Fundamentals
Avaya Bulk Configuration Manager

Avaya BCM 2.3
NN48021-100
02.03
June 2011

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

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

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Bulk Configuration Manager Fundamentals* (NN48021–100) for Release 2.3.

Features

See the following sections for information about feature changes:

BCM device support for COM 2.3

The Avaya Bulk Configuration Manager (Avaya BCM) offers device support for the following devices:

- Virtual Services Platform (VSP) 9012 v.3.0 and v.3.1
- Wireless LAN 8180 v.1.0
- ERS 4500 v.5.5
- ERS 8800

For more information about changes to the BCM tools, see the following sections:

- Configuration Backup and Restore on page 16
- Configuration Update Generator on page 18
- Device Password Manager on page 20
- Inventory on page 23
- Software Version Updater on page 27

Importing devices from COM

You can import the device inventory from the Configuration and Orchestration Manager (COM) to the Avaya BCM. For more information about the import from COM feature, see Importing devices from COM on page 52.

Other changes

See the following section for information about changes that are not feature-related.

Figures

Figures in this document are updated.

Chapter 2: Customer service

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

Navigation

Getting technical documentation

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

Getting product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Chapter 3: Roadmap

This chapter describes the information that you need to use the Avaya Bulk Configuration Manager (Avaya BCM).

About this guide

Avaya Bulk Configuration Manager Fundamentals guides you through the Avaya BCM application interface.

Purpose

The purpose of this guide is to teach a user how to configure and use Avaya BCM.

Audience

The intended audience for this guide are the administrators of Avaya BCM.

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
INV	Inventory
LOG	Log Browser
BCM	Avaya Bulk Configuration Manager

Acronym	Description
SCH	Scheduler
SNAS	Secure Network Access Switch
SVU	Software Version Updater
TGD	Tunnelguard Distributor
UCM	Avaya Unified Communication Management

Avaya BCM functions

The following is the list of icons for Add Task, Edit Task, Delete Task, and Activate Task.

Icon	Function
	Filter Tasks
	Add Task
	Duplicate Task
	Delete Task
	Edit Task
	Import Device(s) from .csv File
	Export Inventory to .csv file
	Import from VPFM
	Activate Task

Special messages used in this guide

The following special message highlights critical information.

Important:
Alerts you to important information.

Chapter 4: Introduction

The Avaya Bulk Configuration Manager (Avaya BCM) 2.3 Fundamentals guide 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.

Avaya BCM is part of Avaya Unified Communication Management (Avaya UCM) but can function as a standalone product with an embedded UCM Common Services for its own use on a separate server. The Common Services component adds to the flexibility of Avaya BCM to move from a stand-alone to an integrated deployment with ease and deploys a common set of tools to provide network configuration management services for multiple devices.

Navigation

Chapter 5: Overview

Avaya Bulk Configuration Manager (Avaya BCM) is an application in the Avaya Unified Communication Management (Avaya UCM) 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

Navigation

- Logon page on page 15
- Configuration Backup and Restore on page 60
- Configuration Update Generator on page 18
- Device Password Manager on page 20
- Log Browser on page 22
- Inventory on page 23
- License on page 25
- Scheduler on page 26
- Software Version Updater on page 27
- Tunnelguard Distributor on page 29

Logon page

To access the Avaya BCM, you must log on to the Configuration and Orchestration Manager (COM) through the UCM. The Avaya BCM contains a default administrative account with a user name admin. The initial password is the password assigned when you install UCM. 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 120 minutes. In both cases when 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 Quantum page. For more information about configuring these timers, see *Unified Communications Management Fundamentals* (NN48014-100).

Configuration Backup and Restore

Use the Configuration Backup and Restore (CBR) tool to back up and restore device configuration parameters.

During the backup process, a human readable text format of the saved configuration is also created for all supported devices except BSR-s. This file is automatically saved in the backup archive into the compare folder. This file is for restore archive comparison only and it is 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 own 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 own 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.

