



Release Notes for Resource Manager Essentials 4.1 on Solaris

These Release Notes contain information about new features. They provide pointers to device support information and also provide information about the known and resolved problems in this release.

For the details, about the supported Solaris versions, see the Installation and Setup Guide for Resource Manager Essentials 4.1 on Solaris.

These Release Notes provide:

- [New Features](#)
- [Product Documentation](#)
- [Additional Information Online](#)
- [Caveats](#)
- [Known Problems in RME 4.1](#)
- [Resolved Problems in RME 4.1](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Open Source License Acknowledgements](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

New Features

This section discusses the new features in RME 4.1.

Support for 10k Devices

The managing capacity of RME is enhanced to support 10k devices with the minimum requirement of Dual CPU and 4GB RAM. A single server with CS 3.1 and RME 4.1 installed in it is equipped with the capacity of managing 10k devices thus optimizing performance and meeting the scalability prerequisite.

The support for 10k devices for RME is applicable only for CW-LMS-3.0-10K-K9 license of LMS 3.0.

For more information on licenses, refer to the *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0*.

Support for IOS Software Modularity Images

Cisco IOS Software Modularity images allow you to apply Maintenance Packs to overcome critical security issues without the need to upgrade to a new software release.

The RME Software Management component allows for distribution of Cisco IOS Software Modularity images as well as Maintenance Packs.

Software Modularity images can be downloaded from Cisco.com to the Software Repository. For detailed hardware support of Software Modularity images please consult the 12.2SX Release Notes.

PSIRT Summary Report

You can use the PSIRT Summary Report to ascertain security vulnerabilities that could affect the devices running IOS in your network. You can generate this Inventory report by selecting this option from the Report Generator dialog box under RME Reports.

The Cisco.com Fetch Interval option helps you to set the frequency of retrieving PSIRT information from Cisco.com and store it in the RME database.

The Report Generator, retrieves information from this database. It also queries the RME Inventory to retrieve information about the impacted devices and generates the PSIRT Summary Report.

End of Sale/End of Life Report

You can use the End of Sale/End of Life Report to ascertain the End of Sale or End of Life details that impact the devices and modules in your network. You can generate this Inventory report by selecting the End of Sale/End of Life option from the Report Generator dialog box under RME Reports.

The Cisco.com Fetch Interval option helps you to set the frequency of retrieving End of Sale/End of Life information from Cisco.com and store it in the RME database.

The Report Generator, retrieves information from this database. It also queries the RME Inventory to retrieve information about the impacted devices and modules and generates the End of Sale/End of Life Report.

Performance Tuning Tool

You can tune system parameters using PTT to improve RME performance. Now you can use PTT to tune Sync Archive, NetConfig, Syslog, Device Management, Check Device Attributes (CDA) and Inventory Collection sub systems of the RME application.

External TFTP Server Support

The Remote Staging and Distribution now allows you to use an external TFTP server as the staging server, to distribute images to all the devices available in RME.

First the image to be distributed is staged to the external TFTP server manually. Then the staged image is upgraded on all the selected devices.

Device Manageability Status

Now you can use this new reporting option to ascertain possible Inventory or Configuration Collection Failure and take timely actions. You can select the required devices and generate an immediate report. This Device Manageability Status report displays the status of Inventory and Configuration Collection.

Dual Supervisor Support

RME Software Image Management now supports upgrading both active and standby supervisor engines or route processors for the following devices:

Catalyst 4500, Catalyst 6500 (running Cisco IOS/Cisco IOS Software Modularity), Cisco 7600 Routers, Cisco 10000 Routers.

Secondary Credentials Fallback

The Secondary Credentials page available under System Preferences tab of RME Admin allows you to enable or disable fallback to secondary credentials when authentication through Primary Credentials is not successful.

Notification on Inventory / Configuration Failure

You can use the Collection Failure Notification window to configure the receipt of Trap messages on Inventory Collection or Configuration Fetch failure. This Trap is sent for each device from the RME server whenever the collection does not happen.

Other network management stations can use this Trap to know about RME Inventory or Configuration collection failure status. You can configure the destination IP address to which the traps are sent in the env.properties file.

Any third party Trap receivers in the hosts mentioned in the env.properties can receive the Trap messages on Config collection/Inventory collection failure.

Netconfig Reload Task

You can use the Reload Task available under RME NetConfig to reload selected devices in one step. This feature can be accessed from both GUI and CLI.

You can use the NetConfig Reload task in the following scenario in conjunction with Software Management (SWIM). During Software Distribution using SWIM, the images are distributed to the selected devices. You can use the **Reload task** to reload those devices for which, you have not selected **Reboot immediately after download** while scheduling the distribution of the images.

Syslog Support for CSS Devices

From this release, the CSS Syslog messages are also supported.

Software Management Command Line Interface

You can use the new Software Management CLI utility to list software images available in the Software Management Repository as well as export images from the Software Management Repository.

CWCLI Support for CDA Jobs

The CDA jobs are now provided CWCLI support. Apart from using the GUIs for CDA jobs, you can use CWCLI to create, list, stop, cancel, delete CDA jobs as well as verify the CDA job status.

GUI Based Write2Start Option

The Write2Start option can now be executed from both CLI and GUI.

Enhanced Severity Level Summary Report

This report has been enhanced to provide more comprehensive details about the Syslogs for each severity for each device. The Syslogs are categorized based on severities as Emergencies, Alerts, Criticality, Errors, Warnings, Notifications, Informational messages and Debug messages.

For each device, count of syslogs is provided for each severity. Clicking on any severity count link corresponding to a device, in the report provides detailed information about the messages for that severity.

GUI Based Option to Export Images from Software Repository

Now you can export software images from Software Repository using the GUI based Export button.

SysUpTime Attribute for Inventory Custom Reports

SysUpTime is a new attribute added for Inventory Custom Reports.

New Device Support

For a list of all devices supported in RME 4.1, including devices supported in previous versions of RME, see the *Supported Device Table for Resource Manager Essentials 4.1* on Cisco.com:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Product Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The following documents are provided in PDF on your product Documentation CD:

- *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0.*
- *User Guide for Resource Manager Essentials 4.1*

Adobe Acrobat Reader 6.0 or later is required.

Use these guides to learn how to install and use Resource Manager Essentials 4.1:

- *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0.*

Provides installation instructions, including both server and client system requirements, steps for installing and uninstalling, and installation troubleshooting information for LMS 3.0. This guide also contains installation instructions for RME 4.1

- *User Guide for Resource Manager Essentials 4.1*

Provides information on using RME 4.1.

- *User Guide for Common Services 3.1*

Provides information about setting up, administering, and accessing CiscoWorks Common Services 3.1.

- *Resource Manager Essentials Online help*

Provides task-oriented and context-sensitive help from every window that contains a Help button.

Also contains all of the information available in *User Guide for Resource Manager Essentials 4.1*. This ensures you have complete information even if you do not have the manual readily available while using RME.

For more details on the new features in RME 4.1, and the procedures mentioned in this document, see the *User Guide for Resource Manager Essentials 4.1*.

Additional Information Online

For information about RME supported devices, refer to the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

For the latest technical tips, suggestions for troubleshooting common issues, and frequently asked questions (FAQs) on most RME applications:

Login to Cisco.com and select **Products and Services > Network Management > CiscoWorks LAN Management Solution > CiscoWorks Resource Manager Essentials > Product Literature**.

Service Pack (SP) for RME 4.1 is a collection of updated files necessary for RME to support new Cisco devices. In addition to the devices supported, this package also contains fixes to known problems, as well as additional newly discovered problems.

If you are a registered user, you can download the latest version of SP for RME 4.1 from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>

Caveats

For more information on caveats, see the *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0*.

Known Problems in RME 4.1

This section contains the following known problems for RME 4.1.

- [Installation and Upgrade Known Problems](#)
- [Administrator Known Problems](#)
- [Device Management Known Problems](#)
- [Device/Agent Known Problems Impacting ANI Server and RME Functionality](#)
- [Inventory Known Problems](#)
- [Archive Management Known Problems](#)
- [NetConfig Known Problems](#)
- [Config Editor Known Problems](#)
- [NetShow Known Problems](#)
- [Software Management Known Problems](#)
- [Change Audit Known Problems](#)
- [Syslog Known Problems](#)
- [Contract Connection Known Problems](#)
- [Bug Toolkit Known Problems](#)
- [Server, Browser, UI, and Desktop Known Problems](#)
- [Common/Other Known Problems](#)

For more information about known problems:

-
- Step 1** Go to <http://www.cisco.com>
- Step 2** Select **Technical Support & Documentation > Tools & Resources**.
- Step 3** Select the Software sub-section and click **Bug Toolkit**.
-

Alternatively, go to: <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>

You will be prompted to log into Cisco.com.

