



# **Avaya Bulk Configuration Manager Fundamentals**

Release 3.1  
NN48021-100  
Issue 05.01  
August 2014

© 2014 Avaya Inc.

All Rights Reserved.

## Notice

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

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 Avaya hardware and software. 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 website: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

## Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

## Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product 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 unless expressly authorized by Avaya. 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

## Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can

result in substantial additional charges for your telecommunications services.

#### **Avaya Toll Fraud intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

#### **Trademarks**

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(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, Hosted Service(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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

#### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

#### **Contact Avaya Support**

See the Avaya Support website: <http://support.avaya.com> for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

<b>Chapter 1: Introduction</b> .....	8
Purpose.....	8
Related resources.....	9
<b>Chapter 2: New in this release</b> .....	11
Features.....	11
Architecture.....	11
Browser requirements.....	11
Client requirements.....	12
Server requirements.....	12
Supported devices.....	12
CLI mode support for ERS 8600/8800.....	13
Obtaining a BCM license.....	13
<b>Chapter 3: Overview</b> .....	14
Logon page.....	14
Configuration Backup and Restore.....	14
Configuration Update Generator.....	18
Device Password Manager.....	20
Inventory.....	22
Log Browser.....	23
License.....	24
Scheduler.....	25
Software Version Updater.....	27
Tunnelguard Distributor.....	29
<b>Chapter 4: Avaya BCM licensing</b> .....	31
Prerequisites.....	31
Node based licensing for BCM.....	31
Interaction with Avaya BCM tools.....	32
Licensing failure.....	32
License information.....	32
Obtaining a license.....	33
Obtaining a BCM license to be installed on a physical server.....	33
Obtaining a BCM license to be installed on a Virtual Machine.....	35
Installing an Avaya Bulk Configuration Manager license.....	37
<b>Chapter 5: Administration tools</b> .....	40
Network device configuration and management.....	40
Creating template files.....	40
Configuration files and tasks management.....	42
Uploading a user-defined configuration file.....	42
Removing a user-defined configuration file from the Avaya BCM server.....	43

Viewing or editing a user-defined configuration file.....	43
Exporting a user-defined configuration files.....	43
Creating a CUG task.....	44
Filtering the CUG tasks view.....	44
Duplicating a CUG task.....	44
Editing a CUG task.....	45
Deleting a CUG task.....	45
Executing a configuration task.....	46
Viewing the progress of a configuration task.....	46
CUG Wizard.....	46
Variable definitions.....	47
Launching the CUG Wizard.....	47
Creating a task.....	48
Variable definitions.....	49
Creating a template file.....	50
Variable definitions.....	50
Editing a template file.....	51
Variable definitions.....	52
Creating a variable mapping file.....	53
Variable definitions.....	53
Scheduling and saving a task.....	54
Variable definitions.....	55
Variable definitions.....	55
Logging and log browsing.....	56
Refreshing the logs list.....	56
Filtering the logs.....	56
Configuring log settings.....	56
Customizing the Log Browser list view.....	57
Clearing all view filtering.....	57
Exporting log browser information.....	58
Inventory management.....	58
Adding devices to Inventory.....	58
Filtering the devices.....	59
Duplicating devices in the Inventory.....	59
Editing items in the Inventory.....	60
Importing devices to Inventory.....	60
Exporting devices to .csv file.....	61
Removing items from the Inventory.....	62
Importing devices from COM.....	62
Device Password Manager.....	62
Managing DPM tasks.....	62
Creating a DPM task.....	63
Filtering the DPM tasks.....	63

Duplicating a DPM task.....	63
Editing a DPM task.....	64
Executing a DPM task.....	64
Deleting a DPM task.....	64
Viewing the progress of a password management task.....	65
Software version upgrades.....	65
Managing software version images on the file server.....	65
Adding an image package to the file server.....	65
Removing an image package from the file server.....	66
Editing files from a package.....	66
Creating an SVU task.....	66
Filtering the SVU tasks.....	67
Duplicating an SVU task.....	67
Running an SVU task.....	68
Editing an SVU task.....	68
Deleting an SVU task.....	68
Viewing the progress of a software update task.....	69
Configuration Backup and Restore.....	69
Managing the backup tasks.....	69
Managing the restore tasks.....	75
Scheduling tasks on Avaya BCM.....	78
Adding a schedule.....	78
Filtering the schedule tasks.....	79
Editing a schedule.....	79
Deleting a schedule.....	79
Refreshing the schedule list.....	80
Security management.....	80
TunnelGuard Distributor.....	80
Adding previously created TunnelGuard policies.....	80
Filtering the TGD tasks.....	81
Duplicating a TGD task.....	81
Editing a TGD task.....	82
Deleting a TGD task.....	82
Executing a TGD task.....	82
Viewing the progress of a tunnelguard task.....	83
<b>Chapter 6: Directory structure.....</b>	<b>84</b>
<b>Chapter 7: Troubleshooting.....</b>	<b>85</b>
Firewall Configuration.....	85
FTP servers.....	85
NAT.....	85
Saving CLI/ACLI correspondence with a device to a file.....	85
Terminal length.....	86
COM e-mail settings.....	86

**Chapter 8: Device types and limitations**..... 89

**Chapter 9: SVU file types**..... 91

**Chapter 10: Sample configuration scripts**..... 93

    VPN router configuration..... 93

    NSNAS and VPN gateway configuration..... 94

    Secure Router 1001, 1001s, 1002/1004, 3120, and 4134 configuration..... 95

    Avaya Ethernet Routing Switch 2500, 4500, and 5500 configuration..... 96

    Avaya Ethernet Routing Switch 8300 and 8600 configuration..... 98

# Chapter 1: Introduction

## Related Links

[Purpose](#) on page 8

[Related resources](#) on page 9

---

## Purpose

This document provides information about the Avaya Bulk Configuration Manager (Avaya BCM) application and includes procedures for configuring and using Avaya BCM to manage your network. Avaya BCM is an application in the Avaya Aura System Manager solution and consists of a suite of tools that allow you to perform a variety of management tasks across multiple device types using a Web-based interface.

The *Avaya Bulk Configuration Manager Fundamentals* guide is intended for administrators, and provides information about the Avaya BCM application, and how to use it to manage your network. You install the Avaya BCM with the Configuration and Orchestration Manager (COM); you cannot install the Avaya BCM as a standalone product. To use the Avaya BCM, you must install the Avaya BCM license.

---

## Acronyms

The following table lists the abbreviations that appear in this document.

Acronym	Description
CBR	Configuration Backup and Restore
CUG	Configuration Update Generator
DPM	Device Password Manager
BCM	Avaya Bulk Configuration Manager
SNAS	Secure Network Access Switch
SVU	Software Version Updater
TGD	Tunnelguard Distributor
SMGR	Avaya Aura <sup>®</sup> System Manager



---

## Related resources

### Related Links

- [Introduction](#) on page 8
- [Documentation](#) on page 9
- [Training](#) on page 9
- [Viewing Avaya Mentor videos](#) on page 9
- [Support](#) on page 10

---

## Documentation

See the following related documents:

Title	Purpose	Link
Avaya Configuration and Orchestration Manager Fundamentals (NN47226-100)	Fundamentals	<a href="http://support.avaya.com">http://support.avaya.com</a>
Avaya Configuration and Orchestration Manager Installation (NN47226-300)	Deployment	<a href="http://support.avaya.com">http://support.avaya.com</a>
Avaya Configuration and Orchestration Manager Administration (NN47226-600)	Administration	<a href="http://support.avaya.com">http://support.avaya.com</a>
Avaya Bulk Configuration Manager Fundamentals (NN48021-100)	Fundamentals	<a href="http://support.avaya.com">http://support.avaya.com</a>
Avaya System Manager Common Services Fundamentals (NN48014-100)	Fundamentals	<a href="http://support.avaya.com">http://support.avaya.com</a>

### Related Links

- [Related resources](#) on page 9

---

## Training

Ongoing product training is available. For more information or to register, you can access the Web site at <http://avaya-learning.com/>.

### Related Links

- [Related resources](#) on page 9

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

## About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

## Procedure

- To find videos on the Avaya Support site, go to <http://support.avaya.com> and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

### **Note:**

Videos are not available for all products.

## Related Links

[Related resources](#) on page 9

---

## Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

## Related Links

[Related resources](#) on page 9

# Chapter 2: New in this release

The following sections detail what is new in *Avaya Bulk Configuration Manager Fundamentals* (NN48021–100) for Release 3.1.

- [Features](#) on page 11

---

## Features

See the following section for information about feature changes.

---

## Architecture

Prior to Release 3.1, the Avaya Configuration and Orchestration Manager (COM) application was deployed on the Unified Communications Management-Common Services (UCM-CS) platform. In Release 3.1, COM is deployed on the System Manager-Common Service based on Avaya Aura System Manager version 6.3.

As a result of Avaya's strategic decision to use a single platform for all J2EE applications, the System Manager (SMGR) platform was chosen. SMGR is a J2EE compliant platform already being used in Avaya's Aura products. Like all other SMGR applications, COM 3.1 migrates from the UCM-CS platform to SMGR-CS platform. SMGR-CS is a scaled down SMGR platform that contains only those platform services required for Avaya NMS applications. COM 3.1 moves to SMGR platform that further provides a common integrated management solution for Avaya voice and data customers.

For more information about the SMGR-CS platform, refer to *Avaya System Manager Common Services Fundamentals* (NN48014-100).

---

## Browser requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports Internet Explorer versions 8.x, 9.x, and 10.x, and Firefox versions 19, 20, and 21.

## Client requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports Internet Explorer versions 8.x, 9.x, and 10.x, and Firefox versions 19, 20, and 21.

## Server requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 is supported on the following servers:

- Red Hat Enterprise Linux v5.6 and v5.7 (both 64-bit only)
- Microsoft Windows 2008 Server R2 (64-bit, standard and enterprise flavors)

**\* Note:**

The server requirements apply to a new installation of COM Release 3.1 and to an upgrade to COM 3.1.

## Supported devices

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports the following new devices and new software versions.

Device	Support	Version
ERS 45xx and ERS 48xx	Full	5.6.3 and 5.7
	Partial	5.8 (Discovery and EDM Plugin launch)
ERS 5000	Full	6.2.7, 6.3.1, and 6.6
VSP 8000	Full	4.0
ERS 3500	Full	5.1.1 and 5.2
VSP 4000	Full	3.0.1 and 3.1
	Partial	4.0 (Discovery and EDM Plugin launch)
VSP 9000	Full	3.4 (Sapphire Chassis) and 4.0
VSP 7000	Full	10.2.1, 10.3, and 10.3.1
	Partial	Discovery and EDM Plugin launch) for 10.3.1 (New model type support - VSP 7024XT)

---

## ACLI mode support for ERS 8600/8800

Avaya Command Line Interface (ACLI) is a text-based interface used to configure, manage, and monitor the Avaya devices. Earlier releases of Avaya Configuration and Orchestration Manager (COM) supported ERS8x00 devices running in Passport CLI only.

COM Release 3.1 supports Passport CLI and ACLI mode for ERS8600/ERS8800 v7.2 and v7.2.10, and ERS8300 v4.2 devices.

ACLI features are supported in the following modules:

- BCM tools
  - Backup and Restore
  - Configuration Update Generator
  - Device Password Manager
  - Software Version Updater
- Configuration Auditing Tool
- Inventory Manager
- Wizard
  - SMLT wizard
  - VSN wizard

For information about ACLI and Passport CLI commands for ERS8600/ERS8800 and ERS8300 devices, see *Avaya Command Line Interface Commands Reference* (NN46205–106) and *Command Line Interface Reference* (NN46205–105), respectively.

---

## Obtaining a BCM license

You can obtain a BCM license from the FlexLM licensing service to be installed on a physical server or on a virtual machine.

For more information about obtaining a BCM license, see [Obtaining a license](#) on page 33.

---

## Bug fixes

For more information about bugs that have been fixed for Avaya Configuration and Orchestration Manager (COM) release 3.1, see *Avaya Configuration and Orchestration Manager Release Notes*.

# Chapter 3: Overview

Avaya Bulk Configuration Manager (Avaya BCM) is an application in COM which is part of the Avaya System Manager (SMGR) solution. Avaya BCM consists of a suite of tools that allow you to perform a variety of management tasks across multiple device types using a Web-based interface.

Avaya BCM provides the following tools:

- Configuration Backup and Restore
- Configuration Update Generator
- Device Password Manager
- Inventory
- Log Browser
- License
- Scheduler
- Software Version Updater
- TunnelGuard Distributor

---

## Logon page

To access the Avaya BCM, you must log on to the SMGR-CS and start the COM application, you then can launch the BCM Manager. The Avaya BCM contains a default administrative account with a user name admin. The initial password is **admin123**. If no activity occurs on the Avaya BCM web client for 30 minutes, the idle timer expires. If there is activity, the session timer expires after 1440 minutes. In both cases you attempt to use the client again, you are redirected to the logon page and must log on again. The idle timer and the session timer can be configured in the Security Management page.

---

## Configuration Backup and Restore

You can use the Configuration Backup and Restore (CBR) tool to back up and restore device configuration parameters. You can configure the COM application to perform a backup diff based on a previous config or baseline. When the backup occurs, the system generates a readable copy of

the running device configuration. You can use these readable files to list diff values for a selected device in a report format.

When you create a backup task, you also can set up an e-mail alert function to e-mail the diff between backups. The config diff settings that you set in the diff type preferences determine what the system e-mails and when.

## Backup and restore tool

During the backup process, a human readable text format of the saved configuration is created for all the supported devices except BSR-s. This file is automatically saved in the backup archive in compare folder on COM/BCM server. The windows default subdirectory for the file save is `C:\Avaya\smgr\COM\Avaya\Diff\device IP Address`. The Linux default folder for the file save is `/opt/avaya/smgr/com/avaya`

### Note:

This backup file is for restore archive comparison only and it must not be applied to the device during restore procedure.

Backup uses FTP, SFTP, SCP, and TFTP protocols for transporting configuration files from or to the devices; therefore keep the ports used by these protocols open.

### Important:

For those devices that have FTP servers, it is mandatory to enter the FTP credentials for the server in the Credentials page so that Avaya BCM can use it. For those devices that have SFTP servers or support SCP protocols for transferring files, it is mandatory to enter the SSH credentials for the server in the Credentials page so that Avaya BCM can use it.

The CBR tool automatically reboots the device after a restore operation.

## Reporting feature

The reporting feature works in tandem with the backup and restore tool. You can use the reporting feature to run diff reports on any device that has more than one backup. This report feature allows you to select the devices and the backups you wish to see in the diff report. You have the option to see your report in either an html or a pdf format.

## E-mail alert function

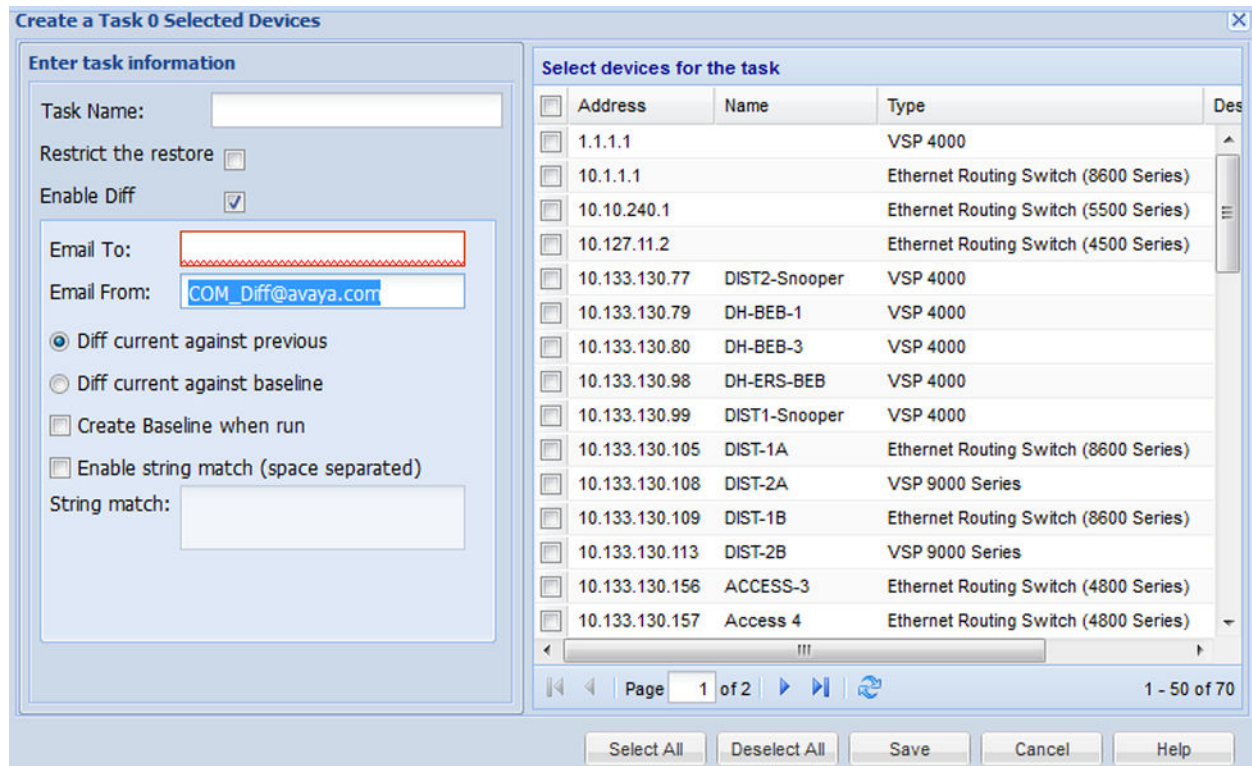
The BCM e-mail alert function requires the user to have the COM 3.1 upgrade 1200-1500 license.

When configured correctly, you can direct the system to e-mail a backup diff. The system sends an e-mail that contains the diff between backup copies based on your diff type preferences: the diff between a previous backup or a baseline. The system generates an e-mail alert after the first two backup events have occurred for the same device.

The e-mail alert is sent to the user that you designated in the SMTP preference during the setup. All changes on the devices that are recorded by the system are presented in the e-mail alert. Changes include device configuration changes, additions, and removals.

You can use the diff type settings to determine when the system sends an e-mail alert and what the alert contains. When you create a backup task, you can specify a string match value. If the string value in the diff type settings match diff lines in the backup, the system sends an e-mail alert. The e-mail alert only contains backup information for the device that contains your string match value.

The following figure is an example of the Create a Task dialog box with Enable Diff selected to configure the e-mail function.



For more information about the e-mail feature, see [Creating a configuration backup task](#) on page 70.