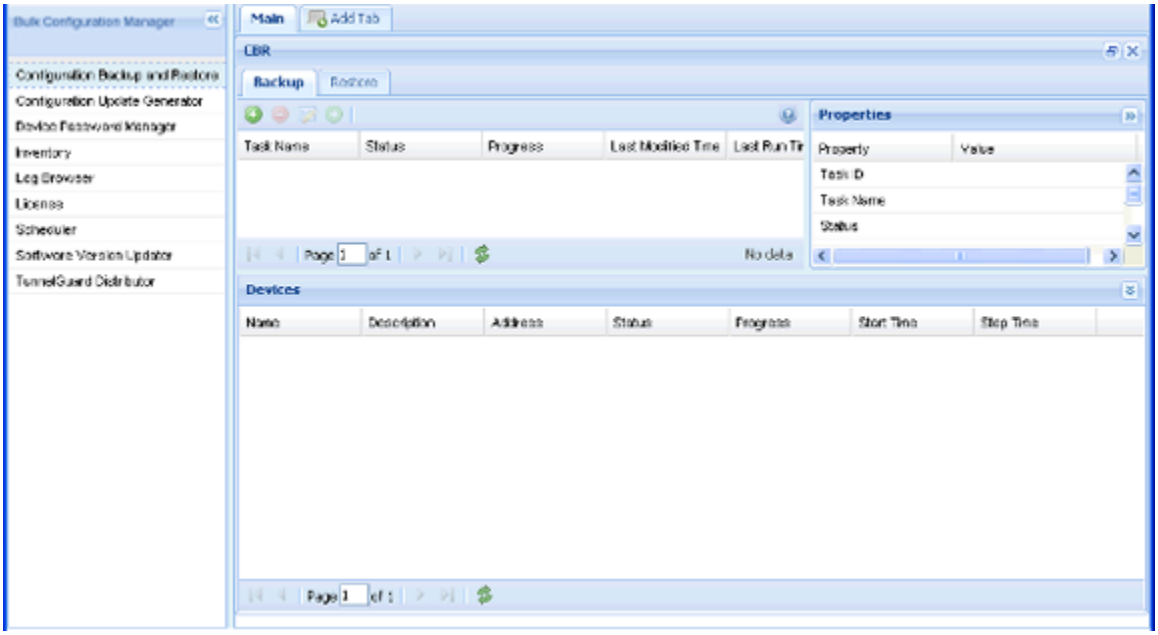

Figure 1: Configuration Backup and Restore

The Configuration Backup and Restore tool supports the VSP 9012, the Wireless LAN 8180, the ERS 4500, and the ERS 8800.

Tables 1, 2, and 3 describe the fields of the Configuration Backup and Restore tool, the devices where backup is performed, and show 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.

Attribute	Value	Description
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.
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.

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.

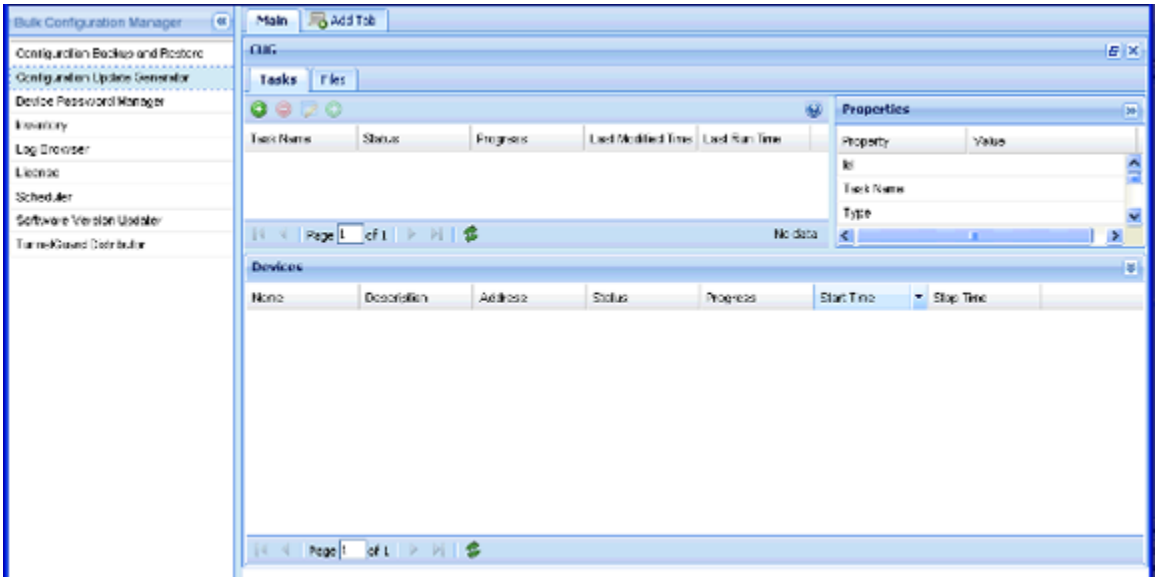

Figure 2: Configuration Update Generator

The Configuration Update Manager supports the VSP 9012, the Wireless LAN 8180 and the ERS 8800. However, COM and BCM do not support the configuration of a configuration file on the VSP 9012 device. For both the VSP 9012 and the Wireless LAN 8180, the CUG tool starts executing the user script in configuration mode and saves the configuration on exit.

Tables 4, 5, and 6 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 4: CUG task table

Attribute	Value	Description
Task Name	<textbox>	The task name.
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).
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 5: 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 6: 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.

