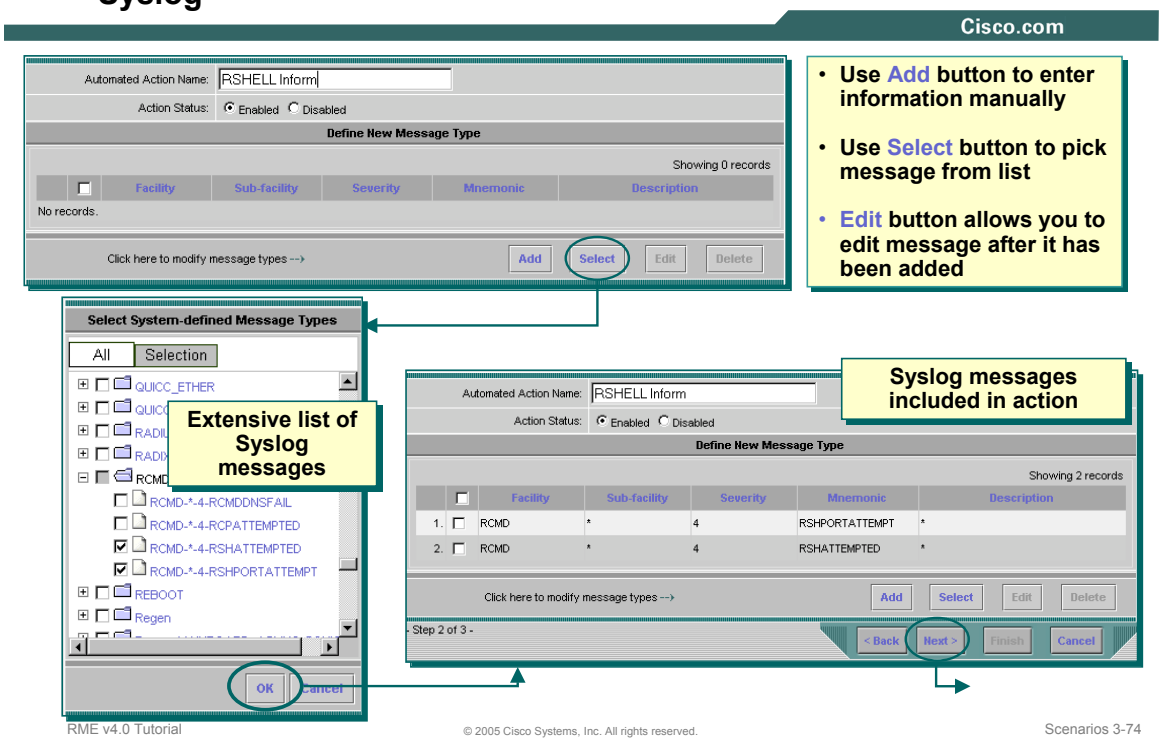


Syslog Automated Action

In reviewing Syslog reports Ted has noticed some attempts to RSHELL into the branch router. Ted wants to be notified the next time this behavior occurs. Since the condition was reported by a Syslog message, Sally decides to create an Automated Action that will send Ted an e-mail whenever someone attempts to access a device using RSHELL.

1. Select **RME > Tools > Syslog > Automated Actions**. The Automated Actions dialog is displayed listing all currently defined actions. RME comes pre-configured with two actions that cannot be edited or deleted. These actions upon receipt of a Syslog message indicating either a configuration or inventory change will initiated a fetch of the new information.
2. Click **Create**. The first step in the Create Automated Syslog Action wizard is displayed for device selection. Syslog automated actions can be tailored for specific devices or all devices. Since Ted is worried about all devices, select **All Managed Interfaces** (individual devices or device categories cannot be selected when suing this option.)
3. Click **Next**.

Automated Actions
Syslog

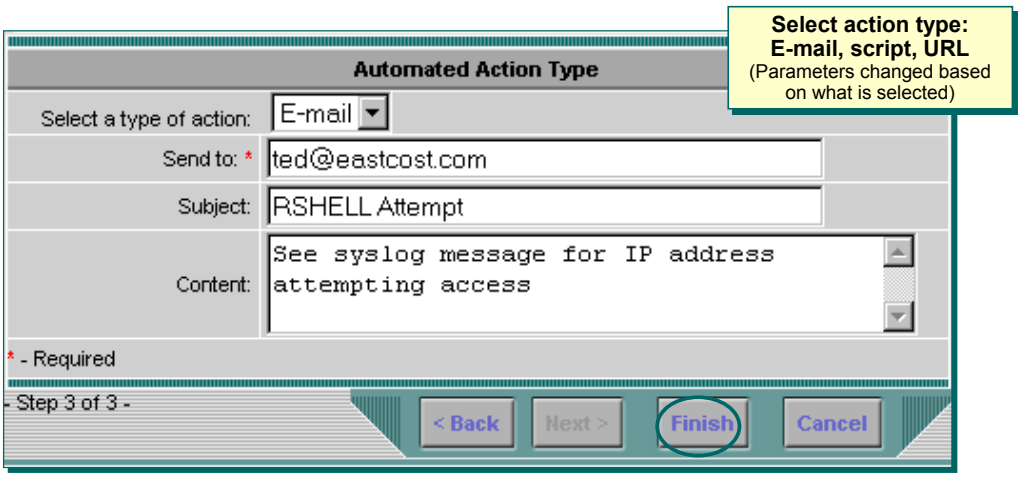


Syslog Automated Action

4. The Define Message Type step is displayed. Use this screen to select the Syslog message(s) to be filtering for to trigger the automated action. Enter a Name and Enable the action. If the format of the Syslog to be filtered on is known, select **Add** and fill in the appropriate fields. Else, select **Select** and a new dialog is opened providing an extensive list of Syslog messages to choose from. Find the desired messages and select them. Click **OK**. The selected messages are displayed in the Define Message Type dialog. To further fine tune the message (for example the description field), select the message and click **Edit**.
5. When finished adding messages, click **Next**.

Automated Actions
Syslog

Cisco.com



Syslog Automated Action

6. The final step in the wizard is the Automated Action Type dialog. The parameters vary depending on the type of action to perform (E-mail, Script, URL). Sally selects E-mail from the 'Select a type of Action' pull down list, enters Ted's e-mail address, a subject for the e-mail, and a brief message to be included in the e-mail.
7. Click **Finish** to start using the automated action.

At the next occurrence of RSHELL access activity, Ted received the following e-mail message:

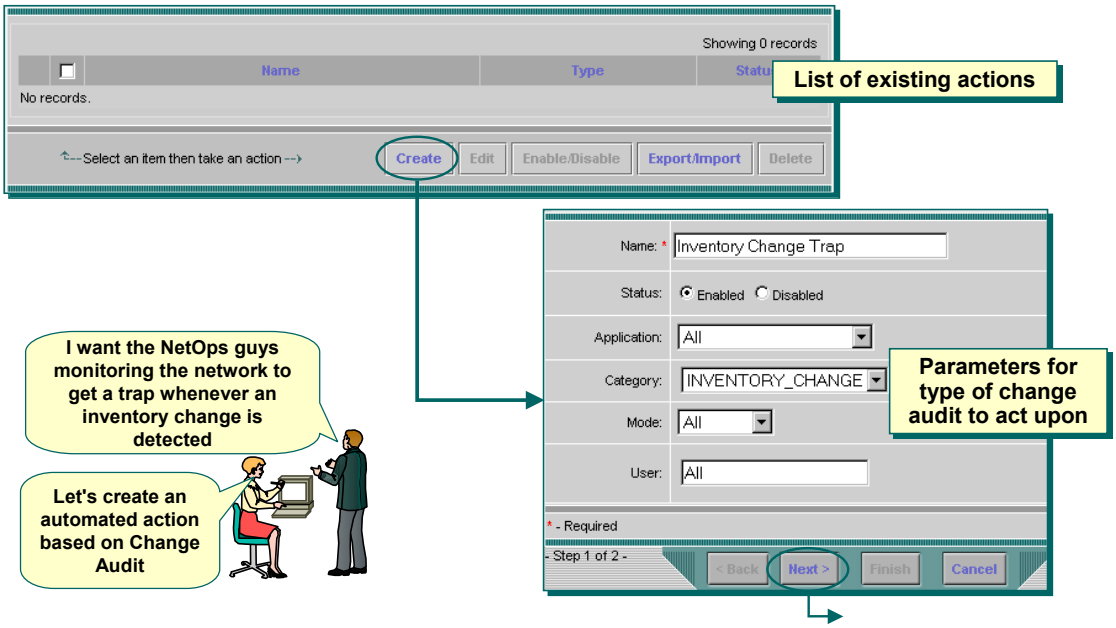
> *See Syslog message for IP address attempting access: Jan 21 03:02:39 192.168.159.106 189: *Jan 21 02:29:35: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.152.136*

Detailing that RSHELL access to device 192.168.159.106 was attempted on January 21st at approximately 2:30 AM from address 192.168.152.136.

Automated Actions
Change Audit

Cisco.com

RME > Tools > Change Audit > Automated Actions



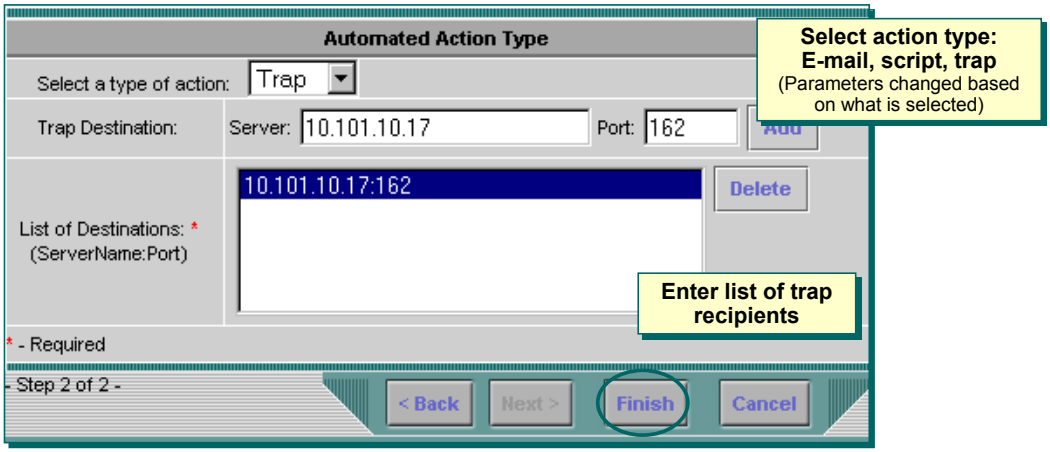
Change Audit Automated Actions

The operations manager, Sam, complains that he is the last to hear when Engineering makes an inventory change to the network (i.e. new blade in a switch). Ted shows Sam how to look at the daily change report (configured in an earlier scenario) detailing all changes to the network in the previous 24 hours. Sam likes the information presented but further complains that he and his people already have too much to do and don't want to have to look at a daily report that might not have any inventory changes and the info could be a day old. He wants to know right away. Ted has seen how efficiently RME tracks changes and decides to send a trap to Sam's Enterprise Management application, that is monitored 24/7, whenever Change Audit detects an inventory change. Upon receipt of the trap, Sam could then look at the RME report to see the details.

