ExtremeManagement™

Bulk Device Configuration Management using Extreme Fabric Orchestrator

Release 1.2
NN48100-502
Issue 03.01
December 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks 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 or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks’ 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

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

“Hosted Service” means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks 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 Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE (“EXTREME NETWORKS”).

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 Extreme Networks or an Extreme Networks 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 set of Designated Processors that hosts (physically or virtually) 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 type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks 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 Extreme Networks through electronic means established by Extreme Networks 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 Extreme Networks, 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.

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 Extreme Networks' prior consent and payment of an upgrade fee.

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 Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks 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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks 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 Extreme Networks' website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. 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 only 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS 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 EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS 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

You acknowledge and agree that it is Your responsibility 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 Extreme Networks 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.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

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

Contact Avaya Support

See the Avaya Support website: https://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: https://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 Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks 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 Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

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

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface

Purpose

This document provides information about Bulk Device Configuration Management and includes procedures for configuring and managing your network. Bulk Provisioning is a feature in Extreme Fabric Orchestrator (EFO) 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.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

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.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

New in this document

The following sections detail what is new in this document. See *Extreme Fabric Orchestrator Release Notes* for a list of supported features.

Upgrade a VOSS device without rebooting

The device upgrade without rebooting feature support is extended to VOSS and APLS devices.

The user can now choose to upgrade the VOSS and APLS devices without rebooting by unselecting **Reboot after image download** checkbox in the Software Version Updater (SVU) task window.

Special characters in task names

Special characters are allowed in task names in all Device Software Management (DSM) portlets such as Configuration Backup and Restore (CBR), Configuration Update Generator (CUG), Device Password Manager (DPM), Software Version Updater (SVU), and TunnelGuard Distributor (TGD).

Device filtering and searching in Device Software Management tasks

The system supports device filtering and searching while adding devices to a task. You can can filter the list of devices based on the selected columns. The search field allows you to search for the required device from the device list. The device list auto updates once you start a search. Searching without any search criteria selects all devices listed. The search field searches all columns and when a match occurs the device row is selected and highlighted.

Interactive CLI commands in Configuration Update Generator scripts

The system supports interactive CLI commands in Configuration Update Generator scripts. This feature enables the user to input the details requested by the device. The delay and reconnect interactive CLI commands allow the user to specify the delay in rebooting the device and attempt to reconnect to a disconnected device at a specified interval. The password interactive CLI command ensures that the password is not written in plain text.

Configuration Backup and Restore compare switch configuration updates

The device Configuration Backup and Restore compare feature now uses SmartDiff tool instead of Java Web Start. Using Java Web Start required installation of JRE on the client browser which was not allowed due to security considerations. The SmartDiff tool eliminates the need to install JRE.

Enhanced RBAC for Configuration Update Generator templates

The system provides the ability to restrict the creation, deletion, or modification of Configuration Update Generator (CUG) templates. All network administrators can execute the templates.

A new EFO Device Config Template Administrator role is available with read-execute and write-execute permissions for Device Config Templates. The pre-existing EFO Network Administrator role is available with read-execute permissions.

Chapter 3: Bulk device overview

Overview

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

Bulk Provisioning provides the following tools:

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

You can customize the Bulk Device Management work area and add portlets of the tools you choose from the navigation panel. When you click the tool, you get the option to open a new or an existing portlet and the portlet window is added in the work area. You can customize your work area by adding multiple portlets and arrange them using the drag and drop feature. You can **Collapse**, **Maximize**, or **Close** a portlet window. When a portlet is maximized, that single portlet is displayed in the entire work area.

The following figure shows the Bulk Device Management work area containing portlets.

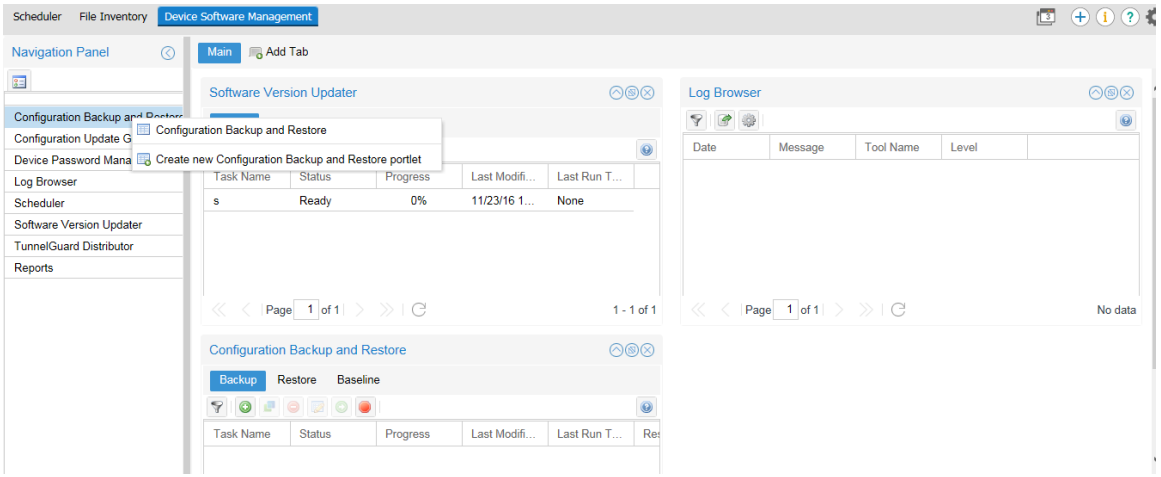


Figure 1: Portlets

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 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.