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 community changes are successful on the device, the new values are updated in the Unified Communication Manager (UCM) Credentials.

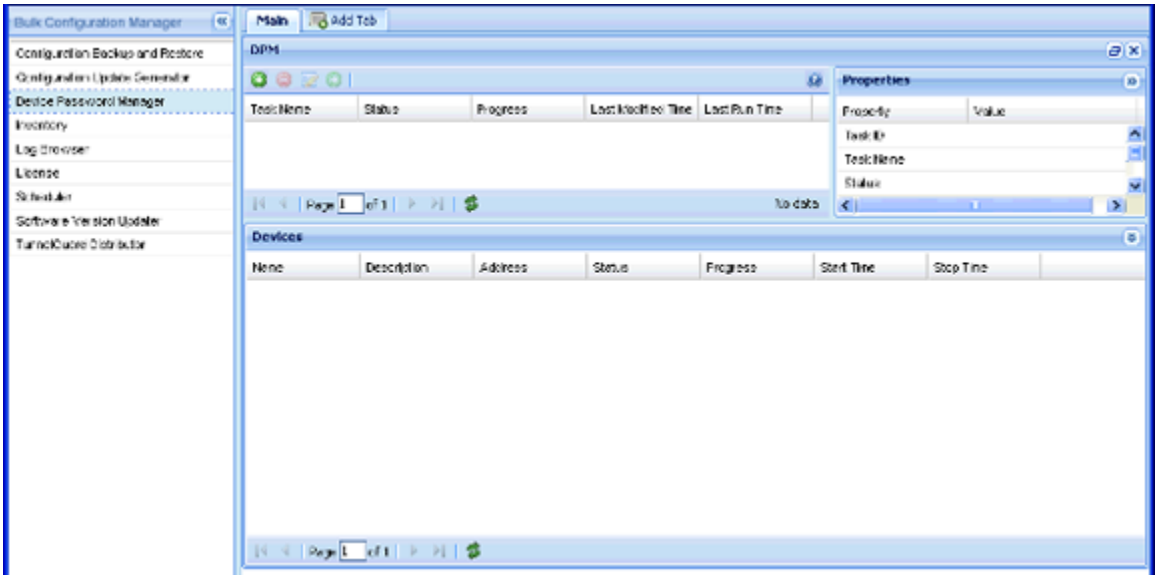

Figure 3: Device Password Manager

The Device Password Manager supports the VSP 9012, the Wireless LAN 8180, the ERS 4500, and the ERS 8800.

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

Table 7: 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 8: 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.

Attribute	Value	Description
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.

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 server/default/log folder. This file rolls over to a new file when the size reaches 10 megabytes. Every time you do a refresh in the Log Browser, these files are copied to `<install-folder>Avaya/LOGS` folder. You can browse a maximum of two files, the current log file and the most recent 10 megabyte log archive. 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.

