Bulk Device Configuration Management using Avaya Fabric Orchestrator

Release 1.0
NN48100-502
Issue 01.01
November 2015

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

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

This document is intended for administrators.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document title	Use this document for:	Audience
Avaya Fabric Orchestrator Solution Description, NN48100–100	Description of each verified reference configuration.	System administrator
Deploying Avaya Fabric Orchestrator, NN48100–101	Installing, configuring, initial administration, and basic maintenance checklist and procedures.	System administrator
Getting Started and Locating the latest software and Release Notes for Avaya Fabric Orchestrator, NN48100–102	Locating the latest software and product release notes.	System administrator
Network Monitoring using Avaya Fabric Orchestrator, NN48100–500	Monitoring the managed objects in AFO.	System administrator

Table continues…

Document title	Use this document for:	Audience
Network Configuration using Avaya Fabric Orchestrator, NN48100–501	Configuring and managing Avaya Enterprise family of devices from discovered network.	System administrator
Bulk Device Configuration Management using Avaya Fabric Orchestrator, NN48100–502	Performing a variety of management tasks across multiple device types using a web-based interface.	System administrator
Virtualization Configuration using Avaya Fabric Orchestrator, NN48100–503	Connecting the vCenter server to AFO, to help the data center administrator to configure the network changes that apply to the data center.	System administrator
IP Flow Configuration using Avaya Fabric Orchestrator, NN48100–504	Collecting and analyzing IP flows from IPFIX-, NetFlow v5-, and NetFlow v9- enabled devices.	System administrator
Administration using Avaya Fabric Orchestrator, NN48100–600	AFO System administration procedures.	System administrator
Avaya Fabric Orchestrator Traps and Trends Reference, NN48100–700	Viewing a list of supported traps and trends.	System administrator
Avaya Fabric Orchestrator Supported Devices, Device MIBs, and Legacy Devices Reference, NN48100–701	Confirming support for devices and MIBs.	System administrator

Training

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Subscribing to e-notifications

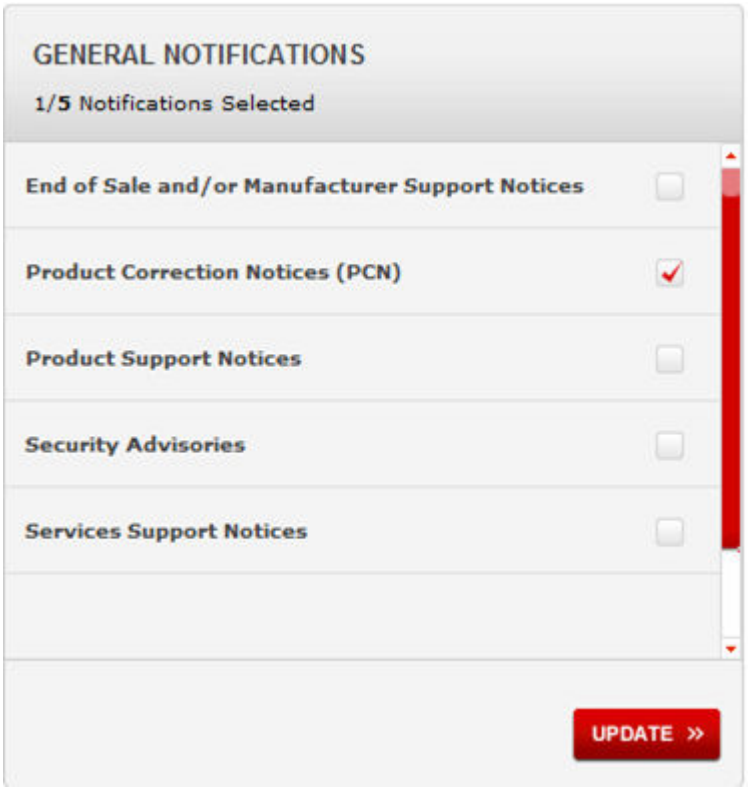
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

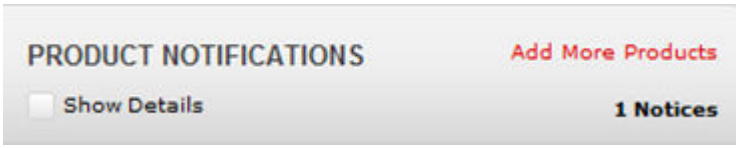
You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

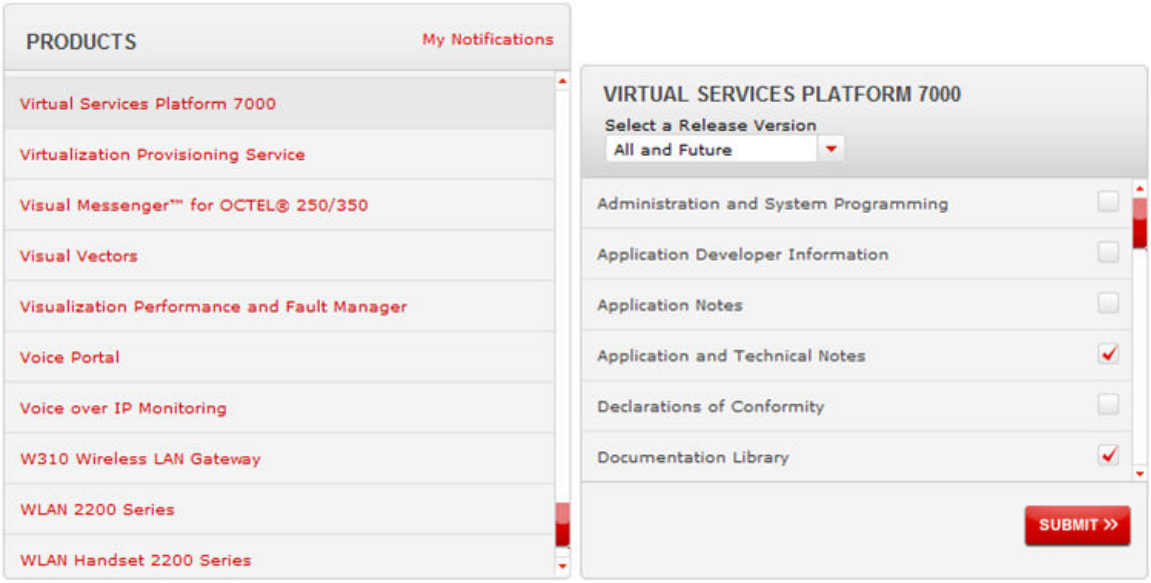
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Support