The Configuration Backup and Restore supports the following devices:

- VOSS
- APLS
- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/3600/4500/4800/4900/5500/5600/5900/8300/8600/8800

- Ethernet Switch 350/450/470
- VSP 4000/7000/7200/8000/9000
- Wireless LAN 8180

For more information about supported devices, see *Network Management Supported Devices, Device MIBs, and Legacy Devices Reference*, NN48100–701.

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 Business Secure Routers. This file is automatically saved in the backup archive on the 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 Bulk Device 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 Bulk Device Provisioning can use it.

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

Reporting

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 alerts

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 25.

CBR user interface

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

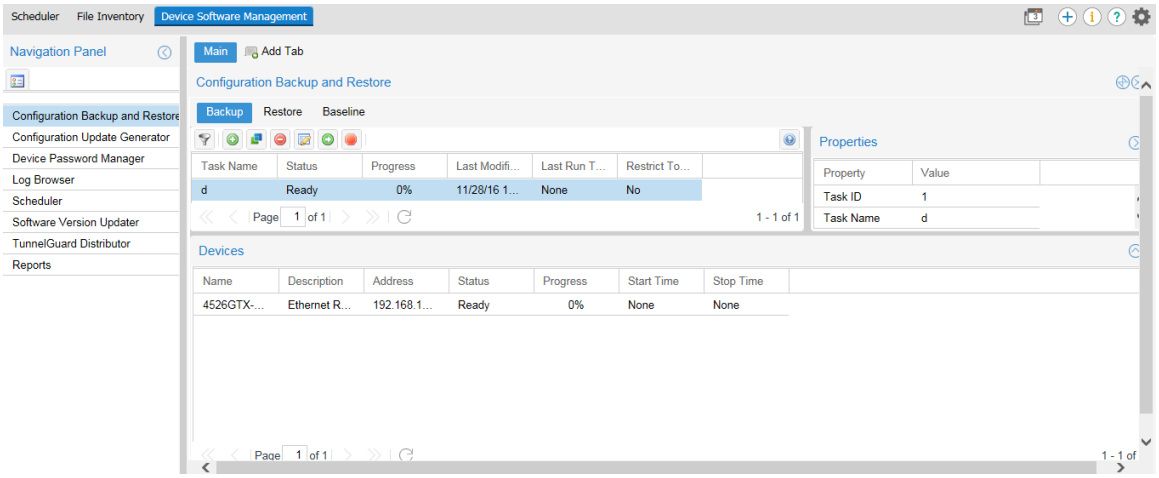


Figure 2: Configuration Backup window

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 identifier.

Table 2: Backup Device table

Field	Description
Name	The name of the device.
Description	The device.
Address	The IP address of the device.
Status	The status of the device.

Table continues…

Field	Description
Progress	The progress of the operation on the device.
Start Time	The start time of the operation on the device.
Stop Time	The stop time of the operation on the device.

The following figure shows the view of the Configuration Restore user interface.

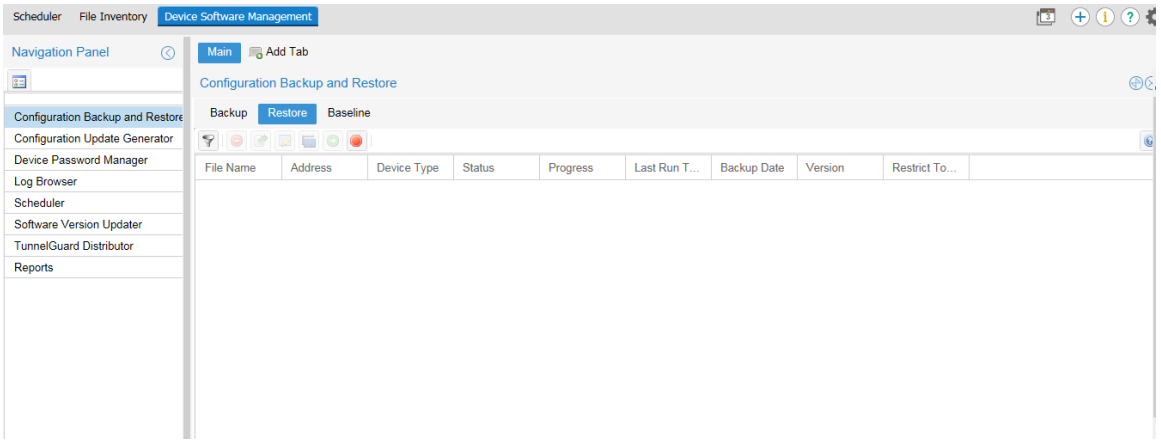


Figure 3: Configuration Restore window

Table 3: CBR restore task table

Field	Description
File Name	The name of the restore task.
Address	The address of the device.
Device Type	The type of device used in the backup task.
Status	The status of the task.
Progress	The progress of the task.
Last Run Time	The last run time of the task
Backup Date	The day, month, year, and time of the backup.
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.