## User interface

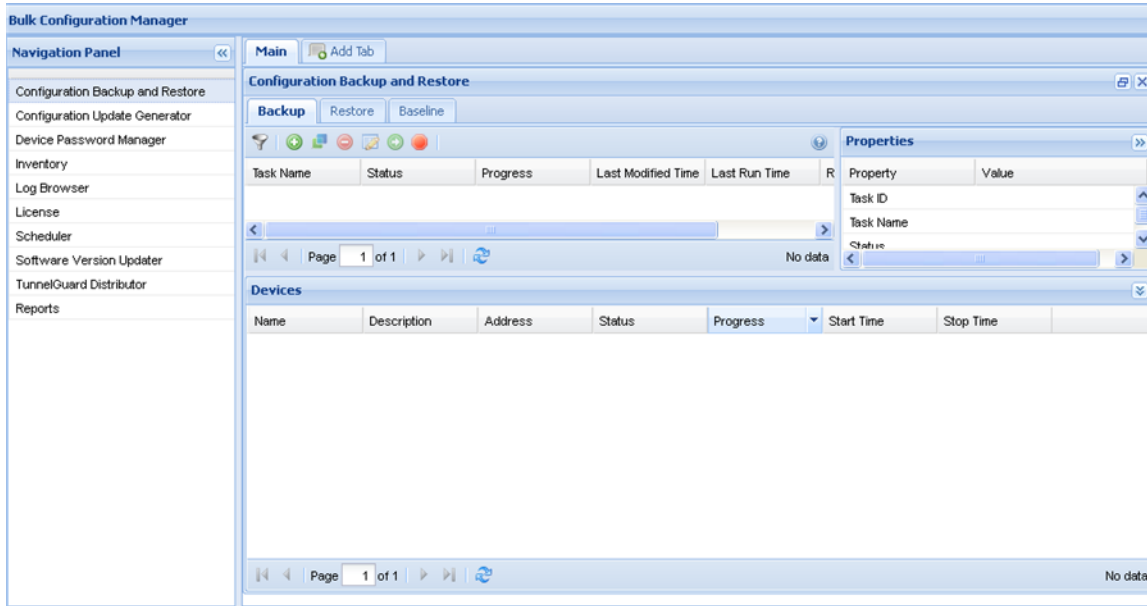
The following figure shows the view of the Configuration Backup and Report user interface.

The Configuration Backup and Restore tool supports the following devices:

- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/4500/4800/5500/5600/8300/8600/8800
- Ethernet Switch 350/450/470
- VSP 4000/7000/8000/9000
- Wireless LAN 8180

For more information about supported device versions, refer to [Supported devices](#) on page 12.





**Figure 1: Configuration Backup and Restore**

The following tables describe the fields of the Configuration Backup and Restore tool, the devices where the backup is performed, and the fields of an archived backup.

**Table 1: CBR backup task table**

Attribute	Value	Description
Task Name	<textbox>	The name of the backup task.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Modified Time	<textbox>	The last time a task was modified.
Last Run Time	<textbox>	The last run time.
Restrict to Same Version	<textbox>	If the restore can only be performed on the same version as the backup version.
Task ID	<textbox>	The task index.

**Table 2: Backup Device table**

Attribute	Value	Description
Name	<textbox>	The name of the device.
Description	<textbox>	The device.
Address	<IP address>	The address of the device.
Status	<textbox>	The status of the device.
Progress	<textbox>	The progress of the device.
Start Time	<numerical value>	The start up time of the device.

Attribute	Value	Description
Stop Time	<numerical value>	The stop time of the device.

**Table 3: CBR restore task table**

Attribute	Value	Description
File Name	<textbox>	The name of the restore task.
Address	<IP Address>	The address of the device.
Backup Date	<DD-MM-YYYY 00:00>	The day, month, year, and time of the backup.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Run Time	<textbox>	The last run time of the task
Version	<textbox>	The software version on the device at the time of the backup.
Restrict to Same Version	<textbox>	If the restore can only be performed on the same version as the backup version.
Task ID	<textbox>	The task index.

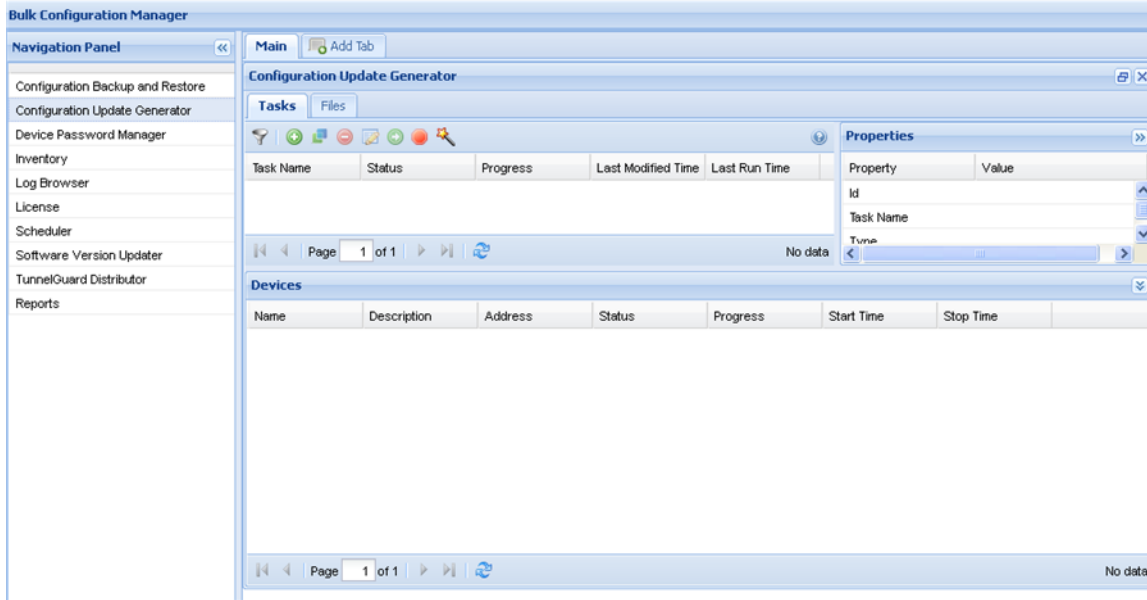
**Table 4: CBR baseline table**

Attribute	Value	Description
Address	<IP Address>	The address of the device.
Device Type	<textbox>	The type of device used in the backup task.
Backup Date	<DD-MM-YYYY 00:00>	The day, month, year, and time of the backup.

---

## Configuration Update Generator

You can use the Configuration Update Generator (CUG) service tool to run a common set of configuration commands on multiple system devices. With this tool, you can apply previously created template files to multiple devices with a single action. For example, this tool can quickly shut off or enable a service such as Simple Network Management Protocol (SNMP) or set up firewalls on multiple network elements of the same type on a network. To deploy a parameter change on multiple devices, you can create a template file with the parameter as a variable and a data file where the variable takes a different value for each device IP. After the completion of deployment of the CUG file, for devices on which CUG applies changes, Avaya BCM automatically reboots them and for devices on which CUG does not applies changes, Avaya BCM drops the connection, and waits for a minute, and then reconnects again for only checking the device connectivity.



**Figure 2: Configuration Update Generator**

The Configuration Update Manager supports the following devices:

- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/4500/4800/5500/5600/8300/8600/8800
- Ethernet Switch 350/450/470
- VSP 4000/7000/8000/9012
- Wireless LAN 8180

However, COM and BCM do not support the configuration of a configuration file on the VSP devices. For both the VSP devices and the Wireless LAN 8180, the CUG tool starts executing the user script in configuration mode and saves the configuration on exit.

The following tables describe the fields of the CUG tool, the devices, and the fields of the script or data files you upload to the Avaya BCM server.

**Table 5: CUG task table**

Attribute	Value	Description
Task Name	<textbox>	The task name.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Modified Time	<textbox>	The last time a task was modified.
Last Run Time	<textbox>	The last run time of the task.

Attribute	Value	Description
Id	<textbox>	The task index.
Type	Configuration CLI Script	The file type to deploy.
Template File	<filename>	The template file name (previously created).
Data File	<filename>	The data file name (previously created).
Device IDs	<textbox>	The IDs of the device.

**Table 6: CUG device table**

Attribute	Value	Description
Name	<textbox>	The name of the device.
Description	<textbox>	The device.
Address	<IP address>	The address of the device.
Status	<textbox>	The status of task for the device.
Progress	<textbox>	The progress of the task for the device.
Start Time	<numerical value>	The start up time of task for the device.
Stop Time	<numerical value>	The stop time of the task for the device.

**Table 7: Template or data files**

Attribute	Value	Description
Name	<filename>	The file name of the script or data file.
Size	<numerical value>	The file size of the script or data file.

---

## CUG Wizard

With the Configuration Update Generator (CUG) Wizard, you can quickly configure and deploy multidevice configuration update generator (CUG) tasks in a well-defined step by step process.

For more information about the CUG Wizard, see [CUG Wizard](#) on page 46.

---

## Device Password Manager

With the Device Password Manager (DPM), you can select a group of managed devices and change the administrator password and the SNMP read-only and read/write community string.

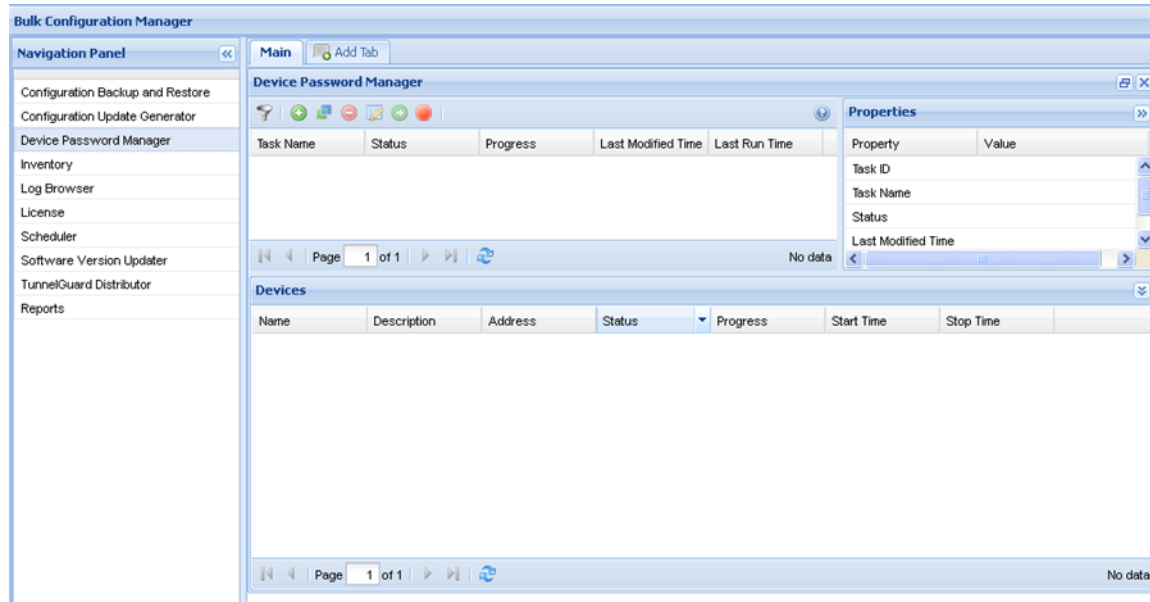
 **Note:**

The read write community string modification applies to SNMP v1 and v2 only, for all devices.

If the password and/or community changes are successful on the device, the new values are updated in the System Manager (SMGR) Credentials. A new entry on the credential page will be created with new value for this device IP, if the same IP is part of IP Address range on some other entry.

**\* Note:**

The new password and/or community value will not be updated successfully for a device when there exists more than one credential entry for that device and they have different password/community values.



**Figure 3: Device Password Manager**

The Device Password Manager supports the following devices:

- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/4500/4800/5500/5600/8300/8600/8800
- Ethernet Switch 350/450/470
- VSP 4000/7000/8000/9000
- Wireless LAN 8180

Tables 7 and 8 describe the fields of the DPM tool, and the devices for which you can change the password.

**Table 8: DPM task table**

Attribute	Value	Description
Task Name	<textbox>	The name of the DPM task.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Modified Time	<textbox>	The last time a task was modified.
Last Run Time	<textbox>	The last run time of the task.
Task ID	<textbox>	The task index.

**Table 9: DPM device table**

Attribute	Value	Description
Name	<textbox>	The name of the device.
Description	<textbox>	The device.
Address	<IP address>	The address of the device.
Status	<textbox>	The status of the task for the device.
Progress	<textbox>	The progress of the task for the device.
Start Time	<numerical value>	The startup time of the task for the device.
Stop Time	<numerical value>	The stop time of the task for the device.

---

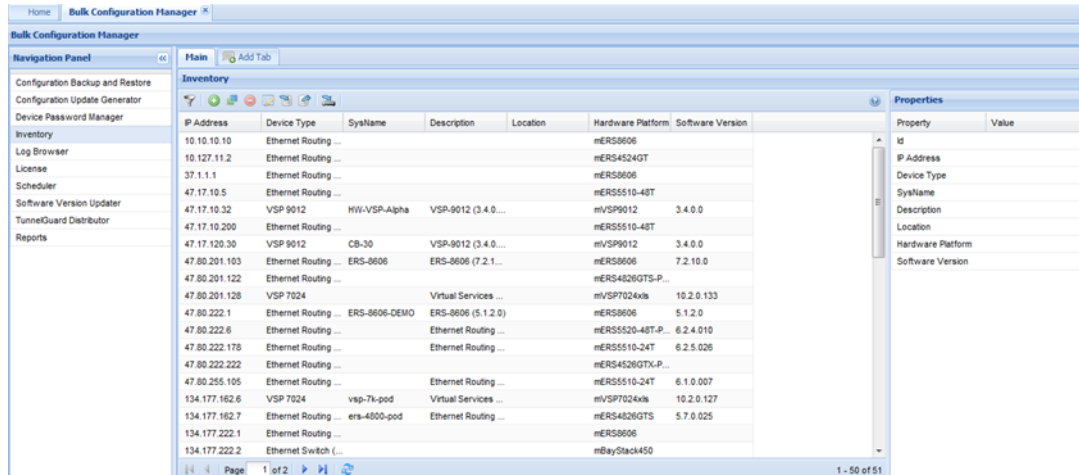
## Inventory

You can use the Avaya BCM Inventory feature to add, store, and import devices. The devices from the COM inventory are automatically imported when BCM is launched for the first time. After BCM is open, the inventory is not automatically updated when the inventory in COM changes. Use the Import from COM option to manually import COM inventory into BCM inventory. Also, if you delete a device from the COM inventory, the device is not deleted from the Avaya BCM database. Similarly, if you delete a device from the Avaya BCM database, the device does not affect the COM inventory.

You can manually add devices one at a time or import a list of devices from a comma-delimited (\*.csv) file. When you add devices, either manually or from a .csv file, the required fields are IP Address or Device Name, and Device Type. When you import devices from a .csv file all previously imported devices are replaced. Devices that were manually added are retained.

**\* Note:**

Deleting inventory devices used in tasks and adding them back manually to the Inventory does not make them functional in the tasks because the devices in the tasks are linked to Inventory through the device ID. Importing inventory devices from a csv file replaces the previously imported devices.



**Figure 4: Inventory**

The Inventory tool supports the following devices:

- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/4500/4800/5500/5600/8300/8600/8800
- Ethernet Switch 350/450/470
- VSP 4000/7000/8000/9000
- Wireless LAN 8180

**Table 10: Inventory table**

Attribute	Value	Description
Name	<textbox>	The name of the device
IP Address	<IP address>	The IP address of the device
Device Type	<textbox>	The device type
Description	<textbox>	The device description
Location	<textbox>	Location of the device
Hardware Platform	<textbox>	Platform of the hardware
Software Version	<textbox>	Version of the software
Task ID	<textbox>	The task index

## Log Browser

You can use the Log Browser to access Avaya BCM logging information.

Avaya BCM logs all interactions with devices to a common file stored in the COM\_HOME/log folder. This file rolls over to a new file when the size reaches 10 megabytes. You can open each log file or export the log for offline inspection or for transfer to Avaya customer service. You can modify your view of the Log Browser by filtering the log based on date and time, tool name, or keyword. You can also modify the automatic refresh interval and configure different colors for Info, Warning, and Error log messages.

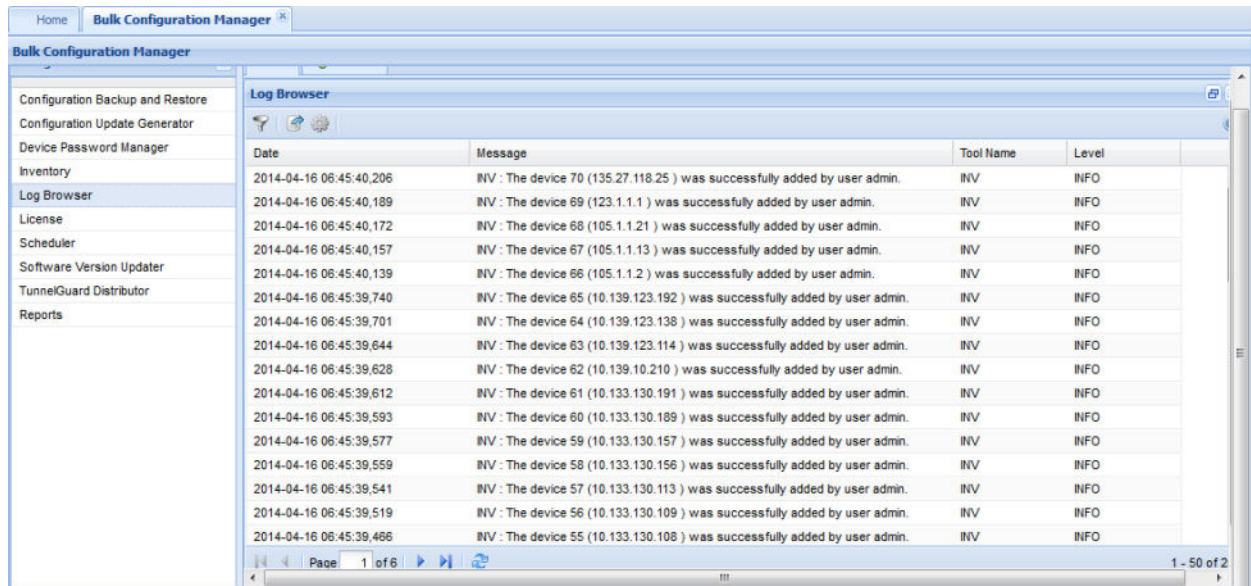


Figure 5: Log Browser

Table 11: Log Browser table

Attribute	Value	Description
Date	<YYYY-MM-DD 00:00:00,000>	The day, month, year, and time of the log
Message	<textbox>	The log message that appears
Tool Name	<textbox>	Name of the Avaya BCM tool
Level	<textbox>	The log level

## License

The Avaya BCM License is a node-based license that provides license-tracking functions for the Avaya BCM tools.

The following list outlines the four types of BCM node-based licenses.