Installation and Upgrade Known Problems

Table 1 *Installation and Upgrade Known Problems*

Bug ID	Summary	Explanation
CSCsa93329	Daemon manger dumps core when configjob/DCMA displays OutOfMemory exception	<p>The daemon manager sometimes dumps core but no processes go down.</p> <p>This sometimes occurs during a Quick Config Deploy operation from Config Management.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Stop the daemon manager. 2. Increase the swap space of the system. 3. Restart the daemon manager.
CSCsa33360	Device groups migrated for users (Approvers and Network Operators) cannot be edited by users with the same roles in RME 4.0 and above.	<p>Users with Approver and Network Operator roles cannot edit or delete device groups in RME 4.x that were created in RME 3.x by users with the same roles.</p> <p>This happens when the device groups created in RME 3.x by users with Approver and Network Operator roles, are migrated to RME 4.0 and above.</p> <p>Workaround:</p> <p>None.</p>
CSCsa33365	Network Administrator cannot edit or delete device groups in RME 4.x that they created in RME 3.x, after migration.	<p>After migration from RME 3.x to RME 4.x, a user with a Network Administrator role cannot edit/delete groups in RME 4.x that the user created in RME 3.x.</p> <p>This happens when the device groups created in RME 3.x by a user with a Network Administrator role, are migrated to RME 4.x.</p> <p>Workaround:</p> <p>None.</p>
CSCsa34359	Change Audit details are not available for some of the NetConfig records after data migration from RME 3.x to RME 4.x.	<p>The change details cannot be identified for some of the NetConfig records.</p> <p>This is because you have purged configuration files in the RME 3.x server where the backup was taken for migration.</p> <p>These purged configuration files are not available in RME 4.x server after data migration.</p> <p>An error appears, Internal Error: Config File information not available.</p> <p>Workaround:</p> <p>None.</p>

Table 1 *Installation and Upgrade Known Problems (continued)*

Bug ID	Summary	Explanation
CSCsa22623	Data inconsistency on restoring data backed up with jobs in running state	<p>After restoring RME 4.x data on a system, the job status is not the same as that of the system where the backup was taken.</p> <p>When a backup is triggered while a job is running, the Restore command is not aware of the state of the jobs in the backed-up machine.</p> <p>Additionally, the Backup/Restore command does not backup/restore the state of the systems. It is only the data that is backed-up and restored.</p> <p>Workaround:</p> <p>Ensure that while backing up data, there are no jobs running on the system.</p>
CSCsi89107	Restore operation fails when LMS 2.2/2.5/2.5.1/2.6 data is restored to LMS 3.0	<p>This happens when you:</p> <ol style="list-style-type: none"> 1. Backup the LMS 2.2/2.5/2.5.1/2.6 data 2. Perform a Remote migration from LMS 2.2/2.5/2.5.1/2.6 to LMS 3.0 <p>The space check is done in RME to confirm if two times free space than the backup size is available for a smooth restore.</p> <ol style="list-style-type: none"> 3. Restore the backed up data. <p>The data restore happens under NMSROOT as well as RME backup folder.</p> <p>The filebackup.tar file is extracted in the RME backup folder.</p> <p>A space crunch arises as the size of the extracted backup file exceeds twice its size. Twice the size of the backup amounts to the available space. The restore operation fails. The error messages are recorded in the restorebackup.log file.</p> <p>Workaround 1:</p> <p>Ensure that the backup is available in the same drive in which the product is installed. If this is ensured, this drive will contain five times free space than that of the backup resulting in a successful restore.</p> <p>Example:</p> <p>If the backup size is 5GB then the free space should be minimum 25GB.</p>

Table 1 *Installation and Upgrade Known Problems (continued)*

Bug ID	Summary	Explanation
CSCsi89107 (Continued)		<p>Workaround 2:</p> <p>If the backup data is in a drive other than the drive in which the product is installed, ensure that the drive (in which the product is installed) consists of three times free space than the size of the backup. This will result in a successful restore.</p> <p>Example:</p> <p>If the backup size is 5GB then the free space should be minimum 15GB.</p>
CSCsi73325	Error messages logged in restorebackup.log when LMS 2.5.1 backedup data is restored to LMS 3.0 using remote migration.	<p>This happens when you:</p> <ol style="list-style-type: none"> 1. Backup LMS 2.5.1 data. 2. Install LMS 3.0 3. Restore the LMS 2.5.1 backed up data to LMS 3.0 using Remote migration <p>The Restore operation is successful but there are some error messages related to Syslog that get recorded in restorebackup.log. These error messages are also displayed in the CLI screen.</p> <p>Workaround:</p> <p>None.</p>

Administrator Known Problems

Table 2 *Administrator Known Problems*

Bug ID	Summary	Explanation
None	Some of the RME processes are suspended.	<p>If you start RME by logging in as root and entering <code>/etc/init.d/dmgt start</code>, make sure you do not suspend the session with the <code>suspend</code> command.</p> <p>If you suspend the root session after manually starting RME, other processes, such as Daemon Manager, and ICServer, are also suspended.</p> <p>Workaround:</p> <p>Resume the suspended session.</p>

Device Management Known Problems

Table 3 *Device Management Known Problems*

Bug ID	Summary	Explanation
CSCsa18790	Device moves from Pending to Normal to Conflicting state	<p>During device import, devices may appear as Normal Devices for a very short span of time but later on move to Conflicting or Alias states after Conflict detection or Alias detection, respectively.</p> <p>This may occur when you add a large number of duplicate or conflicting devices.</p> <p>Workaround:</p> <p>Wait for all devices to be processed for management. This may take some time depending on the number of devices added.</p>
CSCsa22830	DLMS fails in SSL mode	<p>This happens when you get or set credentials using DLMS in SSL mode.</p> <p>Workaround:</p> <p>SSL support for DLMS is not available in RME 4.x and therefore there is no workaround.</p>
CSCed47422	Device Management State Summary show wrong record count.	<p>A label on right top of Device Management State Summary screen shows, for example:</p> <p>Showing 7 records</p> <p>This problem occurs because of the default display provided by the underlying UI component (HTML Scrolling table).</p> <p>Workaround:</p> <p>This caption should be read as the number of records displayed on that screen — not the number of devices or the number of device states.</p>
CSCsa36278	AUS should not be displayed in the Picker list while adding devices to RME.	<p>Auto Update Servers (AUS) appear in the Add Devices screen.</p> <p>This happens when you are adding new devices into RME, and PIX devices managed by Auto Update Servers are also a part of the list of devices to be managed in RME.</p> <p>Workaround:</p> <p>If Auto Management option is enabled, delete Auto Update Servers after they are added to the Normal Devices list.</p> <p>If you select devices from the Add Devices screen filter out these Auto Update Servers.</p>

Table 3 *Device Management Known Problems (continued)*

Bug ID	Summary	Explanation
CSCsa45574	Alias detection fails for some devices.	<p>Alias detection does not work for devices that are accessed using a virtual management IP address.</p> <p>This happens when you add devices with virtual management IP address.</p> <p>Workaround:</p> <p>Manually resolve aliases by deleting duplicate entries from the Normal Devices dialog box.</p> <p>See the User Guide for Resource Manager Essentials for details.</p>
CSCsa52951	Device Credential Verification does not run when device moves from conflicting to normal state.	<p>Device Credential Verification is not triggered when a device moves from Conflicting to Normal state.</p> <p>This happens when the device type conflict is resolved and the device moves to Normal state.</p> <p>Workaround:</p> <p>Manually trigger Device Credential Verification for such devices.</p>

Device/Agent Known Problems Impacting ANI Server and RME Functionality

Table 4 *Device /Agent Known Problems Impacting ANI Server and RME Functionality*

Bug ID	Summary	Explanation
CSCsa39153	Archive Management tasks fail for Catalyst 4507 device.	<p>Archive Management tasks fail for Catalyst 4507 device, if you have selected TFTP as the transport protocol.</p> <p>The happens because of incorrect implementation on the device.</p> <p>Workaround:</p> <p>Select a different transport protocol using Resource Manager Essentials > Admin > Config Mgmt.</p> <p>See Supported Device Table for Archive Management Application on Cisco.com for supported transport protocols information for the Archive Management application:</p> <p>http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</p>
CSCsa19145	SSH connection to the device fails because of SSH disconnection packet.	<p>This problem occurs in a slow network when RME tries to contact device using SSH connection.</p> <p>This happens because of incorrect implementation of SSH daemon (sshd) on the device.</p> <p>Workaround:</p> <p>None.</p>

Table 4 *Device /Agent Known Problems Impacting ANI Server and RME Functionality (continued)*

Bug ID	Summary	Explanation
CSCsa44813	Archive Management tasks on startup configuration using TFTP do not work	<p>Archive Management tasks on startup configuration using TFTP protocol do not work.</p> <p>This happens because the device supports only OLD-CISCO-CONFIG-MIB for TFTP and this MIB does not support tasks on startup configuration.</p> <p>Workaround:</p> <p>Select a different transport protocol using Resource Manager Essentials > Admin > Config Mgmt.</p> <p>See Supported Device Table for Archive Management Application on Cisco.com for supported transport protocols information for the Archive Management application:</p> <p>http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html</p>
CSCsa40523	Chassis slot incorrect for MDS 9509	<p>MDS device with software version 1.3(4a) renders incorrect values for its chassis number of slots.</p> <p>This problem is identified in software version 1.3(4a).</p> <p>Workaround:</p> <p>Install software version 2.0(1).</p>
CSCed88554	Supervisor software version value is 0	<p>Device does not return Supervisor software version.</p> <p>This happens when the device has to be SNMP configured.</p> <p>Workaround:</p> <p>None.</p>
CSCsa07154	Cannot query containment AG for Catalyst 5000 devices.	<p>If the device happens to run with Cisco Catalyst Operating System Software, Version 4.5(13a), it is likely that SNMP query fails for numSlots (SysObjectID > "1.3.6.1.4.1.9.5.1.3.1.1.25").</p> <p>This happens when the device has to be SNMP configured. The problem occurs because support in the Catalyst OS fails for this SysObjectID.</p> <p>Workaround:</p> <p>None.</p>

Table 4 *Device /Agent Known Problems Impacting ANI Server and RME Functionality (continued)*

Bug ID	Summary	Explanation
CSCsa36845	Processor Port and Module Port section are missing from DDR for 4506 IOS	The device running IOS, Version 12.1(22)E2 fails for correlation between the port and the interface because ifIndex is rendered Null. This happens when the device is configured for SNMP. Workaround: The problem does not occur with the IOS, Version 2.1(9a). Upgrade the device to this version.
CSCsa28210	<code>cwcli export</code> for CSS 11800 information is missing	Software Identity is missing in <code>cwcli export</code> , in the case of CSS 11800. This happens when the CSS 11800 device has to be SNMP configured. The device does not return the processor component, while queried using SNMP. Workaround: None.