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

Chapter 2: New in this document

New in this document

Bulk Device Configuration Management using Avaya Fabric Orchestrator, NN48100–502 is a new document for Release 1.0 so all the features are new in this release. See *Avaya Fabric Orchestrator Release Notes* for a list of supported features.

Chapter 3: Bulk device overview

Overview

AFO Bulk Provisioning tools allow you to perform a variety of management tasks across multiple device types using a Web-based interface.

AFO Bulk Provisioning provides the following tools:

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

Configuration Backup and Restore

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

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

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

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

Backup and restore tool

During the backup process, a human readable text format of the saved configuration is created for all the supported devices except BSR-s. This file is automatically saved in the backup archive in compare folder on Avaya Fabric Orchestrator Configuration (AFO Configuration) or AFO Bulk Provisioning server. The Linux default folder for the file save is `/opt/avaya/afo/shared/config/`.

Note:

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

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

Important:

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

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

Reporting feature

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

E-mail alert function

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

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

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

For more information about the e-mail feature, see Creating a configuration backup task on page 26.

User interface

The Configuration Backup and Restore tool supports the following devices:

- Tasman
- BSR 222/252

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

For more information about supported device versions, refer to Supported Devices on page 65.

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

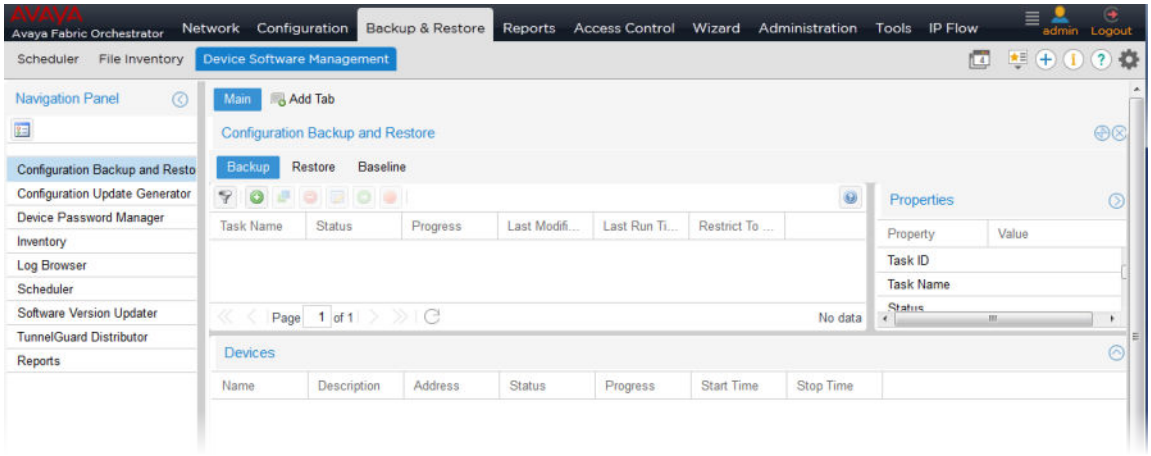


Figure 1: Configuration Backup and Restore

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

Table 1: CBR backup task table

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

Table 2: Backup Device table

Field	Description
Name	The name of the device.

Table continues…

Field	Description
Description	The device.
Address	The address of the device.
Status	The status of the device.
Progress	The progress of the device.
Start Time	The start up time of the device.
Stop Time	The stop time of the device.

Table 3: CBR restore task table

Field	Description
File Name	The name of the restore task.
Address	The address of the device.
Backup Date	The day, month, year, and time of the backup.
Status	The status of the task.
Progress	The progress of the task.
Last Run Time	The last run time of the task
Version	The software version on the device at the time of the backup.
Restrict to Same Version	If the restore can only be performed on the same version as the backup version.
Task ID	The task index.

Table 4: CBR baseline table

Attribute	Description
Address	The address of the device.
Device Type	The type of device used in the backup task.
Backup Date	The day, month, year, and time of the backup.

Configuration Update Generator

You can use the Configuration Update Generator (CUG) 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, AFO Bulk Provisioning automatically reboots them and for devices on which CUG does not applies changes, AFO Bulk Provisioning drops the

connection, and waits for a minute, and then reconnects again for only checking the device connectivity.

The Configuration Update Manager supports the following devices:

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

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

The following tables describe the fields of the CUG tool, the devices, and the fields of the script or data files you upload to the AFO Bulk Provisioning.

Table 5: CUG task table

Field	Description
Task Name	The task name.
Status	The status of the task.
Progress	The progress of the task.
Last Modified Time	The last time a task was modified.
Last Run Time	The last run time of the task.
Id	The task index.
Type	The file type to deploy.
Template File	The template file name (previously created).
Data File	The data file name (previously created).
Device IDs	The IDs of the device.

Table 6: CUG device table

Field	Description
Name	The name of the device.
Description	The device.
Address	The address of the device.
Status	The status of task for the device.
Progress	The progress of the task for the device.