1. Select **RME > Tools > Change Audit > Automated Actions**. The Change Audit Automated Actions dialog is displayed listing any currently defined actions for Change Audit events.
2. Select **Create**. The Define Automated Action dialog is displayed. Enter a meaningful name for the action, select **Enable**, choose **All** application, Choose **INVENTORY_CHANGE** as the category, **All** as the mode, and **All** for the user field.
3. Click **Next**.

Automated Actions
Change Audit

Cisco.com



Change Audit Automated Actions

4. The Automated Action Type dialog is displayed. The parameters vary depending on the type of action to perform (E-mail, Script, Trap). Sally selects Trap from the 'Select a type of Action' pull down list, enters the IP address of the Enterprise manager, the standard Trap port, and clicks Add to included it as a recipient of a trap whenever an inventory change is detected by Change Audit..
5. Click **Finish** to start using the automated action.

A trap will now be sent from RME to the Enterprise server whenever an inventory change is detected by Change Audit.

This concludes the Scenarios portion of this tutorial. The scenarios presented will allow users to quickly perform the initial configuration of RME and also provided a good head start on the use of the product and its many functions. RME is an extremely powerful and flexible product. The tasks presented showed only a few of the many possible options within each function. The reader was hopefully able to follow along the scenarios on an actual system and also explored other reports and options not presented here to further enhance their understanding of RME.

Thank You!

Continue on to Chapter 4 to learn about some of the administrative tasks not yet discussed.

RME System Administration

Chapter 4

Chapter 4 Outline

Cisco.com

- **System Requirements**
  - Server
  - Client
  - Installation
- **RME Administration**
- **Task Reference**

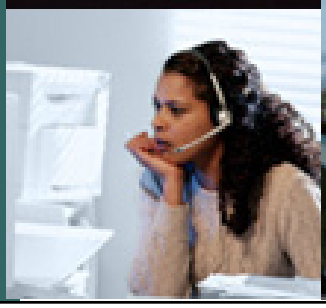
Chapter 4 Outline

This chapter starts out by covering some basic requirements for both the CiscoWorks server with the Common Services (CS) and RME installed, and the client used to access the CiscoWorks applications. Following the system requirements is a section that briefly covers some remaining administrative maintenance tasks that are optionally, but allow the system administrator to customize the overall configuration of RME.

For detailed installation procedures or information on upgrading from previous versions of RME, refer to the RME Installation and Setup Guide.

System Requirements

- System Requirements
- RME Administration
- Task Reference



Requirements
Windows Server

Cisco.com

Common Services v3.0 and RME v4.0*

Minimum System Configuration	Syslog	Configuration Management	Inventory and Software Image Management
Pentium 4 1 GHz **Memory: 2GB** **Virtual Memory: 4 GB** **Disk Space: 80 GB**	0-50,000 messages per day	0-300 managed devices *Restricted License <300 devices*	0-300 managed devices
Pentium 4, 1 GHz **Memory: 4 GB** **Virtual Memory: 8 GB** **Disk Space: 80 GB**	50,000-150,000 messages per day	300-2,500 managed devices *Unrestricted License <300 devices*	300-2,500 managed devices
Pentium 4, 1 GHz **Memory: 4-8 GB** **Virtual Memory: 8 GB** **Disk Space: 80 GB**	150,000+ messages per day	2,500-5,000 managed devices	2,500-5,000 managed devices

** RME requires Common Services to be installed before installing RME. Installing additional CiscoWorks applications on the same server may require additional resources.*

Windows Server Requirements

Two different types of software licenses are available for LMS. The restricted license will allow CiscoWorks to manage up to 300 devices. The unrestricted license allows for CiscoWorks to manage an unlimited number of devices, theoretically.

The server resources required for RME depends on how many elements the server will be managing. The above chart provides minimum system requirements for a Windows server for several usage scenarios based on the number of managed devices and expected Syslog messages per day.

Note(s):

- *To reduce the number of Syslog messages, message filters can be created, and remote Syslog collectors can also be configured. (Refer to Chapter 2 in this tutorial.)*
- *It should be noted that the system configurations above are for a CiscoWorks server with Common Services and RME only. Installing additional CiscoWorks applications may require additional resources.*
- *Common Services must be installed prior to all CiscoWorks applications.*
- *Always check the latest CiscoWorks release notes for up-to-date information regarding system requirements.*

Requirements
Windows Server

Cisco.com

- **Additional Requirements**
  - **System Software**
    - Windows 2000 Professional, Server, Advanced Server with terminal services (in remote admin mode), and Service Pack 3 or 4 or
    - Windows 2003 Server and Enterprise Edition with terminal services(in remote admin mode)
    - ODBC Driver Manager 3.5.10
  - **Hard Drive**
    - NTFS Formatting
    - 4 GB disk space required for program alone
    - 16 MB in the Windows temporary directory

Windows Server Requirements

RME is tested and supported for a finite number of system configurations. The previous page detailed minimum hardware requirements and this page lists the software and configuration requirements. Currently, RME has been certified to run on Windows 2000 Professional, Server, and Advanced Server with terminal services in remote admin mode and Service Pack 3 or 4, or Windows 2003 Server and Enterprise edition with terminal services in remote admin mode.

The only other system software required is ODBC Driver Manager 3.5.10.

As far as the physical disk drive, the Common Services and RME software require 4 GB of disk space. Additional disk space is required for device configuration files, software images, inventory data, Syslog messages, and paging space. For security and space reasons, the hard disk should be formatted as NTFS.

Requirements
Solaris Server

Cisco.com

Common Services v3.x and RME v4.x*

Minimum System Configuration	Syslog	Configuration Management	Inventory and Software Image Management
UltraSparc IIIi 1GHz **Memory: 2 GB** **Swap Memory: 4 GB** **Disk Space: 80 GB**	0-50,000 messages per day	0-300 managed devices *Restricted License <300 devices*	0-300 managed devices
UltraSparc IIIi 1GHz **Memory: 4 GB** **Swap Memory: 8 GB** **Disk Space: 80 GB**	50,000-150,000 messages per day	300-2,500 managed devices *Unrestricted License <300 devices*	300-2,500 managed devices
UltraSparc IIIi 1GHz **Memory: 4-8 GB** **Swap Memory: 16 GB** **Disk Space: 80 GB**	150,000+ messages per day	2,500-5,000 managed devices	2,500-5,000 managed devices

** RME requires Common Services to be installed before installing RME. Installing additional CiscoWorks applications on the same server may require additional resources.*

Solaris Server Requirements

Like the Windows server, two different types of software licenses are available for LMS. The restricted license will allow CiscoWorks to manage up to 300 devices. The unrestricted license allows for CiscoWorks to manage an unlimited number of devices, theoretically.

Additionally, the minimum system configuration for a Solaris platform depends on how many elements the server will be managing. The above chart provides minimum system requirements for a Solaris server for several usage scenarios based on the number of managed devices, and expected Syslog messages per day.

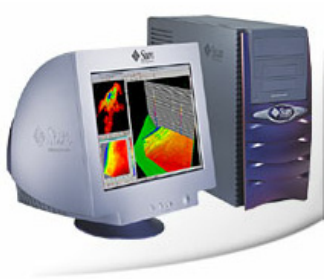
Note(s):

- *To reduce the number of Syslog messages, message filters can be created, and remote Syslog collectors can also be configured. (Refer to Chapter 2 in this tutorial.)*
- *It should be noted that the system configurations above are for a CiscoWorks server with Common Services and RME only. Installing additional CiscoWorks applications would require additional resources.*
- *Common Services must be installed prior to all CiscoWorks applications.*
- *Always check the latest CiscoWorks release notes for up-to-date information regarding system requirements.*

Requirements
Solaris Server

Cisco.com

- **Additional Requirements**
  - **System Software**
    - Solaris 2.8 or Solaris 2.9
    - RME only supports US-English and Japanese versions of Solaris OS
  - **Hard Drive**
    - 4 GB required for program alone



Solaris Server Requirements

In the Solaris environment, RME has currently only been tested and certified to run on US-English and Japanese versions of Solaris 2.8 or 2.9.

As far as the physical disk drive, the Common Services and RME software require 4 GB of disk space. Additional disk space is required for device configuration files, software images, inventory data, Syslog messages, and paging space.

Requirements
Client

Cisco.com

System Hardware	• **IBM PC Compatible, 300 MHz Pentium** • **Sun UltraSparc IIIi** • **Color Monitor with video card set to 24-bits color depth**
System Software	• **Windows 2000 SP3** • **Windows 2000 Professional or Server SP4** • **Windows XP SP1 or 2** • **Windows 2003 Server and Enterprise edition without terminal services** • **Solaris 2.8 or 2.9**
Memory	• **512 MB** - **Set virtual memory / swap space to twice the size of RAM**

Browser	• **Windows**
	  • **2000/XP – Microsoft IE 6.0.26 or 6.0.28**
	  • **2003 – Microsoft IE 6.0.3790.0**
	  • **Netscape Navigator 7.1**
	  • **Mozilla 1.7**
	• **Solaris**
	  • **Netscape Navigator 7.0**
	  • **Mozilla 1.7**

Minimum requirements. Some memory and processor intensive operations might require more resources (I.e. NetConfig jobs for more than 300 devices)

RME v4.0 Tutorial System Admin 4-8

Client Requirements

Access to the installed CiscoWorks applications is achieved using a standard web browser. On Windows based platforms, CiscoWorks has been tested and certified using Microsoft Internet Explorer (6.0.26 and 6.0.28 for Windows 2000/XP and 6.0.3790.0 for Windows 2003), Netscape Navigator 7.1, and Mozilla 1.7. Solaris based platforms running US-English or Japanese versions of Solaris 2.8 or 2.9 can use Netscape Navigator 7.0 or Mozilla 1.7. Client systems should have at least 512 MB of memory, but will need more when scheduling large scale configuration and software image deployment jobs.