Inventory Known Problems

Table 5 *Inventory Known Problems*

Bug ID	Summary	Explanation
CSCsb28200	Grouping rules that are built using equality matches on <code>:RME:INVENTORY:Device.System.SystemOID</code> do not find matches.	This happens if the sysObjectID on which the match is performed does not begin with a leading dot. All sysObjectIDs in RME are stored with a leading dot. Workaround: Either specify the leading dot in the match value, or change the operator from Equals to EndsWith or Contains.
CSCsa86823	A device in the normal state appears with ? icon and cannot be selected.	The Device Selector shows ? as the icon for a normal device for which configuration collection is successful. Device and Credential Repository (DCR) did not have the device type information while the device was added. Inventory collection failed because of SNMP time-out. Workaround: <ul style="list-style-type: none"> Update the device type information in DCR. Make sure that the inventory collection succeeds (if required, increase the SNMP time-out value). SNMP timeout exceptions can be seen in <code>IC_server.log</code> . For details on editing device information in DCR, increasing SNMP time-out values, etc., see the <i>User Guide for Resource Manager Essentials 4.1</i> or the RME 4.1 Online help.

Table 5 Inventory Known Problems (continued)

Bug ID	Summary	Explanation
None	IP addresses of cable modemsubr904 andubr924 may change between reboots.	These devices get the IP address of the cable interface using DHCP from head-end cable router. The IP address might change between reboots. Workaround: You must import cable modemsubr904 andubr924 using fully qualified pathnames.
None	Cannot manage PIX Firewall device without RME server IP address.	PIX Firewall device cannot be managed in RME without the IP address of the RME server. Workaround: 1. Configure the PIX Firewall device so that it can be managed. 2. Enter the IP address of the RME server.
None	Check Device Attributes fails for devices that are already managed through the host name.	This happens when the IP address of the device host name is changed on the DNS server or on the local hosts file (/etc/hosts). Workaround: Restart the daemon manager.
CSCsa36932	The Inventory Job Status page shows deleted device information.	When a device is deleted, the associated change records are deleted, but the device is still a part of the scheduled jobs. Hence, the job browser shows the status of the job as: Successful: With Changes However, when you click View Details , a message appears: No changes for a job that has already run. This is because the changes have already been deleted. Workaround: None.
CSCsa38526	RAM, NVRAM information duplicated for some multi-processor devices	In the Processor Information section of the Detailed Device Report, Processor details such as, RAM and NVRAM information are duplicated for some multi-processor devices. This happens when the multi-processor devices do not have support for CISCO-ENTITY-EXT-MIB. Workaround: None.
CSCsa15342	NS 7.1—Hardware Report: Save in CSV format saves as export.csv.do in Solaris.	When you try to save the Hardware Report in the CSV format, although RME sends the default name <code>export.csv</code> , the Netscape client adds the <code>.do</code> extension. Workaround: Edit the name and give <code>.xls</code> or <code>.csv</code> as the extension for the file.

Table 5 Inventory Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa16772	Cannot create a Private Custom Template with the same name for different users.	<p>If a template with the name ABC, is created by user X, with any access type, then user Y cannot create a template with the same name ABC.</p> <p>However, user Y cannot see the template named ABC, which user X has created with private access. This may confuse user Y.</p> <p>Workaround:</p> <p>Use the following CLI command to view all template names (Private and Public access):</p> <pre>cwcli invreport -u username -p password -listreports.</pre> <p>This will display all the templates defined in the system. Also, avoid template names that are already in use.</p>
CSCsa22899	Device Credential Verification reports no value to test for Enable when Telnet password is blank	<p>If you do not enter the Telnet Username and Password and only enter the Enable Password, Device Credential Verification reports <code>DID NOT TRY</code> for its the Enable Password check.</p> <p>The condition under which this problem occurs is that both Telnet Username and Password are not provided in Device and Credential Repository.</p> <p>Workaround:</p> <p>None.</p>
CSCse26973	NVRAM and Total RAM information missing in Hardware report for IGESM device.	<p>The IGESM device does not consist of NVRAM and Total RAM details. So when you generate a Hardware report for this device, the NVRAM and Total RAM details do not appear in the report.</p> <p>Workaround:</p> <p>None.</p>
CSCsd11513	Inventory Reports page, takes more time to launch.	<p>The output of Detailed Device Report for 10k devices takes a long time to launch. This occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Reports 2. Select 10k devices and schedule a Detailed Device Report with Schedule Type as Once. 3. Ensure that this job is completed. 4. Go to RME > Reports > Report Jobs. 5. Select the Job ID of the job you scheduled in Step 2 and click Show Output. <p>The Detailed Device Report output page is not launched.</p> <p>After 30 minutes, the following error message appears:</p> <pre>The file is damaged and could not be repaired.</pre> <p>Workaround:</p> <p>None.</p>

Table 5 Inventory Known Problems (continued)

Bug ID	Summary	Explanation
CSCsd31552	Device Selector does not list 10k devices if the All Devices node is expanded.	<p>The Device Selector is not listing 10k devices when the All Devices node is expanded. This occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Devices > Device Management. 2. Expand the All Devices node. <p>When the total number of devices managed is 10k, the Device Selector does not list all the devices on expanding the All Devices node.</p> <p>Instead, the following error message is displayed:</p> <pre>Showing 4992 out of 10037 number of nodes only in Group/RME@rmetest-sf440/All Devices to prevent performance degradation.</pre> <p>To render all nodes, please avoid having multiple groups open.</p> <p>Workaround: None.</p>

Archive Management Known Problems

Table 6 Archive Management Known Problems

Bug ID	Summary	Explanation
CSCsa85666	WLAN Module: Sync Archive fails when TFTP is used.	<p>The Sync Archive operation fails for the WLAN module when TFTP is the only transport protocol that is used.</p> <p>TFTP is not supported since Config-Copy-MIB is not supported by this device.</p> <p>Workaround:</p> <p>You can do a configuration Fetch operation using Telnet and SSH.</p> <p>Enable these protocols in the Config Transport Settings page (Resource Manager Essentials > Admin > Config Mgmt) and then trigger the configuration collection.</p> <p>For details, see the <i>User Guide for Resource Manager Essentials 4.1</i>.</p>

Table 6 *Archive Management Known Problems (continued)*

Bug ID	Summary	Explanation
CSCsa97886	Config deploy in the Merge-mode download fails in C2970G-24T-E because of Certificate	<p>Configuration deployment in the Merge mode fails for C2970G-24T-E when you try to deploy certificate commands.</p> <p>This is because:</p> <ul style="list-style-type: none"> • The configuration that you are trying to deploy has certificate configuration, which is fetched from the running configuration. and • The configuration archived from the running configuration has certificate commands with the private keys missing. <p>Workaround:</p> <p>Make sure that the configuration you are deploying has the certificate commands properly configured (including the private keys).</p> <p>If you want to deploy non-certificate commands from the configuration, remove all certificate-related commands from the configuration.</p>
None	Banner commands containing (") and (^C) characters cause configuration applications to function incorrectly.	<p>If banner values are contained between quotation marks (") in Config Archive and between Ctrl-C (^C) characters in a device, the configuration applications do not function correctly.</p> <p>Workaround:</p> <p>Do not add Ctrl-C characters to the banner commands while downloading them to the device.</p>
None	Module configuration is not retrieved even if the module has valid credentials for a CAT switch.	<p>Configurations of IP addressable modules are not retrieved along with Supervisor even if the module has same credentials as the Catalyst switch. IP addressable modules should be managed as a separate device.</p> <p>Configurations of non-IP addressable modules are fetched along with Supervisor configuration only if the selected protocols are Telnet or SSH, provided the module has same credentials with Supervisor. Other protocols are not supported.</p> <p>Workaround:</p> <p>None.</p>
CSCsa44963	Archival fails in Cisco Content Services Switch 11050.	<p>Configuration archival fails in the Quick Configuration deployment job in the Merge mode for Cisco Content Services Switch 11050.</p> <p>Workaround:</p> <p>None.</p>

Table 6 Archive Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa35699	VPN configs coloring scheme is incorrect for Compare Configs.	In the Config Diff Viewer, the diffs of modified commands are shown in blue instead of red. For VPN 3000 devices, the diff viewer shows the modified commands in blue text instead of red, as in other devices. Workaround: None.
CSCsa37473	Issue in Config for device CSS 11050	Archived configuration does not contain the complete running configuration. This problem occurs when the image on the device is Content Switch SW Version 5.02 Build 3 with SNMPv1/v2c Agent. This happens when configuration fetch is tried with both Telnet and TFTP protocols. Workaround: None.
CSCsa55997	Sync Archive Fails for few NAM devices	Sync Archive of NAM devices fails. If the previous deploy job failed with a timeout exception, subsequent sync archive jobs for that NAM device will fail. Workaround: Either: <ul style="list-style-type: none"> Stop and restart the ConfigMgmtServer service at Common services > Server > Admin > Processes. Make sure that no other jobs are running. If they are running, perform this task operation after the jobs complete. Or <ul style="list-style-type: none"> For the specific device, fetch the startup or running configuration using the Startup or Running hyperlinks respectively at Resource Manager Essentials > Config Mgmt > Archive Mgmt > Version Summary.
CSCsh36359	Write2Start does not work properly for PIX devices.	This occurs, when you: Download a configuration to the startup configuration of a PIX device. Workaround: Use the adhoc template in RME NetConfig to download the command to copy the configuration from external TFTP server to startup configuration for a PIX device.