The following figure shows the view of the Configuration Baseline user interface.

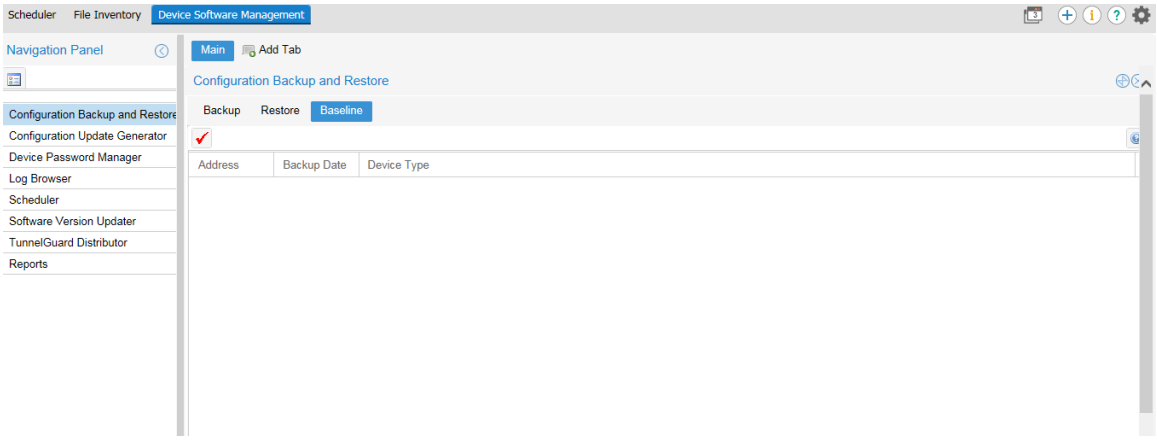


Figure 4: Configuration Baseline window

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, Bulk Provisioning automatically reboots them and for devices on which CUG does not applies changes, 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:

- VOSS
- APLS
- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/3600/4500/4800/4900/5500/5600/5900/8300/8600/8800

- Ethernet Switch 350/450/470
- VSP 4000/7000/7200/8000/9000
- Wireless LAN 8180

For more information about supported devices, see *Network Management Supported Devices, Device MIBs, and Legacy Devices Reference*, NN48100–701.

However, Bulk Provisioning does not support applying the configuration 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 figure shows the view of the Configuration Update Generator user interface.

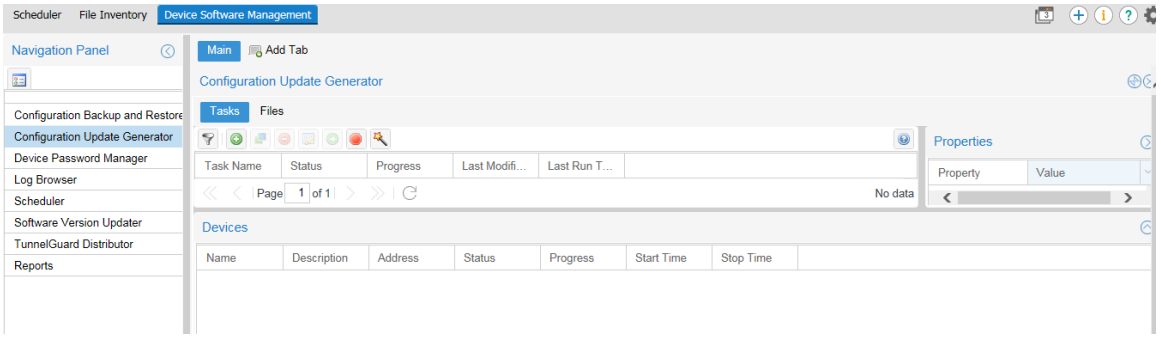


Figure 5: Configuration Update Generator window

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 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 identifier.
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 IP address of the device.
Status	The status of task for the device.
Progress	The progress of the task for the device.
Start Time	The start time of the task.
Stop Time	The stop time of the task.

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 41.

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:

- VOSS

- APLS
- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/3600/4500/4800/4900/5500/5600/5900/8300/8600/8800
- Ethernet Switch 350/450/470
- VSP 4000/7000/7200/8000/9000
- 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 identifier.

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.