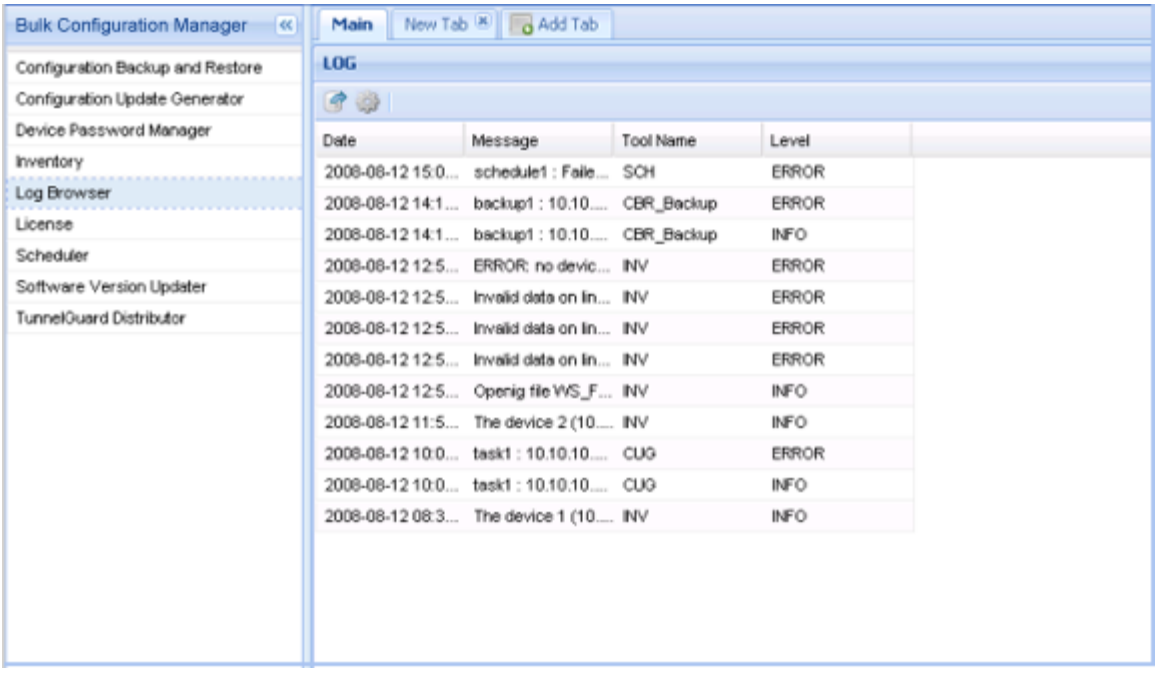

Figure 4: Log Browser

Table 9: Log Browser table

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

Inventory

You can use the Avaya BCM Inventory feature to add and store devices.

You can manually add devices one at a time or import a list of devices from a comma-delimited (*.csv) file and from the VPFM. When you add devices, either manually or from a file, the required fields are IP Address and Device Type.

You can Import a device inventory from VPFM if a discovery is not in progress. Inventory devices can also be exported to a csv file for easier editing.

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 from a csv or from VPFM updates the device and keeps the device ID.

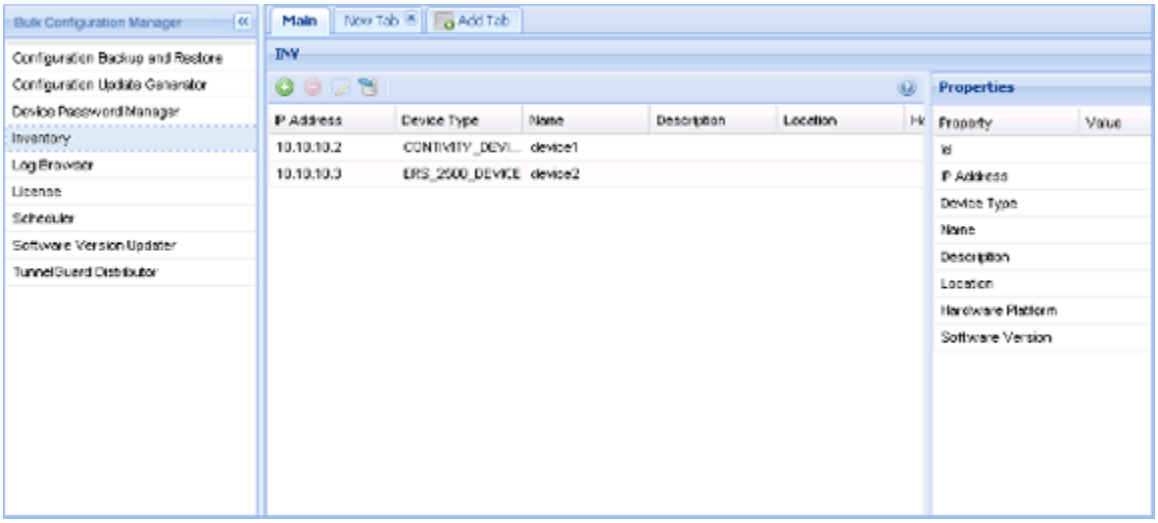

Figure 5: Inventory

The Inventory tool supports the VSP 9012, the Wireless LAN 8180, the ERS 4500, and the ERS 8800.

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 version	<textbox>	Version of the hardware
Software version	<textbox>	Version of the software
Task ID	<textbox>	The task index

Note:

You cannot import the description, location, hardware version, and software version from VPFM.

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.