NetConfig Known Problems

Table 7 NetConfig Known Problems

Bug ID	Summary	Explanation
CSCsa78026	Adhoc Enable Mode command, <code>sh run</code> fails for some string patterns	<p>When you create a NetConfig Job with the Adhoc Enable Mode Command <code>sh run</code>, the job status may be reported as <code>Failed</code> even if the commands have been successfully downloaded.</p> <p>This may occur when the successfully downloaded command output contains well-known error messages such as <code>ERROR:</code>, <code>%ERROR:</code> etc., (which are ideally a part of the command output during error conditions only).</p> <p>Workaround: None.</p>
CSCsa88829	Problem with credentials removal in DCR with NetConfig job, when AAA new-model is enabled	<p>When you are disabling credentials using NetConfig, the device may become unreachable from within RME.</p> <p>However the device remains reachable outside RME.</p> <p>This may occur when you disable or remove credentials such as Telnet password using a system-defined task in NetConfig.</p> <p>Workaround: To enable TACACS authentication, you should use the TACACS+ task and not the Telnet Password task. To disable one kind of authentication, you should enable another kind of authentication. For example, if you want to disable Telnet authentication and enable TACACS+ authentication, you can simply enable TACACS + authentication.</p>
CSCsa15482	Network Time Protocol template does not generate proper rollback commands.	<p>When the download command fails on a device, the successfully downloaded commands are rolled back, if the Rollback policy is on.</p> <p>If the command <code>ntp authentication-key</code> is already present in the device and if you attempt a rollback of the command, it fails.</p> <p>Workaround: None.</p>
CSCsa16093	Trap notifications fail for certain image features.	<p>For Cisco IOS devices, if you select certain trap notification types for the <code>snmp-server host</code> command in the traps template, it might lead to command download failure.</p> <p>Workaround: None.</p>

Table 7 NetConfig Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa19184	Rollback for the SSH key bit configuration command does not restore the original number of key bits.	<p>This happens when you have enabled SSH on a device with a certain number of key bits and then enable or disable the key bits through an SSH template download.</p> <p>The download of commands other than the key bits command fails.</p> <p>Workaround: None.</p>
CSCsa22697	Rollback for the ntp server command does not restore the original command on the device.	<p>This happens when you have an ntp server command on the device with the key option enabled.</p> <p>If you change the command on the device through an NTP template download, the download of all other commands fail.</p> <p>Workaround: None.</p>
CSCsa24300	Authentication method of non-ip addressable sub-modules is not updated.	<p>When you update the authentication method for the Supervisor module using the tacacs+ template, it does not update the authentication method.</p> <p>It also does not update the passwords of the non-ip addressable sub-modules.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Add a Telnet or Enable password template and apply commands with the same password to the modules. 2. Add a tacacs+ template to update the authentication method for the Supervisor module. Use the same password as above for this template.
CSCsa25755	Rollback of a job changes the password on the device.	<p>This happens when you rollback a job containing two credential templates. When you change the Enable password, it might change the password on the device.</p> <p>For example, Radius and enable or Tacacs+ and enable.</p> <p>Workaround: Do not have two different templates changing the Enable password credentials in the same job.</p>
CSCsa27946	CSS: NTP: Server IP address alone allowed. Download fails for hostname	<p>While configuring SNTP server, the IP Address of the SNTP server has to be specified. Instead of the IP Address, if the SNTP server hostname is specified, the template fails.</p> <p>This is applicable for all versions from 5.0 onwards.</p> <p>Workaround: Specify the IP Address of SNTP server instead of the SNTP server hostname.</p>

Table 7 NetConfig Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa44983	The commands fails only for Content engine devices running ACNS 5.2 or later versions.	<p>This happens when the commands deployed using Syslog task on Content Engine devices fails for logging priority configuration.</p> <p>Workaround:</p> <p>Do not configure logging priority using Syslog system defined task on Content Engine devices running ACNS version 5.2 or later.</p> <ol style="list-style-type: none"> 1. Create a user-defined task for configuring logging priority with commands specific to ACNS 5.2 or later 2. Use that for deploying on Content Engine devices running ACNS 5.2 or later.
CSCsa44626	IOS-enable TACACS fails when <code>aaa new-model</code> is enabled.	<p>Download of TACACS commands such as <code>login tacacs</code>, <code>tacacs server</code> etc., fail.</p> <p>This occurs when the command, <code>aaa new model</code> is present on the device.</p> <p>Workaround:</p> <p>Disable the <code>aaa new model</code> command. To do this use either the TACACS+ or RADIUS template before adding the TACACS template commands.</p>
CSCsa23231	Job Creation wizard loses context when multiple templates are opened.	<p>This problem occurs while creating a NetConfig job, in the second step of the wizard (Add Tasks).</p> <p>If you open multiple task windows simultaneously and try to add the tasks to the job, there are problems with the wizard.</p> <p>Workaround:</p> <p>Open only one window at a time.</p>
CSCsh38157	NetConfig job to deploy TACACS+ templates to NAM devices fails.	<p>This problem happens when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Config Mgmt > NetConfig 2. Schedule a NetConfig job with TACACS+ template to NAM devices. 3. Try to update DCRusing: <ul style="list-style-type: none"> <code>ip http tacacs+ enable 5.3.6.3 <R>*<R>*</code> <p>The interactive commands are not handled properly and the job fails with the following error message:</p> <p>Command(s) failed on device.</p> <p>Workaround:</p> <p>None.</p>

Config Editor Known Problems

Table 8 Config Editor Known Problems

Bug ID	Summary	Explanation
CSCsb78495	Config Editor overwrite job does not work for PIX devices	<p>A Config Editor job in the overwrite mode, does not work for PIX devices. That is, when you are deploying a configuration that you have edited using Config Editor, to a PIX device, in the overwrite mode, the deployment is unsuccessful.</p> <p>This happens if you:</p> <ol style="list-style-type: none"> 1. Edit the configuration of a device using Config Editor and save it. 2. Create a job to deploy that configuration to a PIX device, using the Overwrite mode. <p>The job fails.</p> <p>However, the job, succeeds in the Merge mode.</p> <p>Workaround: None.</p>
CSCsa36347	SNMP Authentication/privacy passwords not masked in device response	<p>SNMP security password and Privacy passwords appear in an argument list in the Device Details page.</p> <p>This happens when Debug is enabled in the device.</p> <p>Workaround: Disable Debug on the device.</p>
CSCsa39790	Config Editor updates the Device and Credential Repository with an encrypted string.	<p>If service password-encryption is enabled on the device, the credential is encrypted in the show config output of the device.</p> <p>The Device and Credential Repository is updated with this encrypted password, if you:</p> <ol style="list-style-type: none"> 1. Create a Config Editor job in Merge mode using Telnet as the transport protocol. 2. Deploy this command using the Config Editor application. <p>Workaround: Use the NetConfig application to update the encrypted credential command.</p>

Table 8 Config Editor Known Problems (continued)

Bug ID	Summary	Explanation
CSCsb82197	The Config Editor deploy job fails when <code>set length length</code> command is downloaded manually in Merge or Overwrite mode.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Config Mgmt > Config Editor 2. Edit a configuration and schedule a Deploy job to deploy that configuration to a device. 3. Manually download <code>set length length</code> command to that device. Where <i>length</i> is the terminal length. <p>The Config Editor deploy job fails with the following error message:</p> <pre>Command(s) failed on the device TFTP. Check whether you have provided the correct credentials. If credentials are correct, ensure that the TFTP server is up and running.</pre> <p>Workaround:</p> <p>Do not manually download the <code>set length length</code> command while deploying a Config Editor job in merge or overwrite mode.</p>
CSCsh65909	Write2Start does not work properly for MDS devices.	<p>This occurs, when you:</p> <p>Download a configuration to the startup configuration of a MDS device.</p> <p>The job fails with the following error message:</p> <pre>Transport operation failed, No commands applied on the device.</pre> <p>Workaround:</p> <p>Use the adhoc template in RME NetConfig to download the command to copy the configuration from external TFTP server to startup configuration for a MDS device.</p>

Table 8 Config Editor Known Problems (continued)

Bug ID	Summary	Explanation
CSCsi48034	Config Editor/NetConfig job failed when hostname is changed using Telnet or SSH protocol.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Config Mgmt > Config Editor 2. Select a configuration and change the hostname using Config Editor. 3. Schedule a job to deploy the changed configuration. 4. Set the protocol as Telnet for this job. <p>The job fails with the message:</p> <pre>Deploy succeeded, Synchronization of RME archive wth Device Config failed.</pre> <p>The same problem occurs when you set SSH as the protocol. When you:</p> <ol style="list-style-type: none"> 1. Go to RME > Config Mgmt > Netconfig 2. Schedule a job to use an Adhoc task in Netconfig to change the hostname. 3. Set the protocol as Telnet for this job. <p>The job fails with the message:</p> <pre>Deploy succeeded, Synchronization of RME archive with Device Config failed</pre> <p>Workaround:</p> <p>After the Netconfig job is completed and the error message appears, you can run a Sync archive job for that particular device to archive the latest configuration.</p>
CSCsi59716	Configurations edited in Processed mode does not support Write2Start.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Config Mgmt > Config Editor 2. Open a configuration and edit it in Processed mode. 3. Schedule a job to write this configuration to the startup configuration of a device. <p>The job fails.</p> <p>Workaround:</p> <p>Edit the configuration in Raw mode and schedule a job to write this configuration to the startup of a device.</p>