- BCM\_100\_base, (100)
- BCM\_Upgrd100\_1200\_base, (1200)
- BCM\_Upgrd100\_5000\_base, (5000)

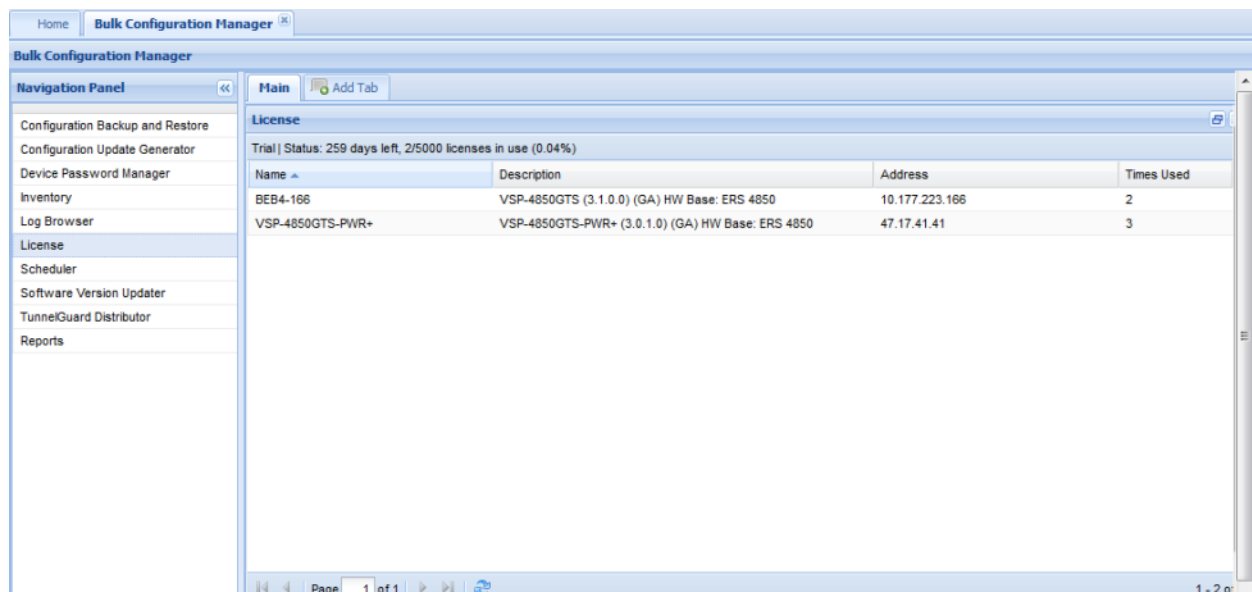


- BCM\_Upgrd1200\_5000\_base (5000)

Licenses in use are calculated across all Avaya BCM tools and tasks. If multiple tools or tasks use the same device, only one license is used.

The Avaya BCM License is a read-only portlet.

For more information about the Avaya BCM License, see [Avaya BCM licensing](#) on page 31.



**Figure 6: Avaya BCM License**

The following table outlines the Avaya BCM license fields.

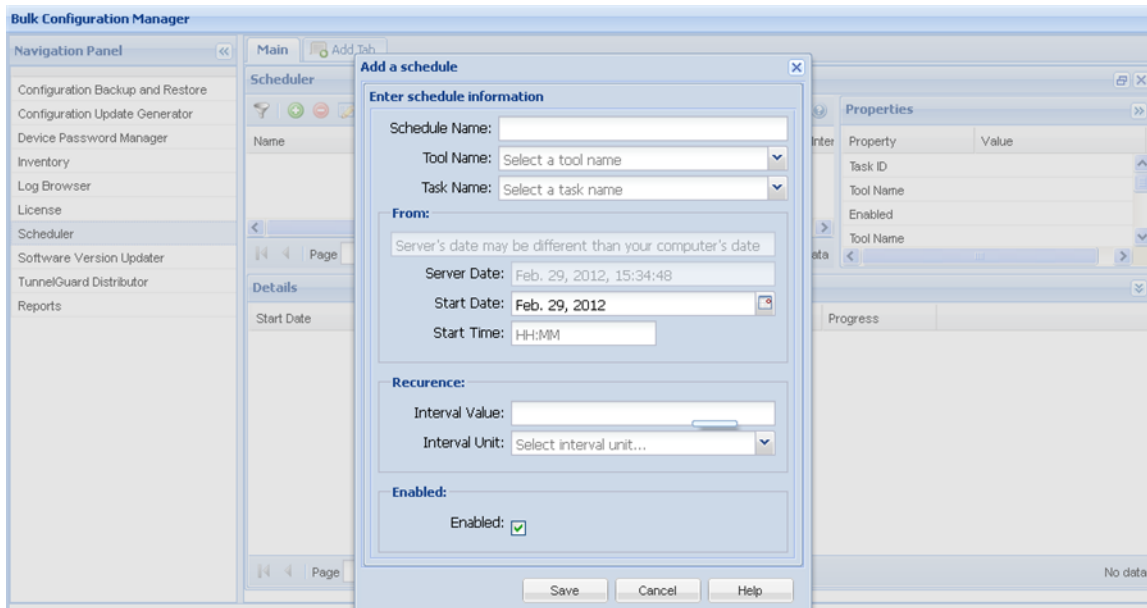
**Table 12: Avaya BCM License task table**

Attribute	Description
Name	The name of the device.
Description	The device.
Address	The address of the device.
Times Used	The number of tasks using the device.

## Scheduler

You can use the Scheduler feature to schedule Avaya BCM tasks. You can select a tool from a drop down list of Avaya BCM tools. After you select a tool, you can select a previously created task from a drop-down list that is populated with tasks of that tool. After a task is selected, you can choose the date and time to activate the task. You can also choose to repeat the activation of the task in selected increments of seconds, minutes, hours, days, or weekly.

You can choose to enable or disable a schedule. You can view the Schedule portlet in maximized view, the progress and status of the scheduled task. The following graphic depicts the scheduler add dialogue box.



**Figure 7: Scheduler**

**Table 13: Scheduler table**

Attribute	Value	Description
Name	<textbox>	The name of the scheduled activity
Enabled	<textbox>	The state of the scheduled activity. You can enable or disable a schedule..
Tool Name	<IP address>	The tool name
Task Name	<textbox>	The name of the task
Next Date	<Day>, <Month> <Date> <Year>	The next date on which the task will be executed
Repeat Interval	<textbox>	The interval for task to repeat
Repeat Unit	<textbox>	The unit of time for the repeat interval
Status	<textbox>	The status of the scheduled activity.
Progress	<textbox>	The progress of the scheduled activity.
Last Modified Time	<Day>, <Month> <Date> <Year> 00:00:00 <AM/PM>	The time you last modified the schedule.
Task ID	<textbox>	The task index.

**Table 14: Details table**

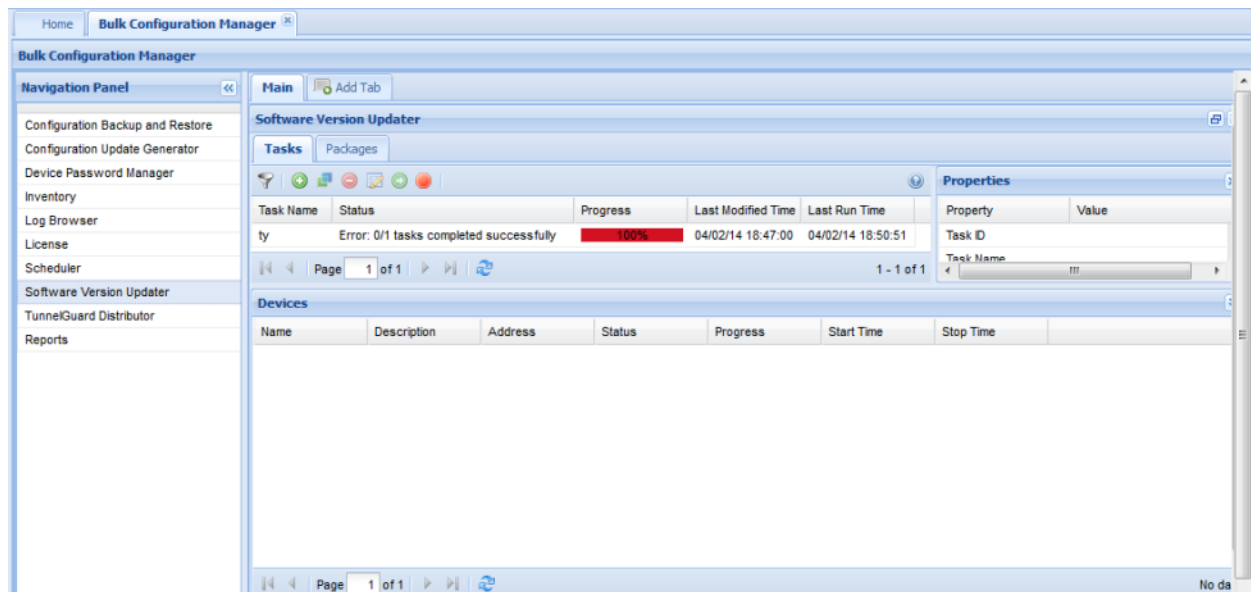
Attribute	Value	Description
Start Date	<textbox>	The start date of the scheduled activity.
Stop Date	<textbox>	The stop date of the scheduled activity.
Status	<textbox>	The status of the scheduled activity.
Progress	<textbox>	The progress of the scheduled activity.

## Software Version Updater

Software Version Updater (SVU) tool enables you to perform updates of device images. You can also create an SVU package to update a group of devices of the same type.

### ! Important:

The SVU tool supports only software upgrades; support is unavailable for downgrades or reloads on devices with the current version.

**Figure 8: Software Version Updater**

The Software Version Updater supports the following devices:

- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/4500/4800/5500/5600/8300/8600/8800
- Ethernet Switch 350/450/470

- VSP 4000/7000/8000/9000
- Wireless LAN 8180

For the VSP devices, Avaya BCM uses the FTP protocol to transfer the image from the COM server to the VSP; therefore you must configure the FTP server to operate on the VSP device. If you do not provide the FTP credentials for the VSP FTP server in the SMGR credentials manager, the SVU uses the device login credentials to connect as an FTP client to the VSP device.

Tables 12, 13, and 14 show the fields of the SVU tool, the devices on which you can update the software, and the fields of SVU image files.

**Table 15: SVU task table**

Attribute	Value	Description
Task Name	<textbox>	The name of the task.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Modified Time	<numeric>	The last time a task was modified.
Last Run Time	<numeric>	The last run time.
Task ID	<textbox>	The task index.
Device Type	<textbox>	The device type.
Package Name	<textbox>	The package name.
Reboot Image	<textbox>	Identifies the status of the task reboot.
Enabled Email	<textbox>	Identifies if e-mail is enabled or disabled.
Email To	<textbox>	The e-mail address of the recipient.
Email From	<textbox>	The e-mail address of the sender.
Additional Info	<textbox>	Identifies additional information about the task.

**Table 16: SVU device table**

Attribute	Value	Description
Name	<textbox>	The name of the device
Description	<textbox>	The device description
Address	<IP address>	The address of the device
Status	<textbox>	The status of the device
Progress	<textbox>	The progress of the device
Start Time	<numeric>	The startup time of the device
Stop Time	<numeric>	The stop time of the device

**Table 17: Package table**

Attribute	Value	Description
Device Type	<textbox>	The type of the device

Attribute	Value	Description
Package Name	<filename> .pkg .tar.gz .Z .img	The file name of the image file. SNAS routers requires .pkg files. VPN Router requires .tar.gz files. Secure Router 1000/3100 requires .Z files.

Table 18: File table

Attribute	Value	Description
File Name	<filename>	The file name.
Size	<numeric>	The file size.

## Tunnelguard Distributor

The Tunnelguard Distributor (TGD) tool copies a tunnelguard rule from one device to multiple devices. A tunnelguard rule is in a group, and a group is in a domain. For example, consider that the source device has a domain D1, and D1 has a group called G1 and G1 has a tunnelguard rule TG1. To copy TG1 to a destination device, the destination device must have a domain D1 and a group G1 created in the domain D1. If the domain and the group from the source SNAS device do not exist on the destination SNAS device, the tunnelguard is not copied, and an error message is generated. Alternatively, you can designate a group index. This means that the group need not be on the destination device with the same name as the group on the source device, but a group with the same index must exist. Domains also use indexes. You can use the TGD tool only on a SNAS.

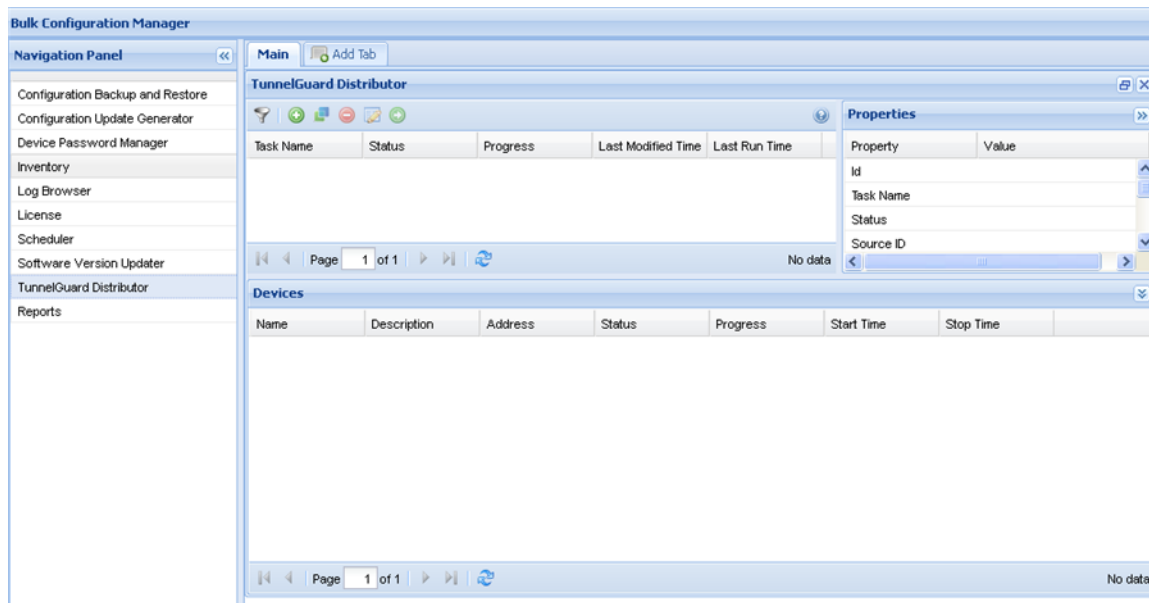


Figure 9: Tunnelguard Distributor

Tables 16 and 17 show the fields of the TGD tool, and the devices to which a tunnelguard rule is distributed.

**Table 19: TGD task table**

Attribute	Value	Description
Task Name	<textbox>	The name of the task.
Status	<textbox>	The status of the task.
Progress	<textbox>	The progress of the task.
Last Modified Time	<textbox>	The last time a task was modified.
Last Run Time	<textbox>	The last run time.
Task ID	<textbox>	The task index.

**Table 20: TGD device table**

Attribute	Value	Description
Name	<textbox>	The name of the device.
Description	<textbox>	The device.
Address	<IP address>	The address of the device.
Status	<textbox>	The status of the device.
Progress	<textbox>	The progress of the device.
Start Time	<numeric>	The startup time of the device.
Stop Time	<numeric>	The stop time of the device.

# Chapter 4: Avaya BCM licensing

This chapter contains information about licensing, interaction with Avaya BCM tools, licensing failure, and license information.

---

## Prerequisites

- You must have credentials for SNMP communities, SSH, Telnet, and FTP for all the tools to be fully functional.

---

## Node based licensing for BCM

The Bulk Configuration Manager (BCM) depends on COM. The BCM resides in COM and follows the same COM rules and restrictions, except that the BCM user gets all supported devices automatically, and skips the device assignment process. To enable the BCM for COM, you must acquire a separate license. The BCM license is node based, but only counts individual uses of a node. A base license is 100 nodes. If you have a 100 node license, you may have more than 100 devices in inventory. However, after you create tasks that use 100 unique devices, you cannot create tasks for more devices; a license error appears informing you that you have reached the limit and should purchase more increments. If no BCM license is supplied, you can still launch BCM from the COM managers screen to create tasks and import devices, but you cannot run the tasks without a license.

The following list outlines the four types of BCM node based licenses:

- BCM\_100\_base, (100)
- BCM\_Upgrd100\_1200\_base, (1200)
- BCM\_Upgrd100\_5000\_base, (5000)
- BCM\_Upgrd1200\_5000\_base (5000)

 **Note:**

BCM supports device imports from COM.

---

## Interaction with Avaya BCM tools

All Avaya BCM tools must contact the Avaya BCM licensing service before add, edit, delete, or task activation actions can take place. The Avaya BCM licensing service calculates the available licenses. If you have reached your licensing limit, the Avaya BCM tool alerts you that your requested action cannot continue.

---

## Licensing failure

Licensing failure occurs when the number of devices exceeds the licensed device limit. Avaya BCM licensing returns a failure based on your action and the current license status:

- expired trial license
  - delete only is permitted
- user exceeds base, incremental, or enterprise license limit
  - add task and activate task actions are not permitted
  - delete task is permitted
  - edits are permitted if the number of devices in use decreases to be within the license limits

---

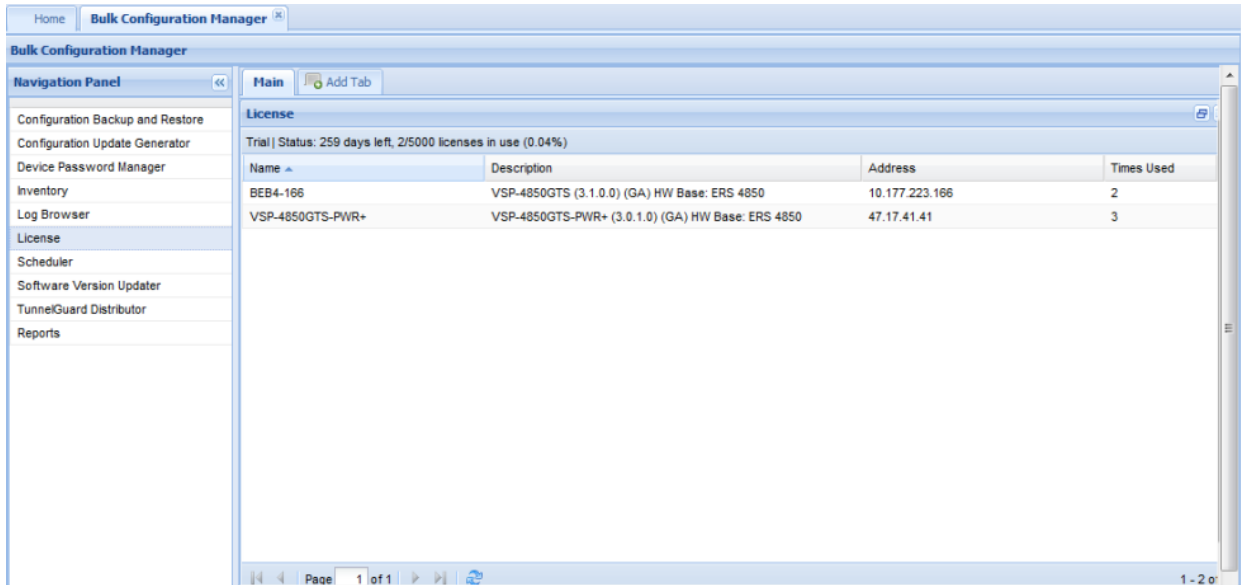
## License information

The Avaya BCM license portlet and table are read-only.