Note(s):

- *It is always a good idea to check the latest CiscoWorks release notes for up-to-date information regarding client requirements.*
- *Client platforms not conforming to the above requirements may also work, but have not been tested and certified by Cisco and therefore will not be supported should problems arise.*

Requirements
Installation

Cisco.com

- **Use Administrator (Windows) or Root (Solaris) accounts**
- **If installing on multiple servers, synchronize clocks on servers**
- **Install Common Services (CS) v3.0 first**
  - Reboot Machine
- **RME installed in same directory as CS**
- **Migration from RME 3.4 or 3.5 (requires CS upgrade to v3.0 first)**
- **Quick Start Guide for installation procedure**
  - License file required

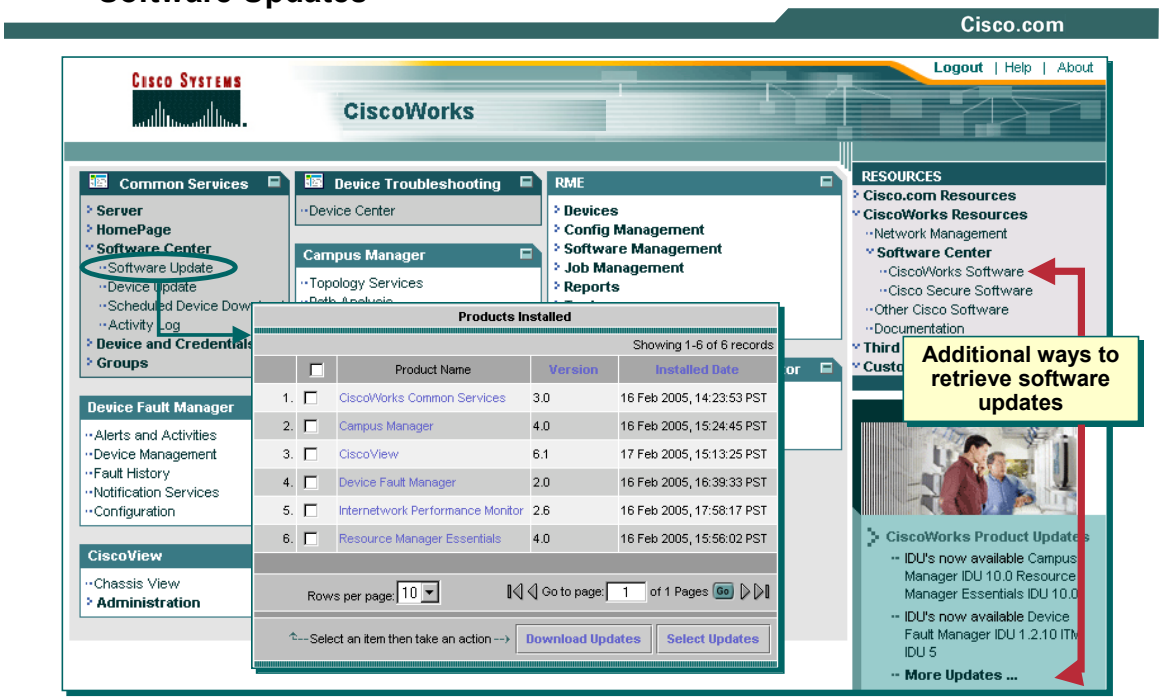
Installation Requirements

Installation of RME should be performed according to the steps detailed in the Installation and Setup Guide. It should be noted, however, that RME is not a stand-alone application. Like all CiscoWorks applications, RME depends on services supplied by the Common Services (CS) software. Therefore, prior to installing RME, CS should first be installed and the machine rebooted.

RME will be installed in the same directory selected for CS. All CiscoWorks applications should be installed using the root user account on Solaris platforms and the Administrator (not a cloned account) user account on Windows platforms.

Additionally, if CiscoWorks LMS is split between multiple servers, synchronize the clock on the servers so that the sharing of information using security certificates works properly.

Requirements
Software Updates



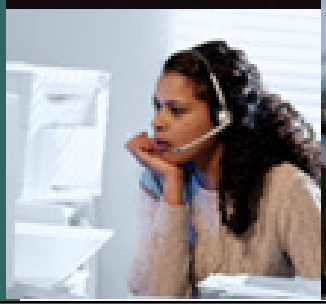
Software Updates

From time to time, updates to all CiscoWorks applications are made available on Cisco.com. Typically, Incremental Device Updates (IDUs) are made available every 3 months. The CiscoWorks Home Page provides numerous ways to retrieve these updates:

- The lower right hand corner of the home page presents CiscoWorks Product Update notes with a link to all available updates.
- The Resource section of the home page (upper right-hand corner) contains a link to all CiscoWorks Software including updates.
- The Common Services Software Center contains a Software Update task. Selecting this task will display the currently installed CiscoWorks applications and a mechanism to retrieve updates.

RME Administration

- System Requirements
- ➢ RME Administration
- Task Reference



RME Administration
Steps

Cisco.com

- **Common Services**
  - Register applications (See Common Services User Guide v3.0)
  - Add devices to DCR (See Common Services User Guide v3.0)
  - Create users and assign user roles (See Common Services User Guide v3.0)
  - E-mail Configuration (See Chapter 3)
- **RME**
  - Add Devices (See Chapter 3)
  - Add/Edit/Verify Credentials (See Chapter 3)
  - Schedule updates (See Chapter 3)
  - Miscellaneous configuration
    - Purge Jobs
    - Transport Settings

RME Administration Steps

The first two scenarios in Chapter 3 are enough to get RME up and running. This section of Chapter 4 briefly discusses some remaining administrative tasks mainly used for maintenance and troubleshooting. These tasks are mainly found under the 'Admin' tab of the application. The Admin tab includes tasks for each of the functional areas of RME and associated sub-tasks, such as Inventory, Configuration, Software Images, and more.

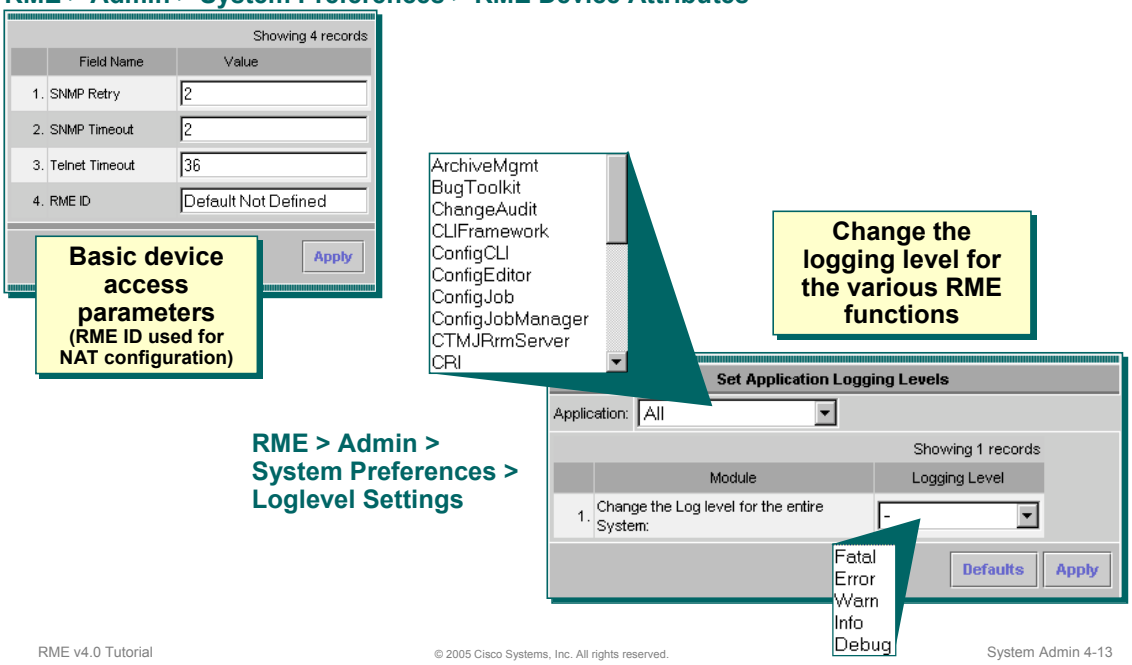
The above list, with the exception of the Miscellaneous Configuration item, provides the basic steps to jump-starting RME. Many of these steps were detailed in the first two scenarios of Chapter 3, however, there are three important configuration steps associated with Common Services tasks that are pre-requisites to any RME tasks. *(Please review the Common Services User Guide for assistance in performing these steps.)*

Again, this section will focus on the 'Miscellaneous Configuration' steps mainly used for maintenance and troubleshooting purposes.

RME Administration
System Preferences

Cisco.com

RME > Admin > System Preferences > RME Device Attributes



RME > Admin > System Preferences > Loglevel Settings

RME v4.0 Tutorial © 2005 Cisco Systems, Inc. All rights reserved. System Admin 4-13

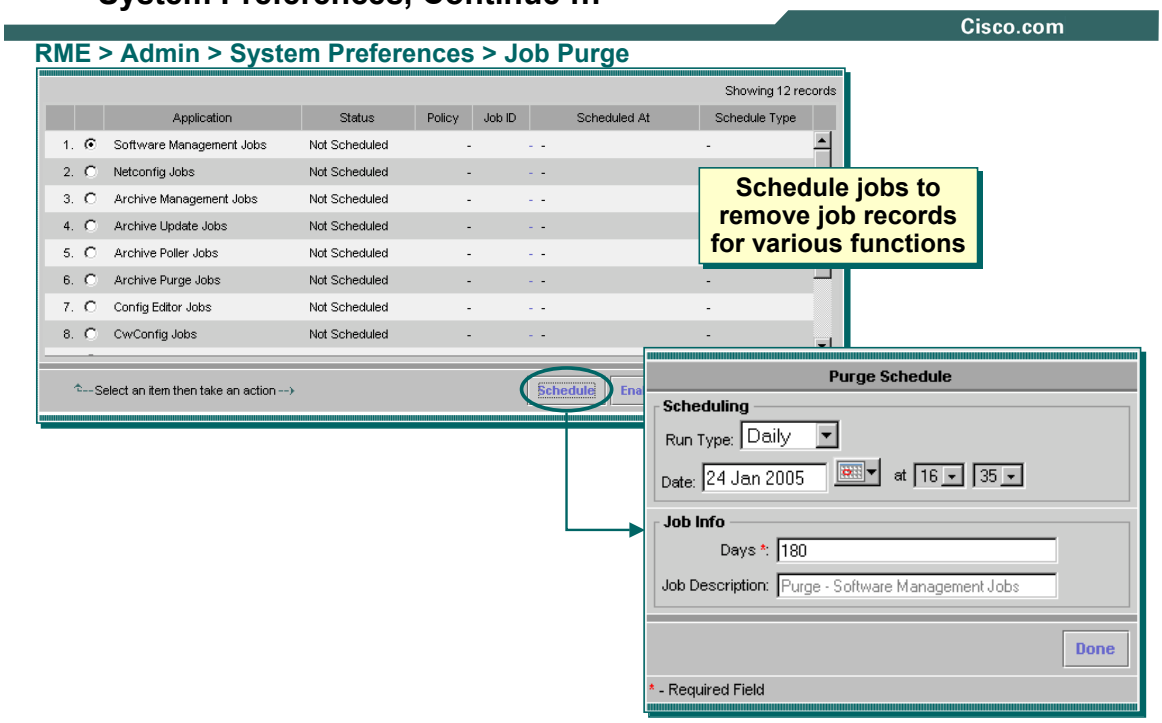
System Preferences

There are several sub-tasks associated with the System Preferences task under the Admin tab of RME. The *RME Device Attributes* sub-task is used to set basic device access timeout values. Busy devices or a congested network will sometimes necessitate the increasing of these values to insure proper operation and data collection. The RME server ID is the translated address of the RME server as seen from the network where the devices reside. It is used when RME tries to contact devices outside the Network Address Translation (NAT) boundary. (See the Common Services User Guide to enable support for NAT.)