NetShow Known Problems

Table 9 NetShow Known Problems

Bug ID	Summary	Explanation
CSCsa86905	Custom commands, that are not assigned to any Command Sets, are not migrated	<p>This occurs if:</p> <ol style="list-style-type: none"> 1. In RME 3.x, in NetShow, you had a few isolated custom commands that were not associated with any command set. 2. You backed up and migrated these custom command sets into RME 4.1. <p>These isolated custom commands do not exist in RME 4.1 NetShow after migration.</p> <p>Workaround:</p> <p>You can associate these isolated custom commands with any user-defined command set in RME 3.x, before taking a backup. Then these custom commands will be migrated as if they were a part of a command set.</p>
CSCsa73709	Cannot remove an Adhoc command from the Available Commands list	<p>You may not be able to delete an Adhoc command from the Available Commands list (in the Select Commands page of the Resource Manager Essentials > Tools > NetShow > Command Sets flow) even if it is in only one command set.</p> <p>This occurs when you:</p> <ol style="list-style-type: none"> 1. Go to the Resource Manager Essentials > Tools > NetShow > Command Sets flow 2. Go to the Command Sets page, select the command set you want to edit and click Edit. <p>The Select Device Category page appears.</p> <ol style="list-style-type: none"> 3. Click Next. 4. Select the ad hoc command that you want to delete, from the Selected Commands list and click Remove. <p>The command moves to the Available Commands list.</p> <ol style="list-style-type: none"> 5. Select the command from the Available Commands list and click Delete Adhoc. <p>An error appears:</p> <pre>NS0011:The command(s) show run are not deleted because they may be system-defined or part of a command set or in the selected commands list.</pre> <p>The Adhoc command is not deleted.</p> <ol style="list-style-type: none"> 6. Select the command from the Available Commands list and click Delete Adhoc. <p>A message appears that the command is successfully deleted</p>

Bug ID	Summary	Explanation
CSCsa73709 (Continued)	Cannot remove an Adhoc command from the Available Commands list (Continued)	<p>Workaround:</p> <ol style="list-style-type: none"> 1. In the Edit flow detailed above, after Step 3, click Finish. 2. Re-enter the Edit flow from the Commands Sets page (in the Resource Manager Essentials > Tools > NetShow > Command Sets flow and from the Command Sets page, select the command set you want to edit and click Edit) and follow the same procedure detailed above. 3. Select the command from the Available Commands list and click Delete Adhoc. <p>You will see a message that the command is successfully deleted.</p>
CSCsa75907	Cannot add Adhoc commands that are device-specific, in the same command set.	<p>You cannot add device type-specific Adhoc commands in the same command set. The Adhoc commands that you have added in a specific command set apply to all the device types that you have selected.</p> <p>This scenario occurs when, in the command set creation flow of NetShow (Resource Manager Essentials > Tools > NetShow > Command Sets), you:</p> <ol style="list-style-type: none"> 1. Choose device categories 2. Add Adhoc commands. 3. Complete the flow. <p>These Adhoc commands will be applicable to all the device types that you have selected.</p> <p>For example, if you choose device types Content Networking and Router and add an Adhoc command, this command will be applicable to both Content Networking and Router device types.</p> <p>Workaround:</p> <p>Create different command sets for different device types.</p> <p>For details on creating command sets, see <i>User Guide for Resource Manager Essentials 4.1</i></p>
CSCsb09234	OutOfMemoryexception on printing job output	<p>A 500 server error appears with an out-of-memory exception when you print NetShow Job Results.</p> <p>This may occur when the job has more than 1500 devices and has a high number of commands that produce voluminous output.</p> <p>Workaround:</p> <p>Do any of the following:</p> <ul style="list-style-type: none"> • Use the Per-device Print option. • Increase the Tomcat heap-size. • Reduce the number of devices in the job.

Software Management Known Problems

Table 10 Software Management Known Problems

Bug ID	Summary	Explanation
CSCsb68458	Software Management fails on Catalyst 5500 with an error	<p>An error, SWIM1035, appears when you try to distribute new software to Catalyst 5500</p> <p>This occurs:</p> <ul style="list-style-type: none"> • When RME 4.0 (or later) is installed. • When the device is Catalyst 550x with Supervisor III (WS-X5530) <p>The content of the error message is :</p> <pre>SWIM1035: Error while performing Recommendation operation. Runtime error encountered while filtering images caused by a problem with a running image on the device. See the Troubleshooting section of the RME 4.0 help.</pre> <p>Workaround:</p> <p>None.</p>
CSCsb42968	RME 4.1 does not distribute images to Cisco Catalyst 6500 series devices running CAT OS.	<p>This problem occurs when the image is being copied to:</p> <ol style="list-style-type: none"> 1. bootflash: using TFTP or RCP. 2. Slot0: using RCP only. <p>Workaround:</p> <p>Use Slot0: with TFTP for distribution.</p>
CSCsa92049	Software Management-SOL: Edit Admin Preferences displays an error	<p>In Software Management, when you make a change to Admin Preferences (Admin > Software Mgmt > View/Edit Preferences) the operation fails with an error</p> <pre>Failed to execute df -k command</pre> <p>This happens when there is not enough swap space on the server to create a new java process.</p> <p>Workaround:</p> <p>Increase swap space and retry the operation.</p>
None	Cannot undo image upgrade of tar images for DSBU switches.	<p>After performing an image upgrade of tar images for DSBU switches, you cannot undo the job.</p> <p>Workaround:</p> <p>Select the tar image and schedule a new distribution job.</p>
CSCin19501	Software Management includes the bootflash of MSFC as a storage option.	<p>This happens for Cat6000 supervisors running IOS.</p> <p>Storing the IOS images in the bootflash might bring the device down.</p> <p>Workaround:</p> <p>Do not select the bootflash to store the image while upgrading Cat6000 devices running IOS.</p> <p>Select a different storage location.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa29037	Image upgrade using Remote Stage fails if the image size exceeds 32 MB.	<p>In the Remote-Stage flow, the only protocol that is supported currently between Remote Stage device and target device, is TFTP.</p> <p>Here, it uses the TFTP server of IOS on the RS device.</p> <p>There is a limitation in the Cisco IOS TFTP server for transferring files exceeding 32MB from Remote Stage device to Target device.</p> <p>Workaround:</p> <p>Please upgrade the IOS image to any of the following versions which has the 32 MB fix:</p> <ul style="list-style-type: none"> • 12.2(18)SXE • 12.003(009.008) • 12.0(29.03)S • 12.2(17d)SXB07 • 12.2(18)SXD04 12.2(25.04)S • 12.3(09.08)T
CSCsa32595	Software Management distribution fails for all devices running Cisco IOS Release 12.3(5x).	<p>This happens because CISCO-FLASH-MIB returns the Flash partition name as Flas instead of Flash.</p> <p>This problem occurs in all devices running Cisco IOS Release 12.3(5x).</p> <p>Workaround:</p> <p>None.</p>
CSCsa33864	Add Image or distribution fails in Software Management.	<p>If the tftpboot directory is either a symbolic link or a soft link to a different directory, Software Management Add Image or Distribution operations fail.</p> <p>Workaround:</p> <p>None.</p>
CSCsa35853	Software Management Add Image from device and Image Distribution flows fail.	<p>This occurs when there are a large number of Cisco Catalyst 2900XL and 3500XL Series Switches selected in the workflow.</p> <p>These devices will be in pre-deployed state or might have invalid Telnet credentials in the Device Credential Repository.</p> <p>The application attempts to connect to the device to obtain Flash device and image file information.</p> <p>Workaround:</p> <p>We recommend that you do not include a large number of pre-deployed Cisco Catalyst 2900XL and 3500XL Series Switches in the workflow.</p>