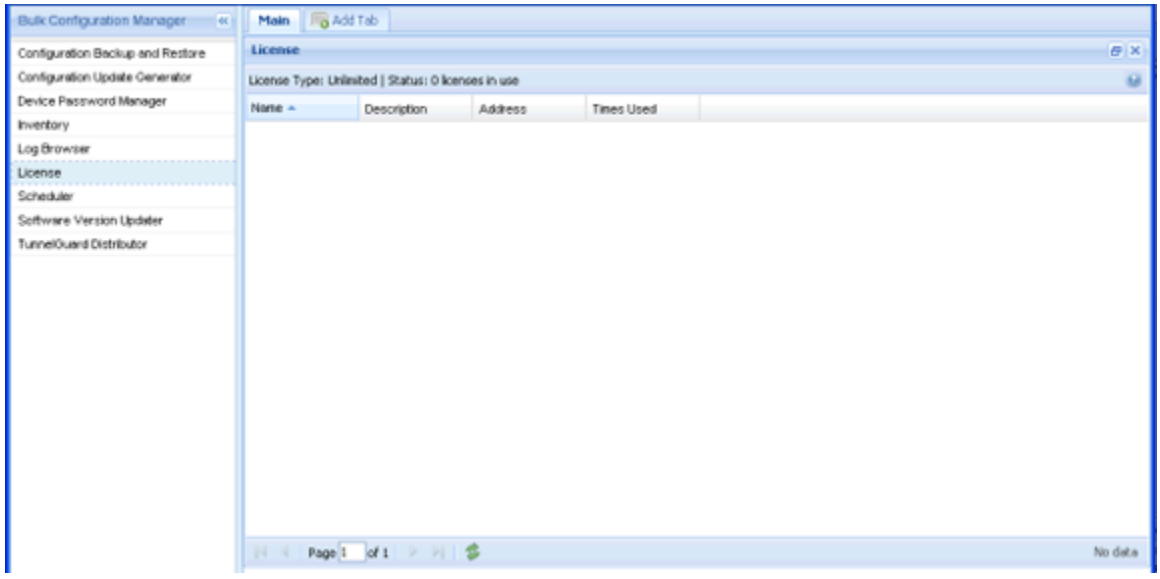

Figure 6: Avaya BCM License

The following table outlines the Avaya BCM license fields.

Table 11: Avaya BCM License task table

Attribute	Description
Name	The name of the device.

Attribute	Description
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, weekly or monthly.

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.

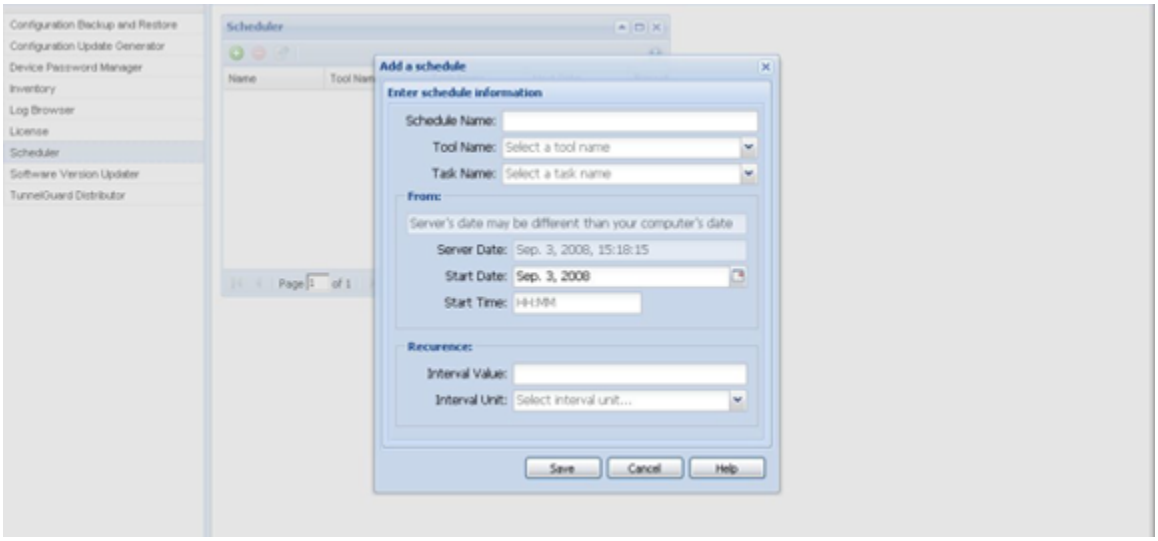

Figure 7: Scheduler

Table 12: Scheduler table

Attribute	Value	Description
Name	<textbox>	The name of the scheduled activity
Tool Name	<IP address>	The tool name
Task Name	<textbox>	The name of the task

Attribute	Value	Description
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
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.

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.