The *Loglevel Settings* sub-task is used to set the level of information logged for troubleshooting. Typically you will be directed by TAC to use this to help them troubleshoot the system.

RME Administration

System Preferences, Continue …



System Preferences (Continue …)

RME has many functions that require jobs to be created in order to execute. Each invocation of these jobs result in a job record indicating the details about the job execution. After a while the number of job records can become quite large. The *Job Purge System Preferences* sub-task allows the scheduling of a job to purge these records. A separate schedule is set up for each RME function so that some job records deemed more important can be kept for longer periods of time. By default, no job records will be purged until scheduled to do so by this sub-task.

RME Administration
Change Audit

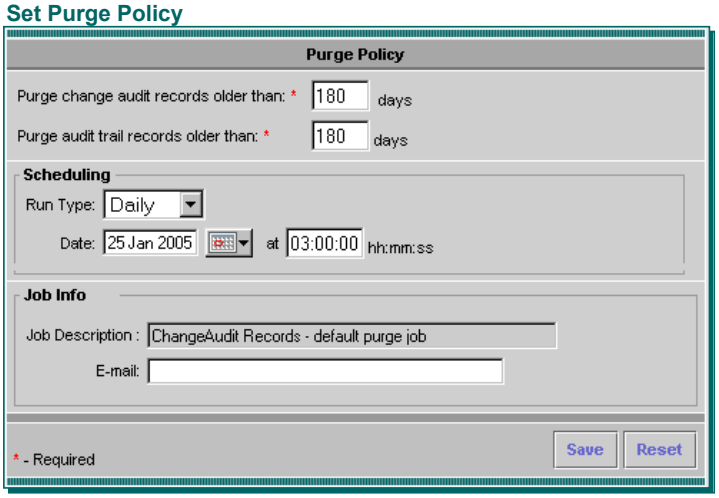
Cisco.com

RME > Admin > Change Audit

TOC
- Set Purge Policy
- Force Purge

Schedule jobs to remove Change Audit and Audit Trail records

Set Purge Policy



Change Audit Administration

The RME Change Audit service creates a change record each time it detects a change to either the RME inventory, a configuration file, or the software image of a device. These records act as both documentation for a desired change and also as quick justification that something has changed possibly causing a problem. Either way, the records will probably at some time become obsolete or un-needed. From the Change Audit task under the Admin tab, there are two sub-tasks to purge the change records based on age.

The *Set Purge Policy* sub-task allows for the scheduling of a recurring job to remove these records based on age. This job is also used to remove the Audit Trail records detailing the behavior of users during each login session.

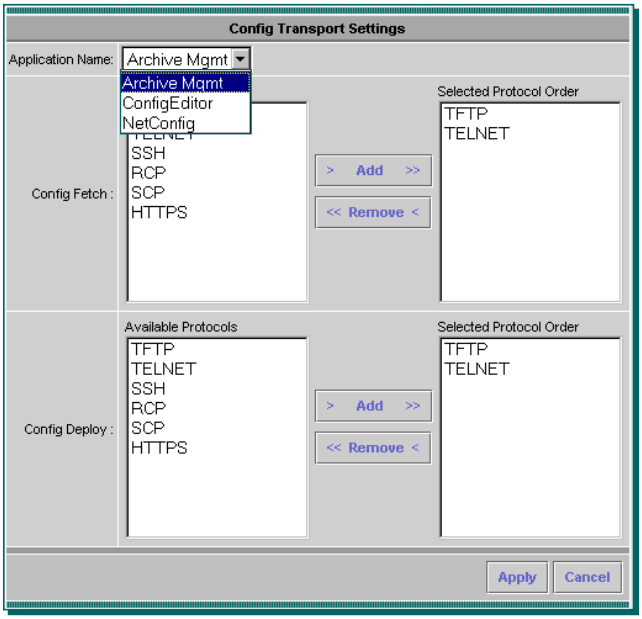
The *Force Purge* sub-task is similar to the Set Purge Policy sub-task except it is a one time job that runs and purges the Change Audit and Audit trail records based on age.

RME Administration
Config Management

Cisco.com

RME > Admin > Config Mgmt

Select transport protocol order for Archive Mgmt, Config Editor and NetConfig jobs



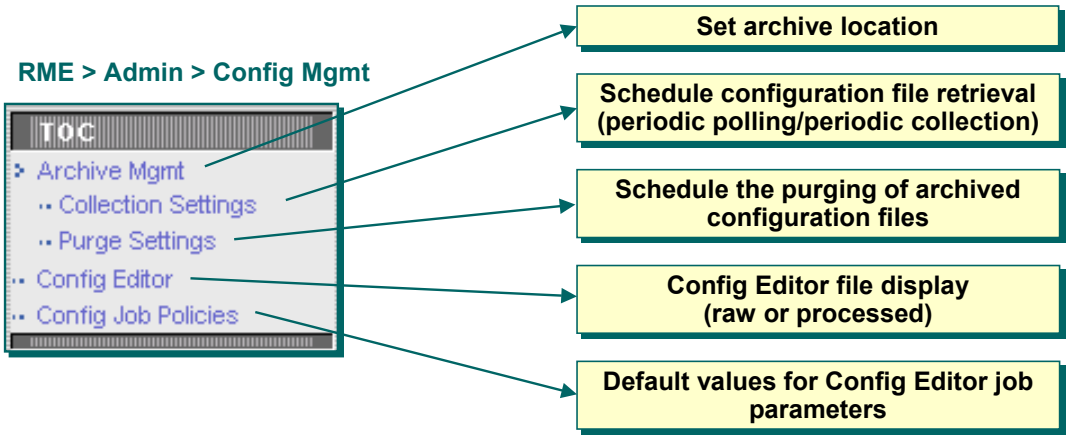
Config Management Administration

The Config Mgmt task under the Admin tab displays a dialog used to configure the transport protocols for Archive Management, NetConfig, and Config Editor jobs. This comes with a default order of protocols that the administrator can change, if desired. To change the order of the selected protocols, they must first be removed from the Selected Protocols and then re-added in the desired order.

RME Administration

Config Management, continue …

Cisco.com



Config Management Administration (Continue …)

Besides the task just describe, the Config Mgmt task under the Admin tab also includes five sub-tasks, as described below.

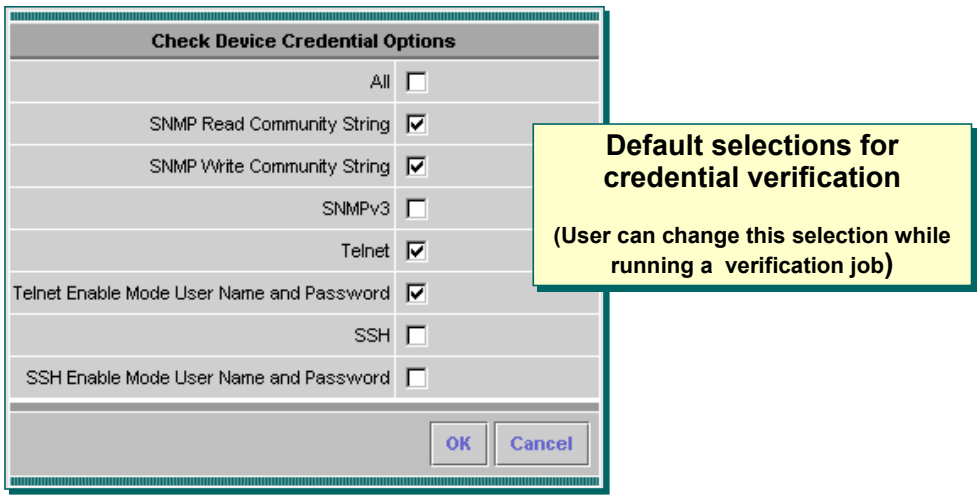
The *Archive Mgmt* sub-task is used to define the directory location where RME will store the retrieved configuration files. In other words, this is the location of the Configuration Archive.

The *Collection Settings* sub-task was seen in detail in the second scenario of Chapter 3. It allows for the scheduling of collection and polling jobs to ensure that the archive is kept up-to-date.

Since the archive can grow quite large, the *Purge Settings* sub-tasks allows the administrator to configure how to purge configuration files from the archive. The archive can be purged based on the age of the file and/or total number of files per device. If the settings are 30 days and 5 copies, the sixth configuration file retrieved will purge the first (only 5 copies kept in the archive). Also, any configuration file that was archived more than 30 days ago will also be purged. The archive will always have at least one archived file per device (the latest). Configuration files of special interest can also be labeled, using the task *RME > Config > Mgmt > Archive Mgmt > Label Configs*. Labeling configuration files is great for searching purposes and these files can also be configured by this sub-task to be exempt from the purge settings.

The final two sub-tasks are used for the Config Editor function. The *Config Editor* sub-task sets the default display mode for files opened with Config Editor to either *Processed* or *Raw*. A raw configuration file looks exactly like the command line interface, *show config* command. The Processed configuration file has the configuration statements broken down into configlets or organized groupings of commands. The *Config Job Policies* sub-task allows the administrator to set the default job properties for a Config Editor job and whether or not the properties can be altered by the user configuring the Config Editor job.

RME > Admin > Device Mgmt > Device Credential Verification Settings



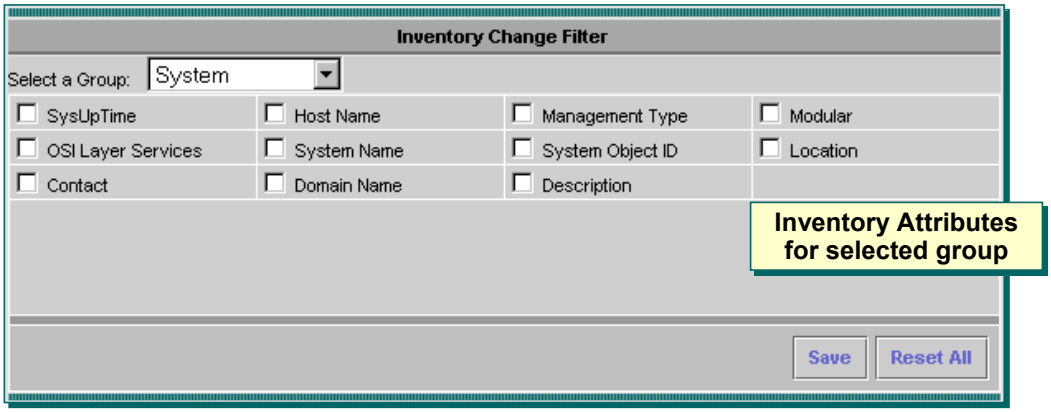
Device Management Administration

The Device Mgmt task under the Admin task has two sub-tasks. In the first scenario of Chapter 3, the *Device Management Settings* sub-task was discussed. This sub-task determines if devices are automatically added to RME from the DCR or must be manually added.

The other sub-task, *Device Credentials Verification Settings*, is used to set the defaults for what credentials will be verified when running a *Check Device Credentials Verification* Job. These values can still be changed when launching the Check Device Credentials Verification Job.

