



Release notes

EPM 5.1
Enterprise Policy Manager
Document Status: **Standard**
Document Number: **NN48011-400**
Document Version: **02.03**
Date: **December 2010**

© 2010 Avaya Inc.
All Rights Reserved.

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://SUPPORT.AVAYA.COM/LICENSEINFO/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and/or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Contents

Chapter 1	
Getting started	5
About this guide	5
Audience	5
Symbols and text conventions	6
Related publications	8
How to get Help	9
Chapter 2	
Enterprise Policy Manager	11
Operational notes	11
Installation	11
EPM data migration	11
Backup and Restore	11
Known issues	12
Limitations	12
Chapter 3	
UCM Common Services	13
Operational notes	13
Installation	13
Security	14
Backup and restore	15
Device and server credentials	15
License	15
User interface	16
Known issues	16
Limitations	16

Chapter 1

Getting started

Enterprise Policy Manager (EPM) is a system-level software application for implementing policy-based management in the enterprise environment. You use EPM to create, deploy, and manage the policies that you have designed to provide the policy framework for your network. You can use EPM to:

- prioritize network traffic and allocate computing resources
- control the quality of service (QoS) experienced by networked applications and users, including voice and video
- establish and maintain a high level of flexible network security and establish user-based policies in networks that support IEEE 802.1x with Extensible Authentication Protocol
- provide a way to direct and control service levels and performance management

About this guide

This guide is part of the EPM documentation suite and lists the release notes associated with the EPM 5.1.

Audience

This guide is intended for network engineers and administrators who use the Enterprise Policy Manager to configure and manage networks. This guide is based on the assumption that you have the following background:

- understanding of networking terminology, theories, and practices
- knowledge of the Windows operating system or Linux systems and graphical user interfaces (GUI)

Symbols and text conventions

These symbols highlight critical information for the NRM system:



Caution: Alerts you to conditions where you can damage the equipment.



Danger: Alerts you to conditions where you can get an electrical shock.



Warning: Alerts you to conditions where you can cause the system to fail or work improperly.



Tip: Alerts you to additional information that can help you perform a task.



Note: A Note alerts you to important information.



Security Note: Indicates a point of system security where a default should be changed, or where the administrator needs decide the level of security required for the system.



Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.



Warning: Alerts you to remove the NRM main unit and the expansion unit power cords from the AC outlet before performing any maintenance procedure.

These text conventions are used in this guide to indicate the information described:

Convention	Description
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the info command. Example: Enter show ip {alerts routes} .
<i>italic text</i>	Indicates book titles

Convention	Description
plain Courier text	Indicates command syntax and system output (for example, prompts and system messages). Example: <code>Set Trap Monitor Filters</code>
angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: <code><InstallDir>\database\tftp</code>
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is <code>setAccess {o g w}</code> , you must enter <code>setAccess o</code> , <code>setAccess g</code> , or <code>setAccess w</code> .
brackets ([])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is <code>echo [-newline]</code> , you can enter either <code>echo</code> or <code>echo -newline</code> .
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is <code>which [<command_name>] . . .</code> , you enter <code>which</code> and as many command names as needed.
<i>italic text</i>	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is <code>spawn telnet <ip_address></code> , you enter <code>spawn telnet 192.48.33.7</code> .
separator (>)	Shows menu paths. Example: Choose View > Sort > by Name.
vertical line ()	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is <code>array NewArray = [<reference> <referenceList>]</code> you enter either <code>array NewArray = <reference></code> or <code>array NewArray = <referenceList></code> , but not both.

Related publications

For more information about using EPM, refer to the following publications:

- *EPM Fundamentals (NN48011-100)*
- *EPM Installation Guide (NN48011-300)*
- *EPM Configuration - Devices (NN48011-500)*
- *EPM Configuration - Policies (NN48011-501)*
- *EPM User-Based Policies (NN48011-502)*
- *EPM Administration (NN48011-600)*

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- “Getting technical documentation”
- “Getting product training”
- “Getting help from a distributor or reseller”
- “Getting technical support from the Avaya Web site”

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 2

Enterprise Policy Manager

This guide lists the release notes associated with the EPM 5.1.

This chapter provides the following information:

- [“Operational notes” on page 11](#)
- [“Known issues” on page 12](#)
- [“Limitations” on page 12](#)

Operational notes

This section provides operational notes for the Enterprise Policy Manager 5.1 release.