Table 10 **Software Management Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsa32962	<p>Device reboot fails when upgraded or downgraded to images with Cisco IOS Release 12.2(14)SY*.</p> <p>The device goes into ROMMON mode.</p>	<p>This happens when the device is upgraded or downgraded to 12.2(14)SY* versions, that is, 12.2(14)SY4, 12.2(14)SY6.</p> <p>However, Software Management operations cannot be performed after the upgrade, since the CISCO-Flash-Mib is broken.</p> <p>Workaround:</p> <p>If you have 12.2(14)SY* images, upgrade to a higher version available on Cisco.com.</p> <p>If you have to upgrade or downgrade to these versions, do not select Reboot Immediately in the Software Management Job Options window.</p> <p>Reboot the device manually.</p>
CSCsa37036	<p>copyFromFlash on Aironet device always returns Success even when there are no files on Flash.</p>	<p>This problem occurs in all Aironet devices. These devices do not have proper Flash instrumentation.</p> <p>Workaround:</p> <p>None.</p>
CSCsa22845	<p>Catalyst 5000—Discrepancy in Image Import from Device and Add Image from Network</p>	<p>Image import from the network is not supported for Catalyst 5000.</p> <p>Workaround:</p> <p>None.</p>
CSCsa39312	<p>C10700: Distribution fails because of too many boot commands.</p>	<p>If there are too many valid boot commands in the device startup-config, the boot command for the new image will not get added to device bootvar.</p> <p>This happens during device upgrade using Software Management.</p> <p>If you select the Reboot option because of this, the device is rebooted but it does not boot with the new image.</p> <p>This happens only if many valid boot commands exists on the device before upgrade through Software Management.</p> <p>Workaround:</p> <p>Remove some boot commands from startup-config before trying the Software Management job.</p>
CSCin50067	<p>CE: Reboot verification fails when comparing the image version</p>	<p>Reboot verification may fail when images with version prior to 5.1.x, are distributed to Content Engine devices. As a result, Software Management distribution jobs show the status as <code>Failed</code> although the job is successful.</p> <p>Content Engine devices running ACNS 5.1 or lower, may not return a string that indicates the build number of the software release.</p> <p>For example, ACNS 5.1.3b17 will be returned in <code>ceAssetSoftwareRevision</code> as 5.1.3.</p> <p>Workaround:</p> <p>Manually check the reload.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsa08356	Reboot verification is not performed for Standby Supervisor card	<p>This problem occurs because the image version for Standby Supervisor is not available in the MIB. This is because IOS devices do not have dual supervisor support.</p> <p>Workaround 1: Manually verify the reboot for Standby Supervisor.</p> <p>Workaround 2:</p> <ol style="list-style-type: none"> 1. Make sure the Auto Sync feature is configured in the device. By default this option is configured in the device. This will synchronize active and standby startup configurations. 2. Schedule a Software Management distribution job to copy the new image to the active supervisor by selecting active supervisor flash device. The active supervisor flash devices will not have the prefix <i>slave</i> in their display name. Do not select the Reboot Immediately after Downloading option in Distribution Job 3. Use the same device again to schedule a swim distribution job with the same new image used in Step 2 but selecting the similar standby flash device. The standby supervisor flash devices will have the prefix <i>slave</i> in their display name. For instance, if you have selected disk0 as the flash device in step2 then select slave-disk0 as the flash device now. Select Do not insert new boot commands into configuration file in Distribution Job while scheduling the second job. 4. Reboot the device after the above steps have completed successfully. Now the active and standby supervisors should be running the new image. <p>When the cat4500 devices are reloaded, there will be a switch over of the supervisors. That is the current active will become the standby and vice versa (this behaviour is different in the case of cat6500 IOS devices where the supervisors retain the same state). This can only be carried out individually for each device, since you need to select Flash devices for manual upgrade.</p>

Table 10 **Software Management Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsf28724	Device selection not properly retained when back button is pressed in SWIM Remote Staging flow.	<p>While performing Remote Staging through SWIM, the devices that are selected are not retained when the Back button is clicked. This occurs in the following flows:</p> <ul style="list-style-type: none"> • Selection of Different Devices: <ul style="list-style-type: none"> a. Select Resource Manager Essentials > Software Mgmt > Software Distribution. The Distribution Method dialog box appears. b. Select Use remote staging and click Go. The Select Remote Stage Device dialog box appears. c. Select Device A in the Remote Stage Device Selection dialog box. d. Select the Device B in the Remote Staging and Distribution dialog box. e. Click Next. f. Click Back and go to the previous screen and select another device in the Remote Stage Device Selection dialog box. g. Click Next. You will find Device A selected instead of Device B in the Remote Staging and Distribution screen.

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsf28724 (continued)		<ul style="list-style-type: none"> • Selection of same device: <ol style="list-style-type: none"> a. Select Resource Manager Essentials > Software Mgmt > Software Distribution. The Distribution Method dialog box appears. b. Select Use remote staging and click on Go. The Select Remote Stage Device dialog box appears. c. Select Device A in the Remote Stage Device Selection dialog box. d. Click Next e. Select Device B in the Remote Staging and Distribution dialog box. f. Click Next. g. Click Back and go to the previous screen and select the same device in the Remote Stage Device Selection dialog box. h. Click Next .You will find Device A selected instead of Device B in the Remote Staging and Distribution dialog box. Also the following error is displayed: You have selected the Remote Stage device for upgrade. This device cannot be upgraded in the same job. Deselect this device from the devices to be upgraded. <p>Workaround:</p> <ul style="list-style-type: none"> • Use Cancel button instead of back button in Device Recommendation dialog box. or • Deselect the remote stage device and select list of target devices again.

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCse74422	Sup3 (SUPERVISOR 3_6000) is not getting renamed to Sup720 (SUPERVISOR720_6000) when RME 4.0.4 is upgraded to RME 4.0.5 or above.	<p>When you upgrade from RME 4.0.4 to RME 4.0.5 or above, the Sup3 of Cat6k devices is not renamed to Sup720. The Sup720 was referred to as Sup3 in RME 4.0.4.</p> <p>However, it is referred to as Sup720 from RME 4.0.5 release onwards. This is the scenario for Cat6k devices running on Cat OS managed by RME.</p> <p>While upgrading from RME 4.0.4 to RME 4.0.5 or above, the Sup3 is not changed to Sup720 and so recommendation of software images from the Software Repository does not take place properly.</p> <p>Workaround:</p> <ul style="list-style-type: none"> When you are upgrading from RME 4.0.4 to RME 4.0.5 or later and the Software Repository contains any Sup3 images, you must re-add those images manually to the repository to reflect the latest image type SUPERVISOR720_6000. When you are upgrading from RME 4.0.4 to RME 4.1, you can export the Sup3 images to any directory and import it again. <p>This way the images automatically reflect as Sup720 (SUPERVISOR720_6000).</p>
CSCsd36547	CatOS image import from CCO reports Pass/Fail status as Pass.	<p>When a CatOS image is imported into RME from Cisco.com, the Image Requirements column reports NA but the PASS/FAIL column reports Pass.</p> <p>Workaround:</p> <p>None.</p>
CSCse53270	Undo does not work for successful image distribution jobs for IGESM and 2960G.	<p>When you try to undo a successful image distribution job consisting of tar images for IGESM and 2960G devices, the following error message is displayed:</p> <pre>Internal Error while fetching image information from Cisco.com. This may be caused by a runtime error. Contact Cisco TAC (Technical Assistance Center) with required debug logs.</pre> <p>This error mainly occurs for tar pre-upgrade images. Undoing a successful image distribution job works well for bin pre-upgrade images.</p> <p>Workaround:</p> <p>Add the Software tar images that existed prior to the successful image distribution to the Software repository and perform image distribution using Distribute by Device or Distribute by Image flow.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCse18070	Verification fails saying that RAM on device is not sufficient to proceed with Software image distribution for IGESM devices.	<p>During software distribution to IGESM devices, the RAM details are shown less than that is available on the devices.</p> <p>If you use a image whose minimum RAM attribute value is more than the actual RAM space available on the device, then the verification fails.</p> <p>Workaround:</p> <p>You can manually edit and downgrade the RAM attribute value for that particular image in the Software repository.</p> <p>The downgrade value should be less than the RAM available for the device.</p> <p>This workaround is not applicable for images that are selected directly from Cisco.com for distribution.</p> <p>The selecting of images directly from Cisco.com for Software distribution is also called a Slam dunk job.</p>
CSCse38083	Incompatible images are recommended during Software distribution for MDS9500 devices.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Add images for MDS9500 devices through Cisco.com to Software repository. To do this, select: RME > Software Management > Software Repository > Add Images from Cisco.com The images for Supervisor 1(Vegas) and Supervisor 2 (Isola) are not distinguished and are added to Software Repository. 2. Schedule a Software Distribution job, using either of the following flows: <ul style="list-style-type: none"> - RME > Software Management > Software Distribution > ByDevice - RME > Software Management > Software Distribution > By image Both the images are recommended. 3. Continue with the Software Distribution flow. The distribution fails because the recommended images consisted of incompatible images. <p>Workaround:</p> <p>You can select the required compatible images from the list of recommended images before proceeding with Software Distribution.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCse54126	Software Distribution and Upgrade Analysis flows show devices twice in the reports.	<p>This problem occurs in either of the following instances:</p> <p>Scenario 1:</p> <ol style="list-style-type: none"> 1. Go to RME > Software Distribution 2. Select Distribution By Devices or By Image. 3. Select an image and applicable devices. 4. Click Next <p>The Device Recommendation page appears with the selected devices appearing twice.</p> <p>Scenario 2:</p> <ol style="list-style-type: none"> 1. Go to RME > Software Distribution > Upgrade Analysis. 2. Select Cisco.com or Repository as the upgrade source. 3. Click Go. <p>The Upgrade Analysis report appears with the selected devices appearing twice.</p> <p>Workaround:</p> <p>Since both displayed reports are the same, the duplicate information can be ignored.</p>
CSCse56927	Software Distribution by device fails when the protocol used is RCP for 2960 series devices.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Software Management > Software Distribution > Distribute by devices (basic). 2. The Distribute by devices page appears. 3. Select the required devices. 4. Continue with rest of the instructions to schedule a Software distribution job. <p>The job fails if the protocol used is RCP.</p> <p>The job also fails if you use Telnet to connect to the device and try Software image distribution using manual RCP.</p> <p>Workaround:</p> <p>You can use the SCP protocol to distribute the images to devices. SCP is a more secure protocol than RCP.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCse63584	Software Distribution by device (Advanced) fails when the protocol used is RCP for IGESM series devices.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Go to RME > Software Management > Software Distribution 2. Select any of the distribution methods. 3. Continue with rest of the instructions to schedule a Software distribution job. <p>The job fails if the protocol used is RCP.</p> <p>The job also fails if you use Telnet to connect to the device and try Software image distribution using manual RCP.</p> <p>Workaround:</p> <p>You can use the SCP protocol to distribute the images to devices. SCP is a more secure protocol than RCP.</p>
CSCsf20973	Incompatible images are recommended during Software distribution for CBS3040 devices.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Add images for CBS3040 device family through Cisco.com to Software repository using RME > Software Management > Software Repository > Add Images from Cisco.com <p>The images for CBS30x0 device family are added to Software Repository.</p> <ol style="list-style-type: none"> 2. Schedule a Software Distribution job, using RME > Software Management > Software Distribution > By Device <p>Instead of recommending images applicable for CBS3040, all CBS30x0 images are recommended.</p> <ol style="list-style-type: none"> 3. Continue with the Software Distribution flow. <p>The distribution fails because the recommended images consisted of incompatible images.</p> <p>Workaround:</p> <p>You can select the required compatible images from the list of recommended images before proceeding with Software Distribution.</p>
CSCsf22065	Applicable Software images not recommended for CMM devices during Software distribution.	<p>This problem occurs when you schedule a Software Distribution job for CMM devices, using tRME > Software Management > Software Distribution > By Device</p> <p>Software images are not recommended for CMM devices.</p> <p>Workaround:</p> <p>You can select the required compatible images from the list of recommended images before proceeding with Software Distribution.</p>