Select attributes *not* to be considered as inventory changes

RME > Admin > Inventory > Inventory Change Filter



Inventory Attributes for selected group

Inventory Administration

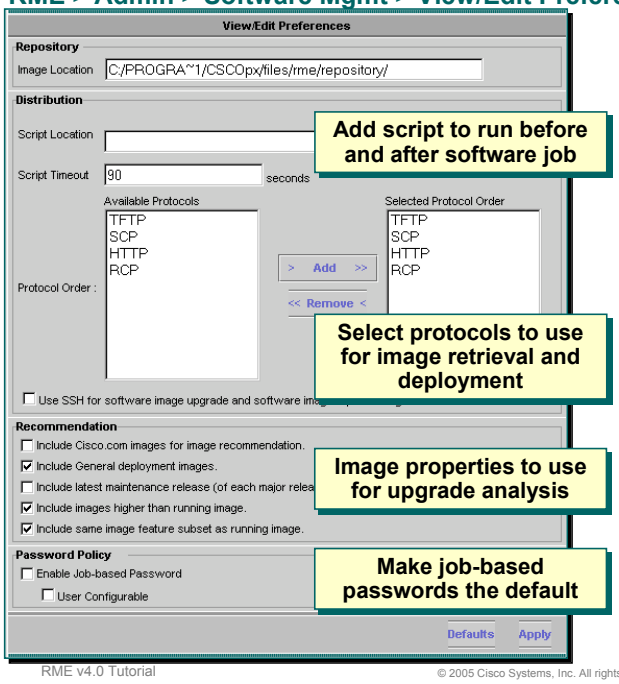
The Inventory task under the Admin tab also has two sub-tasks. The *System Job Schedule* was detailed in the second scenario in Chapter 3. This task configured the collection and polling of devices for inventory information to ensure the inventory has the most current information.

This inventory information retrieved during these collections is compared against the data currently in the database. Any differences in information are flagged as changes to the inventory and an Inventory Change Audit record is created. The inventory of a device consists of many variables. Some users may not consider some of these variables as a change worthy of generating a change record. In this case, the administrator can use the *Inventory Change Filter* sub-task to eliminate this variable from change consideration. The value for this variable will still be collected and stored in the database, it just won't generate a change record if it is different then the value currently in the database.

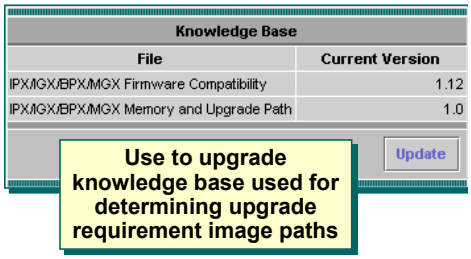
RME Administration
Software Management

Cisco.com

RME > Admin > Software Mgmt > View/Edit Preferences



RME > Admin > Software Mgmt > Update Upgrade Information

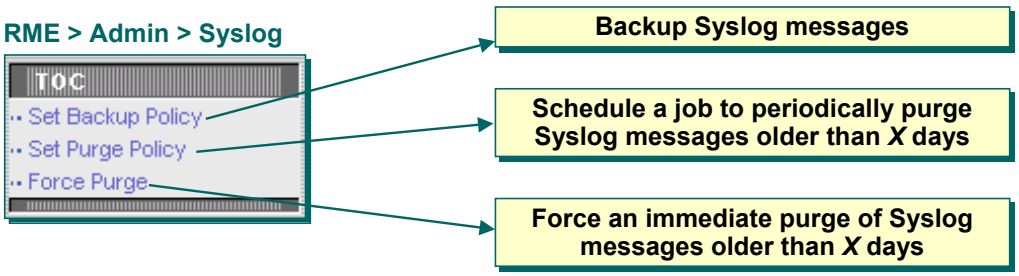


Software Management Administration

The *Software Mgmt* task under the Admin tab includes a sub-task to set the default values for various software management jobs. The *View/Edit Preferences* sub-task can be used to set the following options:

- Define the location of the image library
- Define a script location to be run before and after a distribution job, if desired
- Define the image transport protocol order
- Define the criteria for images to be recommended for upgrade
- Enable job-based passwords, if used

The other sub-task, *Update Upgrade Information*, is used to view and update the knowledge base used to make recommendations for IPX/IGX/BPX/MGX devices. The update is retrieved from Cisco.com, thus requiring a Cisco.com account.

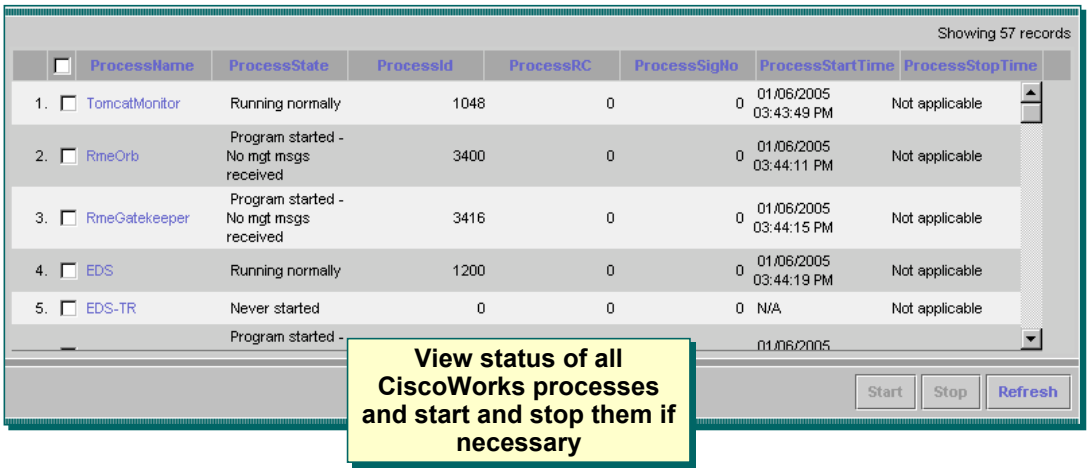


Syslog Administration

A couple of the *Admin* > *Syslog* sub-tasks are similar to ones discussed previously. The *Set Purge Policy* sub-task sets up a recurring job to purge Syslog messages by age and the *Force Purge* sub-task performs a one time purge of Syslog messages based on age.

Because literally thousands of Syslog messages can be received a day, it may be prudent to purge messages older than one or two weeks old to reduce processing time for Syslog reports. To maintain these messages for longer periods of time, the *Set Backup Policy* sub-task allows Syslog messages to be saved to a flat file. This is an immediate job and cannot be scheduled.

Common Services > Server > Admin > Processes



View status of all CiscoWorks processes and start and stop them if necessary

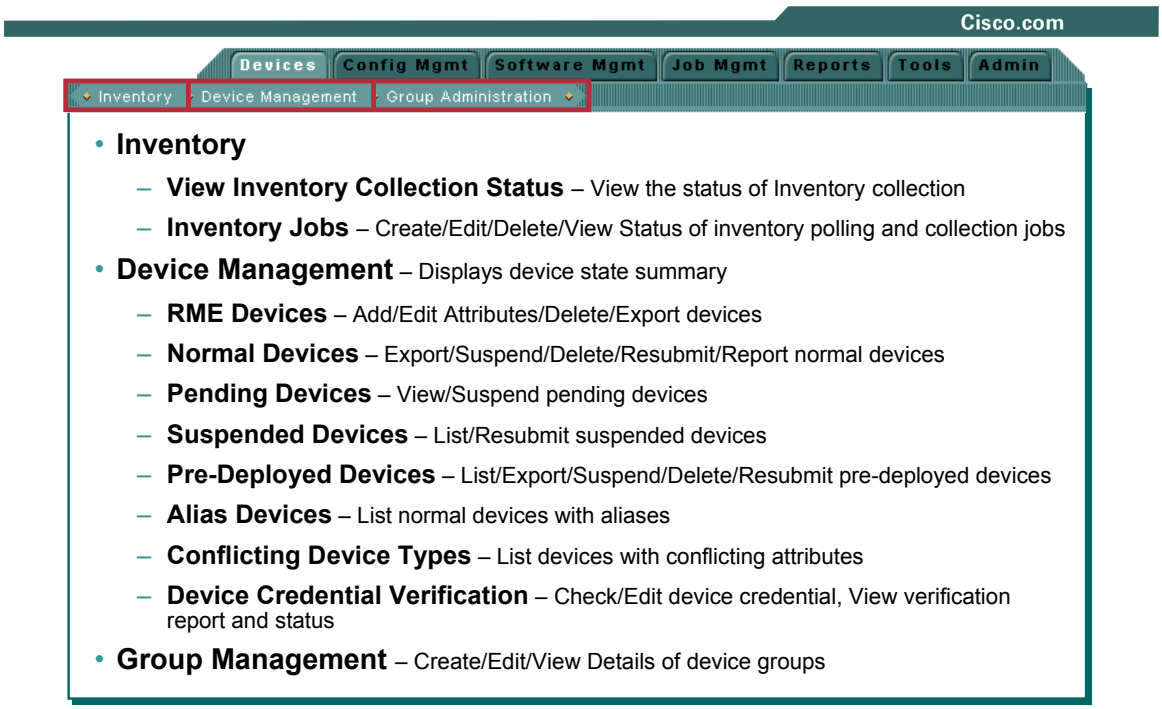
Process Management

The final administrative piece to be discussed isn't an RME task, but a Common Services task used to manage all CiscoWorks processes. In the event something doesn't quite seem right with RME, the administrator should first check the processes to ensure that they are running. If not, they can be restarted, or stopped and restarted, in an attempt to fix the problem. The processes can be viewed by running the *Common Services* > *Server* > *Admin* > *Processes* task. The Admin task under the Server tab in Common Services also has tasks to run self-tests and collect information on the CiscoWorks server.

Task Reference

- System Requirements
- RME Administration
- ➢ Task Reference

Task Reference
Devices Tab



Task Reference – Devices Tab

This section provides the reader with a task reference for each tab to assist with the use of RME. A brief description of each task is provided.