The Avaya BCM portlet displays the following information:

- license type
- status
  - number of days remaining for a trial license
  - number of available and total number of licenses for Base and Incremental licenses
  - number of licenses in use for enterprise license
- device table
  - Name – name of the device
  - Description – device and version
  - Address – device IP address
  - Times Used – number of times the license was used





## Prerequisites

- You must be in the Configuration and Orchestration Manager.

## Procedure steps

- From the Managers panel, click **Bulk Configuration Manager** to open BCM portlets.
- Select **License** to open a BCM License portlet.

---

## Obtaining a license

Perform the following procedures to obtain a BCM license through the FlexLM licensing service to be installed on a physical server or on a virtual machine.

---

## Obtaining a BCM license to be installed on a physical server

### About this task

Perform the following steps to obtain a BCM license to be installed on a physical server.

### Procedure

- Open a Web browser window and navigate to the **Electronic Licensing Portal**: <http://www.avayadatalicensing.com>.

The Electronic Licensing For Avaya Networking window displays.



ELECTRONIC LICENSING

### ELECTRONIC LICENSING FOR AVAYA NETWORKING

NOTE: ELECTRONIC LICENSING ACTIVITIES FOR AVAYA DATA NETWORKING PRODUCTS HAS CHANGED.

PLEASE ENTER INFORMATION BELOW, SELECT THE ACTIVITY YOU REQUIRE, AND PROVIDE ADDITIONAL INFORMATION FOR THE SPECIFIC ACTIVITY TO COMPLETE YOUR REQUEST.

First Name  Last Name   
 Company  E-mail   
 Phone Number

SELECT REQUIRED ACTIVITY FOR EACH LICENSE REQUEST:

- Create/Generate a License file for your Avaya data product running on a physical server (provide LAC, MAC, and filename)
- Create/Generate a VM License file for your Avaya data product running on VM server (provide LAC, NOTICE, IP Address, and filename)
- Replace or Swap a MAC address in an existing license file (provide LAC if known, new MAC address, and filename)
- Contract LACs

2. Type your first name, last name, company name, e-mail address, and phone number in the appropriate fields at the top of the page.
3. Select **Create/Generate a License file for your Avaya data product running on a physical server (provide LAC, MAC, and filename)**.
4. In the LICENSE INFORMATION REQUIRED section, type your License Authorization Code in the License Authorization Code field.

LICENSE INFORMATION REQUIRED

License Authorization Code:   
Example: WS13-xxxx-xxxx

MAC Information:  +Add  
Example: 0A:XX:XX:XX:XX:XX

Number of Existing Licenses (WLAN 2300/8100 Only):

Serial Number or Computer Name (WLAN 2300 Only):

Bank Name (Optional):

License File Name (Optional):

\* A confirmation email will be sent to the supplied email address.  
 Please contact [Avaya Data Licensing](#) with any questions.

5. Type the MAC address for the server where BCM is installed in the MAC Information field. Type upper case letters, separated by colons.
6. Click **Submit Request**.  
 A confirmation message informs you that the license was created.  
 A license (.lic) file is sent to the e-mail address specified in Step 2.
7. Copy the license file to a location on the server on where BCM is installed.

Avaya recommends that you copy the license to the default license directory:

- Linux: /opt/avaya/smgr/LSM/licenses
- Windows: C:\Avaya\smgr\LSM/licenses

## Field definitions

This section provides field descriptions.

License Authorization Code	This code is provided on the License Certificate.
Switch MAC Address	Enter the base MAC address of the device to be licensed.
Number of Existing Licenses	Required for WLAN 2300/8100 only.
Serial Number or Computer Name	Required for WLAN 2300 only.
Bank Name	Optional
Output License File Name	The name of the license file that will be emailed when the license is generated. <ul style="list-style-type: none"> <li>• Maximum of 63 alphanumeric characters (lower case).</li> <li>• No spaces or special characters allowed.</li> <li>• An underscore “_” is permitted.</li> <li>• A period followed by a three letter extension is required.</li> </ul>

## Obtaining a BCM license to be installed on a Virtual Machine

### About this task

Perform the following steps to obtain a license for COM to be installed on a virtual machine.

#### Note:

To install COM 3.1 on a virtual machine with more than one Network Interface Card (NIC), download **LicensingInfo.zip** from <http://support.avaya.com/> to obtain the proper IP and Notice information required for the virtual machine license. You can download **READMElicensingInfo-Utility.txt** for instructions on how to execute the LicensingInfo utility file.

### Procedure

1. Open a Web browser window and navigate to the **Electronic Licensing Portal**: <http://www.avayadatalicensing.com>.

The Electronic Licensing For Avaya Networking window displays.



ELECTRONIC LICENSING

### ELECTRONIC LICENSING FOR AVAYA NETWORKING

NOTE: ELECTRONIC LICENSING ACTIVITIES FOR AVAYA DATA NETWORKING PRODUCTS HAS CHANGED.

PLEASE ENTER INFORMATION BELOW, SELECT THE ACTIVITY YOU REQUIRE, AND PROVIDE ADDITIONAL INFORMATION FOR THE SPECIFIC ACTIVITY TO COMPLETE YOUR REQUEST.

First Name  Last Name   
 Company  E-mail   
 Phone Number

SELECT REQUIRED ACTIVITY FOR EACH LICENSE REQUEST:

- Create/Generate a License file for your Avaya data product running on a physical server (provide LAC, MAC, and filename)
- Create/Generate a VM License file for your Avaya data product running on VM server (provide LAC, NOTICE, IP Address, and filename)
- Replace or Swap a MAC address in an existing license file (provide LAC if known, new MAC address, and filename)
- Contract LACs

2. Type your first name, last name, company name, e-mail address, and phone number in the appropriate fields at the top of the page.
3. Select **Create/Generate a License file for your Avaya data product running on VM server (provide LAC, NOTICE, IP Address, and filename)**.
4. In the LICENSE INFORMATION REQUIRED section, type your License Authorization Code in the License Authorization Code field.

LICENSE INFORMATION REQUIRED

License Authorization Code:   
Example: WS13-xxxx-xxxx

IP Address:   
Example IPv4: 192.168.255.255

NOTICE:   
Example: 564DAC8D-2591-6067-1805-07FCB439AC6E [Help me find this?](#)

Bank Name (Optional):

VM License File Name (Optional):

\* A confirmation email will be sent to the supplied email address.  
 Please contact [Avaya Data Licensing](#) with any questions.

© Avaya Inc. 2009-2013

5. Type the IP Address for the server where BCM is installed.
6. Type the NOTICE information.  
 Click **Help me find this** provides instructions on how to find NOTICE information.
7. Click **Submit Request**.  
 A confirmation message informs you that the license was created.  
 A license (.lic) file is sent to the e-mail address specified in Step 2.
8. Copy the license file to a location on the server on where BCM is installed.

Avaya recommends that you copy the license to the default license directory:

- Linux: /opt/avaya/smgr/LSM/licenses
- Windows: C:\Avaya\smgr\LSM\licenses

---

## Installing an Avaya Bulk Configuration Manager license

Use this procedure to install an Avaya Bulk Configuration Manager (Avaya BCM) license.

### Before you begin

- You must execute this procedure on the server where the Avaya BCM components reside.
- You must obtain the license and store it on the server before you can proceed. For more information, see [Obtaining a license](#) on page 33.
- You must know where the license resides on the server.
- You must know the directory path of <SMGR\_home>. To locate the directory path for your operating system, see [Directory structure](#) on page 84.

### Procedure

1. Start a Web browser supported by COM.
2. In the **Address** field, enter the Fully Qualified Device Name (FQDN) of the COM server.

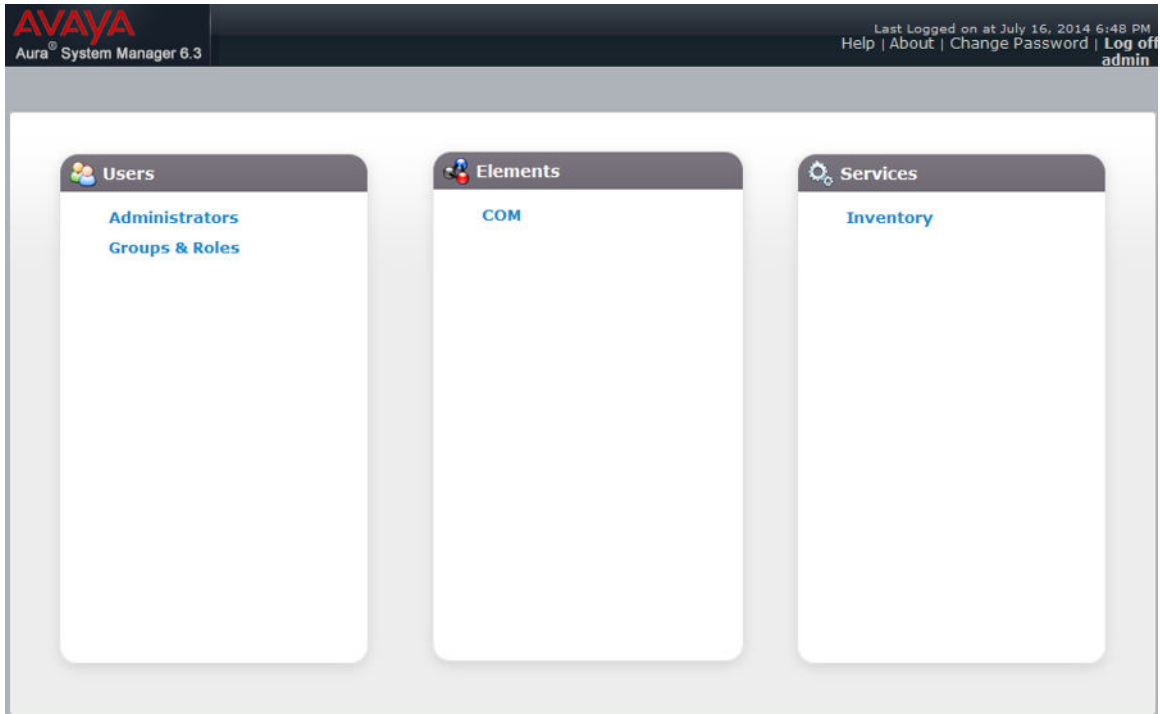
The Avaya Aura® System Manager log in window displays.

The screenshot shows the Avaya Aura System Manager 6.3 login interface. At the top left, the Avaya logo and 'Aura System Manager 6.3' are displayed. The main content area is divided into three sections:

- Disclaimer (Left):** A text box containing the following information:
  - This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.
  - Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.
  - The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.
  - All users must comply with all corporate instructions regarding the protection of information assets.
- Login Form (Center):** A form with two input fields: 'User ID:' and 'Password:'. Below the fields are two buttons: 'Log On' and 'Reset'.
- Supported Browsers (Bottom Right):** A notice indicating supported browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

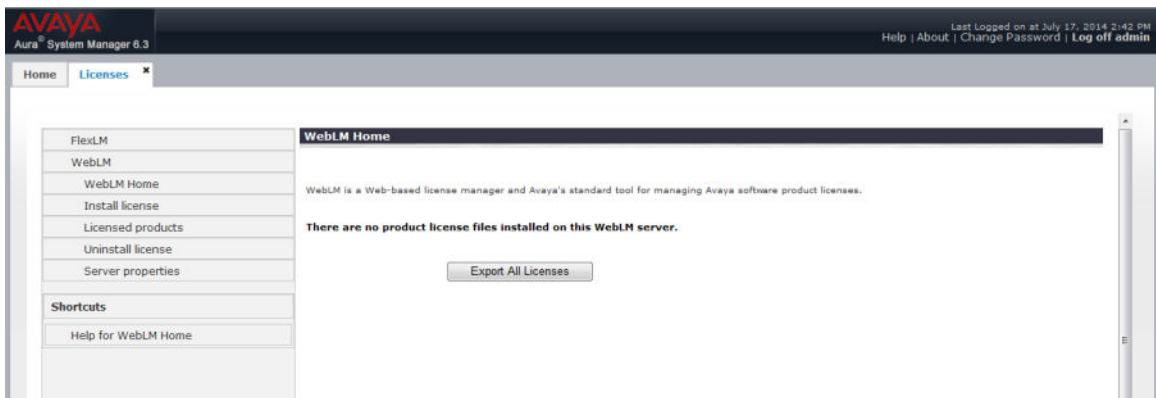
3. Click **Log On**.

The System Manager window displays.



4. Below Services, click **Licenses**.

The Licensing page displays.

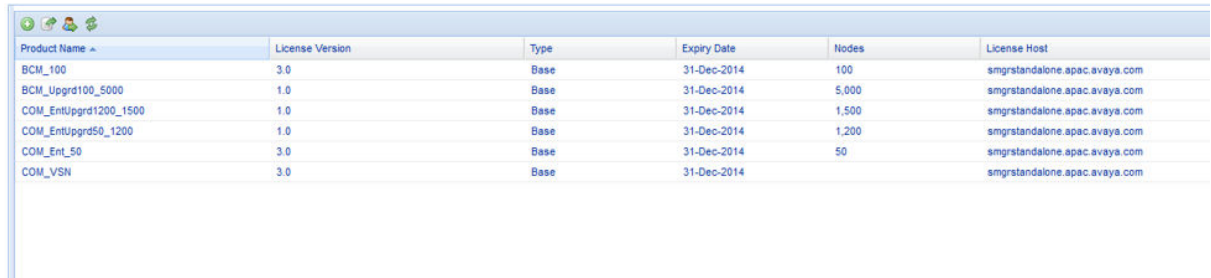


5. In the left Navigation pane, click **FlexLM**.

**\* Note:**

WebLM is not supported in COM 3.1.

The Licensing Administration page displays.

**Licensing Administration**


Product Name	License Version	Type	Expiry Date	Nodes	License Host
BCM_100	3.0	Base	31-Dec-2014	100	smgrstandalone.apac.avaya.com
BCM_Upgrd100_5000	1.0	Base	31-Dec-2014	5,000	smgrstandalone.apac.avaya.com
COM_EntUpgrd1200_1500	1.0	Base	31-Dec-2014	1,500	smgrstandalone.apac.avaya.com
COM_EntUpgrd50_1200	1.0	Base	31-Dec-2014	1,200	smgrstandalone.apac.avaya.com
COM_Ent_50	3.0	Base	31-Dec-2014	50	smgrstandalone.apac.avaya.com
COM_VSN	3.0	Base	31-Dec-2014		smgrstandalone.apac.avaya.com

6. Click **Add License**. (The green button with + symbol).  
The **Add License** dialog box displays.
7. Browse for the license file in the **License** field.
8. From the **License Host** list, select a license host.
9. Click **Add** to add the license to the SMGR.

# Chapter 5: Administration tools

Use the administration tools to manage network devices, perform upgrades, and back up device information. Tools are available to simultaneously monitor the performance of one or multiple devices.

---

## Network device configuration and management

With the Configuration Update Generator (CUG) tool, you can distribute template script files to multiple devices.

**\* Note:**

Avaya recommends that you use DPM to change SNMP parameters or the administrator password. Do not use the CUG tool to make these changes.

The following sections describe configuration operations.

---

## Creating template files

You must create the template and data files that the CUG uses.

Two types of template files exist: script and configuration files. A script file contains the CLI/ACL commands you need to configure a device type. When you create a script, write it so that it begins just after a successful login to the device. For example, if the script needs to enter a configuration mode, such as `config term`, your script must provide that navigation. For devices, such as Contivity, SR 1000/3000/4000, ERS 2500/4500/5500/5600 devices, which enter into the configuration mode by issuing `conf t` command, do not insert the command `conf t` in the script because the CUG automatically enters the configuration terminal mode. Writing a configuration to memory (such as the case of a secure router) or applying a candidate configuration (such as NSNA 4050) is handled by Avaya BCM; you do not need to add these commands to your script.

This section provides examples of scripts that you can distribute using the CUG tool.

The next example shows how to configure an interface on NSNAS or NVG.

```
/cfg/sys/host 1/interface 2/.
ip 12.12.12.12
netmask 255.255.0.0
gateway 12.12.12.1
```



```
vlan id 3
mode failover
primary 0
```

The next example shows how to add the ARP timeout to one or more Secure Router 3120s. You must create a script file that contains the command necessary to configure the ARP timeout from the CLI of a Secure Router 3120.

```
arp_timeout 4444
```

A configuration file contains configuration information in a specific format for the device type. Before using CUG, you must generate a configuration file from a network device and transfer that file to the Avaya BCM server. For example, to get a complete configuration file from a Secure Router 3120, you must connect to the router by using Telnet or secure shell (SSH) and issue the command `Save <filename>`. A device configuration file is generated. The following is a partial example of a generated file, that can be used in a CUG config.

```
router rip
distance 100
timers update 30
timers holddown 120
timers flush 180
exit rip
```

To override the values for an attribute, you must replace the values in the template file with a unique string, preceded by three question marks (???). For example, in the previous configuration file example, if you want to set one ARP timeout value on some routers and set a different ARP timeout value on others, you create a file that replaces the actual value of the ARP timeout attribute.

```
arp_timeout ???ARP_TIMEOUT
```

A data file is a CSV file generated by Microsoft Excel. You create a spreadsheet with each column consisting of a unique override value found in the template file, and each row is a device in the task. Each cell in the table contains the value to use for that field on that device. See the following for sample values for a data file.

```
, ???ARP_TIMEOUT
10.1.1.1, 1111
10.1.1.2, 2222
10.1.1.3, 3333
```

The configuration or script files that the tool generates are stored on the server in the following file folder:

```
<install dir>/Avaya/ConfigUpgradeGenerator/UserFiles/Templates.
```

The data files are stored in `<install dir>/Avaya/ConfigUpgradeGenerator/UserFiles/Values`.

For more examples of configuration files and scripts, see [Sample configuration scripts](#) on page 93.

**!** **Important:**

Do not attempt to use the CUG to change the host name on Avaya VPN Gateway routers. If you change the host name, CUG cannot reconnect to the device.

---

## Configuration files and tasks management

For more information about managing configuration files and tasks, see [Configuration Update Generator](#) on page 18.