Table continues…

Field	Description
Start Time	The start up time of task for the device.
Stop Time	The stop time of the task for the device.

Table 7: Template or data files

Field	Description
Name	The file name of the script or data file.
Size	The file size of the script or data file.

CUG Wizard

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

For more information about the CUG Wizard, see CUG Wizard on page 38.

Device Password Manager

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

Note:

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

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

Note:

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

The Device Password Manager supports the following devices:

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

The following tables describe the fields of the DPM tool, and the devices for which you can change the password.

Table 8: DPM task table

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

Table 9: DPM device table

Field	Description
Name	The name of the device.
Description	The device.
Address	The address of the device.
Status	The status of the task for the device.
Progress	The progress of the task for the device.
Start Time	The startup time of the task for the device.
Stop Time	The stop time of the task for the device.

Inventory

You can use the AFO Bulk Provisioning Inventory feature to store and import devices. The devices from the AFO Configuration inventory are automatically imported when AFO Bulk Provisioning is launched for the first time. Once the AFO Bulk Provisioning is open, the inventory is not automatically updated when the inventory in AFO Configuration changes. Use the Import from AFO Configuration option to manually import AFO Configuration inventory into AFO Bulk Provisioning inventory.

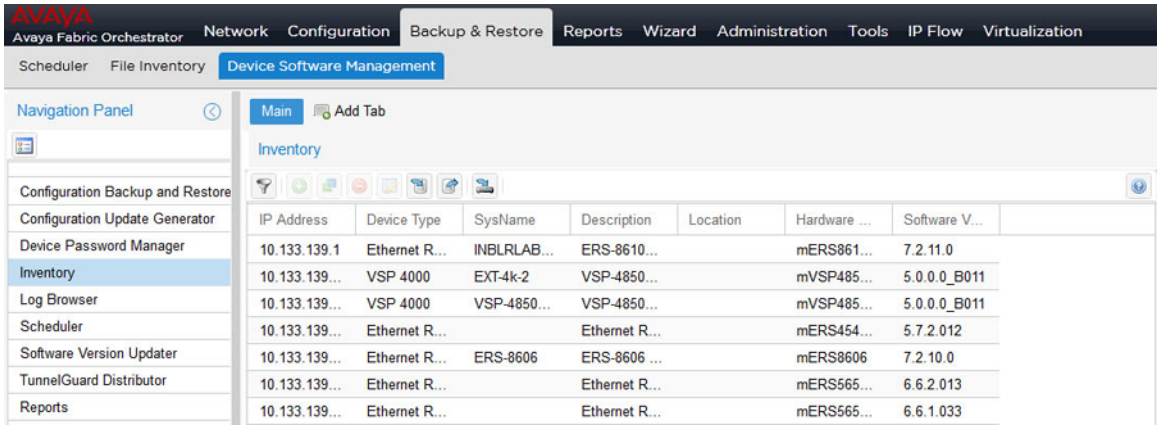


Figure 2: Inventory

The Inventory tool supports the following devices:

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

Table 10: Inventory table

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

Log Browser

You can use the Log Browser to access AFO Bulk Provisioning logging information.

AFO Bulk Provisioning logs all interactions with devices to a common file stored in the `COM_HOME/log` folder. This file rolls over to a new file when the size reaches 10 megabytes. You

can open each log file or export the log for offline inspection or for transfer to Avaya customer service. You can modify your view of the Log Browser by filtering the log based on date and time, tool name, or keyword. You can also modify the automatic refresh interval and configure different colors for Info, Warning, and Error log messages.

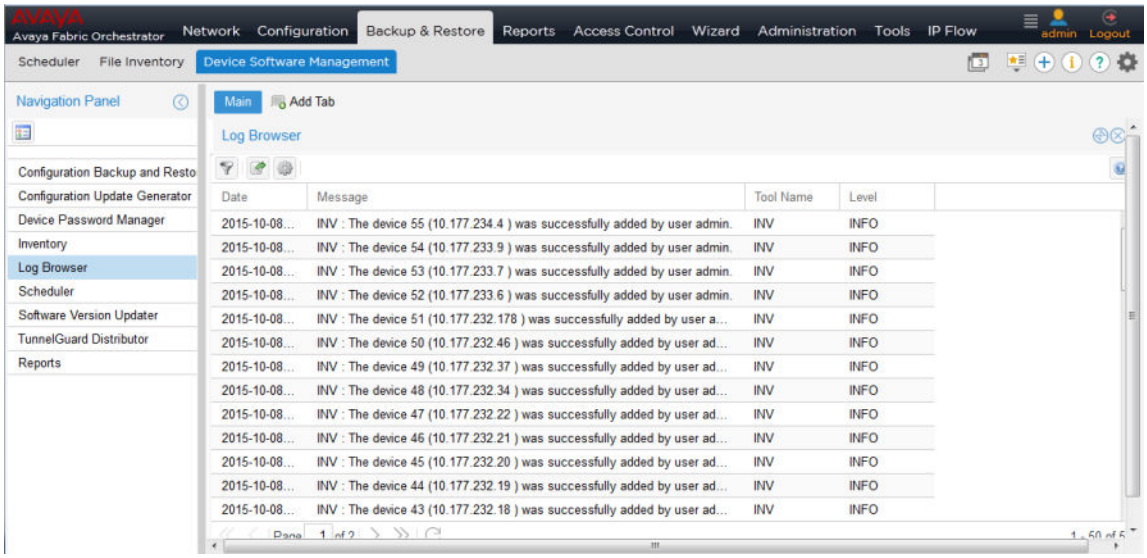


Figure 3: Log Browser

Table 11: Log Browser table

File	Description
Date	The day, month, year, and time of the log
Message	The log message that appears
Tool Name	Name of the AFO Bulk Provisioning tool
Level	The log level

Scheduler

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

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

Table 12: Scheduler table

Field	Description
Name	The name of the scheduled activity
Enabled	The state of the scheduled activity. You can enable or disable a schedule.
Tool Name	The tool name
Task Name	The name of the task
Next Date	The next date on which the task will be executed
Repeat Interval	The interval for task to repeat
Repeat Unit	The unit of time for the repeat interval
Status	The status of the scheduled activity.
Progress	The progress of the scheduled activity.
Last Modified Time	The time you last modified the schedule.
Task ID	The task index.