Table 10 **Software Management Known Problems (continued)**

Bug ID	Summary	Explanation
CSCsh89021	RME Software Management cannot download multiple images from Cisco.com.	<p>This problem occurs when you schedule a job in RME Software Management to download multiple software images from Cisco.com to Software repository.</p> <p>The following error is displayed:</p> <p>No response stream was obtained for the download request.</p> <p>Workaround:</p> <p>Manually download images from Cisco.com and import them to Software Repository.</p>
CSCsi20525	Boot variable changed to .tar instead of .bin for image upgrade through RME Software Management for 2900x1s and 3500x1s devices.	<p>This problem occurs when you schedule image upgrade for 2900x1s/3500x1s devices through RME Software Management.</p> <p>The boot variable is changed to .tar instead of .bin.</p> <p>Workaround:</p> <ul style="list-style-type: none"> • Performs individual distribution jobs for each device (or) • Performs distribution job with single targeted image and multiple devices of same family 2900x1 or 3548x1.
CSCsi53367	Bootling of device fails when IOS image upgrade is done through RME Software Management.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> 1. Schedule a IOS software image upgrade using RME Software Management. 2. Reload the device which has undergone IOS software image upgrade. <p>Bootling of the device fails.</p> <p>When devices have more than one location to store IOS images RME does not recognize which partitions can be used for booting an IOS image. This may occur if you have selected a wrong partition.</p> <p>Workaround:</p> <p>Choose a suitable partition for the location of the new IOS image.</p>
CSCsh69321	Slamdunk distribution job fails for PIX515 devices.	<p>Schedule a Slamdunk distribution job for PIX515 devices.</p> <p>Slamdunk distribution refers to distribution of software images directly from Cisco.com to devices using RME Software Management.</p> <p>The distribution fails.</p> <p>Workaround:</p> <p>Add the image from Cisco.com to Software repository and then schedule the distribution job.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsi27337	Image filtering not proper for IOS Software Modularity images in Slamdunk and Upgrade analysis flows of RME Software Management	<p>This problem occurs in the following instances:</p> <p>Scenario 1:</p> <ol style="list-style-type: none"> Go to RME > Admin > View/Edit Preferences and select Include images higher than running image option. Try a Slamdunk distribution for a Cat6k supervisor720 device. Slamdunk distribution refers to distribution of software images directly from Cisco.com to devices using RME Software Management. None of the higher images in Cisco.com are filtered and recommended. Try Upgrade Analysis for a Cat6k supervisor720 device. None of the higher images in Cisco.com are filtered and recommended. <p>Scenario 2:</p> <ol style="list-style-type: none"> Go to RME > Admin > View/Edit Preferences and select Include images higher than running image option. Try a Slamdunk distribution for a Cat6k supervisor720 device. None of the images in Cisco.com with same image feature subset as running image are recommended. Try Upgrade Analysis for a Cat6k supervisor720 device. None of the images in Cisco.com with same image feature subset as running image are recommended. <p>Workaround:</p> <p>Do not select the filter options in the Admin page, if you expect to get the same version images in later releases with different Technology Identifiers.</p>
CSCsh29914	Inconsistency in the number of devices in Remote Staging and Distribution flow.	<p>This problem occurs when you:</p> <ol style="list-style-type: none"> Go to RME > Software Mgmt > Software Distribution > Use remote staging Click Go While selecting a remote stage device, the number of Normal devices consist only of IOS devices according to the filtering. Select a Remote stage device and click Next. Click Back and return to the same device selection screen. <p>The number of devices displayed under Normal devices is more than the number of Normal devices displayed earlier. Now the Normal devices consists of both IOS and Non IOS devices.</p> <p>Workaround:</p> <p>Manually select the devices that support remote staging before continuing with remote staging.</p> <p>For more information on the unsupported devices for remote staging, see <i>User Guide for Resource Manager Essentials 4.1</i>.</p>

Table 10 Software Management Known Problems (continued)

Bug ID	Summary	Explanation
CSCsi40639	Software images not recommended from Cisco.com for 3750 series of devices.	<p>This problem occurs in the following instances:</p> <p>Scenario 1:</p> <ol style="list-style-type: none"> 1. Go to RME > Admin > Software Mgmt > View/Edit Preferences. 2. Check the Include Cisco.com images for image recommendation option and Click Apply. 3. Schedule a slamdunk image distribution job for 3750 devices. <p>Slamdunk distribution refers to distribution of software images directly from Cisco.com to devices using RME Software Management.</p> <p>Images from Cisco.com are not recommended and the following error message is displayed:</p> <pre>SWIM0081: Cannot get any Candidate Images from the Configured Image sources. Check Software Management administration settings, add images to the library, and retry the operation.</pre> <p>Scenario 2:</p> <ol style="list-style-type: none"> 1. Go to RME > Admin > Software Mgmt > View/Edit Preferences. 2. Check the Include Cisco.com images for image recommendation option and click Apply. 3. Go to RME > Software Mgmt > Software Repository 4. Click Add without selecting any images from repository <p>The image source dialog box appears.</p> <ol style="list-style-type: none"> 5. Select Cisco.com and click Go 6. Enter your Cisco.com username and password. <p>If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.</p> <ol style="list-style-type: none"> 7. Click Next. <p>The Device Selection dialog box appears.</p> <ol style="list-style-type: none"> 8. Select the 3750 device from the Device Selection dialog box, and click Next. <p>Images are not listed in the Select cart images dialog box.</p> <p>Workaround:</p> <p>Cisco.com support is not provided for the device with:</p> <p>Sys Object id: ciscoProducts.688</p> <p>and</p> <p>Chassis Vendor Type: cevChassisCat3750Ge12SfpDc.</p> <p>You have to download the image manually from Cisco.com and add the image to repository by using RME > Software Mgmt > Software Repository > Add > From file system.</p> <p>After the image has been added to the repository, you can distribute the image to the device by using tRME > Software Mgmt > Software Distribution > by image.</p>

Table 10 **Software Management Known Problems (continued)**

Bug ID	Summary	Explanation
CSCs158585	RME deletes NVRAM configuration files from 29/35/37xx switches on executing erase flash command.	<p>The following scenario is noticed in DSBU switches (29xx, 35xx, 37xx):</p> <p>Before upgrading to a new IOS image, the RME Software Management jobs require the flash in the device to be erased due to insufficient space. For this purpose, an erase flash is performed before pushing out the new IOS image to the device, to ensure enough space is available for the image. This leads to deletion of NVRAM configuration files.</p> <p>When the device is reloaded to load the new IOS image, few issues are encountered as a result of these missing NVRAM files.</p> <p>Some of the problems are:</p> <ul style="list-style-type: none"> • SSH/HTTPS/SNMPv3 accesses are no longer possible. • ifIndex values are changed <p>Workaround:</p> <p>Before scheduling the Software distribution job ensure that you free up the space in the disk so that the application does not perform an erase flash due to insufficient space.</p>

Change Audit Known Problems

Table 11 **Change Audit Known Problems**

Bug ID	Summary	Explanation
CSCsa33492	ChangeAudit report does not export the grouped records.	<p>Only records shown in the report are exported. Other grouped records that are visible when you click More Records, are not exported.</p> <p>Workaround:</p> <p>None.</p>

Syslog Known Problems

Table 12 Syslog Known Problems

Bug ID	Summary	Explanation
CSCsb87475	Syslogs are not received when the CW Server is inside NAT/Firewall	Syslogs are not received when the CiscoWorks server is inside NAT/Firewall in Solaris. Workaround: None.
CSCsa26519	Dateline Standard Time or Greenwich Mean Time is not supported.	When you see the time zone as (GMT-12:00) Eniwetok, Kwajalein, incorrect Syslog times are sent with the Syslog messages. Workaround: None.
CSCsa33862	Error while specifying backup location.	You cannot specify a mapped drive as backup location. This results in an error message that the location does not exist or that you do not have permission to access it. Workaround: None.
CSCsa15703	MF: Create: UI alignment is lost if subfacility message type is selected	While trying to define message filters by choosing many Syslog message types, the UI alignment of the subfacility field is sometimes lost. This happens only when many Syslog message types are chosen and a scroll bar appears. After the scroll bar appears, if a message type containing a subfacility string is added, this problem is seen. Workaround: None.