User-defined files can be as follows:

- template files
  - configuration files
  - CLI script file
- data files

The following procedures describe how to manage configuration files and tasks on the Avaya BCM server.

---

## Uploading a user-defined configuration file

Upload a user-defined configuration file so that it gets listed in the template and data file lists on the Create Task and Edit Task windows.

**Prerequisites:**

- You must be logged on to the Avaya BCM application.
- You must ensure the CUG portlet is maximized.

**Procedure steps**

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Files** tab and in the **Template Files** or **Data Files** table, click **Add**.  
The Add file dialog box appears.
3. Click **Browse**.
4. Browse to your configuration file.
5. Click **Open**.
6. Click **Upload**.
7. Click **OK**.

---

## Removing a user-defined configuration file from the Avaya BCM server

Remove a user-defined configuration file so that it does not appear in the template and data file lists on the Create Task and Edit Task windows.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Files** tab and in the **Template Files** or **Data Files** table, select the files you want to delete.
3. Click the **delete** icon.
4. Click **Yes**.

---

## Viewing or editing a user-defined configuration file

View or edit any template or data file that was previously imported into Avaya BCM.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Files** tab.
3. Select a file from the **templates** or **data** pane.
4. Click **Edit**.

The Edit file window appears showing the selected file contents.

---

## Exporting a user-defined configuration files

Export a user-defined configuration files to a local system.

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Files** tab.
3. Select the **template** or **data** file that you want to export, and then click **Export File**.

The View Files popup window appears.

4. Click the file name.

The File Download popup window appears.

5. Click **Open** or **Save**.

## Creating a CUG task

Create a CUG task to group devices on which you want to run your configuration commands.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Tasks** tab, and click the **Add Task** icon.
3. Type the task name.
4. Select the deployment file type.
5. Select the template file from the list.
6. Select the data file from the list if you want to deploy on several devices.
7. Select a device from the device list.
8. Click **Save**.

---

## Filtering the CUG tasks view

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Tasks** tab.
3. Click **Filter Tasks**.  
The Add a filter dialog box appears.
4. In the Task Name field, enter the task name or the first letter of the task name you want to filter.

 **Note:**

To display all the tasks, leave the Task Name field empty.

5. Click **Find**.

The filtered information appears in the CUG tasks table.

---

## Duplicating a CUG task

Duplicate the CUG tasks in the CUG tasks table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a new or existing portlet.  
From the **tasks** table, select the task you want to duplicate.
2. Click **Duplicate Task**.  
You are prompted to confirm the task duplication.
3. Click **Yes**.  
The duplicate task appears in the CUG tasks table.

---

## Editing a CUG task

Edit the CUG task to modify the device list or template file for the configuration.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a CUG portlet.
2. Click the **Tasks** tab and select the tasks you want to edit.
3. Click the **Edit Task** icon and edit the following.
  - name
  - deployment file
  - type
  - template file
  - data file
  - device list
4. Click **Save**.

---

## Deleting a CUG task

Delete a CUG task to select the tasks that you want to delete.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator** to open a CUG portlet.
2. Click the **Tasks** tab, select the tasks you want to delete.
3. Click the **Delete Task** icon.
4. Click **Yes** to confirm.

---

## Executing a configuration task

Execute a configuration to activate the task and start deployment.

### Procedure steps

1. From the navigation pane, click **Configuration Update Generator**.
2. Click the **Tasks** tab and select the tasks you want to deploy.
3. Click the **Activate Task** icon.
4. Click **OK** to confirm and start the deploy operation.

The Progress column shows the overall progress for the task and the Devices section shows individual progress for each device and device-specific messages.

### Important:

Task properties cannot be edited if the task is running.

---

## Viewing the progress of a configuration task

With the Status and Progress columns, you can see the progress of the deployment of the configuration. Status and progress are automatically updated while the task is running. Each row in the table reflects each selected device and displays the status of the configuration. The possible status results are deploying file, creating unique configuration file, activating file, transferring file, completed successfully, and error. Possible reasons for errors are also displayed. You can view the status information from your browser while you are logged on to the Avaya BCM client.

---

## CUG Wizard

With the Configuration Update Generator (CUG) Wizard, you can quickly configure and deploy multidevice configuration update generator (CUG) tasks in a well-defined step by step process.

To use the CUG Wizard, you require the following licenses:

- COM 3.1
- BCM

You use the CUG Wizard to create template and mapping files and to deploy and schedule a CUG task. The following procedures are defined in the CUG Wizard:

- Launch CUG Wizard—Launches the CUG task creation wizard from the CUG task grid portlet toolbar.
- Describe the task—Use the initial wizard screen to describe the CUG task primary task properties, which are task name and target devices.

- Define and create a template file—Use the template file wizard screen to create a command template file.
- Define and create a data mapping file—Use the data file screen to create a CSV data file.
- Deploy and schedule the task—Use the final wizard screen to schedule and deploy the task to the CUG task grid.

---

## Variable definitions

The following table describes the command buttons available on the CUG Wizard screens.

**Table 21: CUG Wizard command buttons**

Command button	Description
Select All	Selects all devices for the task.
Save	Saves the task.
Cancel	Closes the CUG Wizard.
Back	Returns to the previous screen.
Next	Advances to the next CUG wizard screen.
Help	Opens the Help interface.

---

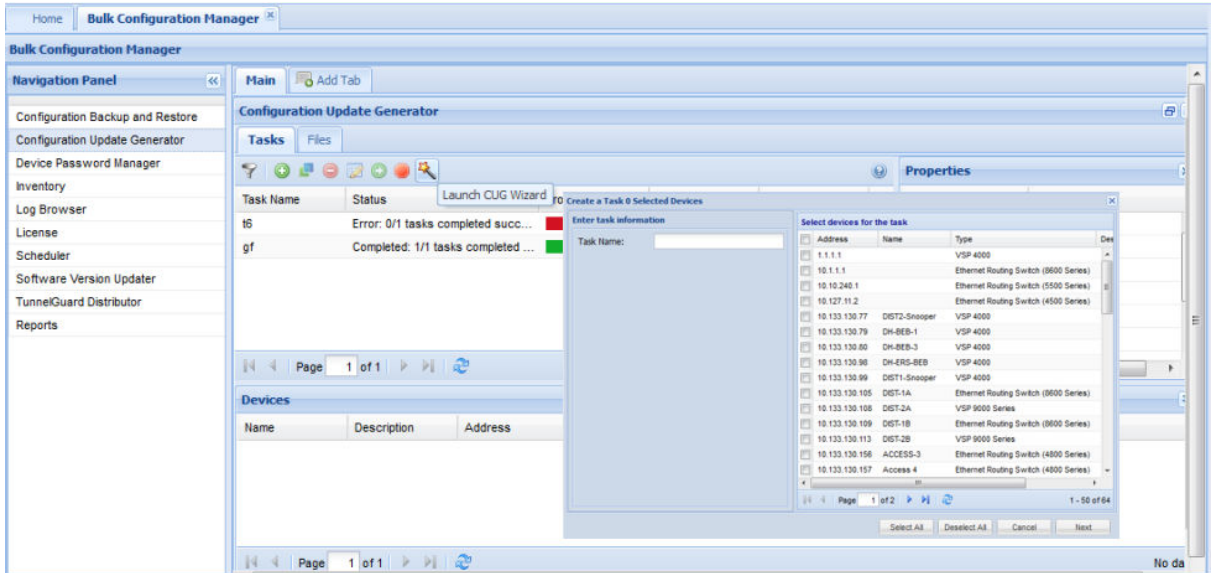
## Launching the CUG Wizard

Perform the following procedure to launch the CUG Wizard from the CUG task toolbar.

### Procedure

1. From the COM navigation panel, expand **Managers**.
2. Click **Bulk Configuration Manager**.
3. From the Bulk Configuration Manager Navigation Panel, click **Configuration Update Generator**, and select a Configuration Update Configuration Generator portlet.
4. From the CUG portlet toolbar on the Tasks tab, click **Launch CUG Wizard**.

The Create a Task window displays.



### Next steps

Perform the procedure for [Creating a task](#) on page 48.

---

## Creating a task

Perform the following procedure to create a task using the CUG Wizard.

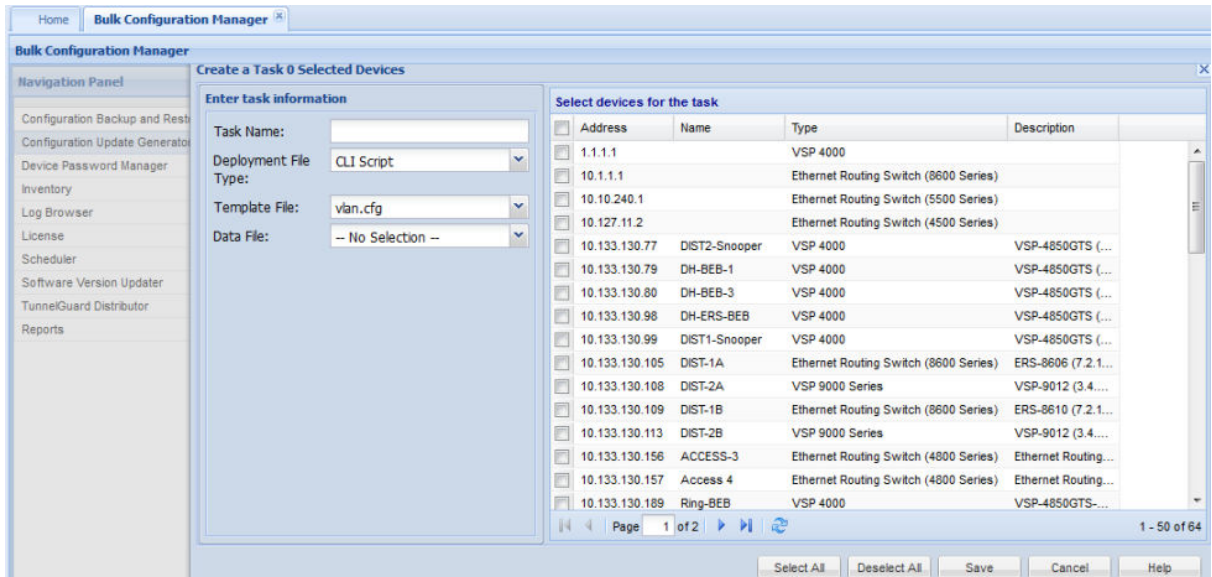
### Before you begin

- Launch the CUG Wizard.



## Procedure

1. From the Create a Task screen, in the Task Name field, enter a task file name.



2. From the Select devices for this task section, check the check box next to one device, or more than one device, for the task.

- Or, to select all devices in the list, click **Select All**.

3. Click **Next**.

## Next steps

Perform the procedure for [Creating a template file](#) on page 50, or [Editing a template file](#) on page 51.

## Variable definitions

The following table describes the fields on the CUG Wizard Create a Task screen.

**Table 22: CUG Wizard Create a Task screen**

Attribute	Value	Description
Task Name	<textbox>	Name of the task.
Address	<IP address>	The IP address of the device.
Type	<textbox>	The device type.
Description	<textbox>	The description of the device.

## Creating a template file

Perform the following procedure to create a template file using the CUG Wizard.

### Before you begin

- Create a task using the CUG Wizard.

### Procedure

1. From the Create a task template file screen, in the File Type section, select **New File**.
2. In the Template Name field, enter the name of the template.
3. Enter the CLI/ACLI commands in the Template file contents section.
4. Click **Next**.

#### \* Note:

If the template file you create does not contain any ??? character sequences denoting a variable definition required in a data mapping file, the Create variable mapping file screen does not appear.

### Next steps

Perform the procedure for [Creating a variable mapping file](#) on page 53.

## Variable definitions

The following table describes the fields on the CUG Wizard Create a task template file screen.

**Table 23: CUG Wizard Create a task template file screen**

Attribute	Value	Description
File Type	Option button	Select file type. You can select from the following options: <ul style="list-style-type: none"> <li>• Create a new file</li> <li>• Edit an existing file</li> </ul>
Template Name	<textbox> Drop-down list box	Enter the name of the template file. If you select an existing file, a drop-down list box of existing templates appears.
Template file contents (CLI/ACLI commands)	Configuration CLI/ACLI script	Contains the actual CLI/ACLI command lines to be executed against each selected target device.  If a CLI command line in the template file contains a variable with a different value depending on target device, the character sequence ??? preceeds the LI/ ACLI command.

Attribute	Value	Description
		<p>For example, in <code>cmd1 ???arg1</code>, the variable <code>arg1</code> accepts different values for different target devices. The following is an example of a template file designed to set a new prompt value and a new history count.</p> <pre>set prompt ???name set history ???count</pre> <p>In the preceding example, the actual values of <code>name</code> and <code>count</code> and the associated target device IP addresses appear in a separate variable mapping file. If args from the template file do not need to be a variable, that is, args do not need to change depending on target device, then you do not create a variable mapping file.</p> <p>For example, the following file example implies that all args have a fixed constant value for all associated target devices.</p> <pre>set prompt `8600 &gt;` set history 10</pre> <p>If the template file contains constant <code>arg</code> values, the variable mapping file creation step is omitted.</p>

## Editing a template file

Perform the following procedure to edit a template file using the CUG Wizard.

### Before you begin

- Create a task.

### Procedure

1. From the Create a task template file screen, in the File Type section, select **Existing File**.
2. In the Template Name field, click the file name that you want to edit.
3. Click **Next**.

#### Note:

If the template file you create does not contain any ??? character sequences denoting variable definition required in a data mapping file, the Create a variable mapping file screen does not appear.

### Next steps

Perform the procedure for [Creating a variable mapping file](#) on page 53.

## Variable definitions

The following table describes the fields on the CUG Wizard Create a task template file screen.

**Table 24: CUG Wizard Create a task template file screen**

Attribute	Value	Description
File Type	Option button	Select file type. You can select from the following options: <ul style="list-style-type: none"> <li>• Create a new file</li> <li>• Edit an existing file</li> </ul>
Template Name	<textbox> Drop-down list box	Enter the name of the template file. If you select an existing file, a drop-down list box of existing templates appears.
Template file contents (CLI commands)	Configuration CLI script	<p>Contains the actual CLI command lines to be executed against each selected target device.</p> <p>If a CLI command line in the template file contains a variable with a different value depending on target device, the character sequence ??? precedes the CLI command.</p> <p>For example, in <code>cmd1 ???arg1</code>, the variable <code>arg1</code> accepts different values for different target devices. The following is an example of a template file designed to set a new prompt value and a new history count.</p> <pre>set prompt ???name set history ???count</pre> <p>In the preceding example, the actual values of <code>name</code> and <code>count</code> and the associated target device IP addresses appear in a separate variable mapping file. If args from the template file do not need to be a variable, that is, args do not need to change depending on target device, then you do not create a variable mapping file.</p> <p>For example, the following file example implies that all args have a fixed constant value for all associated target devices.</p> <pre>set prompt `8600 &gt;` set history 10</pre> <p>If the template file contains constant <code>arg</code> values, the variable mapping file creation step is omitted.</p>

## Creating a variable mapping file

Perform the following procedure to create a variable mapping file using the CUG Wizard.

**\* Note:**

If the template file you create does not contain any ??? character sequences denoting variable definition required in a data mapping file, the Create a variable mapping file screen does not appear.

### Before you begin

- Create a new template or edit an existing template.

### Procedure

1. From the Create a variable mapping file screen, in the Mapping File name field, enter the name of the mapping file.
2. Click on an argument cell associated with a device, and enter a value.

After you select an argument cell, the command line from the template file appears within the lower left of the window frame.

3. To sync a variable, click the **Sync Variable** icon.
4. Click **Next**.

### Next steps




Perform the procedure for [Scheduling and saving a task](#) on page 54.

## Variable definitions

The following table describes the fields on the CUG Wizard Create a variable mapping file screen.

**Table 25: CUG Wizard Create a variable mapping file screen**

Attribute	Value	Description
Mapping File name	<textbox>	Name of the mapping file.
Sync Variable	Button	Syncs an argument value to all instances, therefore using the same value for all devices.
Address	<IP address>	IP address of a device.
arg1	<???variable name>	Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value.

Attribute	Value	Description
		<p> <b>Note:</b></p> <p>After you select an argument cell, the command line from the template file appears within the lower left of the window frame.</p>
arg2	<???variable name>	<p>Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value.</p> <p> <b>Note:</b></p> <p>After you select an argument cell, the command line from the template file appears within the lower left of the window frame.</p>
arg3	<???variable name>	<p>Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value.</p> <p> <b>Note:</b></p> <p>After you select an argument cell, the command line from the template file appears within the lower left of the window frame.</p>

---

## Scheduling and saving a task

Perform the following procedure to schedule and save a task with the CUG Wizard.

### Before you begin

- Create a new template or edit an existing template.
- Create a variable mapping file, if available.

### Procedure

1. On the CUG Task description screen, confirm Task Name, Template File Name, and Map File Name.
2. Click **Next**.
3. Perform one of the following actions:
  - Click **Finish** and proceed to final step.
  - Click **Schedule Task** to start the task configuration.
4. On the Add a schedule screen, enter the following information enter the schedule name.
5. Select the Tool Name.
6. Select the Task Name.
7. Enter the Start date.

8. Enter the Start time.
9. Enter the Internal Value.
10. Select an Internal Unit.
11. Check the Enabled check box.
12. Click **Save**.

---

## Variable definitions

The following table describes the fields on the CUG Task description screen.

**Table 26: CUG Wizard CUG Task description screen**


Attribute	Value	Description
Task Name	<textbox>	Name of the task.
Template File Name	<textbox>	Name of the template file.
Map File Name	<textbox>	Name of the map file.

---

## Variable definitions

The following table describes the fields on the CUG Wizard Add a schedule screen.

**Table 27: CUG Wizard Add a schedule screen**

Attribute	Value	Description
Schedule Name	<textbox>	Name of the CUG task schedule.
Tool Name	Drop-down list box	Name of the Bulk Configuration Manager tool.
Task Name	Drop-down list box	Name of the CUG task.
Server Date	Predetermined date	The start date the server assigns to the schedule.   <b>Note:</b> The server date may be different from the date on your computer.
Start Date	<textbox>	Date you assign the schedule to start.
Start Time	<numeric>	Time you assign the schedule to start.
Internal Value	<textbox>	Number that represents the seconds, minutes, hours, and days for the internal unit setting.
Internal Unit	Drop-down list box	Value you assign to repeat the activation of the task in selected increments of seconds, minutes, hours, days, or weekly.

Attribute	Value	Description
Enabled	Check box	Enables the scheduled task to run.

---

## Logging and log browsing

With Log Browser, you can log all your interactions with devices to a common file. You can browse a maximum of two files to access recent log data.

The following topics describe log browser activities.

---

### Refreshing the logs list

Refresh the logs list to see the most recent messages in the Log Browser.

#### Procedure steps

1. From the navigation pane, click **Log Browser** to open a Log Browser portlet.
2. Click the **Refresh** icon.

The log messages list is updated to display the most recent messages.