Table 13: Details table

Field	Description
Start Date	The start date of the scheduled activity.
Stop Date	The stop date of the scheduled activity.
Status	The status of the scheduled activity.
Progress	The progress of the scheduled activity.

Software Version Updater

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

Important:

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

The Software Version Updater supports the following devices:

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

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

The following tables show the fields of the SVU tool, the devices on which you can update the software, and the fields of SVU image files.

Table 14: SVU task table

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

Table 15: SVU device table

Field	Description
Name	The name of the device
Description	The device description
Address	The address of the device
Status	The status of the device
Progress	The progress of the device
Start Time	The startup time of the device
Stop Time	The stop time of the device

Table 16: Package table

Field	Description
Device Type	The type of the device
Package Name	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 17: File table

Field	Description
File Name	The file name.
Size	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.

The following tables show the fields of the TGD tool, and the devices to which a tunnelguard rule is distributed.

Table 18: TGD task table

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

Table 19: TGD device table

Attribute	Description
Name	The name of the device.
Description	The device.
Address	The address of the device.
Status	The status of the device.
Progress	The progress of the device.
Start Time	The startup time of the device.
Stop Time	The stop time of the device.

Chapter 4: Managing bulk devices

Managing bulk devices

The following sections provide the procedures for managing and configuring bulk devices using AFO.

Configuration Backup and Restore

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

Managing the backup tasks

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

Configuring the e-mail alert settings

Before you can use any e-mail alert function in AFO Bulk Provisioning, you must configure the e-mail alert settings. You can work with the e-mail server settings in Global Preferences page to set up the SMTP values for your e-mail server. You can also use the Configuration Preferences to enable or disable the e-mail alert function. Select the Preferences icon from the quick toolbar to configure the email alert settings.

For more information on configuring the email alert settings and preferences, see *Administration using Avaya Fabric Orchestrator*, NN48100–600.

Creating a configuration backup task

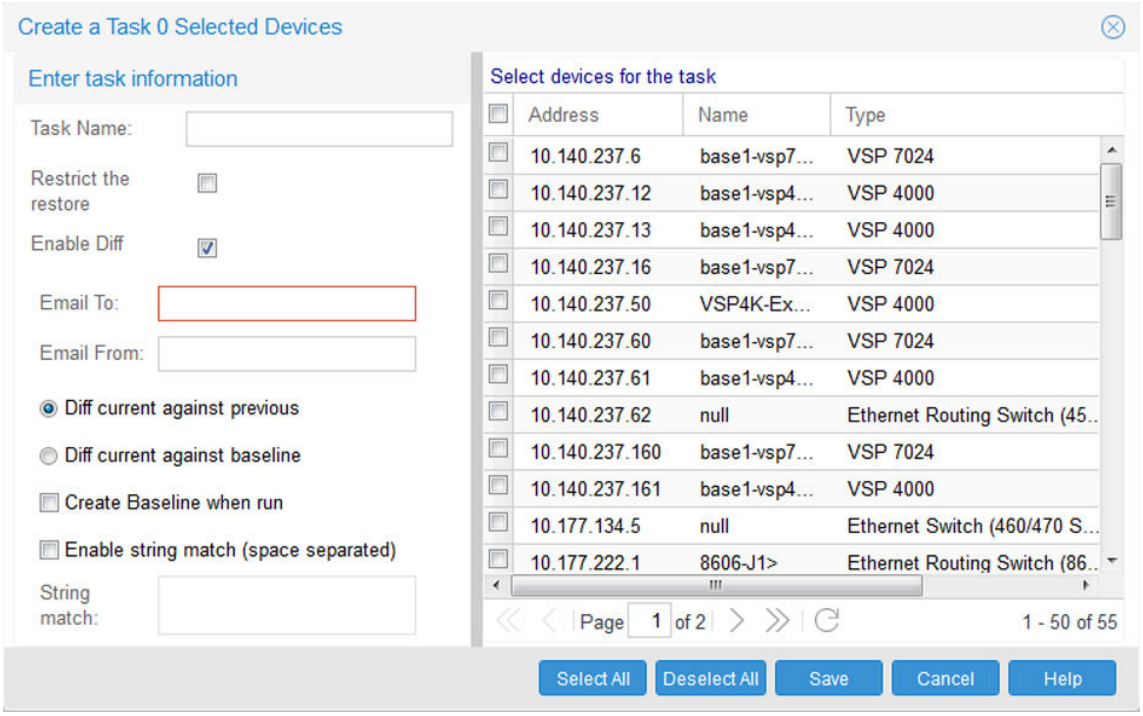
Perform the following procedure to create a configuration backup task:

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup** to open a new or an existing portlet.

2. Click the **Add task** icon.

   The Create a Task window displays.



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

   When enabled, AFO Bulk Provisioning allows the restore operation only on devices that have the same software version at the time of the backup.
5. Select the list of devices to be backed up.
6. Specify whether you want to enable the **Enable Diff** for e-mail alerts.