Log Browser

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

Bulk Provisioning logs all interactions with devices to a common file with filename `BCM_audit.log` stored at `/opt/avaya/smgr/com/log` under config vm for each CONFIG instance. 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 Extreme Networks 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.

For more information, refer to Log Browser tasks on page 51.

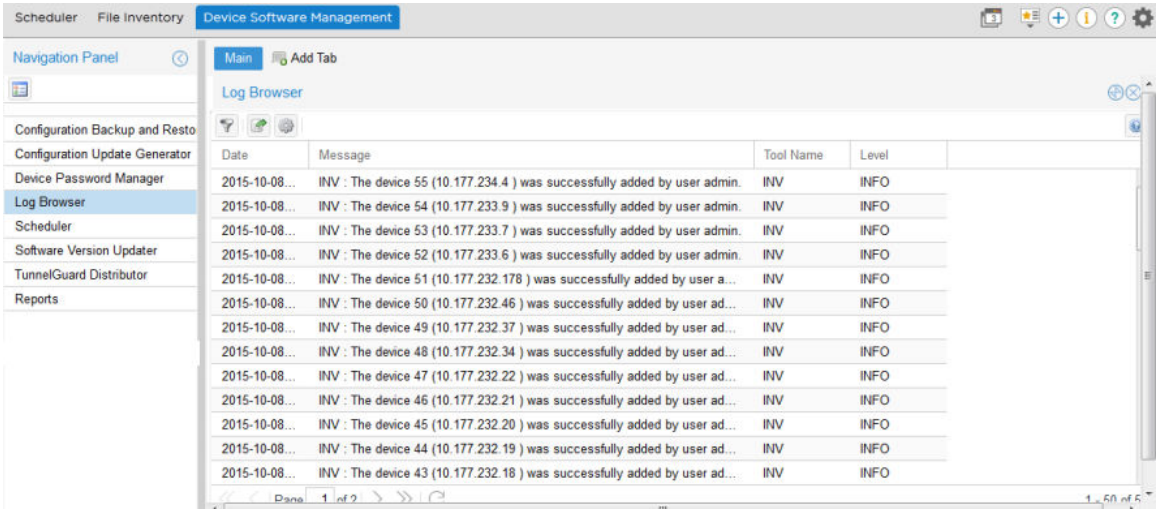


Figure 6: Log Browser

Table 10: 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 Bulk Provisioning tool
Level	The log level

Scheduler

You can use the Scheduler feature to schedule Bulk Provisioning tasks. You can select a tool from a drop down list of 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 11: 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 identifier.

Table 12: 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:

- VOSS
- APLS
- Tasman
- BSR 222/252
- Secure Router 2300
- ERS 1424/1600/2500/3500/3600/4500/4800/4900/5500/5600/5900/8300/8600/8800

- Ethernet Switch 350/450/470
- VSP 4000/7000/7200/8000/9000
- Wireless LAN 8180

For the VSP devices, Bulk Provisioning uses the FTP protocol to transfer the image from the 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 13: 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 identifier.
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 14: 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 15: 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 16: 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 17: 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 identifier.

Table 18: TGD device table

Attribute	Description
Name	The name of the device.
Description	The device.

Table continues…

Attribute	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.

Chapter 4: Managing bulk devices

Bulk device management

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

Configuration Backup and Restore tasks

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

Backup tasks

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

Configuring the e-mail alert settings

Before you can use any e-mail alert function in 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 Extreme Fabric Orchestrator*, NN48100–600.