Inventory

- ***View Inventory Collection Status*** – View the status of Inventory collection
- ***Inventory Jobs*** – Create/Edit/Delete/View Status of inventory polling and collection jobs

Device Management – Displays device state summary

- ***RME Devices*** – Add/Edit Attributes/Delete/Export devices
- ***Normal Devices*** – Export/Suspend/Delete/Resubmit/Report normal devices
- ***Pending Devices*** – View/Suspend pending devices
- ***Suspended Devices*** – List/Resubmit suspended devices
- ***Pre-Deployed Devices*** – List/Export/Suspend/Delete/Resubmit pre-deployed devices
- ***Alias Devices*** – List normal devices with aliases
- ***Conflicting Device Types*** – List devices with conflicting attributes
- ***Device Credential Verification*** – Check/Edit device credential, View verification report and status

Group Management – Create/Edit/View Details of device groups

Task Reference
Config Mgmt Tab

Cisco.com

Devices | Config Mgmt | Software Mgmt | Job Mgmt | Reports | Tools | Admin

Archive Mgmt | Config Editor | NetConfig

- **Archive Management** – Displays archive summary
  - **Sync Archive** - Schedule a job to update the configuration archive for selected group of devices
  - **Out-of-Sync Archive** - Generate report for the group of devices whose running and start-up configurations are out-of-sync
  - **Version Tree** - View all configuration versions for the selected devices
  - **Version Summary** - View all archived configurations for selected devices
  - **Search Archive** – Search archive by string
    - **Custom Queries** – Create and save an archive query
  - **Compare Configs** – Compare two configs (running v. startup, running v. latest, two versions same device, two versions different devices)
  - **Archive Mgmt Jobs** – View status of archive management jobs (baseline, compliance, sync)
  - **Label Configs** – Label select archive files for query or keep from being purged
  - **Baseline Templates** – Create/Edit/Deploy sets of commands with user entered parameters
    - **Compliance** – Report compliance of devices pertaining to selected templates

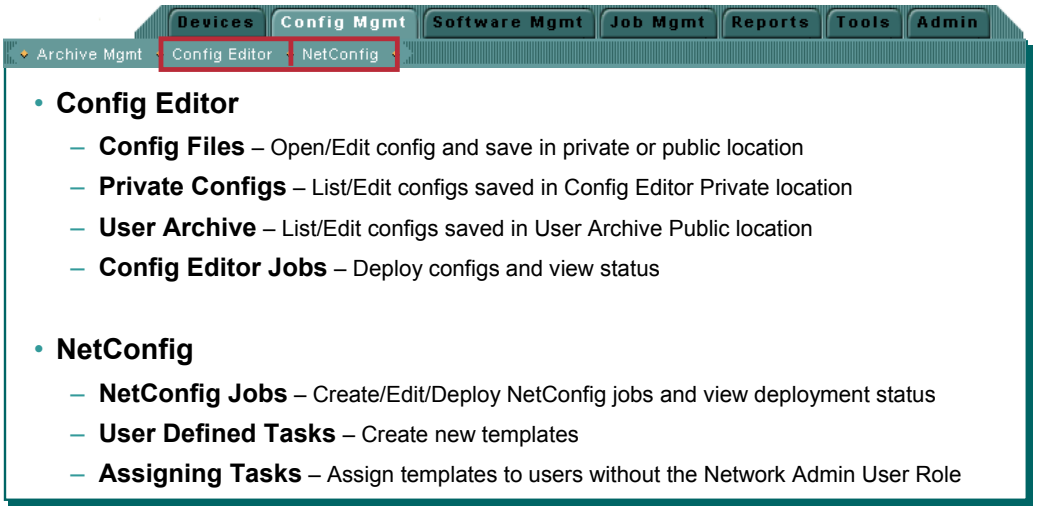
Task Reference – Config Mgmt Tab

Archive Management – Displays archive summary

- ***Sync Archive*** - Schedule a job to update the configuration archive for selected group of devices
- ***Out-of-Sync Archive*** - Generate report for the group of devices whose running and start-up configurations are out-of-sync
- ***Version Tree*** - View all configuration versions for the selected devices
- ***Version Summary*** - View all archived configurations for selected devices
- ***Search Archive*** – Search archive by string
  - ***Custom Queries*** – Create and save an archive query
- ***Compare Configs*** – Compare two configs (running v. startup, running v. latest, two versions same device, two versions different devices)
- ***Archive Mgmt Jobs*** – View status of archive management jobs (baseline, compliance, sync)
- ***Label Configs*** – Label select archive files for query or keep from being purged
- ***Baseline Templates*** – Create/Edit/Deploy sets of commands with user entered parameters
  - *Compliance* – Report compliance of devices pertaining to selected templates

Task Reference
Config Mgmt Tab (Cont)

Cisco.com



Task Reference – Config Mgmt Tab (cont)

Config Editor

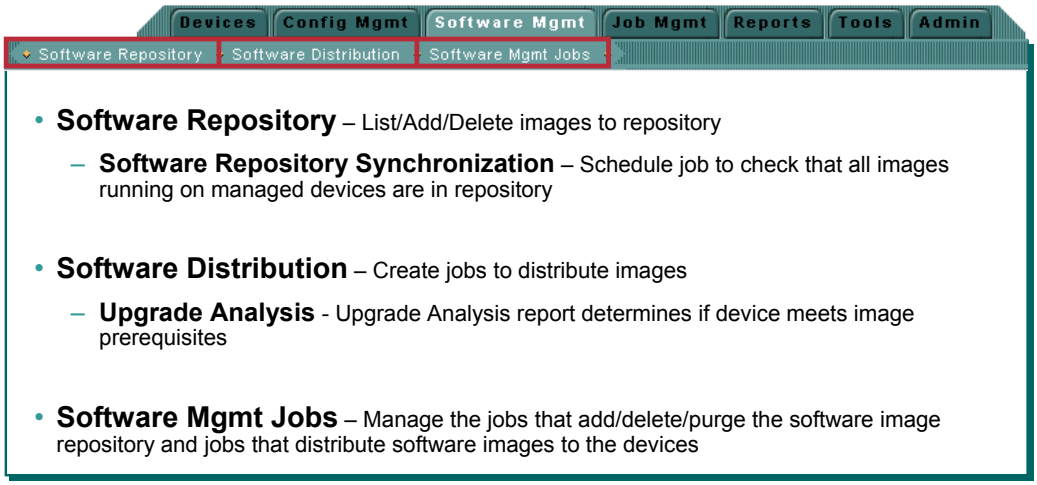
- ***Config Files*** – Open/Edit config and save in private or public location
- ***Private Configs*** – List/Edit configs saved in Config Editor Private location
- ***User Archive*** – List/Edit configs saved in User Archive Public location
- ***Config Editor Jobs*** – Deploy configs and view status

NetConfig

- ***NetConfig Jobs*** – Create/Edit/Deploy NetConfig jobs and view deployment status
- ***User Defined Tasks*** – Create new templates
- ***Assigning Tasks*** – Assign templates to users without the Network Admin User Role

Task Reference
Software Mgmt Tab

Cisco.com



Task Reference – Software Mgmt Tab

Software Repository – List/Add/Delete images to repository

- ***Software Repository Synchronization*** – Schedule job to check that all images running on managed devices are in repository

Software Distribution – Create jobs to distribute images

- ***Upgrade Analysis*** - Upgrade Analysis report determines if device meets image prerequisites

Software Mgmt Jobs – Manage the jobs that add/delete/purge the software image repository and jobs that distribute software images to the devices

Task Reference
Job Mgmt Tab

Cisco.com

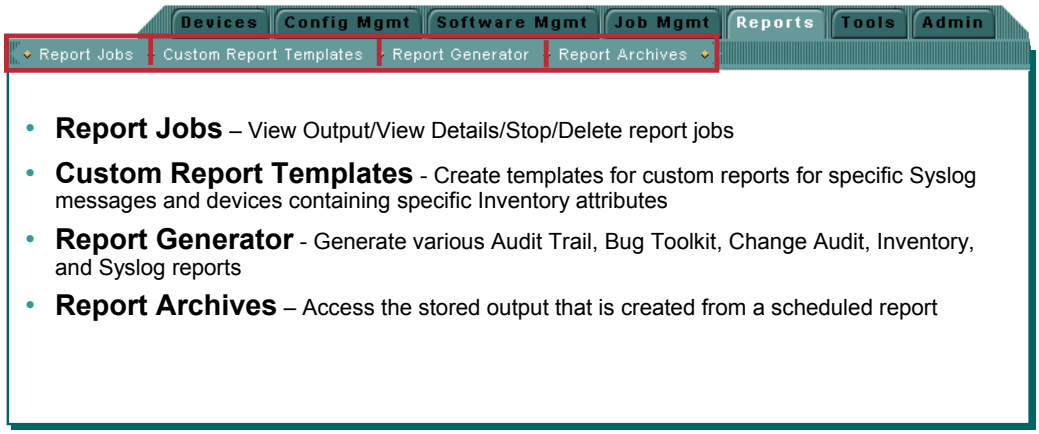
Task Reference – Job Mgmt Tab

RME Jobs – View/Edit/Stop/Delete all RME jobs (NetConfig jobs, Inventory collection or polling jobs, purge jobs, etc.).

Job Approval – View/Approve/Reject jobs pending approval

Task Reference
Reports Tab

Cisco.com



- **Report Jobs** – View Output/View Details/Stop/Delete report jobs
- **Custom Report Templates** - Create templates for custom reports for specific Syslog messages and devices containing specific Inventory attributes
- **Report Generator** - Generate various Audit Trail, Bug Toolkit, Change Audit, Inventory, and Syslog reports
- **Report Archives** – Access the stored output that is created from a scheduled report

Task Reference – Reports Tab

Report Jobs – View Output/View Details/Stop/Delete report jobs

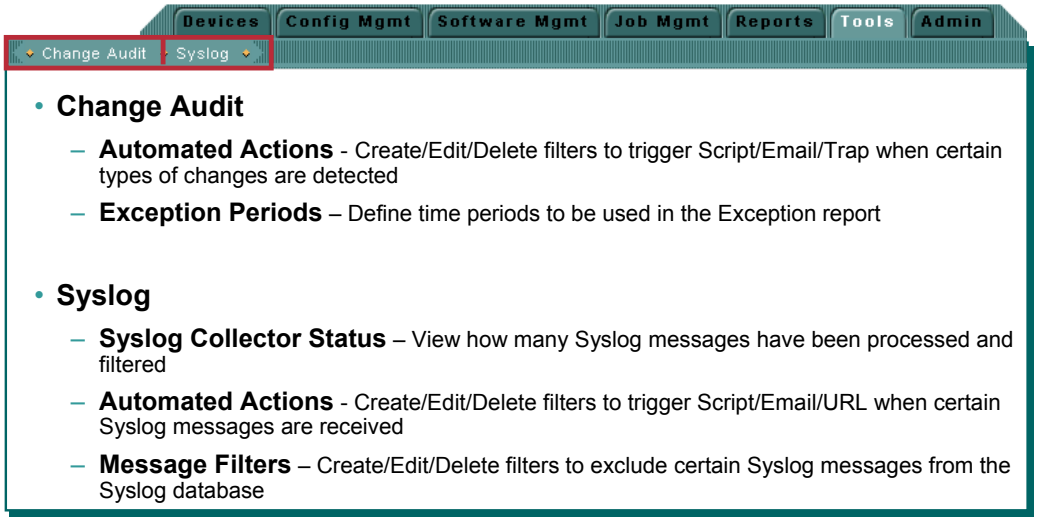
Custom Report Templates - Create templates for custom reports for specific Syslog messages and devices containing specific Inventory attributes

Report Generator - Generate various Audit Trail, Bug Toolkit, Change Audit, Inventory, and Syslog reports

Report Archives – Access the stored output that is created from a scheduled report

Task Reference
Tools Tab

Cisco.com



Task Reference – Tools Tab

Change Audit

- ***Automated Actions*** - Create/Edit/Delete filters to trigger Script/Email/Trap when certain types of changes are detected
- ***Exception Periods*** – Define time periods to be used in the Exception report