---

### Filtering the logs

Filter the logs view to reduce the amount of the information that appears in the portlet to specific subset.

#### Procedure steps

1. From the navigation pane, click **Log Browser** to open a log browser portlet.
2. Click **Filter Log**.  
The View log settings dialog box appears.
3. In the **Start Time** field, specify the start time of the period for which you want to view the logs.
4. In the **End Time** field, specify the end time of the period for which you want the view the logs.
5. In the **Tool Name** field, select the tool name that you want to filter on.
6. In the **Key Word** field, enter the keyword you wish to filter.
7. Click **Save**.

---

### Configuring log settings

Perform the following procedure to configure the log settings.



## Procedure

1. From the navigation pane, click **Log Browser** to open a log browser portlet.
2. Click **Log Settings**.
3. In the Logger refresh section, to enable refreshing of the logs, select **Enable refresh**, and then specify the time in seconds in the **Refresh time** box.
4. In the Colors section, select the **Enable log colors** check box, and then select different colors for the various message levels.
5. Click **Save**.

---

## Customizing the Log Browser list view

Customize the log browser list view to include the columns of your choice.

### Procedure steps

1. From the navigation pane, click **Log Browser** to open a log browser portlet.
2. Click down arrow button.  
A popup window appears with columns.
3. Point to Columns.  
A popup window appears with the available columns that can be displayed in the log browser list view. The columns that are currently visible have the check box beside them selected.
4. To remove a column from the log browser list view, clear the check box beside the column name that you want to remove.  
The customized log browser list appears.
5. To add a column to the log browser list view, select the check box beside the column name that you want to view.  
The customized log browser list appears.

---

## Clearing all view filtering

Clear the view filtering to view all the information on the Log Browser portlet.

### Procedure steps

1. From the navigation pane, click **Log Browser** to open a log browser portlet.
2. Click **Filter**.  
The Apply Filter dialog box appears.
3. Click **Clear**.  
The Log Browser portlet is returned to full view.

## Exporting log browser information

Avaya BCM stores the information that appears in the Log Browser portlet in a file called BCM\_audit.log. When this file reaches 10M, Avaya BCM saves it as BCM\_audit.log.1 and creates a new BCM\_audit.log file. The Log Browser displays the two most recent log files. You can open or save the current log file, or older log files, on your local computer by using the Export Logs feature.

### Procedure steps

1. From the navigation pane, click **Log Browser** to open a log browser portlet.
2. Click **Export Logs**.  
The list of log files appears.
3. Select the file that you want to export.
4. In the dialog box, select **Open** or **Save**.
5. Click **OK**.

---

## Inventory management

Add and store devices on Avaya BCM using Inventory.

The following procedures describe Inventory activity.

---

## Adding devices to Inventory

Add devices to the Inventory to view them on the portlet.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Click **Add Device**.  
The Add a device window appears.
3. Type the **IP address** of the device.
4. Select the **Device Type** from the drop-down menu.

Optionally, you can enter the following information:

- Name
- Description
- Location
- Hardware Platform
- Software version

5. Click **Add**.

---

## Filtering the devices

Filter the devices view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Click the **Filter** devices icon.  
The Add a filter dialog box appears.
3. Select the check box of the device that you want to filter.

**\* Note:**

To display all the devices, select device type check box.

4. (Optional). To filter using the IP address, in the IP address field, enter the IP address of the device that you want to filter.
5. (Optional). To filter using the device name, in the Name field, enter the name of the device that you want to filter.
6. Click **Find**.  
The filtered information appears in the Inventory table.

---

## Duplicating devices in the Inventory

Duplicate devices in the Inventory devices table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Select the device to duplicate, and click **Duplicate Device**.  
The Duplicate a device dialog box appears.
3. In the IP address field, enter the IP address of the device that you to duplicate.

**\* Note:**

You cannot duplicate the IP address.

4. In the remaining fields, change the details as per your requirements.
5. Click **Duplicate**.  
The duplicate device appears in the Inventory table.

---

## Editing items in the Inventory

Edit all the fields in the Inventory portlet except IP Address and Device Type.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Select the device for which you want to change the attributes.
3. Click **Edit**.  
The Edit Device dialog box appears.
4. Edit the element attributes.
5. Click **Save**.

---

## Importing devices to Inventory

Import devices to the Inventory using csv files stored in your system. The following table shows a sample csv file.

120.120.110.1	VPN_ROUTER	device_name_1	description_1	location_1	hardware_type_1	software_type_1
120.120.110.2	SR_TASMAN	device_name_2	description_2	location_2	hardware_type_21	software_type_2
120.120.110.3	SR_TORNADO	device_name_3	description_3	location_3	hardware_type_3	software_type_3
120.120.110.4	SNAS	device_name_4	description_4	location_4	hardware_type_4	software_type_4
120.120.110.5	ERS_8600	device_name_5	description_5	location_5	hardware_type_5	software_type_5
120.120.110.6	ERS_8300	device_name_6	description_6	location_6	hardware_type_6	software_type_6
120.120.110.7	ERS_2500	device_name_7	description_7	location_7	hardware_type_7	software_type_7
120.120.110.8	ERS_4500	device_name_8	description_8	location_8	hardware_type_8	software_type_8
120.120.110.9	ERS_5500	device_name_9	description_9	location_9	hardware_type_9	software_type_9
120.120.110.10	NVG	device_name_10	description_10	location_10	hardware_type_10	software_type_10
120.120.110.11	ES_470/460	device_name_11	description_11	location_11	hardware_type_11	software_type_11

120.120.110.12	ERS_5600	device_name_12	description_12	location_12	hardware_type_12	software_type_12
120.120.110.13	BSR_222	device_name_13	description_13	location_13	hardware_type_13	software_type_13
120.120.110.14	BSR_252	device_name_14	description_14	location_14	hardware_type_14	software_type_14
120.120.110.15	ERS_8800	device_name_15	description_15	location_15	hardware_type_15	software_type_15
120.120.110.16	VSP_DEVICE	device_name_16	description_16	location_16	hardware_type_16	software_type_16
120.120.110.17	WC_8180_DEVICE	device_name_17	description_17	location_17	hardware_type_17	software_type_17

### Procedure steps

1. From the navigation pane, click **Inventory** to open an Inventory portlet.
2. Click **Import**.

The Import device(s) from csv file window appears.

3. Browse to locate the csv file.
4. Click **Import**.

The import completes. The imported devices appear in the inventory devices table.

#### **Note:**

Devices that were previously imported are replaced in the inventory devices table with the new imported devices. Only manually imported devices are retained.

---

## Exporting devices to .csv file

Export devices to .csv file.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Select the device that you want to export.
3. Click **Export Inventory to .csv**.

The Insert file name to export to dialog box appears.

4. Type the file name, and then click **Export**.

The File Download popup window appears.

5. Select **Open** to open the .csv file or **Save** to save the file on your local system.

## Removing items from the Inventory

Remove items that you no longer need from your Inventory.

### Procedure steps

1. From the navigation pane, click **Inventory** to open an inventory portlet.
2. Select the device that you want to remove.
3. Click **Delete**.
4. Click **Yes** to confirm.

---

## Importing devices from COM

Perform the following procedure to import the device inventory from the Configuration and Orchestration Manager (COM) to the Avaya Bulk Configuration Manager (Avaya BCM).

### Prerequisites

Ensure that you log on to COM as an administrator.

### Procedure steps

1. From the Navigation pane, expand the **Managers** pane, and click **Bulk Configuration Manager**.
2. From the Bulk Configuration Manager navigation panel, click **Inventory**.
3. From the Inventory portlet tool bar, click **Import from COM**.  
The Import from COM dialog box appears.
4. Click **Yes**.

The Status of Import window appears to indicate that the import from COM was successful.

---

## Device Password Manager

The following topics describe how to manage Device Password Manager (DPM) tasks.

---

## Managing DPM tasks

Complete the following procedures to manage password management tasks.

### Prerequisites

- You must be logged on to the Avaya BCM.
- You must have Security Administrator rights to use DPM.

---

## Creating a DPM task

Create the DPM task to group devices that have the same credentials.

### Procedure steps

1. From the navigation pane, click **Device Password Manager** to open a new or existing DPM portlet.
2. Click **Add Task**.  
The Create a Task dialog box appears.
3. Type the task name.
4. Type and confirm the administrator password and/or SNMP Read/write community string data.
5. Select the list of devices to be added to the task.
6. Click **Save**.

---

## Filtering the DPM tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

1. From the navigation pane, click **Device Password Manager** to open a DPM portlet.
2. Click the **Filter** icon.  
The Add a filter dialog box appears.
3. In the Task Name field, type the task name or the first letter of the task name you want to filter.

 **Note:**

To display all the tasks, leave the Task Name field empty.

4. Click **Find**.

The filtered information appears in the DPM tasks table.

---

## Duplicating a DPM task

Duplicate a DPM task in the DPM tasks table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

### Procedure steps

1. From the navigation pane, click **Device Password Manager** to open a DPM portlet.
2. Select the task to duplicate.

3. Click the **Duplicate Task** icon.  
You are prompted to confirm the task duplication.
4. Click **Yes**.  
The duplicate task appears in the DPM tasks table.

---

## Editing a DPM task

Edit a DPM task to modify the device list.

### Procedure steps

1. From the navigation pane, click **Device Password Manager** to open a DPM portlet.
2. Select the task you want to edit.
3. Click **Edit** to edit the following.
  - task name
  - list of devices
  - password and/or the communities
4. Click **Save**.

---

## Executing a DPM task

Execute a DPM task to activate the task and to start deployment.

### Procedure steps

1. From the navigation pane, click **Device Password Manager** to open a DPM portlet.
2. Select the task you want to run.
3. Click **Activate Task**.
4. Click **OK** to confirm.

The deploy operation starts. The Progress and Status in the Device Table show overall progress for the task, individual progress for each device, and device-specific messages.

---

## Deleting a DPM task

Delete a DPM task to remove the tasks that you do not require.

### Procedure steps

1. From the navigation pane, click **Device Password Manager** to open a DPM portlet.
2. Select the tasks you want to delete.
3. Click **Delete Task(s)**.



4. Click **Yes** to confirm.

---

## Viewing the progress of a password management task

The Status and Progress columns shows the progress of the task for each device in the Device table. Status and progress are automatically updated while the task is running. Each row in the table reflects the selected device and displays the status of the task; the status and progress are updated while the task runs. Example status results are establishing connection to device, changes successfully applied, and error. The possible reasons for error appear. You can view the status information from your browser while you are logged on to the Avaya BCM client. You can view the table only in maximized view.

---

## Software version upgrades

The following topics describe software upgrade tasks.

### Important:

If you perform an upgrade in the Bulk Configuration Manager using the Software Version Updater, the BCM may not accept certain characters such as brackets. For example, if you download a device code that contains brackets, and the BCM does not accept the format, you must remove the brackets and rename the file.

---

## Managing software version images on the file server

Complete the following procedures to manage software version images on the file server. For more information about managing software version images, see [Software Version Updater](#) on page 27.

### Prerequisites

- You must be logged on to the Avaya BCM.
- You must have entered the required device information.

---

## Adding an image package to the file server

Use this procedure to add an image package to the server. An image package contains all the files necessary for an upgrade. You can use SVU to update a group of devices of the same type.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Click the **Packages** tab, and click **Add**.

The Create Package window appears.

3. Select the device type.
4. Type the package name.
5. Click **Browse**.

A file browser dialog box appears.

6. Browse to the image file in the browser window.
7. Click **Open**.
8. Click **Upload file**.

The file transfers to the server and appears in the file table. Repeat steps 5-8 until all files in the software package are added.

9. Click **Close**.

---

## Removing an image package from the file server

Use the following procedure to remove an image package from the server.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Click the **Packages** tab, and select the image package you want to delete.
3. Click **Delete**.
4. Click **Yes** to confirm.

---

## Editing files from a package

Edit files from a package to add or edit files.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Click the **Packages** tab, and select the package to edit.
3. Click **Edit**.  
An Edit Package window appears.
4. Select the files you want to delete from the package.
5. Click **Delete selected files**.
6. Click **Yes** to confirm.

---

## Creating an SVU task

Create an SVU task to group devices to be updated.

## Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Select the Tasks tab.
3. Click **Add Task**.
4. Type the task name.
5. Select the device type from the list.

**\* Note:**

For the Avaya Ethernet Routing Switch 8600, the Avaya BCM provides option to save the upgraded image on a PCMCIA card.

6. Select the package name from the list.
7. Select the list of devices to update from the list that appears.
8. Click **Save**.

---

## Filtering the SVU tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Select the **Tasks** tab.
3. Click **Filter Tasks**.

The Add a filter dialog box appears.

4. In the Task Name field, type the task name or the first letter of the task name you want to filter.

**\* Note:**

To display all the tasks, leave the Task Name field empty.

5. Click **Find**.

The filtered information appears in the SVU tasks table.

---

## Duplicating an SVU task

Duplicate an SVU in the SVU tasks table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Select the **Tasks** tab.
3. Select the task to duplicate.

4. Click the **Duplicate Task** icon.  
You are prompted to confirm the task duplication.
5. Click **Yes**.  
The duplicate task appears in the SVU tasks table.

---

## Running an SVU task

Run the SVU task to update the devices in the task list that you created.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Select the **Task** tab.
3. Select the task you want to run.
4. Click **Activate Task(s)** from the task table field.
5. Click **OK** to confirm the activation.

---

## Editing an SVU task

Edit an SVU task to modify your device list for the task.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Click the **Tasks** tab and select the task you want to edit.
3. Click **Edit**, and edit the following.
  - name
  - device type
  - package name
  - list of devices
4. Click **Save**.

---

## Deleting an SVU task

Delete an SVU task that you no longer require.

### Procedure steps

1. From the navigation pane, click **Software Version Updater** to open an SVU portlet.
2. Select the tasks you want to delete.
3. Click **Delete**.

4. Click **Yes** to confirm.

---

## Viewing the progress of a software update task

The Status column shows the progress of the task for each device in the Device table. Each row in the table reflects each selected device and displays the status of the task. Example status results are establishing connection to device, deploying file, completed successfully, and error. The possible reasons for error appear. You can view the status information from your browser while you are logged on to the Avaya BCM client. You can view the table only in maximized view.

---

## Configuration Backup and Restore

The following topics describe how to manage Configuration Backup and Restore (CBR) tasks.

---

### Managing the backup tasks

The following section contains information about how to manage configuration backup tasks.

#### Configuring the location for backup archives

You can configure the location to store the backup archive in the file system or to external mounted disks.

#### Configuring the usage space

You can configure the usage space to alert you when there is 20% or less space on the file system for the backup archive. If there is 5% usage space left on the file system the backup should not be initiated.

#### Configuring the e-mail alert settings

Before you can use any e-mail alert function in COM, you must configure the e-mail alert settings. You can work with the e-mail server preferences to set up the SMTP values for your e-mail server. You also can use the COM preferences to enable or disable the e-mail alert function.

Perform the following procedure to configure an e-mail alert:

##### Procedure

1. From the Navigation pane, open **Admin** and then select **Preferences**.

The Preferences window opens.

2. In the Email Server section on the **General** tab, enter values in the following fields:

- SMTP Host

- SMTP User Name
- SMTP Password
- From User (optional)
- To Recipient (optional)
- Port

In the Preferences tool, if you enter values in the From User and To Recipient fields, and then configure a backup task, SVU task, or trap parser, the From User and To Recipient fields from the tasks are automatically populated with the corresponding information from the Preferences tool. However, you can override the preference information in the task creation.

3. Specify whether you want to enable the e-mail alert function.

Option	Enable E-mail
Enabled	Selected
Disabled	Cleared

4. Click **Save Preferences**.
5. **(Optional)** Click the **Test Email** button to test the e-mail function.

**\* Note:**

When the **Test Email** button is clicked you may receive an error message stating your anti-virus software is blocking mass e-mail or e-mail worms. This can happen when anti-virus software installed on the COM Server is configured to block mass mailing. In order to avoid this, disable the blocking option through the anti-virus software installed on the COM server. For more information, see [COM email settings](#) on page 86.

## Creating a configuration backup task

You can use the Configuration Backup and Restore (CBR) tool to back up and restore device configuration parameters. You can configure the COM application to perform a backup diff based on a previous config or baseline. When the backup occurs, the system generates a readable copy of the running device configuration. You can use these readable files to list diff values for a selected device in a report format.

When you create a backup task, you also can set up an e-mail alert function to e-mail the diff between backups. The config diff settings that you set in the diff type preferences determine what the system e-mails and when.

You can set e-mail alert baselines to determine when the system sends an e-mail alert and what the alert contains. When you create a backup task, you use the diff type settings to specify a string match value. If the string value in the diff type settings match diff lines in the backup, the system sends an e-mail alert. Also, the e-mail alert only contains backup information for the device that contains your string match value.

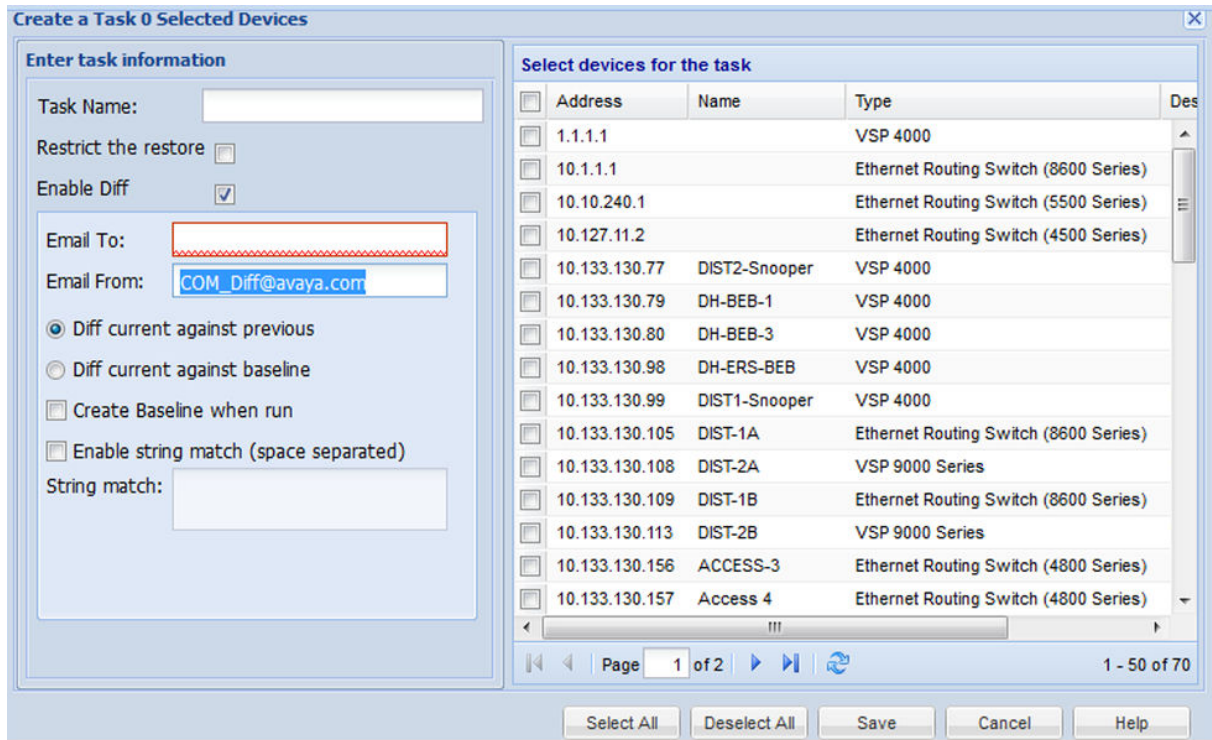
The system generates an e-mail alert after the first two backup events have occurred for the same device.