Installation

When you install EPM 5.1, you must uninstall any previous installation of EPM before you begin.

EPM data migration

You can use the EPM Data Migration Tool available on the UCM page to migrate EPM data from release 4.3 to release 5.1.

To migrate EPM data between EPM 5.0 and EPM 5.1, perform the following steps:

- 1 Run the backup script on the EPM 5.0 machine.
- 2 Run the `restoreAllData.bat` (Windows) or the `restoreAllData.sh` (Linux) script from `[UCM_HOME]/bin`.
- 3 Run the `upgradePatch.bat` (Windows) or `upgradePatch.sh` (Linux) script in `[EPM_HOME]`.

Backup and Restore

You can use the backup and restore script to migrate EPM data within the 5.1 release.

Known issues

The following table lists the known issues and workarounds for EPM 5.1.

Table 1 Known issues and workarounds

CR Number	Description
Q02003002	After the maximum session time, the session expires although you chose to disable the feature. Workaround: User needs to login back to UCM page and launch EPM.
Q02019274	8600Legacy: Old filters are not deleted when performing policy reload. Workaround: The filters need to be deleted manually from the device.
Q02027179	SR4k:Filters not removed if device is deleted when network connection is down. Workaround: The filters need to be deleted manually from the device.
Q02030082	SR4k :IM unresponsive if modify policy when network conn. is down (Intermittent). Workaround: Restart the Interface Manager.
Q02037518	Uninstaller loops when use an empty password. Workaround: Kill the uninstaller process and restart the uninstaller.

Limitations

The following table lists the limitations for EPM 5.1.

Table 2 Limitations

CR Number	Description
Q02024488	COPS: After deleting a cops device twice, it reappears as duplicate.
Q02027111	8600Legacy: A filter with Src/Dst port and with operator 'ne' is not retrieved.
Q02037650	8600 R: Java exception when import filters having TCP/UDP port criteria.
Q02038329	Scenario2: all NMOS components are installed with non default HTTP/S ports-Issue.

Chapter 3

UCM Common Services

This guide lists the release notes associated with the UCM Common Services.

This chapter provides the following information:

- [“Operational notes” on page 13](#)
- [“Known issues” on page 16](#)
- [“Limitations” on page 16](#)

Operational notes

This section provides operational notes for the UCM Common Services. It provides information on the following topics:

- [“Installation” on page 13](#)
- [“Security” on page 14](#)
- [“Backup and restore” on page 15](#)
- [“Device and server credentials” on page 15](#)
- [“License” on page 15](#)
- [“User interface” on page 16](#)

Installation

- English is the only language supported.
- Installation locations of the product and common services are greyed out. They can only be changed by clicking the 'Choose' button.
- If MySQL is already existing in the system and running, it needs to be stopped so that the Avaya UCM MySQL can be installed.
- Ports in the 1-1023 range (other than 80 and 443 for HTTP/HTTPS) should not be used. These are TCP/UDP ports that are used by a variety of applications : FTP (20,21), Telnet 23, SNMP 161 and so on. Choosing them may result in applications not working and other conflicts.
- Information about type of server:
 - Primary Security Server - Security Administration is installed.
 - Member Security Server - Security Administration not installed, redirected to primary server.

- Backup Security Server - Takes over the function of primary in case of primary server failure.
- Central Server - Device Credentials and License Module are installed.
- Check the host file entries on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts). Correct format of Fully-Qualified Domain Name (FQDN):

```
127.0.0.1    localhost
102.54.94.97 rhino.acme.com  rhino
```

Note: The value of FQDN mapped in hosts file will appear as default on Windows, and if it is DNS resolvable, also on Linux. Otherwise, the FQDN will have to be inserted manually. When multiple networks interfaces are active, the FQDN must be inserted manually. An eventual default value is not guaranteed to be the desired one. In member or backup mode installation, the hosts file should have entry for primary server. In non-central mode installation, the hosts file should have entry for central server.