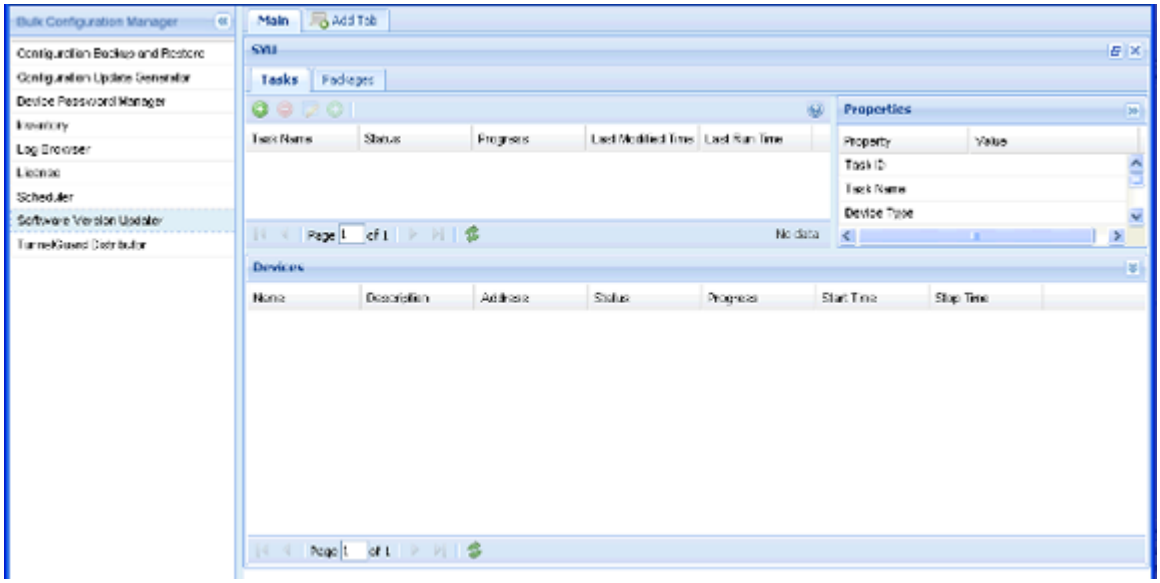

Figure 8: Software Version Updater

The Software Version Updater supports the VSP 9012, the Wireless LAN 8180, the ERS 4500, and the ERS 8800. For the VSP 9012, Avaya BCM uses the FTP protocol to transfer the image from the COM server to the VSP 9012; therefore you must configure the FTP server to operate on the VSP 9012. If you do not provide the FTP credentials for the VSP 9012 FTP server in

the UCM credentials manager, the SVU uses the device login credentials to connect as an FTP client to the VSP 9012 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 13: SVU task table

Attribute	Value	Description
Task Name	<textbox>	The name of the task
Device Type	<textbox>	The device type
Package Name	<textbox>	The package name
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

Table 14: 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 15: Package table

Attribute	Value	Description
Device Type	<textbox>	The type of the device
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 16: 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.

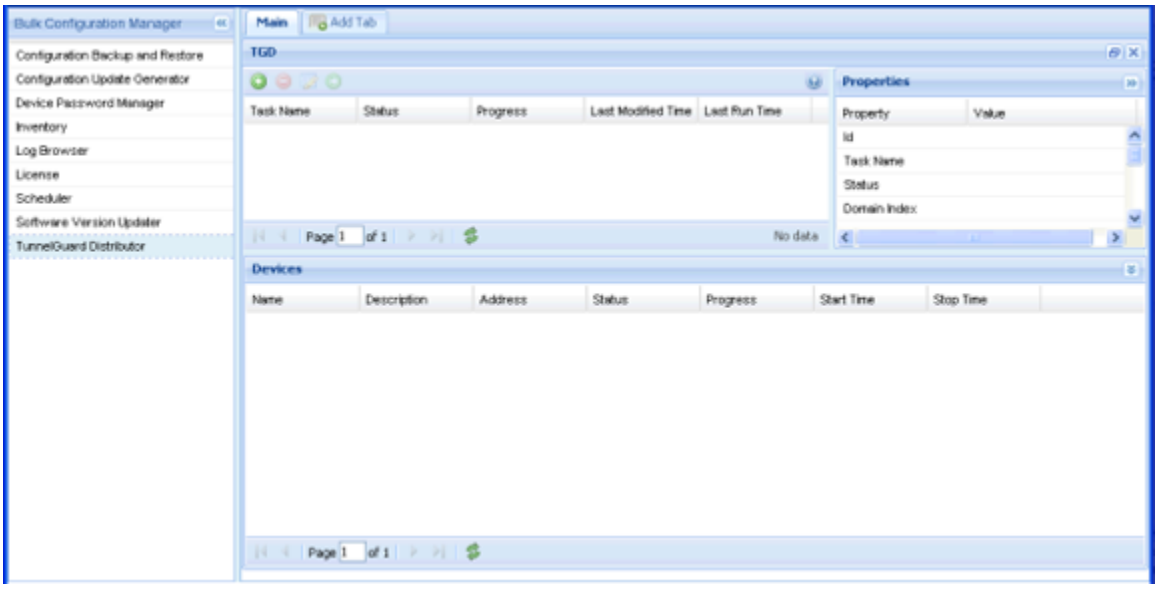

Figure 9: Tunnelguard Distributor

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

Table 17: 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 18: 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 6: Avaya BCM licensing

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

Navigation

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 or VPFM.

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

devices under license and the number of tasks using that device are listed in this table

Prerequisites

You must be in the Configuration and Orchestration Manager.

Procedure steps

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

Obtaining an Avaya Bulk Configuration Manager license

Perform the following procedure to obtain an Avaya Bulk Configuration Manager (Avaya BCM) license.