Creating a configuration backup task

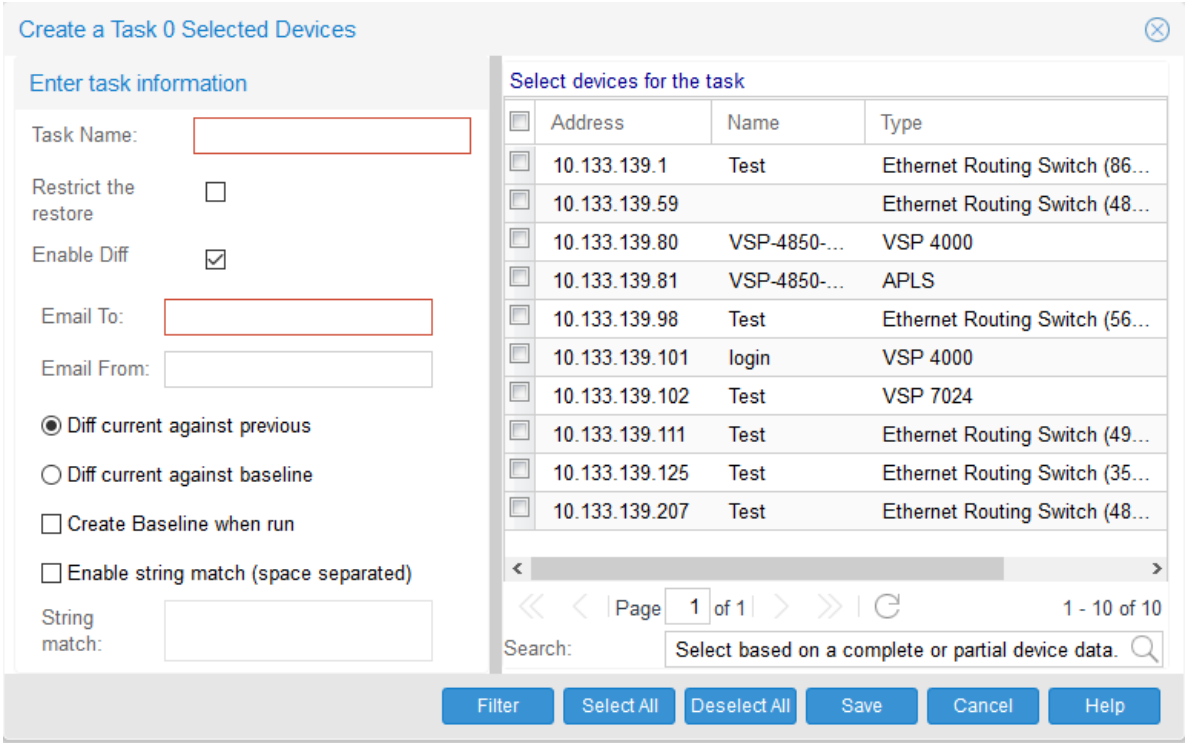
Perform the following procedure to create a configuration backup task:

Procedure

1. From the 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.

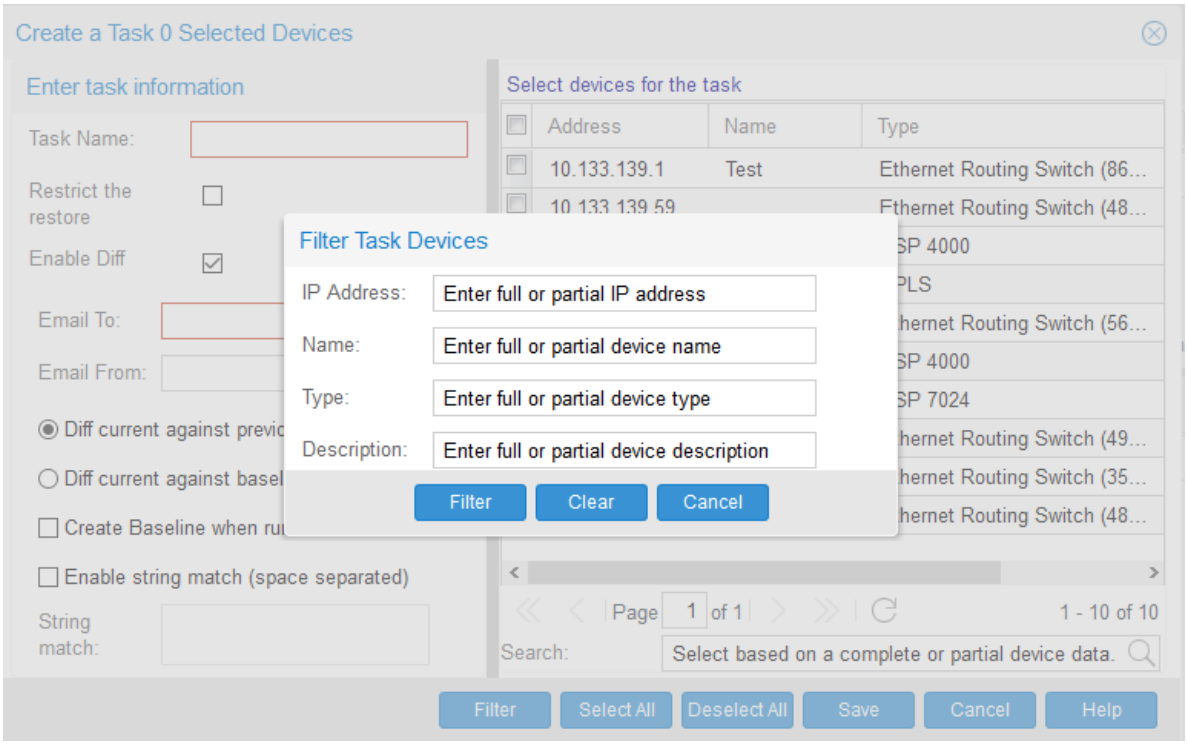
   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].

4. Specify whether you want to enable the **Restrict the restore** field.

   When enabled, Bulk Provisioning allows the restore operation only on devices that have the same software version at the time of the backup.

5. **(Optional)** Enter the required device data in the **Search** field to auto select devices from the list of devices.

6. **(Optional)** Click **Filter** to filter the list of devices based on IP Address, Name, Type, and Description.