Syslog

- ***Syslog Collector Status*** – View how many Syslog messages have been processed and filtered
- ***Automated Actions*** - Create/Edit/Delete filters to trigger Script/Email/URL when certain Syslog message is received
- ***Message Filters*** – Create/Edit/Delete filters to exclude certain Syslog messages from the Syslog database

Task Reference
Admin Tab

Cisco.com

- **Approval**
  - **Approval Policies** - Enable Job Approval for NetConfig, Config Editor, Archive Management, and Software Management jobs
  - **Approver Details** - Enter and maintain information about users with CiscoWorks Approver roles
  - **Create/Edit Approver Lists** – Create/Edit Approver lists
  - **Assign Approver Lists** - Assign approver lists to NetConfig, Config Editor, Archive Management, and Software Management
- **Change Audit**
  - **Set Purge Policy** – Schedule recurring job to purge Change Audit and Audit Trail records older than X days
  - **Force Purge** – Force immediate purge of Change Audit and Audit Trail records older than X days

Task Reference – Admin Tab

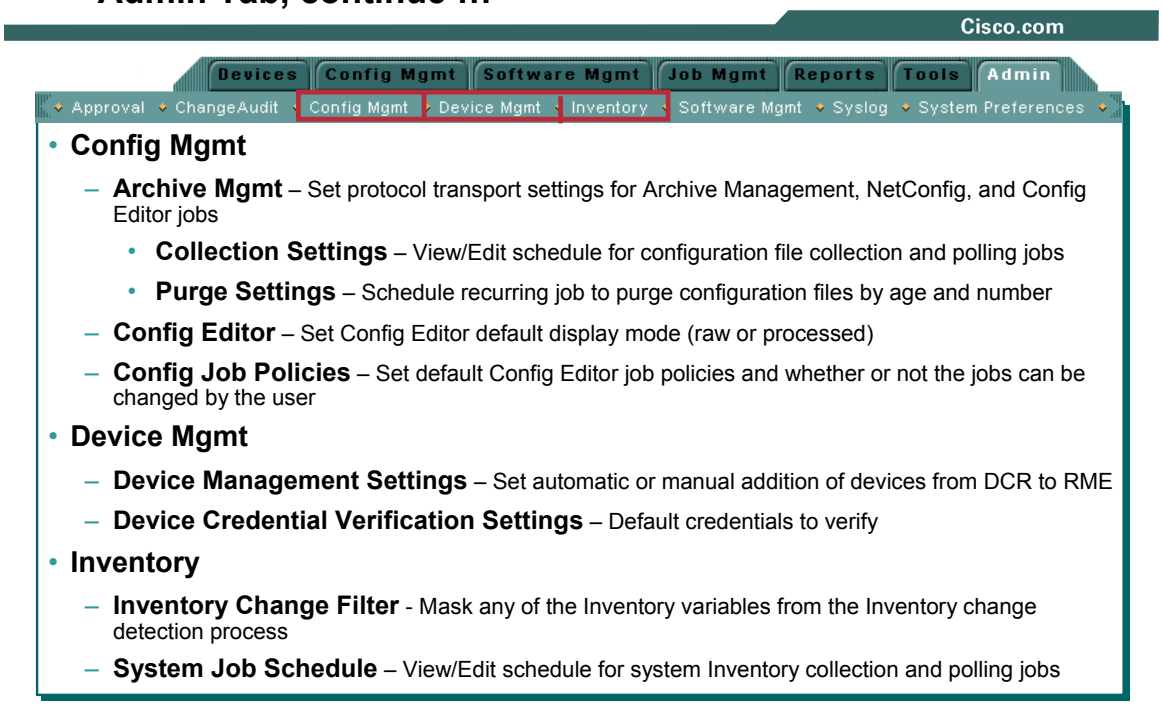
Approval

- ***Approval Policies*** - Enable Job Approval for NetConfig, Config Editor, Archive Management, and Software Management jobs
- ***Approver Details*** - Enter and maintain information about users with CiscoWorks Approver roles
- ***Create/Edit Approver Lists*** – Create/Edit Approver lists
- ***Assign Approver Lists*** - Assign approver lists to NetConfig, Config Editor, Archive Management, and Software Management

Change Audit

- ***Set Purge Policy*** – Schedule recurring job to purge Change Audit and Audit Trail records older than X days
- ***Force Purge*** – Force immediate purge of Change Audit and Audit Trail records older than X days

Task Reference
Admin Tab, continue …



Task Reference – Admin Tab (Cont)

Config Mgmt

- ***Archive Mgmt*** – Set protocol transport settings for Archive Management, NetConfig, and Config Editor jobs
  - ***Collection Settings*** – View/Edit schedule for configuration file collection and polling jobs
  - ***Purge Settings*** – Schedule recurring job to purge configuration files by age and number
- ***Config Editor*** – Set Config Editor default display mode (raw or processed)
- ***Config Job Policies*** – Set default Config Editor job policies and whether or not the jobs can be changed by the user

Device Mgmt

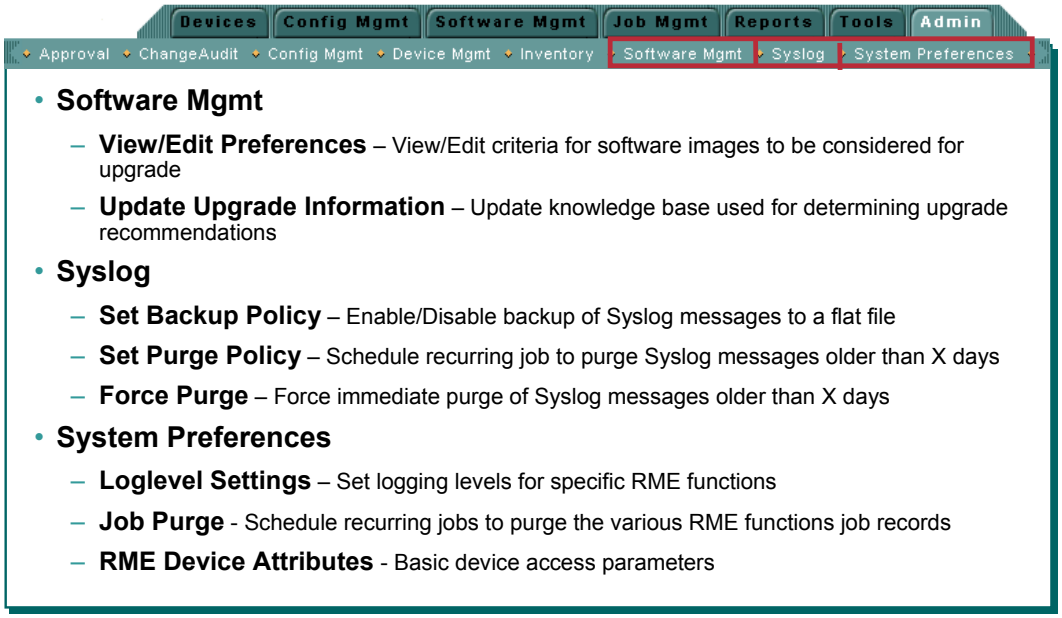
- ***Device Management Settings*** – Set automatic or manual addition of devices from DCR to RME
- ***Device Credential Verification Settings*** – Default credentials to verify

Inventory

- ***Inventory Change Filter*** - Mask any of the Inventory variables from the Inventory change detection process
- ***System Job Schedule*** – View/Edit schedule

Task Reference
Admin Tab , continue …

Cisco.com



Task Reference – Admin Tab (Cont)

Software Mgmt

- ***View/Edit Preferences*** – View/Edit criteria for software images to be considered for upgrade
- ***Update Upgrade Information*** – Update knowledge base used for determining upgrade recommendations

Syslog

- ***Set Backup Policy*** – Enable/Disable backup of Syslog messages to a flat file
- ***Set Purge Policy*** – Schedule recurring job to purge Syslog messages older than X days
- ***Force Purge*** – Force immediate purge of Syslog messages older than X days

System Preferences

- ***Loglevel Settings*** – Set logging levels for specific RME functions
- ***Job Purge*** - Schedule recurring jobs to purge the various RME functions job records
- ***RME Device Attributes*** - Basic device access parameters

Thank You!

We hope that you have enjoyed using Resource Manager Essentials and have found its features to be an important part of your network-management toolkit.

Cisco Systems

RME v4.0 References

Chapter 5

Reference Materials

Many Cisco reference documents have been created to help users understand the use of the CiscoWorks application, Resource Manager Essentials (RME). However, finding help and documentation can often be a challenge. This reference chapter has been created to assist you in your pursuit of additional product information. Below are links to documents and Web pages that provide further details on the RME product.

- **Resource Manager Essentials (RME) v4.0 Product Information**
  - **Data Sheet (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/products_data_sheet0900aecd8022099a.html
  - **Quick Start Guide (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2425/products_quick_start_list.html
  - **User Guide (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/products_user_guide_book09186a008026e94c.html
  - **Installation and Setup Guides (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_installation_guides_list.html
  - **Release Notes (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_release_notes_list.html
  - **Supported Devices (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_table09186a00803f30ac.html
  - **Frequently Asked Questions (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2073/products_qanda_item0900aecd8021bf9a.shtml

- **Related Material**
  - **CiscoWorks LAN Management Solution (LMS) (URL)**

    Learn more about CiscoWorks solutions bundled in LMS:
    www.cisco.com/go/lms/

  - **CiscoWorks Common Service (CCS) v3.0 (URL)**

    Required for all CiscoWorks applications:
    http://www.cisco.com/en/US/products/sw/cscowork/ps3996/ps5672/index.html

  - **Cisco's SNMP Object Navigator (URL)**

    http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

  - **Solaris Patches (URL)**

    To obtain the patches, contact your Sun Microsystems representative or download them from the Sun web site:
    sunsolve.sun.com/

  - **LMS Documentation (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_technical_documentation.html
    - **Quick Start Guide**
    - **Release Notes**

- **Online Bug Tracker**

  Search for known problems on the Cisco bug tracking system tool, called Bug Toolkit.
  To access Bug Toolkit, perform the following steps:
  - Click on the link above (www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)
  - Login to Cisco.com
  - Click ***Launch Bug Toolkit***.
  - Locate CiscoWorks Device Fault Manager from the list of Cisco Software Products
  - Then click ***Next***.

- ## Technical Notes / White Papers

  - **Network Management Systems: Best Practices White Paper (URL)**

    http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml

    The objective of this paper is to provide some deployment guidelines for all areas of network management: Fault, Configuration, Accounting, Performance, and Security (FCAPS).

  - **CiscoWorks LAN Management Solution White Papers (URL)**
    www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

    - **LMS Deployment Guide**

      The objective of this paper is to review the steps to properly deploying the LMS suite of applications.

    - **Cost Analysis Using CiscoWorks LAN Management Solution**

      The CiscoWorks product family can provide a quantifiable financial and IT benefit to an organization, through the automation of routine labor, as well as helping to mitigate network degradation due to device failures. While it is difficult to derive an exact figure of the true and potential cost savings for every customer situation, the Cost Analysis Tool can provide an understanding of the scale of savings involved. At this point, the question that needs to be asked is not "What is the cost of the product?" but "What is the cost of NOT using CiscoWorks?"