   If you chose to disable the diff function for e-mail alerts, go to the final step.
7. In the **Enable Diff** section, enter values in the following fields:
   - **Email To** — Specifies the recipient of the e-mail alert.
   - **Email From** — Specifies the sender of the e-mail alert.
8. Select a radio button option to specify the type of backup diff you would like to use:
   - **Diff current against previous** — Run a backup diff based on a previous config.

     If you choose this option, select the devices for which you want to perform a diff on a previous config. Your selections must be made in the **Select devices for the task list** box.
   - **Diff current against baseline** — Run a backup diff based on a baseline.

     If you choose this option, you must set a backup baseline for a device in the **Baseline** tab in the CBR portlet.
9. Specify whether you want to create a baseline when the backup is run.

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

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

11. Click **Save**.

Example

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

Next steps

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

Filtering the configuration backup tasks

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

Procedure steps

1. **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup** to open a new or an existing portlet.
2. Click the **Filter Tasks** 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 Backup tasks table.

Setting a backup baseline for a device

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

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

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

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Baseline**.

2. Select the IP address of the device in which you want to set a baseline.
3. Select a backup date value from the drop down menu to set a baseline backup date for the device.
4. Click **Set selected config as Baseline**.

Duplicating a configuration backup task

Duplicate a configuration backup task in Backup tasks table. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the task that you want to duplicate in the Backup tasks table.
3. Click the **Duplicate Task** icon.

   You are prompted to confirm the task duplication.
4. Click **Yes**.

   The duplicate task appears in the Backup tasks table.

Editing a configuration backup task

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

Perform the following procedure to edit a configuration backup task:

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the task to be edited and click the **Edit Task** icon.
3. **(Optional)** Edit the values in the following fields:
   - **Task Name**
   - **Restrict the restore**

     When selected, AFO Bulk Provisioning allows the restore operation only on devices that have the same software version as at that of the backup.
   - **Enable Diff**

     When selected, you can use the diff type settings to determine when an e-mail alert is sent and what the alert contains.
4. **(Optional)** Edit the following field values in the Diff Type section:
   - **Email To**
   - **Email From**
   - **Diff current against previous**

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

- **Diff current against baseline**

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

- **Create Baseline when run**
- **Enable string match**

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

5. Click **Save**.

Next steps

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

Activating a configuration backup task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the task you want to activate.
3. Click the **Activate Task(s)** icon.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the tasks to be deleted.
3. Click **Delete**.
4. Click **OK**.
5. Select **Yes** to confirm.

Managing the restore tasks

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

Filtering the configuration restore tasks

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Click the **Filter Tasks** icon.

   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 AFO Bulk Provisioning.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Click the **View Backup Details** icon.

   The View Backup Details dialog window appears.
3. From the file list, select the file that you want to view.

   The File Download dialog window appears.
4. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Select the task to be edited.
3. Click the **Edit task** icon.

   The Edit a task dialog box appears.
4. Enable or disable the **Restrict the same version** field.

   When selected, AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Select the two files that you want to compare. Use the **Ctrl** or **Shift** key to select the files.
3. Click **Compare**.

   The Compare dialog window displays and you are prompted to compare the files.
4. Click **Yes**.

   The File Download dialog window displays.
5. Click **Open** or **Save**.

   If you choose to open the file, the Smart Diff dialog 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Select the backup archive you want to restore.
3. Click the **Activate Task(s)** icon.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Select the archives to be deleted.
3. Click the **Delete Task(s)** icon.
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.

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.

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/ACLI 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 AFO Bulk Provisioning; 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 AFO Bulk Provisioning 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:

`/opt/avaya/afo/shared/config/ConfigUpgradeGenerator/UserFiles/Templates`.

The data files are stored in `/opt/avaya/afo/shared/config/ConfigUpgradeGenerator/UserFiles/Values`.

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

User-defined files can be as follows:

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

The following procedures describe how to manage configuration files and tasks on the AFO Bulk Provisioning server.

Uploading a user-defined configuration file

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Files** > **Add File**.

   The Add file dialog box displays.
3. Click **Browse** to browse and open the configuration file.
4. Click **Upload** to upload the file.
5. Click **OK**.
6. Close the Add file dialog box.

Removing a user-defined configuration file

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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Files**, and select the files to be deleted.
3. Click **delete File**.
4. Click **Yes** to confirm the deletion.

Viewing or editing a user-defined configuration file

View or edit any template or data file that was previously imported into AFO Bulk Provisioning.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Files** and select a file to edit from the Template Files section.
3. Click **Edit File**.

   The Edit file window displays the selected file contents.
4. Edit the file and click **Save**.
5. **Close** the Edit File window.

Exporting a user-defined configuration file

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

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click the **Files** tab.
3. Select the Template file to export, and then click **Export File**.

   The View Files window displays.
4. Click the file name.

   The File Download window displays.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Select **Tasks** > **Add Task**.

   The Add a task window displays.
3. Complete the fields as appropriate.
4. Click **Save**.

Filtering the CUG tasks view

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Select **Tasks** > **Filter Tasks**.

   The Add a filter dialog box displays.
3. In the **Task Name** field, enter the task name or the first letter of the task name to be filtered.

   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. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Tasks** and select the task to be duplicated.
3. Click **Duplicate Task**.
4. Click **Yes** to confirm.

Editing a CUG task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Tasks** and select the task to edit.
3. Click **Edit Task** and edit the information as required.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Tasks** and select the task to be deleted.
3. Click **Delete Task**.
4. Click **Yes** to confirm.

Activating a configuration task

Execute a configuration to activate the task and start deployment.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Tasks** and select the tasks to be activated.
3. Click **Activate Task**.
4. Click **OK** to confirm.

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 for the active task.

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.