7. Select the list of devices to be backed up.
8. 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.
9. 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.
10. 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.
11. Specify whether you want to create a baseline when the backup is run.
12. 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.

13. 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

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup** to open a new or an existing portlet.
2. Click the **Filter Tasks** icon.
3. In the **Task Name** field, type the `task name` or the first letter of the task name you want to filter.

   Note:

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

Result

The filtered information appears in the Backup tasks table.

Setting a backup baseline for a device

You can configure 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 Bulk Provisioning performs the backup baseline diff. Your backup date selection determines the date for which the 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 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

You can duplicate a configuration backup task in Backup tasks table. 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

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the tasks you want to duplicate from the Backup tasks table.
3. Click the **Duplicate Task** icon.
4. Click **Yes** to confirm the duplication.

Result

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 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, 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

You can execute a configuration backup tasks to activate the backup task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the task you want to activate from the Backup tasks table.
3. Click the **Activate Task** icon.
4. Click **Yes** to confirm.

Result

The backup task activates.

Deleting a configuration backup task

You can delete configuration backup tasks to discontinue configuration backups for the listed devices.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup**.
2. Select the tasks you want to delete from the Backup tasks table.
3. Click the **Delete** icon.
4. Click **OK**.
5. Click **Yes** to confirm.

Result

The backup tasks selected are deleted.

Restore tasks

The following section provides information about how to manage restore backup 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

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore** to open a new or an existing portlet.
2. Click the **Filter Tasks** icon.
3. In the **Task Name** field, type the `task name` or the first letter of the task name you want to filter.

   Note:

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

Result

The filtered information appears in the Restore tasks table.

Viewing backup details

View the backup details of file that was previously added into Bulk Provisioning.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore** to open a new or an existing portlet.
2. Click the **View Backup Details** icon.
3. From the View Backup Details window, select the file you want to view from the **file list**.
4. From the File Download window, select **Open** or **Save**.

Editing a configuration restore task

You can edit a configuration restore task to modify the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore** to open a new or an existing portlet.
2. Select the task to be edited.
3. Click the **Edit task** icon.
4. From the Edit a task window, you can enable or disable the **Restrict the same version** field.

Note:

When enabled, restore operations are allowed only on devices that have the same version of software as the backup.

5. Click **Save**.

Comparing configuration restore files

You can compare the configuration restore files and view differences between the restore files.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore** to open a new or an existing portlet.
2. Select the two files you want to compare. Use the Ctrl or Shift key to select multiple files.

   Note:

   The files that you choose must belong to the same device type.
3. Click **Compare**.
4. From the Compare window, click **Yes** to compare the selected files.
5. Click **Open** or **Save**.

Result

If you chose to open the file, the Smart Diff window shows the configuration differences between the files.

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

Activating a configuration restore task

You can execute a configuration restore task to activate the restore task.

Procedure

1. 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** icon.
4. Click **Yes** to confirm.

Result

The restore task activates.

Deleting a configuration restore task

You can delete configuration restore task to discontinue configuration restoration for the listed devices.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Restore**.
2. Select the backup archives you want to delete.
3. Click the **Delete** icon.
4. Click **OK**.
5. Click **Yes** to confirm.

Result

The backup archives selected are deleted.

Viewing progress of a backup or restore task

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Backup and Restore** > **Backup** or **Restore** to open a new or an existing portlet.
2. View the **Status** and **Progress** columns.

   Each row in the Backup or Restore Device Table reflects each selected device and displays the status of the backup or restore task for that device
3. Click **Refresh** to retrieve the current status of the listed tasks.

   The status results are ready, in progress, completed, or error. If an error status is shown, the possible reasons for error is displayed.

   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 SMGR-CS 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.

Configuration Update Generator tasks

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

Note:

You can use the Device Password Manager (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.

User-defined files for CUG

User-defined files for the Configuration Update Generator (CUG) 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 Bulk Provisioning server.

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

Two types of template files exist: script and configuration files. A script file contains the CLI commands you need to configure a device type. When you create a script, write it so that it begins just after a successful login to the device.

Note:

For devices, such as Contivity, SR 1000/3000/4000, ERS 2500/4500/5500/5600 devices, the CUG automatically enters the configuration terminal mode by issuing a **`configure terminal`** command. Do not insert the command **`configure terminal`** in the script .

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 Bulk Provisioning; you do not need to add these commands to your script.

Script examples

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.

```
show vlan basic
```

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 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 VPN Gateway routers. If you change the host name, CUG cannot reconnect to the device.

Interactive CLI commands

You can use interactive CLI commands in CUG scripts to enable the user to input the details as per the device prompt. The following directives are supported in CUG scripts:

- Password
- Delay
- Reconnect

Note:

- The interactive commands must be written in a single line in the script and must not be combined with other directives or interactive commands.
- User must specify the expected device prompt or part of the prompt accurately in the interactive command.
- The parameters must be separated by space and within the specified limits.