- Add the server IPs(primary/member/backup) to hosts file on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts).
- High availability is not supported for Device Credentials and Licensing modules. Single Sign-on supports high availability. If a server having Device Credentials and Licensing modules is down/uninstaller/removed all other nodes referring to the server will not have access to Device Credentials and Licensing modules.
- If a primary server is restarted backup and member servers also need to be restarted. Order of restart should be primary, backup, member.
- On IE7 after login if you see a blank page <https://your-fqdn.com/securityserver/UI/> blank . Got to Tools > Security > Click "Restore all zones to default level"
- FQDN needs to have minimum 2 dots.
- When pointing to a CS1k as primary:
 - a) The first product (EPM,NRM/VPFM/IPFM) pointing to CS1k primary needs to be a member. If its absolutely necessary to install the product in backup mode the destination xml files under `JBOSS_HOMEserver\default\deploy-hasingleton\jms\clusteredDestinations` need to be copied manually to the primary
 - b) Q02038117 : If there was/is any product(EPM,NRM/VPFM/IPFM) using CS1k as primary the CS1k jboss needs to be restarted before installing the new product.

Security

- The default SSO token timeout is 120 minutes, regardless of whether there are user activities or not on a session. Additionally, The default idle timeout is 30 minutes, this is affected by user activities.

- The Active Session list in quantum administration page will list all the sessions that are not logged out and are within the application timeout limit.
- Application certificate is the server-side certificate created at installation time and there is 'client.truststore' file corresponding to it (for client-side calls) in the UCM installation folder. At any time users should not change the application's default certificate. Trying to change the application certificate might break some of the security functionalities. (Q01917319)
- IE7 will warn about the Certificate as the product certificate is not verified by the third party certificate authority(CA). User can avoid this warning by changing the IE setting in the advanced tab(Q01921773).
- Firefox issue: Some times we see a error in firefox "Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. (Error code: sec_error_reused_issuer_and_serial)" This happens when the browser is not clearing the cached certificates. Closing the browser might not help. Kill the firefox process and restart the browser. To get the process id "ps -ef | grep firefox" .
- Registration of member/backup to primary is automated. But deregistration after a member/backup is uninstalled is manual. User need to remove the uninstalled member/backup from the elements table via the Security Administration screens.
- When using localhost or IP address in the browser address bar to access UCM page, user will be taken to a login page with a link 'Go to central login for Single Sign-On', clicking the link will switch the url in the address bar to FQDN. Note: Always use FQDN to access UCM page, single-sign-on is only supported on FQDN.

Backup and restore

- Backup and restore can only be run by users in 'Administrators' group (in Windows) or 'root' group (in Linux).
- Stopping backup or restore in the middle of the process (for example by pressing Ctrl-C) is not a supported scenario. The database and system state wont be guaranteed to be stable if this is done. To reduce possibility of users doing this, a warning message will be displayed at the beginning of backup and restore process.
- Restore of users and roles is not supported.
- Restoring will only append the backed up data to the database. Any updates/changes between Backup Restore operation will remain.
- Restoring Device Credentials will replace existing data.

Device and server credentials

- Spaces are not allowed in the device credential ranges.

License

- A known drawback of MacroVision license is that for the Linux platform the user can only use the MAC address associated with the eth0 interface of the server. MAC addresses associated with any other interface would deem the application unlicensed.

- Q02038117 : Export functionality: Selecting multiple rows of same product name might cause unexpected error. By selecting a product row, application exports all the licenses of the product name on all the connected UCM hosts(primary/member/backup).

User interface

- The login warning banner contains "[company name]" instead of a value.To modify it, go to Security Administration -> Security -> Policies. Then click on "Edit" for Security Settings. See ECC-318

Known issues

The following table lists the known issues and workarounds for UCM Common Services.

Table 3 Known issues and workarounds

Issue	Description
IPv6	<p>Problem observed when starting JBoss on Linux. At startup, JBoss is trying to bind an IPv6 IP and it fails. The result is that JBoss is not correctly started.</p> <p>This is happening due to a known bug from JDK 1.5 that was solved in JDK 6. Here is the JIRA issue for this problem:</p> <p>http://jira.jboss.com/jira/browse/JGRP-47</p> <p>Workaround: Add the following option in JBoss startup script (until the switch to JDK 1.6):</p> <p>Djava.net.preferIPv4Stack=true</p> <p>See the JBoss wiki for more information about this issue, at the following location:</p> <p>http://wiki.jboss.org/wiki/IPv6</p> <p>This issue and workaround only apply to hybrid boxes (having both IPv4 and IPv6 support). There is no workaround for pure IPv6 boxes.</p>

Limitations

The following table lists the limitations for UCM Common Services.

Table 4 Limitations

CR Number	Description
Q02038860	Cannot add a IPv6 Address Range in Device and Server Credentials.