• Prerequisites on page 33
• Obtaining a BCM license on page 33

Prerequisites

- You require the LAC for the software you want to license.
- You require the MAC address of the server where the Avaya BCM components reside.
- You require the name and password to the license bank if you want to deposit the license into an existing license bank.

Obtaining a BCM license

Obtain a BCM license.

Procedure steps

1. Open a Web browser window and go to the **Electronic Licensing Portal**: http://www.avayadatalicensing.com.
2. Type your first name, last name, company name, and e-mail address in the appropriate fields at the top of the page.

3. In the **License Bank** area, specify the name and password for an existing license bank where you want to deposit.
4. Specify your e-mail notification options.
5. In the **Submit** field at the bottom of the page, type your LAC.
6. Click the **Activate License**.

   The system deposits a license in your License Bank and sends a message to the e-mail address specified in step 4 to confirm that the license was created.
7. Log on to your license bank using the name and password specified in step 3.
8. Click **Download**.
9. On the **Generate License** page, type the MAC address for the server where the Avaya BCM components reside. Use capital letters, separated by colons (XX:XX:XX:XX:XX:XX).
10. Click **Create License File**.

    A confirmation message informs you that the license was created. The system sends a license (.lic) file to the e-mail address specified in step 4.
11. Copy the license file to the server location where the Avaya BCM components reside.
12. Store your License Certificate in a secure place for future reference.

Installing an Avaya Bulk Configuration Manager license

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

- Prerequisites on page 34
- Adding a license on page 35

Prerequisites

- 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 an Avaya Bulk Configuration Manager license on page 33.
- You must know where the license resides on the server.
- You must know the directory path of <UCM_home>. To locate the directory path for your operating system, see Directory structure on page 73.

Adding a license

For information about adding a license in the License administration page, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014-100).

Chapter 7: 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.

Navigation

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 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 81.

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

Complete the following procedures to manage configuration files and tasks on the Avaya BCM server.

- Editing a CUG task on page 43
- Deleting a CUG task on page 43

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, double-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, double-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, double-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, double-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, double-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.

1. From the navigation pane, double-click **Configuration Update Generator** to open a new or existing portlet.

   The Add a filter dialog box appears.
2. Click **Filter**.
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 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, double-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.

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 **Log Settings**.

   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. 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.
8. In the **Colors** section, select the **Enable log colors** check box, and then select different colors for the various message levels.
9. 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 NRM_audit.log. When this file reaches 10M, Avaya BCM saves it as NRM_audit.log.1 and creates a new NRM_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 INV portlet.
2. Click the **Add** device icon.

   The Add a Device window appears.
3. Type the **IP address** of the device.
4. Select the **Device Type** from the drop-down menu.
5. Click **Save**.

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 INV 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 INV 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 INV 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 INV 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.

Exporting devices to .csv file

Export devices to .csv file.

Procedure steps

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

Importing devices from the VPFM

The device inventory is imported on an on-demand basis; that is, the inventory is not automatically updated in Avaya BCM when the inventory in VPFM changes. If a device is deleted from the VPFM database, it is not deleted from the Avaya BCM database. Similarly, if a device is deleted from the Avaya BCM database, it does not affect the VPFM. You must perform this procedure whenever you want to synchronize the inventories.

If you attempt to import the devices whose IP addresses already exist in the Avaya BCM device inventory, the Avaya BCM does not import the duplicate devices. The Avaya BCM generates a log about the duplicate devices. See the log for information about the duplicate devices.

If there is a discrepancy between the Avaya BCM devices display names and the VPFM devices display names, the Avaya BCM devices display names are displayed in the Inventory list.

Use the following procedure to import the device inventory from the VPFM to the Avaya BCM.

Procedure steps

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

   The VPFM properties window appears.
3. In the **Server Name** field, type the IP address of the server where the VPFM is installed.
4. In the **User Name** field, type the user name for logging into the VPFM.
5. In the **Password** field, type the password for logging into the VPFM.
6. Click **Import**.

   The Avaya BCM retrieves the inventory information from the VPFM, and displays a table that lists all of the devices found.
7. Select the checkboxes beside the device names that you want to import into the Avaya BCM database.
8. Click **Update** to import the devices into the Avaya BCM inventory.

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**.

Device Password Manager

See the following topics to manage Device Password Manager (DPM) tasks:

- Managing DPM tasks on page 52
- Viewing the progress of a password management task on page 55

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.

Navigation

- Creating a DPM task on page 53
- Filtering the DPM tasks on page 53
- Duplicating a DPM task on page 54
- Editing a DPM task on page 54

- Executing a DPM task on page 54
- Deleting a DPM task on page 55

Creating a DPM task

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

Procedure steps

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

- Managing software version images on the file server on page 56
- Viewing the progress of a software update task on page 60

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 procedure 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.