Configuration Update Generator

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

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

- Launch CUG Wizard—Launches the CUG task creation wizard from the CUG task grid portlet toolbar.
- Describe the task—Use the initial wizard screen to describe the CUG task primary task properties, which are task name and target devices.
- Define and create a template file—Use the template file wizard screen to create a command template file.
- Define and create a data mapping file—Use the data file screen to create a CSV data file.
- Deploy and schedule the task—Use the final wizard screen to schedule and deploy the task to the CUG task grid.

Variable definitions

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

Table 20: CUG Wizard command buttons

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

Launching the CUG Wizard

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

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator**.
2. From the CUG portlet toolbar on the Tasks tab, click **Launch CUG Wizard**.

   The Create a Task window displays.

Next steps

Perform the procedure for Creating a task on page 39.

Creating a task

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

Procedure

1. In the Create a Task window, enter the task file name.
2. From the Select devices for the task section, select the device(s) for the task.
3. Click **Next**.

Next steps

Perform the procedure for Creating a template file on page 39 or Editing a template file on page 41.

Variable definitions

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

Table 21: CUG Wizard Create a Task screen

Field	Description
Task Name	Name of the task.
Address	The IP address of the device.
Type	The device type.
Description	The description of the device.

Creating a template file

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

Before you begin

Create a task using the CUG Wizard.

Procedure

1. From the Create a task template file window, in the File Type section, select **New File**.

2. In the Template Name field, enter the name of the template.
3. Enter the CLI commands in the Template file contents (CLI commands) section.
4. Click **Next**.

Note:

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

Next steps

Perform the procedure for Creating a variable mapping file on page 42.

Variable definitions

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

Table 22: CUG Wizard Create a task template file screen

Field	Description
File Type	Select file type. You can select from the following options: • New File • Existing File
Template Name	Enter the name of the template file. If you select an existing file, a drop-down list box of existing templates appears.

Template file contents (CLI commands)	Contains the actual CLI command lines to be executed against each selected target device.
	If a CLI command line in the template file contains a variable with a different value depending on target device, the character sequence ??? preceeds the CLI command.
	For example, in `cmd1 ???arg1`, the variable `arg1` accepts different values for different target devices. The following is an example of a template file designed to set a new prompt value and a new history count.
	`set prompt ???name`
	`set history ???count`
	In the preceding example, the actual values of `name` and `count` and the associated target device IP addresses appear in a separate variable mapping file. If args from the template file do not need to be a variable, that is, args do not need to change depending on target device, then you do not create a variable mapping file.
	For example, the following file example implies that all `args` have a fixed constant value for all associated target devices.
	`set prompt '8600 >'`

Table continues…

Field	Description
	`set history 10` If the template file contains constant `arg` values, the variable mapping file creation step is omitted.

Editing a template file

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

Before you begin

Create a task.

Procedure

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

Note:

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

Next steps

Perform the procedure for Creating a variable mapping file on page 42.

Variable definitions

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

Table 23: CUG Wizard Create a task template file screen

Attribute	Description
File Type	Select file type. You can select from the following options: • New File • Existing File
Template Name	Enter the name of the template file. If you select an existing file, a drop-down list box of existing templates appears.
Template file contents (CLI commands)	Contains the actual CLI command lines to be executed against each selected target device. If a CLI command line in the template file contains a variable with a different value depending on target device, the character sequence ??? preceeds the CLI command.

Table continues…

Attribute	Description

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

Creating a variable mapping file

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

Note:

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

Before you begin

Create a new template or edit an existing template.

Procedure

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

   After you select an argument cell, the command line from the template file appears within the lower left of the window frame.
3. To sync a variable, click the **Sync Variable** icon.
4. Click **Next**.

Next steps

Perform the procedure for Scheduling and saving a task on page 43.

Variable definitions

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

Table 24: CUG Wizard Create a variable mapping file screen

Field	Description
Mapping File name	Name of the mapping file.
Sync Variable	Syncs an argument value to all instances, therefore using the same value for all devices.
Address	IP address of a device.
arg1	Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value. **Note:** After you select an argument cell, the command line from the template file appears within the lower left of the window frame.
arg2	Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value. **Note:** After you select an argument cell, the command line from the template file appears within the lower left of the window frame.
arg3	Arguments defined in the task template file, which are variable names preceded by the ??? character sequence. Set the variable value. **Note:** After you select an argument cell, the command line from the template file appears within the lower left of the window frame.

Scheduling and saving a task

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

Before you begin

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

Procedure

1. In the CUG Task description window, verify the Task Name, Template File Name, and Map File Name.
2. Perform one of the following actions:
   - Click **Finish** and proceed to final step.
   - Click **Schedule Task**. Proceed to the next step to start the task configuration.
3. In the Add a schedule window, enter the schedule information as appropriate.
4. Click **Save**.

Variable definitions

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

Table 25: CUG Wizard CUG Task description screen

Field	Description
Task Name	Name of the task.
Template File	Name of the template file.
Mapping File	Name of the map file.

Variable definitions

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

Table 26: CUG Wizard Add a schedule screen

Field	Description
Schedule Name	Name of the CUG task schedule.
Tool Name	Name of the Bulk Configuration Manager tool.
Task Name	Name of the CUG task.
Server Date	The start date the server assigns to the schedule. **Note:** The server date may be different from the date on your computer.
Start Date	Date you assign the schedule to start.
Start Time	Time you assign the schedule to start.
Internal Value	Number that represents the seconds, minutes, hours, and days for the internal unit setting.
Internal Unit	Value you assign to repeat the activation of the task in selected increments of seconds, minutes, hours, days, or weekly.
Enabled	Enables the scheduled task to run.

Device Password Manager

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

Managing DPM tasks

Complete the following procedures to manage password management tasks.

Prerequisites

- You must have System Administrator rights to use DPM.