Perform the following procedure to create a configuration backup task:

**Procedure**

1. From the navigation pane, double-click **Configuration Backup and Restore** icon to open a CBR portlet.
2. Click the **Backup** tab, and click **Add**.

The Create a Task window displays.



3. Type the backup task name.
4. Specify whether you want to enable the **Restrict the restore** field.

Option	Restrict the restore
Enabled	Selected
Disabled	Cleared

When selected, Avaya BCM allows the restore operation only on devices that have the same software version at the time of the backup.

5. Select the list of devices to be backed up.
6. Specify whether you want to enable the diff function for e-mail alerts.

Option	Enable Diff
Enabled	Selected
Disabled	Cleared

If you chose to disable the diff function for e-mail alerts, go to the final step.

7. In the Diff Type section, enter values in the following fields:

- **Email To** — Specifies the recipient of the e-mail alert.
- **Email From** — Specifies the sender of the e-mail alert.

8. Select a radio button option to specify the type of backup diff you would like to use:

- **Diff current against previous** — Run a backup diff based on a previous config.

If you choose this option, select the devices for which you want to perform a diff on a previous config. Your selections must be made in the **Select devices for the task list** box.

- **Diff current against baseline** — Run a backup diff based on a baseline.

If you choose this option, you must set a backup baseline for a device in the **Baseline** tab in the CBR portlet.

9. Specify whether you want to create a baseline when the backup is run:

Option	Create Baseline when run
<b>Enabled</b>	Selected
<b>Disabled</b>	Cleared

10. Specify whether you want to enable run a backup diff with a string match:

Option	Enable string match
<b>Enabled</b>	Selected
<b>Disabled</b>	Cleared

When selected, you must enter a string match value in the accompanying **String match** list box.

11. Click **Save**.

### Example

To illustrate a string match example, you may want to only see the addition or deletion of ip static routes on a group of 8600 devices. In such a scenario, you enter a string match value of `ip static-route`. When the system runs a backup process and diff is performed, an e-mail alert is generated and sent only if the diff lines contain the string `ip static-route`.

### Next steps

You can set a backup baseline for a device in the **Backup** tab.

## Filtering the configuration backup tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.



2. Click the **Backup** tab, and click **Filter**.

The Add a filter dialog box appears.

3. In the Task Name field, type the task name or the first letter of the task name you want to filter.

**\* Note:**

To display all the tasks, leave the Task Name field empty.

4. Click **Find**.

The filtered information appears in the Backup tasks table.

## Setting a backup baseline for a device

You can configure the COM application to perform a backup diff based on a previous baseline. When you set up the baseline, you have the option to work with a specific IP address and a backup date. Your IP selection determines the device on which the COM application performs the backup baseline diff. Your backup date selection determines the date for which the COM application uses for future backup comparisons.

Ensure that at least one backup event has occurred for the backup task before you set a baseline value.

Perform the following procedure to set a backup baseline for a device:

### Procedure

1. From the navigation pane, double-click the **Configuration Backup and Restore** icon to open a CBR portlet.
2. On the **Baseline** tab, select the IP address of the device in which you want to set a baseline.
3. Select a backup date value from the drop down menu to set a baseline backup date for the device.
4. Click **Set selected config as Baseline**.

## Duplicating a configuration backup task

Duplicate a configuration backup task in Backup tasks table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Backup** tab and select the task that you want to duplicate in the Backup tasks table.
3. Click **Duplicate Task**.  
You are prompted to confirm the task duplication.
4. Click **Yes**.

The duplicate task appears in the Backup tasks table.

## Editing a configuration backup task

Edit a configuration backup task to modify the list of devices in the task.

Perform the following procedure to edit a configuration backup task:

### Procedure

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Backup** tab and select the task to be edited and click **Edit**.
3. **(Optional)** Edit the values in the following fields:
  - **Task Name**
  - **Restrict the restore**  
When selected, Avaya BCM allows the restore operation only on devices that have the same software version as at that of the backup.
  - **Enable Diff**  
When selected, you can use the diff type settings to determine when an e-mail alert is sent and what the alert contains.
4. **(Optional)** Edit the following field values in the Diff Type section:
  - **Email To**
  - **Email From**
  - **Diff current against previous**  
If you choose this option, select the devices for which you want to perform a diff on a previous config. Your selections must be made in the Select devices for the task list box.
  - **Diff current against baseline**  
If you choose this option, you must set a backup baseline for a device in the Baseline tab in the CBR portlet.
  - **Create Baseline when run**
  - **Enable string match**  
When selected, you must enter a string match value in the accompanying **String match** list box.
5. Click **Save**.

### Next steps

You can set a backup baseline for a device in the **Backup** tab.

## Executing a configuration backup task

Execute the configuration backup task to activate the configuration backup task that you created.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.

2. Click the **Backup** tab, and select the task you want to run.
3. Click **Activate**.
4. Select **Yes** to confirm.

## Deleting a configuration backup task

Delete a configuration backup task if you wish to discontinue configuration backups for the listed devices.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Backup** tab, and select the tasks to be deleted.
3. Click **Delete**.
4. Click **OK**.
5. Select **Yes** to confirm.

## Running a backup diff report

The reporting feature works in tandem with the backup and restore tool. You can use the reporting feature to run diff reports on any device that has more than one backup. This report feature allows you to select the devices and the backups you wish to see in the diff report. You have the option to see your report in either an html or a pdf format.

Perform the following procedure to run a backup report:

### Before you begin

You must configure a backup task and the backup function must run twice before you can run a report.

### Procedure

1. From the Navigation pane, double click **Reports**.  
The Reports window opens.
2. In the **Diff Reports** tab, select the first device file listing on the **Backup Date** column.
3. Select the second device file listing on the **Backup Date2** column.
4. Click **Create Report**.

---

## Managing the restore tasks

The following section contains information about how to manage configuration restore tasks.

## Filtering the configuration restore tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab.
3. Click **Filter Tasks**.

The Add a filter dialog box appears.

4. In the Task Name field, enter the task name or the first letter of the task name you want to filter.

 **Note:**

To display all the tasks, leave the Task Name field empty.

5. Click **Find**.

The filtered information appears in the Restore tasks table.

### Viewing the backup details

View the backup details of file that was previously added into Avaya BCM.

#### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab and select the file that you want to view.
3. Click **View Backup Details**.

The View Backup Details popup window appears.

4. From the file list, select the file that you want to view.

The File Download popup window appears.

5. Select **Open** or **Save**.

### Editing a configuration restore task

Edit a configuration restore task to modify the list of devices in the task.

#### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab, and select the task to be edited.
3. Click the **Edit task** icon.

The Edit a task popup window appears. The Task Name, Device Address, and Device Version fields are dimmed and inaccessible.

4. Enable or disable the **Restrict the same version** field; when selected, Avaya BCM allows the restore operation only on devices that have the same software version as that of the backup.

5. Click **Save**.

## Comparing configuration restore files

Use this procedure to compare the configuration restore files and view the differences between them.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab, and select the two files that you want to compare. Use the Ctrl or Shift key to select the files.
3. Click **Compare**.

The popup window appears and you are prompted to compare the files.

4. Click **Yes**.

The File Download popup window appears.

5. Click **Open** or **Save**.

If you choose to open the file, the Smart Diff window displays, indicating the configuration differences between the files.

If you choose to save the file, a copy is downloaded to your desktop.

## Running a configuration restore task

Run a configuration restore task to restore backup archives.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab, and select the backup archive you want to restore.
3. Click **Activate Restore Task**.
4. Click **Yes** to confirm.

## Deleting a configuration restore task

Delete a configuration restore task to discontinue configuration restoration for the listed devices.

### Procedure steps

1. From the navigation pane, click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Restore** tab, and select the archives to be deleted.
3. Click **Delete**.
4. Click **Yes** to confirm.

## Viewing the progress of a backup or restore task

The Status and Progress columns appear in the CBR portlet for backup and restore tasks. Each row in the Backup Device Table reflects each selected device and displays the status of the backup for that device. Click the Refresh button to retrieve the current status of the listed tasks. The possible status results are ready, in progress, completed, and error. The possible reasons for error appear.

You can view the status information from your browser while you are logged on to the Avaya BCM client.

**!** **Important:**

If you backup a device, change the password, then restore the backup, the device password can revert to the backed up password. However, the restore does not change the device password in the UCM credential service. If the restore causes this type of mismatch between passwords, you must manually change the password in the credential services to match the backed up password.

---

## Scheduling tasks on Avaya BCM

Create schedules for tasks for any of the other Avaya BCM tools using Scheduler.

**!** **Important:**

Scheduler uses the server time, rather than the client time, for scheduled tasks.

---

## Adding a schedule

Add a schedule to run tasks at regular, scheduled intervals.

### Procedure steps

1. From the navigation pane, click **Scheduler**.
2. Click the **Main** tab, and click the **Add** icon.  
The Add a Schedule window appears.
3. In the **Enter schedule information** section, configure the following:
  - In the **Schedule Name** field, type a schedule name.
  - Select a **Tool Name** from the drop-down menu. This is the Avaya BCM tool for which the task is scheduled.
  - Select a **Task Name** from the drop-down menu.
4. In the **from** section, configure the following to select the start date using the calendar function:
  - In the **Start Date** field, select the start date.
  - In the **Start Time** field, select the start hour and minutes (HH:MM).
- 5.
6. In the **Recurrence** section, configure the following:
  - In the **Interval Value** field, type the interval value. This is the interval for when the execution of the task is repeated.
  - In the **Interval Unit** field, select the interval unit from the drop-down menu.

7. Select to have the schedule enabled/disabled.
8. Click **Save**.

---

## Filtering the schedule tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **Scheduler**.
2. Click the **Filter** icon.  
The Add a filter dialog box appears.
3. In the **Task Name** field, type the task name or the first letter of the task name you want to filter.

 **Note:**

- To display all the tasks, leave the Task Name field empty.
4. Click **Find**.  
The filtered information appears in the Scheduler tasks table.

---

## Editing a schedule

Use this procedure to edit an existing schedule.

### Procedure steps

1. From the navigation pane, click **Scheduler**.
2. Select the task you want to edit.
3. Click **Edit Schedule**, and edit the details of the scheduled task.
4. Click **Save**.

---

## Deleting a schedule

Delete a schedule if the tasks no longer need to be done regularly.

### Procedure steps

1. From the navigation pane, click **Scheduler**.
2. Select the task you want to delete.
3. Click the **Delete task** icon.  
You are prompted to confirm the deletion.

4. Click **Yes** to proceed.

---

## Refreshing the schedule list

Use the following procedure to update the list of schedules that appear in the Schedules portlet.

### Procedure Step

1. From the navigation pane, click **Scheduler**.
2. Click the **Refresh** icon.

The schedule list is updated.

---

## Security management

The Tunnelguard Distributor (TGD) tool copies a TunnelGuard rule from one device to multiple devices and activates that rule on the associated domain group. TunnelGuard rules can only be applied to SNAS devices.

---

## TunnelGuard Distributor

Use the following procedures to manage TunnelGuard policies.

### Prerequisites

- You must be logged on to the Avaya BCM.

---

## Adding previously created TunnelGuard policies

Create a TGD task to copy an existing policy from one device to many devices.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor** to open a TGD portlet..
2. Click the **Add** icon.
3. Type a task name.
4. Select the source device from which you want to transfer the policy.
5. Click **Next >**.
6. Select the domain.
7. Select how you want the domains to be referenced.
8. Click **Next**.
9. Select the group you want to transfer.



10. Select how you want the groups to be referenced.
11. Select the rule name.
12. Click **Next >**.
13. Select the devices to which you want to transfer.
14. Click **Finish**.

---

## Filtering the TGD tasks

Filter the tasks view to reduce the amount of information that appears in the portlet to a specific subset.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor**.
2. Click **Filter**.  
The Add a filter dialog box appears.
3. In the Task Name field, enter the task name or the first letter of the task name you want to filter.

 **Note:**

To display all the tasks, leave the Task Name field empty.

4. Click **Find**.  
The filtered information appears in the TunnelGuard Distributor tasks table.

---

## Duplicating a TGD task

Duplicate a TGD task in the TGD tasks table. Avaya BCM duplicates a task by keeping all the tasks attributes and attaches a number to the end of the task name to make it unique.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor**.
2. Select the task that you want to duplicate.
3. Click the **Duplicate Task** icon.

You are prompted to confirm the task duplication.

4. Click **Yes**.  
The duplicate task appears in the TGD tasks table.

## Editing a TGD task

Edit a TGD task to change the domain, the group or the tunnel guard rule from the source device and the destination devices.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor**.
2. Select the task you want to edit.
3. Click the **Edit Task** icon.
4. Edit the task name.
5. Edit the source device.
6. Click **Next**.
7. Select the domain.
8. Select how you want the domains to be referenced.
9. Click **Next**.
10. Select the group you want to transfer.
11. Select how you want the groups to be referenced.
12. Select the rule name.
13. Click **Next**.
14. Select the devices to which you want to transfer.
15. Click **Finish**.

---

## Deleting a TGD task

Use the following procedure to delete a TGD task.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor**.
2. Select the tasks you want to delete.
3. Click the **Delete Task** icon.
4. Click **Yes** to confirm.

---

## Executing a TGD task

Execute a TGD task to copy a TunnelGuard rule from one device to multiple devices.

### Procedure steps

1. From the navigation pane, click **TunnelGuard Distributor** to open a TGD portlet.

2. Select the task you want to run.
3. Click the **Activate Task** icon.
4. Click **Yes** to confirm.

The copying operation starts.

---

## Viewing the progress of a tunnelguard task

With the Status and Progress columns, you can view the progress of the tunnelguard transfer. Status and progress are automatically updated while the task is running. Each row in the table reflects the selected source device and destination devices, and displays the status of the transfer. Click Refresh to retrieve the current status of the listed tasks. The possible reasons for error appear. You can view the status information from your browser while you are logged on to the Avaya BCM client.

# Chapter 6: Directory structure

You can install the Avaya Bulk Configuration Manager (BCM) on the following operating systems:

- Windows 2008 R2 (64-bit) (standard and enterprise flavors)
- Red Hat Enterprise Linux v5.6. v5.7 (both 64-bit)

The following table outlines the directory paths for the System Manager applications on each operating system.

Component	64-bit Windows	64-bit Linux
Database	C:\Avaya\smgr\MySQL	/opt/avaya/smgr/MySQL
JBoss	C:\Avaya\smgr\core\JBoss \6.1.0\jboss-as	/opt/avaya/smgr/core/JBoss/6.1.0/ jboss-as
COM	C:\Avaya\smgr\COM	/opt/avaya/smgr/COM

# Chapter 7: Troubleshooting

This chapter provides troubleshooting information for the Avaya Bulk Configuration Manager (Avaya BCM).

---

## Firewall Configuration

Avaya BCM uses Telnet, SSH, FTP, SCP, TFTP and SFTP protocols to communicate with various devices and transfer files. If there is a firewall between your device and the Avaya BCM server, you must open up the affected protocol in your firewall configuration.

---

## FTP servers

Do not install FTP servers on a machine on which Avaya BCM is installed. Avaya BCM starts its own FTP server and installing another FTP server causes the Avaya BCM to malfunction. If you experience problems with Avaya BCM, uninstall any FTP servers and reboot your machine.

---

## NAT

If you use Network Address Translation (NAT) on your network, ensure that the devices being manipulated can reach the Avaya BCM server IP address.

---

## Saving CLI/ACLI correspondence with a device to a file

Perform the following procedure to save CLI/ACLI correspondence with a device to file.

### Procedure steps

1. Create a new traffic.control file in the folder SMGR/COM.

**+ Tip:**

The traffic.control file is not a text or .txt file.

2. Open the file.
3. You can record traffic for all devices or for selected devices.
  - Option 1: To record traffic for all devices, type ALL on the first line of the traffic.control file and then Save and Close. Files of the form xx.xx.xx.xx.traffic are created in SMGR/COM folder.
  - Option 2: To record traffic for selected devices, type the IP address of each device on a separate line, and then Save and Close the file.
4. To disable traffic recording, you can delete the traffic.control file or type NONE on the first line of the traffic.control file so you can keep the information in the file.

---

## Terminal length

If you see an unexpected failure of BCM operation with the message “Error while getting device current running image”, then check the terminal length on the device using CLI. If the terminal length is 0, then set it to a nonzero value. The typical nonzero value is 23.