Password directive

The password directives such as @@@telnet, @@@ssh, and @@@current ensure that passwords that are configured under credentials are used and eliminate the need to enter the

passwords in plain text. The following syntax and example show how to use interactive CLI commands in CUG scripts:

```
[ ||| <prompt from device> ||| <user's response> ||| <next prompt from device> ||| <user's response> … ]
```

Example:

```
Username add rwa role-name RW password ||| Enter new password ||| rwa ||| Confirm new password ||| rwa
```

Note:

- Commands that change the current device credentials that are configured in EFO such as telnet and ssh must not be used. Using such commands results in connection failures.
- The supported password directives are:
  - @@@telnet - Uses configured telnet password
  - @@@ssh - Uses configured ssh password
  - @@@current – Uses the same password used for the ongoing CLI session with the device

Delay directive

The delay directive allows the user to specify the delay in rebooting the device at a specified interval. The following syntax and example show how to use delay directive in CUG scripts.

```
delay seconds <1-180>
```

Example:

```
|||delay 60
```

This directive provides a delay of 60 seconds.

Reconnect directive

The reconnect directive allows the user to attempt to reconnect to a disconnected device at a specified interval. The following syntax and example show how to use reconnect directive in CUG scripts.

```
reconnect [seconds<1-20> retry count<1-5>]
```

Example:

```
|||reconnect 15 4
```

With this directive, the system tries to reconnect once and then attempts to reconnect 4 times with an interval of 15 seconds.

Uploading a user-defined configuration file

You can upload a user-defined configuration file. Configuration files are available in the template and data file lists on the Create Task and Edit Task windows.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.

2. Click **Files** > **Add File**.
3. From the Add file window, click **Browse** and select the configuration file you want to upload.
4. Click **Upload**.
5. Click **OK** to confirm.
6. Close the Add file window.

Result

The user-defined configuration file is uploaded.

Deleting a user-defined configuration file

You can delete a user-defined configuration file. The configuration files deleted are removed from the template and data file lists in the Create Task and Edit Task windows.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Files**, and select the files to be deleted.
3. Click the **Delete File** icon.
4. Click **Yes** to confirm.

Result

The user-defined configuration file is removed.

Editing a user-defined configuration file

You can view or edit any user-defined configuration file that was previously imported.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Files**, and select a file to edit from the Template Files section.
3. Click the **Edit File** icon.
4. From the Edit File window, edit the file, then click **Save**.
5. Close the Edit File window.

Result

The user-defined configuration file is edited and saved.

Exporting a user-defined configuration file

You can export a user-defined configuration file that was previously imported.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Files**, and select a file to export from the Template Files section.
3. Click the **Export File** icon.
4. From the View Files window, click the file name of the file you want to export.
5. From the File Download window, click **Open** or **Save**.

Result

The user-defined configuration file is exported, and then opened or saved on your local system.

Adding a CUG task

You can add a CUG task to group devices on which you want to run user-defined configuration commands.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator**.
2. Click **Tasks**.
3. Click the **Add Task** icon.
4. From the Add a task window, complete the fields as needed.

   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].
5. From the Add a task window, complete the fields as needed.
6. **(Optional)** Click **Filter** to filter the list of devices based on IP Address, Name, Type, and Description.
7. **(Optional)** Enter the required device data in the **Search** field to auto select devices from the list of devices.
8. Click **Save**.

Result

A CUG task is added and saved.

Filtering the CUG tasks

You can filter the CUG tasks view to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator**.
2. Click **Tasks**.

3. Click the **Filter Tasks** icon.
4. From the Add a filter window, in the **Task Name** field enter the first letter or full name of the task you want to filter.

   Tip:

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

Result

The filtered information appears in the CUG tasks table.

Duplicating a CUG task

You can duplicate a CUG task in CUG tasks table. 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

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator**.
2. Click **Tasks**, and select the tasks you want to duplicate.
3. Click the **Duplicate Task** icon.
4. Click **Yes** to confirm the duplication.

Result

The duplicate task appears in the CUG tasks table.

Editing a CUG task

You can edit a configuration restore task to modify the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Tasks**, and select the task to be edited.
3. Click the **Edit Task** icon.
4. From the Edit Task window, edit the information as needed.
5. Click **Save**.

Result

The CUG task is edited and saved.

Deleting a CUG task

You can delete a CUG task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Tasks**, and select the files to be deleted.
3. Click the **Delete Task** icon.
4. Click **Yes** to confirm.

Result

The CUG task is removed.

Activating a configuration task

You can execute a configuration to activate the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or existing portlet.
2. Click **Tasks**, and select the tasks you want to activate.
3. Click the **Activate Task** icon.
4. Click **OK** to confirm.

Result

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

Note:

Task properties cannot be edited for an active task.

Viewing progress of a configuration task

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Configuration Update Generator** to open a new or an existing portlet.
2. Click **Tasks**.
3. View the **Status** and **Progress** columns.

   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 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 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.