Creating a Device Password Manager task

Create the Device Password Manager (DPM) task to group devices that have the same credentials.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or an existing portlet.
2. Click **Add Task**.

   The Create a Task dialog box displays.
3. Enter the Task Name and Password. Complete the other fields as appropriate.
4. Select the list of devices to be added to the task.
5. 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.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a DPM portlet.
2. Click the **Filter** icon.

   The Add a filter window displays.
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 displays in the DPM tasks table.

Duplicating a DPM task

Duplicate a DPM task in the DPM tasks table. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a DPM portlet.
2. Select the task you want to edit.
3. Click **Edit Task**.
4. Edit the Task as required.
5. Click **Save**.

Activating a DPM task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a DPM portlet.
2. Select the task you want to run.
3. Click **Activate Task(s)**.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **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 table only in maximized view.

Inventory management

Add and store devices on AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open a new or an existing inventory portlet.
2. Click **Add Device**.

   The Add a device window appears.
3. Enter the **IP address** of the device and select the **Device Type** from the drop-down menu.
4. **(Optional)** Complete the other fields as appropriate
5. Click **Add**.

Filtering the devices

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an inventory portlet.
2. Click **Filter Devices**.

   The Add a filter dialog box displays.
3. Select the device(s) to be filtered.
4. **(Optional)** To filter the search result by IP address or the device name, enter the details in the **IP address** or **SysName** fields.
5. Click **Find**.

Duplicating devices in the Inventory

Duplicate devices in the Inventory devices table. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an inventory portlet.
2. Select the device to duplicate, and click **Duplicate Device**.

   The Duplicate a device dialog box displays.

3. Enter the IP address of the device that needs to be duplicated.
4. Complete the other fields as appropriate
5. Click **Duplicate**.

Editing items in the Inventory

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an inventory portlet.
2. Select the device that needs to be edited.
3. Click **Edit**.

   The Edit Device dialog box displays.
4. Edit the device information.
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

Table continues…

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_na me_15	description_15	location_15	hardware_t ype_15	software_t ype_15
120.120.110.16	VSP_DEVICE	device_na me_16	description_16	location_16	hardware_t ype_16	software_t ype_16
120.120.110.17	WC_8180_DEV ICE	device_na me_17	description_17	location_17	hardware_t ype_17	software_t ype_17

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an Inventory portlet.
2. Click **Import**.

   The Import device(s) from csv File window displays.
3. Browse to locate the csv file.
4. Click **Import**.

   Note:

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

Exporting devices to .csv file

Export devices to .csv file.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an inventory portlet.
2. Select the device that needs to be exported.
3. Click **Export Inventory to .csv file**.

   The Insert file name to export to dialog box displays.
4. Type the file name, and then click **Export**.

   The File Download popup window displays.
5. Select **Open** to open the .csv file or **Save** to save the file on your local system.

Importing devices from Configuration

Perform the following procedure to import the device inventory from AFO Configuration to AFO Bulk Provisioning.

Prerequisites

Log on to AFO as a system administrator.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Inventory** to open an inventory portlet.
2. Click **Import from Configuration**.

   The Import from Configuration dialog box displays.
3. Click **Yes**.

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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Log Browser** to open an Log Browser portlet.
2. Click **Refresh**.

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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Log Browser** to open an Log Browser portlet.
2. Click **Filter Log**.

   The Filter log dialog box displays.
3. Complete the fields as appropriate.
4. Click **Clear** to clear the settings.
5. Click **Save**.

Configuring log settings

Perform the following procedure to configure the log settings.

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a log browser portlet.
2. Click **Log Settings**.

   The View log settings dialog box displays.
3. Select the appropriate settings.
4. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a log browser portlet.
2. Click the down arrow and point to Columns.

   A popup window appears with the available column options for the log browser list view.
3. Select the required column options.

Clearing all view filtering

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **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

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a log browser portlet.

2. Click **Export Logs**.

   The View log files window displays.
3. Select the file that needs to be exported.
4. Click **Open** or **Save**.
5. Click **OK**.

Scheduling tasks

Create schedules for AFO Bulk Provisioning tools using Scheduler.

Important:

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

Adding a schedule

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Scheduler**.
2. Click **Add**.

   The Add a schedule window displays.
3. Enter the schedule information as appropriate.
4. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Scheduler**.
2. Click **Filter Tasks**.

   The Add a filter dialog box displays.
3. Enter the task name or the first letter of the task name to be filtered.

   Note:

   To display all the tasks, leave the Task Name field empty.
4. Click **Find**.

Editing a schedule

Use this procedure to edit an existing schedule.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Scheduler**.
2. Select the task to be edited.
3. Click **Edit Schedule**, and edit the details of the scheduled task.
4. Click **Save**.

Deleting a schedule

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Scheduler**.
2. Click **Refresh** to update the schedule list.
3. Select the task to be deleted.
4. Click **Delete scheduled Task(s)**.
5. Click **Yes** to confirm the deletion.

Software version upgrades

The following topics describe software upgrade tasks.

Important:

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

Managing software version images on the file server

Complete the following procedures to manage software version images on the file server.

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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Click **Packages** > **Add Package**.

   The Create a Package window displays.
3. Enter the package information.
4. Click **Browse** to browse and open the image file.

5. Click **Upload file** to upload the file.

   The file transfers to the server and appears in the file table. Repeat steps 4-5 until all files in the software package are added.
6. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Click the **Packages** tab, and select the image package to be deleted.
3. Click **Delete Package(s)**.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Click the **Packages** tab, and select the package to edit.
3. Click **Edit Package**.

   An Edit Package window displays.
4. Select the files you want to delete from the Files in package section.
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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Select the Tasks tab.
3. Click **Add Task**.
4. Enter the task information as appropriate.