Resource Manager Essentials (RME) v4.0 Tutorial

Assessment Questions

Based on the information in the RME product tutorial, please answer the following questions.

Q1) Cisco has bundled the RME v4.0 application into CiscoWorks management solutions. Which of the following bundles contain RME? Choose all that apply.

A) The LAN Management Solution (LMS)

B) The Enterprise Management Solution (EMS)

C) The Small Network Management Solution (SNMS)

D) The CiscoWorks Management Solution (CMS)

E) The WAN Management Solution (WMS)

Q2) Which of the following features are provided by Resource Manager Essentials? Choose all that apply.

A) Discovers all the Cisco devices in the network

B) Provides reports on the types of Cisco devices managed by CiscoWorks

C) Automates the download of software image upgrades to Cisco devices managed by CiscoWorks

D) Polls, analyzes, and detects faults and performance issues on device interfaces

E) Displays a graphical topology of Cisco devices in the network

F) Edit/View/Compare configuration files of Cisco devices managed by CiscoWorks

Q3) Match the Device Management Status category with its description.

___ 1. Normal	A. Device not yet processed or contacted by RME
___ 2. Alias	B. Add/Import of device still in progress
___ 3. Pending	C. User requested device to not participate in RME tasks, but current data for the device remains
____4. Conflicting	D. CiscoWorks successfully connected to the device via SNMP
____5. Suspended	E. Device may already exist in RME, but with another hostname or IP address
___ 6. Pre-Deployed	F. Occurs if the sysObjectID in the device and that in the DCR do not match

Q4) CiscoWorks Inventory Management provides which two of the following benefits? Choose two.

A) A listing of only Cisco devices in the network

B) A starting point for other network management functions

C) An up-to-date archive of device configuration files

D) An up-to-date archive of software images in use on the network

E) Reports on devices managed by CiscoWorks and their attributes

F) Reports on devices that have had any type of change

Q5) Devices managed by all CiscoWorks applications are stored in the Device and Credentials Repository. Choose one.

A) True

B) False

Q6) Which of the following is stored in the Device and Credentials Repository? Choose all that apply.

A) Device IP address / hostname

B) Device configuration file

C) Device software image

D) Configured SNMP community strings on the device

E) Configured passwords on the device

Q7) For Inventory Management, what is the primary purpose for device groups? Choose one.

A) To limit which devices are added to the inventory database

B) To limit which devices are to be polled using the Inventory Poller

C) To secure communication between the CiscoWorks server and the managed devices

D) To limit or easily select which devices should be included in a selected report.

Q8) Which of the following are aspects of Device Configuration Management? Choose two.

A) Keep multiple copies of recent device configurations

B) Track which devices have reloaded

C) Track changes made to a device, by whom, and when

D) Identify users in CiscoWorks that can configure groups of devices

E) To upload the latest IOS or CatOS software release to the device

Q9) Which of the following are ways to automatically update the configuration archive? Choose all that apply.

A) Manual Update

B) Listen to Syslog Messages that indicate a config file has changed

C) Out-of-Sync Report

D) Update archive from archive status

E) Poll device MIB for configuration change

F) Schedule a job to update the archive

Q10) Which of the following are true statements about the reports comparing device configurations? Choose all that apply.

A) Only the differences between two configuration files can be viewed

B) A command in one file but not the other is displayed in blue text

C) A command in one file but not the other is displayed in red text

D) The same command in both files but with different parameters is not considered a difference

E) Compare reports can only be executed for configuration files from the same device

Q11) Which of the following are true statements about NetConfig? Choose all that apply.

A) User must enter exact syntax into system templates

B) Syntax is not check when using user-defined templates

C) The same change can be made to all devices on the network in the same NetConfig job

D) Help Desk users can only use NetConfig if assigned a template by a Network Administrator user

E) A Network Administrator user can configure any template without being assigned to it first

Q12) Which of the following are ways that CiscoWorks can retrieve device configuration files? Choose three.

A) Telnet

B) SNMP

C) RCP

D) RSH

E) FTP

Q13) Which of the following is not a benefit of RME Software Management? Choose one.

A) Know which versions of software are in use on the network

B) A copy of current images to facilitate image restoring if necessary

C) Track known bugs for images in the network

D) Compression of image before downloading to a device

E) Controllable mechanism for multiple unattended upgrades

Q14) Which two statements are true regarding software image upgrades using RME Software Management? Choose two.

A) Images for any device type can be scheduled for upgrade in the same job

B) Software Management recommends upgrade images from both the CiscoWorks archive and Cisco.com

C) When upgrading multiple devices, Software Management lets the user determine the order of upgrade to minimize connectivity failure in case of upgrade failure

D) Download jobs should be scheduled to occur during periods of low activity since Software Management requires all upgraded devices to be rebooted after a successful download.

Q15) What benefits are achieved when forwarding Syslog messages to the RME Syslog Analysis function? Choose all that apply.

A) View important events as determined by the device

B) Create automated actions for various messages

C) Change device color an Campus Manger map to indicate problem

D) Monitor the traffic statistics of a device interface

E) Monitor the change made to a configuration file

Q16) Which task can be used to immediately notify a user when a device has been reconfigured? Choose one.

A) Custom Reports

B) Syslog Message Filters

C) Common Services Paging

D) Syslog Automated Actions

E) Change Audit

Q17) What two configuration tasks should be performed to limit the Syslog reports to "important" messages? Choose two.

A) Define Custom Reports

B) Configure devices to limit Syslog messages forwarded based on severity

C) Define Message Filters

D) Configure size of Syslog database

E) Purge Syslog log file daily

Resource Manager Essentials (RME) v4.0 Tutorial

Answers to Assessment Questions

Based on the information in the RME product tutorial, please answer the following questions.

Q1) Cisco has bundled the RME v4.0 application into CiscoWorks management solutions. Which of the following bundles contain RME? Choose all that apply.

A) The LAN Management Solution (LMS)

B) The Enterprise Management Solution (EMS)

C) The Small Network Management Solution (SNMS)

D) The CiscoWorks Management Solution (CMS)

E) The WAN Management Solution (WMS)

Q2) Which of the following features are provided by Resource Manager Essentials? Choose all that apply.

A) Discovers all the Cisco devices in the network

B) Provides reports on the types of Cisco devices managed by CiscoWorks

C) Automates the download of software image upgrades to Cisco devices managed by CiscoWorks

D) Polls, analyzes, and detects faults and performance issues on device interfaces

E) Displays a graphical topology of Cisco devices in the network

F) Edit/View/Compare configuration files of Cisco devices managed by CiscoWorks

Q3) Match the Device Management Status category with its description.

__D__ 1. Normal	A. Device not yet processed or contacted by RME
__E__ 2. Alias	B. Add/Import of device still in progress
__B__ 3. Pending	C. User requested device to not participate in RME tasks, but current data for the device remains
__F__ 4. Conflicting	D. CiscoWorks successfully connected to the device via SNMP
__C__ 5. Suspended	E. Device may already exist in RME, but with another hostname or IP address
__A__ 6. Pre-Deployed	F. Occurs if the sysObjectID in the device and that in the DCR do not match

Q4) CiscoWorks Inventory Management provides which two of the following benefits? Choose two.

A) A listing of only Cisco devices in the network

B) A starting point for other network management functions

C) An up-to-date archive of device configuration files

D) An up-to-date archive of software images in use on the network

E) Reports on devices managed by CiscoWorks and their attributes

F) Reports on devices that have had any type of change

Q5) Devices managed by all CiscoWorks applications are stored in the Device and Credentials Repository. Choose one.

A) True

B) False

Q6) Which of the following is stored in the Device and Credentials Repository? Choose all that apply.

A) Device IP address / hostname

B) Device configuration file

C) Device software image

D) Configured SNMP community strings on the device

E) Configured passwords on the device

Q7) For Inventory Management, what is the primary purpose for device groups? Choose one.

A) To limit which devices are added to the inventory database

B) To limit which devices are to be polled using the Inventory Poller

C) To secure communication between the CiscoWorks server and the managed devices

D) To limit or easily select which devices should be included in a selected report.

Q8) Which of the following are aspects of Device Configuration Management? Choose two.

A) Keep multiple copies of recent device configurations

B) Track which devices have reloaded

C) Track changes made to a device, by whom, and when

D) Identify users in CiscoWorks that can configure groups of devices

E) To upload the latest IOS or CatOS software release to the device

Q9) Which of the following are ways to automatically update the configuration archive? Choose all that apply.

A) Manual Update

B) Listen to Syslog Messages that indicate a config file has changed

C) Out-of-Sync Report

D) Update archive from archive status

E) Poll device MIB for configuration change

F) Schedule a job to update the archive

Q10) Which of the following are true statements about the reports comparing device configurations? Choose all that apply.

A) Only the differences between two configuration files can be viewed

B) A command in one file but not the other is displayed in blue text

C) A command in one file but not the other is displayed in red text

D) The same command in both files but with different parameters is not considered a difference

E) Compare reports can only be executed for configuration files from the same device

Q11) Which of the following are true statements about NetConfig? Choose all that apply.

A) User must enter exact syntax into system templates

B) Syntax is not check when using user-defined templates

C) The same change can be made to all devices on the network in the same NetConfig job (False – only devices of the same type)

D) Help Desk users can only use NetConfig if assigned a template by a Network Administrator user

E) A Network Administrator user can configure any template without being assigned to it first

Q12) Which of the following are ways that CiscoWorks can retrieve device configuration files? Choose three.

A) Telnet

B) SNMP

C) RCP

D) RSH

E) FTP

Q13) Which of the following is not a benefit of RME Software Management? Choose one.

A) Know which versions of software are in use on the network

B) A copy of current images to facilitate image restoring if necessary

C) Track known bugs for images in the network

D) Compression of image before downloading to a device

E) Controllable mechanism for multiple unattended upgrades

Q14) Which two statements are true regarding software image upgrades using RME Software Management? Choose two.

A) Images for any device type can be scheduled for upgrade in the same job

B) Software Management recommends upgrade images from both the CiscoWorks archive and Cisco.com

C) When upgrading multiple devices, Software Management lets the user determine the order of upgrade to minimize connectivity failure in case of upgrade failure

D) Download jobs should be scheduled to occur during periods of low activity since Software Management requires all upgraded devices to be rebooted after a successful download.

Q15) What benefits are achieved when forwarding Syslog messages to the RME Syslog Analysis function? Choose all that apply.

A) View important events as determined by the device

B) Create automated actions for various messages

C) Change device color an Campus Manger map to indicate problem

D) Monitor the traffic statistics of a device interface

E) Monitor the change made to a configuration file

Q16) Which task can be used to immediately notify a user when a device has been reconfigured? Choose one.

A) Custom Reports

B) Syslog Message Filters

C) Common Services Paging

D) Syslog Automated Actions

E) Change Audit

Q17) What two configuration tasks should be performed to limit the Syslog reports to "important" messages? Choose two.

A) Define Custom Reports

B) Configure devices to limit Syslog messages forwarded based on severity

C) Define Message Filters

D) Configure size of Syslog database

E) Purge Syslog log file daily