Navigation

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, double-click **Software Version Updater** to open an SVU portlet.
2. Click **Add**.
3. Type the task name.
4. 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.
5. Select the package name from the list.
6. Select the list of devices to update from the list that appears.
7. 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.

   The Add a filter dialog box appears.
2. Click the **Filter** icon.
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 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 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 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 you want to run.
3. Click **Activate Task** from the task table field.
4. 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

See the following topics to manage Configuration Backup and Restore (CBR) tasks.

- Managing Configuration Backup and Restore tasks on page 60
- Viewing the progress of a backup or restore task on page 66

Managing Configuration Backup and Restore tasks

Complete the following procedures to manage configuration backup tasks.

Navigation

- Creating a configuration backup task on page 61
- Filtering the configuration backup tasks on page 61
- Duplicating a configuration backup task on page 62
- Editing a configuration backup task on page 62

Creating a configuration backup task

Create a CBR task to group devices to be backed up.

Procedure steps

1. From the navigation pane, double-click **Configuration Backup and Restore** to open a CBR portlet.
2. Click the **Backup** tab, and click **Add**.
3. Type the backup task name.
4. Enable or disable the **Restrict the restore** field; 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. Click **Save**.

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.

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.

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 to be edited.
3. Click **Edit**.
4. Edit the name.
5. Enable or disable the **Restrict the restore** field; when selected, Avaya BCM allows the restore operation only on devices that have the same software version as at that of the backup.
6. Edit the list of devices.
7. Click **Save**.

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.

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.

   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 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.

The following procedures describe Scheduler activity.

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 the **Edit Task** icon, 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.

Navigation

- Adding previously created TunnelGuard policies on page 69
- Filtering the TGD tasks on page 70
- Duplicating a TGD task on page 70
- Editing a TGD task on page 71
- Deleting a TGD task on page 71
- Executing a TGD task on page 71

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 at 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 8: Directory structure

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

- 32-bit Windows
- 64-bit Windows (32-bit app)
- 64-bit Windows (64-bit app)
- Linux

The following table outlines the directory paths for the Unified Communications Management (UCM) applications on each operating system.

Application	32-bit Windows	64-bit Windows (32-bit app)	64-bit Windows (64-bit app)	Linux
MySQL	C:\Program Files \Avaya\UCM \MySQL	C:\Program Files (x86)\Avaya\UCM \MySQL	C:\Program Files \Avaya\UCM \MySQL	/opt/Avaya/UCM/ MySQL
JBoss	C:\Program Files \Avaya\UCM\jboss	C:\Program Files (x86)\Avaya\UCM \jboss	C:\Program Files \Avaya\UCM\jboss	/opt/Avaya/UCM/ jboss
COM	C:\Program Files \Avaya\UCM\COM	C:\Program Files (x86)\Avaya\UCM \COM	C:\Program Files \Avaya\UCM\COM	/opt/Avaya/UCM/ COM
VPFM	C:\Program Files \Avaya\UCM \VPFM	C:\Program Files (x86)\Avaya\UCM \VPFM	C:\Program Files \Avaya\UCM \VPFM	/opt/Avaya/UCM/ VPFM
EPM	C:\Program Files \Avaya\UCM\EPM	C:\Program Files (x86)\Avaya\UCM \EPM	C:\Program Files \Avaya\UCM\EPM	/opt/Avaya/UCM/ EPM
IPFM	C:\Program Files \Avaya\UCM\IPFM	C:\Program Files (x86)\Avaya\UCM \IPFM	C:\Program Files \Avaya\UCM\IPFM	/opt/Avaya/UCM/ IPFM

Chapter 9: Troubleshooting

This chapter provides troubleshooting information for the Avaya Bulk Configuration Manager (Avaya BCM) 2.3.

Navigation

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 correspondence with a device to a file

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

Procedure steps

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

Chapter 10: 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 # 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.
- Ethernet Routing Switch 8300 and Ethernet Routing Switch 8600 cannot be booted in ACLI mode.
- 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

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 (4500 Series)	Ethernet Routing Switch (4500 Series)	ERS_4500
Ethernet Routing Switch (2500 Series)	Ethernet Routing Switch (2500 Series)	ERS_2500
VPN Gateway 3050/3070	VPN Gateway 3050/3070	NVG
VSP (9000 Series)	VSP (9000 Series)	VSP_DEVICE
Wireless LAN 8180	Wireless LAN 8180	WC_8180_DEVICE

Chapter 11: 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 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	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/0 module	SuperMezz module	POS module	SSL module	ATM module	WSM module
ERS 8300	p83r3000 .dld					
ERS 8600	p80j4110 .dld	p80m4110 .img	p80p4110 .dld	p80s4110.img	p80t4110.dld	p80w4110.dld

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

Chapter 12: Sample configuration scripts

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

Navigation

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
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
```