   Note:

   For the Avaya Ethernet Routing Switch 8600, the AFO Bulk Provisioning provides option to save the upgraded image on a PCMCIA card.
5. Select the list of devices to update from the Select devices for the task section.

6. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Select the **Tasks** tab.
3. Click **Filter Tasks**.

   The Add a filter dialog box displays.
4. In the Task Name field, type the task name or the first letter of the task name to be filtered.

   Note:

   To display all the tasks, leave the Task Name field empty.
5. Click **Find**.

Duplicating an SVU task

Duplicate an SVU in the SVU tasks table. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Select the **Tasks** tab.
3. Select the task to duplicate.
4. Click **Duplicate Task**.
5. Click **Yes** to confirm the task duplication.

Activating an SVU task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Select the **Task** tab.
3. Select the task you want to run.
4. Click **Activate Task(s)**.
5. Click **OK** to confirm the activation.

Editing an SVU task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Click the **Tasks** tab and select the task to edit.
3. Click **Edit**, and edit the task information as required.
4. Click **Save**.

Deleting an SVU task

Delete an SVU task.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open an SVU portlet.
2. Select the tasks 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 table only in maximized view.

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.

Adding existing TunnelGuard policies

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Click **Add Task**.
3. Enter a task name and select the source device from which the policy requires to be transferred.

4. Click **Next**.
5. Enter the domain information and click **Next**.
6. Select the group to be transferred. Complete the other fields as appropriate.
7. Click **Next**.
8. Select the devices to which the policy requires to be transferred.
9. 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Click **Filter**.

   The Add a filter dialog box displays.
3. In the Task Name field, enter the task name or the first letter of the task name to be filtered.

   Note:

   To display all the tasks, leave the Task Name field empty.
4. Click **Find**.

Duplicating a TGD task

Duplicate a TGD task in the TGD tasks table. AFO Bulk Provisioning 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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Select the task to duplicate.
3. Click **Duplicate Task**.
4. Click **Yes** to confirm duplication.

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 AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Select the task to edit.
3. Click **Edit Task**.

4. Edit the task information and click **Next**.
5. Edit the domain information and click **Next**.
6. Edit the group information and click **Next**.
7. Select the devices to which the policy requires to be transferred.
8. Click **Finish**.

Deleting a TGD task

Use the following procedure to delete at TGD task.

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Select the tasks to delete.
3. Click **Delete Task**.
4. Click **Yes** to confirm the deletion.

Activating a TGD task

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

Procedure steps

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a TGD portlet.
2. Select the task you want to activate.
3. Click **Activate Task**.
4. Click **Yes** to confirm activation.

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.

Running a backup diff report

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

Perform the following procedure to run a backup report:

Before you begin

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

Procedure

1. From the AFO menu bar, select **Backup & Restore** > **Device Software Management** > **Reports** to open a Reports portlet.

   The Reports window displays.

2. In the **Diff Reports** tab, select the first device file listing on the **Backup Date** column.
3. Select the second device file listing on the **Backup Date2** column.
4. Click **Create Report**.

Chapter 5: Troubleshooting

Troubleshooting

The following sections provide troubleshooting information for AFO Bulk Provisioning.

Firewall Configuration

AFO Bulk Provisioning 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 AFO Bulk Provisioning server, you must open up the affected protocol in your firewall configuration.

NAT

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

Saving CLI/ACLI correspondence with a device to a file

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

Procedure steps

1. Create a new traffic.control file in the COM home folder (`/opt/avaya/smgr/COM/`).

   Tip:

   The traffic.control file is not a text or .txt file.
2. Open the file.
3. You can record traffic for all devices or for selected devices.
   - Option 1: To record traffic for all devices, type ALL on the first line of the traffic.control file and then Save and Close. Files of the form xx.xx.xx.xx.traffic are created in the COM home 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.

AFO Configuration e-mail settings

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

Terminal length

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

Appendix A: Device types and limitations

Device types and limitations

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

The following list outlines the limitations of AFO Bulk Provisioning when communicating with devices:

- Contivity VPN routers cannot have # or > in the prompt.
- Avaya Ethernet Routing Switch 2500, 4500, 5500, 8300, and 8600 cannot have more than one # in the prompt.
- SVU on Ethernet Routing Switch 8300/8600 has a set of mandatory files. Image files cannot be uploaded individually.
- Ethernet Routing Switch 8600 SSH works on 3DES or AES depending on software version.
- Ethernet Routing Switch 8300 SSH works only on 3DES and AES.
- For all devices, except devices with two CPUs, to execute an AFO Bulk Provisioning 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 AFO Bulk Provisioning supported devices, and shows how Avaya device names appear on the AFO Bulk Provisioning interface and in the csv files.

Avaya device name	Label on AFO Bulk Provisioning 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

Table continues…

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

SVU file types

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

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

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

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

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

Device	Mandatory I/0 module	SuperMezz module	POS module	SSL module	ATM module	WSM module
ERS 8300	p83r3000 .dld					
ERS 8600/8800	p80j4110 .dld p80k4110.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

Table continues…

Device	SVU file
VSP 8xxx	VSP8200.4.0.0.0.tgz
VSP 4000	VSP4K.4.0.0.0.tgz
VSP 7000	lakemerced_1020.elf.gz

Supported devices

For information about AFO supported devices, see *Deploying Avaya Fabric Orchestrator*, NN48100–101.

Sample configuration scripts

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

VPN router configuration

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

If you use CUG to execute commands on a VPN router, AFO Bulk Provisioning executes the following commands by default:

```
enable
configure terminal
```

After AFO Bulk Provisioning 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, AFO Bulk Provisioning 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, AFO Bulk Provisioning 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, AFO Bulk Provisioning 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, AFO Bulk Provisioning 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, AFO Bulk Provisioning 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
```