Contract Connection Known Problems

Table 13 Contract Connection Known Problems

Bug ID	Summary	Explanation
CSCdm87814	RME problem with Check Contract Status, for Cat OS-based devices	If you select Resource Manager Essentials > Contract Connection > Check Contract Status, the information is generated only for Cisco IOS devices. Workaround: Get information from the Service Contract Center at: http://www.cisco.com/public/scc/

Table 13 Contract Connection Known Problems (continued)

Bug ID	Summary	Explanation
CSCsg73121	Contract Connection reports in RME appear with inconsistencies.	<p>This problem occurs while generating a Contract Connection Report.</p> <p>To get this error:</p> <ol style="list-style-type: none"> 1. Go to RME > Reports > Report Generator. 2. Select Contract Connection from the Application drop down list box, 3. Select Report Based on Contract from the Reports drop down list box, 4. Select the required devices from the Select Devices pane. 5. Select a contract from the Select Contract pane. 6. Specify the job schedule run type as Immediate. 7. Click Finish. <p>A Summary Report is displayed.</p> <ol style="list-style-type: none"> 8. From the Summary Report, click on any link under the Product Family field with corresponding one or more devices in the Devices on Network field. <p>The Contract Status Detailed Report is displayed without any rows.</p> <p>Workaround:</p> <p>Go to the Summary Report and click on a link in Product Family field, again.</p> <p>The rows appear properly in the Contract Status Detailed Report.</p>

Bug Toolkit Known Problems

Table 14 Bug Toolkit Known Problems

Bug ID	Summary	Explanation
CSCsa24273	Bug Toolkit displays different bug counts to different Users logged into Cisco.com.	<p>Data returned from the Bug Toolkit is based on the different security levels of the login IDs, when you use different login IDs to generate the report.</p> <p>Workaround:</p> <p>None.</p>
CSCsa47066	For some bugs, the Locate Devices flow does not display correct devices	<p>For some bugs, the Locate Device flow does not display the correct devices that are affected.</p> <p>This problem can occur at any time.</p> <p>Workaround:</p> <p>None.</p>

Server, Browser, UI, and Desktop Known Problems

Table 15 Server, Browser, UI, and Desktop Known Problems

Bug ID	Summary	Explanation
CSCsa95781	CTMJrmServer goes down after changing to the ACS mode.	<p>The CTMJrmServer process may go down in either of these cases with respect to ACS configuration:</p> <ul style="list-style-type: none"> When you change the AAA setup from the CiscoWorks local mode to the ACS mode (through Common Services > Server > Security > AAA Mode Setup) and register with ACS by enabling the Register all installed applications with ACS option in the AAA Mode Setup dialog box. When you re-register the applications with ACS (by enabling the Register all installed applications with ACS option in the AAA Mode Setup screen) while in the ACS mode. <p>The CTMJrmServer process may go down because of authorization failure at startup. This happens because the System Identity user is not configured properly in ACS.</p>
CSCsa95781	CTMJrmServer goes down after changing to ACS mode. (Continued)	<p>The reasons for CTMJrmServer process to go down in the above cases can be:</p> <ul style="list-style-type: none"> System Identity user (in the System Identity Setup dialog box under Common Services > Server > MultiServer Trust Management > System Identity Setup) is not configured in ACS. <p>Or</p> <ul style="list-style-type: none"> The System identity user configured in ACS does not have the necessary JRM job privileges. <p>Workaround:</p> <ol style="list-style-type: none"> After making the ACS-related security changes, ensure that the System Identity user is configured properly in ACS with the necessary JRM job privileges. To configure the System Identity user, use the System Identity Setup dialog box under Common Services > Server > MultiServer Trust Management > System Identity Setup. Restart the CTMJrmServer process and the other dependent processes (such as Syslog).
CSCsa89512	Difference in log file time-stamp and system time	<p>The time-stamp in the stdout.log file is different from the system time.</p> <p>This occurs only on some Solaris machines.</p> <p>Workaround: None.</p>

Table 15 Server, Browser, UI, and Desktop Known Problems (continued)

Bug ID	Summary	Explanation
CSCin03389	Adhoc template displays <i>Failed</i> for some catalyst devices.	A successful job will be displayed as <i>Unsuccessful</i> . Workaround: Disable debug in the device and run the job.
CSCsf32067	Extra grey spaces appear in few SWIM workflows if number of rows returned is less than 10.	Extra grey spaces appear in following SWIM workflows: <ul style="list-style-type: none"> • Go to RME > Software Mgmt > Software Repository <ul style="list-style-type: none"> a. Click on Add button. The Add Images dialog box appears. b. Select any one of the options: <ul style="list-style-type: none"> Cisco.com Device File System Network Out of Sync report • Go to RME > Software Mgmt > Software Distribution > Upgrade Analysis > Cisco.com • Go to RME > Software Mgmt > Software Distribution > By devices (Advanced) <p>The resulting rows for the above mentioned flows, if less than 10, appears with extra grey space.</p> Workaround: None.
CSCse85024	If you use the Select All option to select 10000 devices in the Search Results tab of RME Device Selector, it takes a long time.	To select 10000 devices using Device Selector: <ol style="list-style-type: none"> 1. Go to any device selector of RME 2. Search for all devices by entering * as the search criteria. All the 10000 devices will be listed. 3. Click the Select All check box in the Search Results tab. <p>It takes more time for all the devices to be selected in the Device Selector.</p> Workaround: None.

Common/Other Known Problems

Table 16 Common/Other Known Problems

Bug ID	Summary	Explanation
CSCsa38849	Ctrl+N and Open in New Window result in unexpected behavior in RME.	RME shows unexpected behavior when you open a new window during any of the work flows. This happens if you press Ctrl+N or select Open in New Window and continue to work on the same flow as the base window. However, two different workflows (not under the same tab) does not cause a problem. Workaround: None.
CSCin17659	RME saves reports as .pl files when using Netscape.	In Netscape, if the file type exported is not pre-configured. The bug reports are saved as .pl files instead of .txt files. Workaround: Add the file type manually. To do so, select Edit > Preferences and specify the default application to open the file.
CSCsa29250	Cannot filter devices based on user-defined fields	Devices cannot be filtered based on User-defined fields. Workaround: Create device groups in Common Services based on user defined fields and use these in the RME workflows. See the User Guide for Common Services 3.0.3 for details on creating Device groups with user-defined fields.

Table 16 Common/Other Known Problems (continued)

Bug ID	Summary	Explanation
CSCSa17529	Special characters such as single quotes, are not supported in a report template name.	<p>When you click on a template name that has unsupported characters (such as single quotes in the link) in the report template table, the following error appears:</p> <p>Page cannot be displayed.</p> <p>This happens only if you use a special character such as single quote in the template name while creating the template.</p> <p>Workaround:</p> <p>Use only this supported character set: {A to Z, a to z, 0 to 9, -, _, .,), (, / and blank space}</p>
CSCSa58546	RME cannot create device groups based on display name attributes	<p>In RME, device groups cannot be created based on the domain name and display name configured in DCR (Device Credential Repository).</p> <p>In RME, a device group can be created, based on device sysName and domain name obtained from device and stored as inventory data.</p> <p>However, these are not the same as the display name and the domain name that is configured in DCR.</p> <p>Therefore, if you create a filter for sysName but if the sysName is not the same as the name of the device in DNS (or the display name), you cannot not see any of your devices that match the filter.</p> <p>In such a case, even hostnames and DNS names with differing cases do not match.</p> <p>Workaround:</p> <p>Create the required device group in Common Services based on DCR's display name domain name. The same groups can be seen in RME flows and can be used.</p>

Resolved Problems in RME 4.1

This section has resolved problems from RME 4.1.

Table 17 describes the problems that were resolved in RME 4.1:

Table 17 **Resolved Problems in RME 4.1**

Bug ID	Component	Summary
CSCsc46237	Restore operation failed with an insufficient disk space error.	This problem has been resolved.
CSCse13013	When an Inventory Collection job was scheduled from RME > Devices > Inventory > Inventory Jobs the scheduled job remained in a running state for a long time. This occurred even if the job was scheduled for a single device.	This problem has been resolved.
CSCsc31440	RME detailed device report showed incorrect serial number for Cat2950	This problem has been resolved.
CSCsf32082	The UI for SFS device category under Netconfig templates were not consistent with other device category UIs.	This problem has been resolved.
CSCsb40088	The Inventory > Hardware Report did not populate RAM, NVRAM, Used NVRAM fields for most CatOS switches in RME 4.0.x.	This problem has been resolved.
CSCsb36330	cwcli export config did not export configuration data to standard output.	This problem has been resolved.
CSCsb84712	When there were more than 9 instances of a job, sorting of the Job ID field in the RME Job Browser is incorrect.	This problem has been resolved.
CSCsa36663	Location of archived reports could not be changed in RME 4.0.x.	This problem has been resolved.
CSCsb56985	Defect subject link did not work properly in Bug Details Report.	This problem has been resolved.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

This document is to be used in conjunction with the documents listed in the [Product Documentation](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Release Notes for Resource Manager Essentials 4.1

Copyright © 2007, Cisco Systems, Inc.

All rights reserved