---

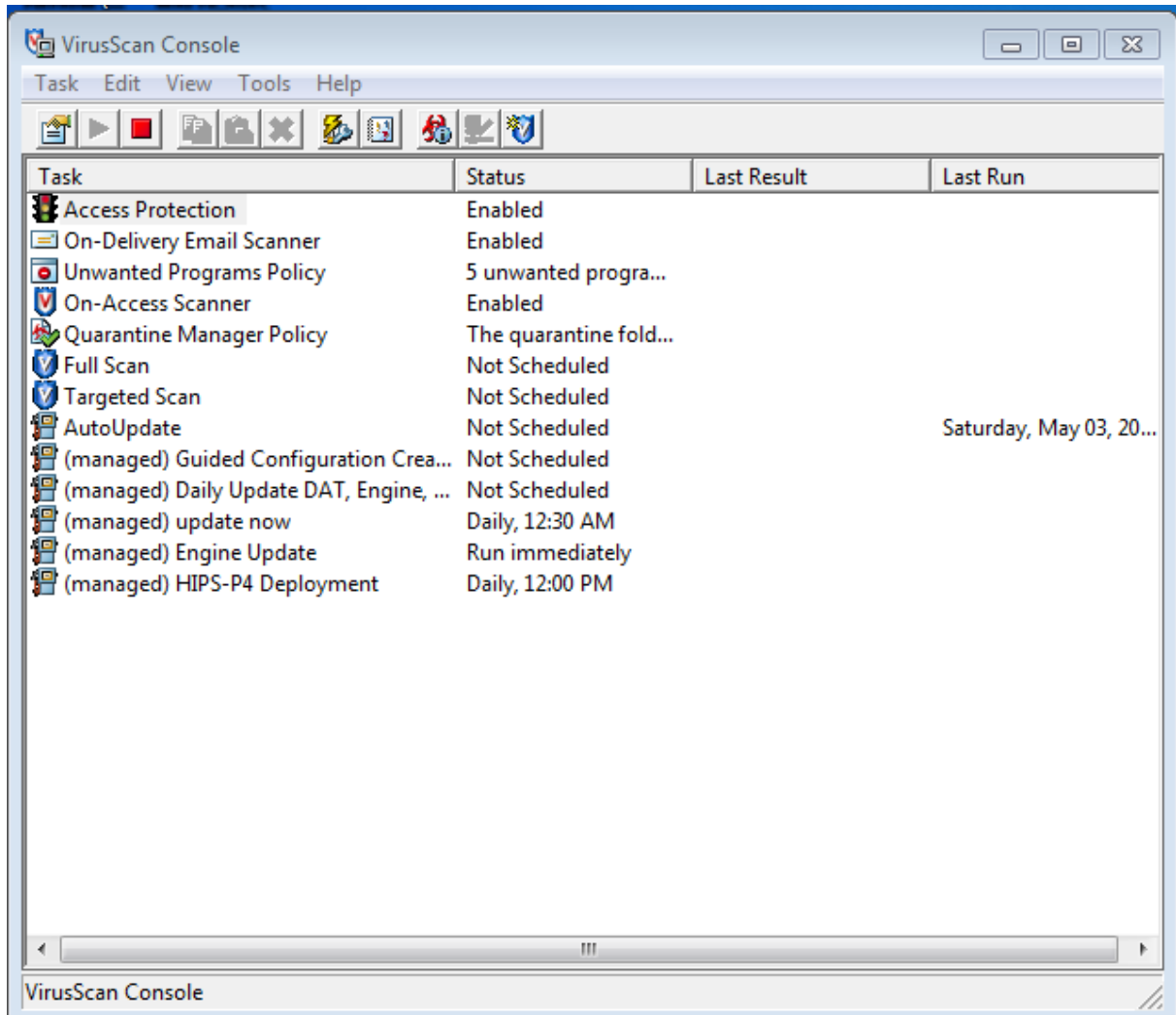
## COM e-mail settings

During e-mail configuration, when the **Test Email** button is clicked you may receive an error message stating your anti-virus software is blocking mass e-mail or e-mail worms. This can happen when anti-virus software installed on the COM Server is configured to block mass mailing. In order to avoid this, disable the blocking option through the anti-virus software installed on the COM server.

If McAfee anti-virus software is installed on COM server, use the following procedure to disable mass e-mail blocking:

## Procedure

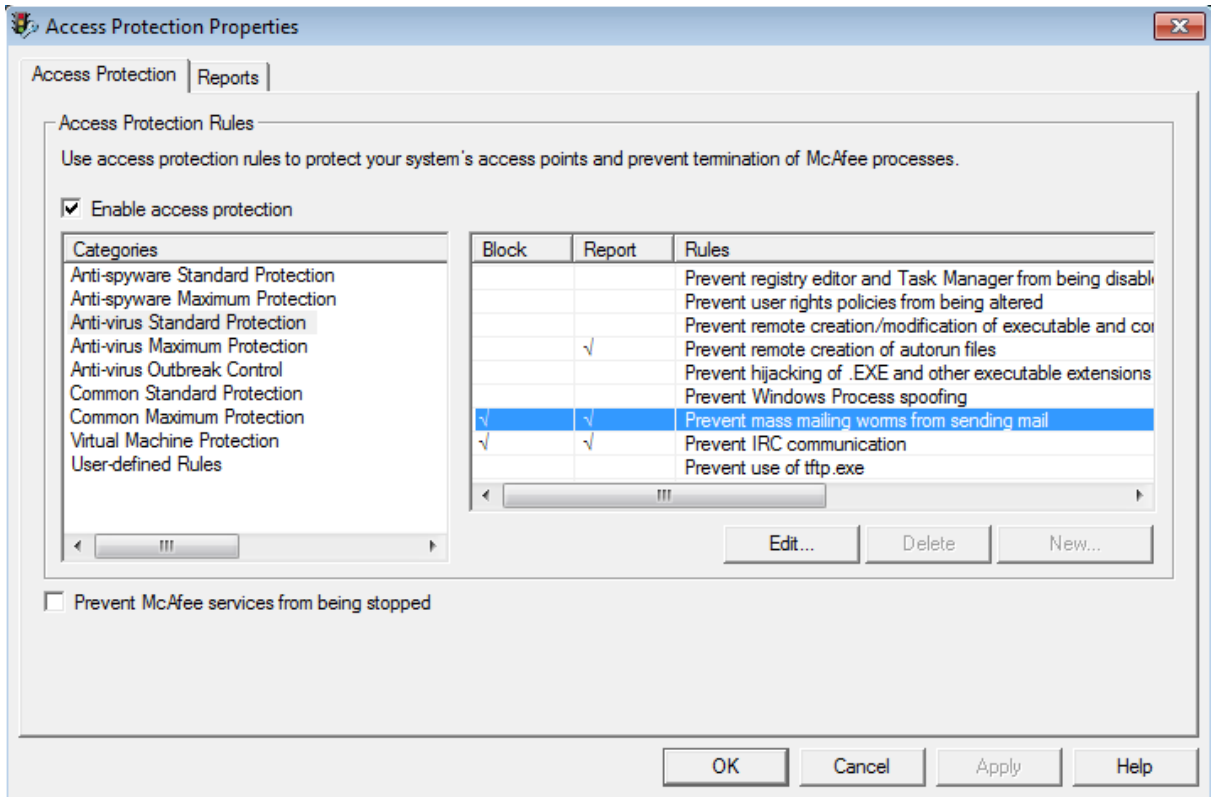
1. Open the McAfee VirusScan Console.



2. Click on **Access Protection**.

The **Access Protection** tab opens.

3. Click **Anti-virus Standard Protection** .



4. Click the check mark in the **Block** column next to **Prevent mass mailing worms from sending mail** to disable e-mail blocking.



# Chapter 8: Device types and limitations

This section lists the limitations of Avaya BCM when communicating with devices, and provides information about how devices display on the Avaya BCM interface and in csv files.

The following list outlines the limitations of Avaya BCM when communicating with devices:

- Contivity VPN routers cannot have # or > in the prompt.
- Avaya Ethernet Routing Switch 2500, 4500, 5500, 8300, and 8600 cannot have more than one # in the prompt.
- SVU on Ethernet Routing Switch 8300/8600 has a set of mandatory files. Image files cannot be uploaded individually.
- Ethernet Routing Switch 8600 SSH works on 3DES or AES depending on software version.
- Ethernet Routing Switch 8300 SSH works only on 3DES and AES.
- For all devices, except devices with two CPUs, to execute an Avaya BCM task, Telnet or SSH must be enabled on the device. The exceptions are: TGD works only with SSH on SNAS, and the 8600/8300 devices with 2 CPUS must have Telnet enabled for a proper connection between the CPUs.

The following table outlines the Avaya BCM supported devices, and shows how Avaya device names appear on the Avaya BCM interface and in the csv files.

Avaya device name	Label on Avaya BCM interface	Inventory csv label
Secure Router 1000/3100	Secure Router 1000/3100	SR_TASMAN
Secure Router 4134	Secure Router 4000	SR_TORNADO
VPN Router 600-5000	VPN Router	VPN_ROUTER
Secure Network Access Switch 4050/4070	Secure Network Access Switch 4050/4070	SNAS
Ethernet Routing Switch (5600 Series)	Ethernet Routing Switch (5600 Series)	ERS_5600
Ethernet Switch 460/470	Ethernet Switch 460/470	ES_470/460
Business Secure Router 222	Business Secure Router 222	BSR_222
Business Secure Router 252	Business Secure Router 252	BSR_252
Ethernet Routing Switch (8800 Series)	Ethernet Routing Switch (8600 Series)	ERS_8800
Ethernet Routing Switch (8600 Series)	Ethernet Routing Switch (8600 Series)	ERS_8600

## Device types and limitations

Avaya device name	Label on Avaya BCM interface	Inventory csv label
Ethernet Routing Switch (8300 Series)	Ethernet Routing Switch (8300 Series)	ERS_8300
Ethernet Routing Switch (5500 Series)	Ethernet Routing Switch (5500 Series)	ERS_5500
Ethernet Routing Switch (5000 Series)	Ethernet Routing Switch (5000 Series)	ERS_5000
Ethernet Routing Switch (4500 Series)	Ethernet Routing Switch (4500 Series)	ERS_4500
Ethernet Routing Switch (3500 Series)	Ethernet Routing Switch (3500 Series)	ERS_3500
Ethernet Routing Switch (2500 Series)	Ethernet Routing Switch (2500 Series)	ERS_2500
VPN Gateway 3050/3070	VPN Gateway 3050/3070	NVG
VSP (7000 and 9000 Series)	VSP (9000 Series)	VSP_DEVICE
VSP (8000 Series)	VSP (8000 Series)	VSP_DEVICE
VSP (4000 Series)	VSP (4000 Series)	VSP_DEVICE
Wireless LAN 8180	Wireless LAN 8180	WC_8180_DEVICE

# Chapter 9: SVU file types

The following tables show the file types used in SVU packages.

Device	SVU file — SSH not supported	SVU file — SSH supported
ERS 2500	2500_400000.img	2500_400000s.img
ERS 3500	3500_512004.img	3500_512005s.img
ERS 4500	4500_501000.img	4500_501001s.img
ERS 5500	55x0_50010.img	55x0_50011s.img
ERS 5600	55x0_600005.img	
BSR 222	VBSR222_2.6.0.0.003.bin	
BSR 252	VBSR252_2.6.0.0.005b1.bin	
ES 460/470	470_37313.img	

Device	SVU file
NVG 3050/3070	SSL-7.0.1.0-upgrade_complete.pkg
SNAS 4050	NSNAS-1.5.1-upgrade_complete.pkg

Device	Run-time image (mandatory)	Boot monitor image (mandatory)	Mandatory — required for SSH	Needed for SNMPv3 — not mandatory	Required only when upgrading from 2.0, 2.1 or 2.2
ERS 8300	p83a3000.img	p83b3000.img	P83c3000.img	p83c3000.aes	p83f3000.img
ERS 8600/8800	p80a4110.img	p80b4110.img	P80c4110.img	p80c4110.aes	

The last five columns in the following table are not mandatory but if the package does not include all mandatory files, SVU fails.

Device	Mandatory I/O module	SuperMezz module	POS module	SSL module	ATM module	WSM module
ERS 8300	p83r3000 .dl d					
ERS 8600/8800	p80j4110 .dl d p80k4110.dl d	p80m4110 .im g	p80p4110 .dl d	p80s4110.img	p80t4110.dld	p80w4110.dld

## SVU file types

Device	.bin image	.Z image
Secure Router 1001	1001_r9[1].2.bin	J1100_92.Z
Secure Router 1001S	1001S_r9[1].2.bin	JP1010.Z
Secure Router 1002	1000_r9[1].2.bin	T1000.Z
Secure Router 3120	3120_r9[1].2.bin	H1000.Z
Secure Router 4134		SR4134.Z

**! Important:**

.bin and .Z files can be uploaded individually by SVU.

**! Important:**

The first letter in the .Z image must not be changed. The flash memory in Secure Routers 1001, 1001S, and 1002 cannot host 2 .Z files. If you attempt to load the incorrect image on these devices, SVU deletes the existing image and the device becomes unreachable.

Device	SVU file
VPN Router 1010, 1050, 1100	V07_00.058.tar.gz (approx. file size ~16MB)
VPN Router 600, 1750, 2700, 2750, 5000	V07_00.058.tar.gz (approx file size ~50MB)
VSP 9012	VSP9K.3.0.0.0.tgz
VSP 8xxx	VSP8200.4.0.0.0.tgz
VSP 4000	VSP4K.4.0.0.0.tgz
VSP 7000	lakemerced_1020.elf.gz

# Chapter 10: Sample configuration scripts

This section provides examples of configuration scripts that you can use with the CUG tool.

---

## VPN router configuration

This section provides information about how to create CUG scripts to configure a VPN router.

If you use CUG to execute commands on a VPN router, Avaya BCM executes the following commands by default:

```
enable
configure terminal
```

After Avaya BCM finishes executing a CUG script, it saves the configuration changes and exits the configure terminal mode. You do not need to add these commands to your script. However, if your script has to execute a command outside of the configure terminal mode, you must include the necessary exit commands in your script. For example, if your script executes a ping command, which is done outside of the configure terminal mode, your script must exit the mode prior to executing the ping command.

You can obtain a configuration script that shows the configuration of the VPN router by executing the following command, and copying the output using the mark and copy functions of the command prompt terminal:

```
enable
show running-config
```

The following scripts are typical examples of how to use the CUG tool on a VPN router.

### **CUG CLI Example 1:**

```
router rip
timers basic 400
```

### **CUG CLI Example 2:**

```
exit
ping 11.126.16.13
```

### **CUG config:**

```
router rip
```

## Sample configuration scripts

```
timers basic 400
```

In the next example, you can assign both of the files to the same CUG task, which allows you to change the same parameter on multiple devices.

### **CUG configuration template with variables:**

```
router rip
timers basic ???a
```

### **CUG configuration data file:**

```
, ???a
10.20.20.130, 400
11.126.16.32, 50
```

---

## NSNAS and VPN gateway configuration

This section provides information about how to create CUG scripts to configure NSNAS and VPN gateways.

When you use CUG to execute commands on NSNAS or a VPN gateway, Avaya BCM executes the following commands by default:

```
apply
```

This command saves the configuration changes when the CUG task is complete.

You can obtain a configuration script that shows the configuration of the NSNAS or VPN gateway by executing the following command, and copying the output using the mark and copy functions of the command prompt terminal:

```
/cfg/dump
```

The following scripts are typical examples of how to use the CUG tool on the VPN gateway or NSNAS.

### **CUG CLI Example 1:**

```
cfg
sys
adm
snmp
snmpv2-mib
sysContact
AvayaTest
```

### **CUG CLI Example 2:**

```
cfg/sys/dns/servers add 11.12.12.12
```

**CUG configuration:**

```

/cfg/sys/host 1/interface 2/.
    ip 12.12.12.12
    netmask 255.255.0.0
    gateway 12.12.12.1
    vlanid 3
    mode failover
    primary 0
/cfg/sys/time/.
    tzone "Europe/Bucharest"
/cfg/sys/dns/servers/.
    add 110.120.120.250

```

In the next example, you can assign both of the files to the same CUG task, which allows you to change the same parameter on multiple devices.

**CUG configuration template with variables:**

```

/cfg/sys/time/.
    tzone ???Time

```

**CUG configuration data file:**

```

, ???TIME
10.20.20.105, "Europe/Rome"

```

**CUG configuration template with variables:**

```

10.20.20.107, "Europe/Paris"
10.20.20.90, "Europe/London"

```

---

## Secure Router 1001, 1001s, 1002/1004, 3120, and 4134 configuration

This section provides information about how to create CUG scripts to configure secure routers.

If you use CUG to execute commands on secure routers, Avaya BCM executes the following command by default:

```
config term
```

Do not include the preceding command in the CLI script.

After executing the script, the CUG executes the following commands:

```
save local
```

```
exit
```

These commands save the configuration changes and terminate the connection to the device when the CUG task completes.

To obtain a configuration script that shows the configuration of the secure router you can execute the following command, and copy the output using the mark and copy functions of the command prompt terminal.

```
show running-config
```

The following scripts are typical examples of how to use the CUG tool on a secure router.

**CUG CLI:**

```
router rip
interface ethernet1
mode 3
```

**CUG configuration:**

```
motd_banner "CUG config example"
```

In the next example, you can assign both of the files to the same CUG task, which allows you to change the same parameter on multiple devices. In this example, IP address 10.20.20.182 is a Secure Router 1001/1001s/1002/1004, and IP address 10.20.20.185 is a Secure Router 3120.

**CUG CLI template with variables:**

```
router rip
interface ???a
mode ???b
```

**CUG CLI data file:**

```
, ???a, ???b
10.20.20.182, ethernet1, 3
10.20.20.185, ethernet0/2, 3
```

---

## Avaya Ethernet Routing Switch 2500, 4500, and 5500 configuration

This section provides information about how to create CUG scripts to configure Avaya Ethernet Routing Switches (ERS) 2500, 4500, and 5500.

When you use CUG to execute commands on Ethernet Routing Switches, Avaya BCM executes the following commands by default:

```
config term
```

Do not include the preceding command in the CLI script.



After executing the script, the CUG executes the following commands:

```
save local
exit
```

These command will save the configuration changes and terminate the connection to the device when the CUG task is complete.

You can obtain a configuration script that shows the configuration of the ERS by executing the following command, and copying the output using the mark and copy functions of the command prompt terminal:

```
show running-config
```

The following scripts are typical examples of how to use the CUG tool on an ERS.

#### **CUG CLI:**

```
vlan create 10 name DVLP type port
vlan members 10 5-7,9
interface fastEthernet 5-7,9
name DVLP
```

#### **CUG configuration:**

```
vlan create 30 name Support type port
vlan members 30 12,14
vlan ports 12,14 pvid 30
```

In the next example, you can assign both of the files to the same CUG task, which allows you to change the same parameter on multiple devices.

#### **CUG CLI template with variables:**

```
vlan create ???a name ???b type ???c
vlan members ???d ???e
interface fastEthernet ???f
name ???g
```

#### **CUG configuration data file:**

```
, ???a, ???b, ???c, ???d, ???e, ???f, ???g
47.17.30.34, 24, ProductVerif, port, 20, 2-5, 2-5, PV
:
```

---

## Avaya Ethernet Routing Switch 8300 and 8600 configuration

This section provides information about how to create CUG scripts to configure Avaya Ethernet Routing Switches (ERS) 8300 and 8600.

If you use CUG to execute commands on Ethernet Routing Switches, Avaya BCM executes the following commands by default:

```
save config
exit
```

The preceding commands save the configuration changes and terminate the connection to the device when the CUG task completes. If the device is equipped with two CPUs, Avaya BCM saves the configuration on both the master and the slave CPU.

You can obtain a configuration script that shows the configuration of the ERS by executing the following command, and copying the output using the mark and copy functions of the command prompt terminal:

```
show config
```

The following scripts are typical examples of how to use the CUG tool on an ERS.

### **CUG CLI:**

```
config ip route-policy "policy1" seq 44 create
```

### **CUG configuration:**

```
config
ip route-policy "policy1" seq 33 create
ip route-policy "policy1" seq 33 enable
back
```

In the next example, you can assign both of the files to the same CUG task, which allows you to change the same parameter on multiple devices.

### **CUG configuration template with variables:**

```
config ip route-policy ???aa seq ???bb create
```

### **CUG configuration data file:**

```
, ???a, ???b
10.20.20.70, "1_policy_1", 88
47.17.30.46, "policy6", 99
```