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 19: 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 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 42.

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.

   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].
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 42 or Editing a template file on page 44.

Variable definitions

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

Table 20: 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.

Note:

Role Based Access Control security is enforced. You must be logged in with a user account that has permission to create a template.

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 45.

Variable definitions

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

Table 21: 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 >'`
	`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.

Note:

Role Based Access Control security is enforced. You must be logged in with a user account that has permission to edit a template.

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 45.

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

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. 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.

Table continues…

Attribute	Description

	`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 46.

Variable definitions

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

Table 23: 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 24: 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 25: 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 tasks

The following section provides information about how to manage Device Password Manager (DPM) tasks. You must be logged on with System Administrator rights to use DPM.

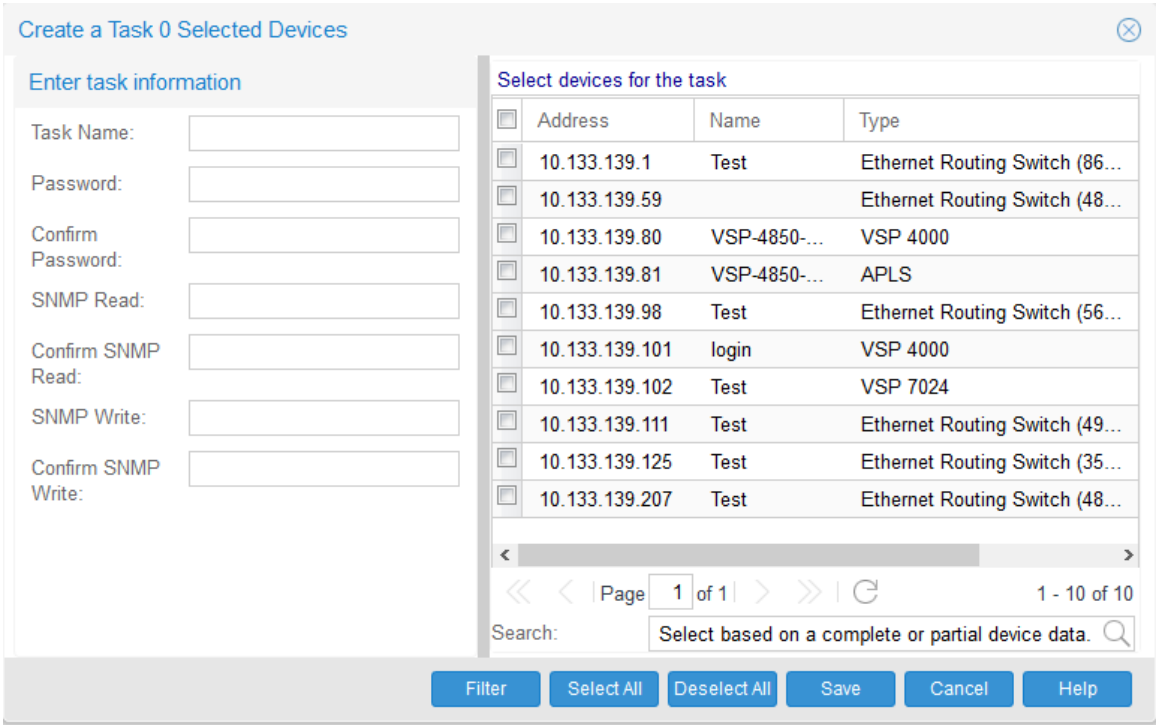
Adding a DPM task

You can add a Device Password Manager (DPM) task to group devices that have the same credentials.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or existing portlet.
2. Click the **Add Task** icon.

The Create a Task window displays.



3. From the Create a Task window, enter a `Task Name` and `Password`. Complete the other fields as needed.

   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].

4. **(Optional)** Click **Filter** to filter the list of devices based on IP Address, Name, Type, and Description.
5. **(Optional)** Enter the required device data in the **Search** field to auto select devices from the list of devices.
6. Select the list of devices to add to the task.
7. Click **Save**.

Result

A DPM task is added and saved.

Filtering the DPM tasks

You can filter the DPM tasks view to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or existing portlet.
2. Click the **Filter Tasks** icon.

3. From the Add a filter window, in the **Task Name** field enter the first letter or full name of the task you want to filter.

   Tip:

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

4. Click **Find**.

Result

The filtered information appears in the DPM tasks table.

Duplicating a DPM task

You can duplicate a DPM task in DPM tasks table. 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

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or existing portlet.
2. Select the tasks you want to duplicate.
3. Click the **Duplicate Task** icon.
4. Click **Yes** to confirm the duplication.

Result

The duplicate task appears in the DPM tasks table.

Editing a DPM task

You can edit a DPM task to modify the device list.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or an existing portlet.
2. Select the task you want to edit.
3. Click the **Edit Task** icon.
4. Edit the task information as needed.
5. Click **Save**.

Result

The DPM task is edited and saved.

Activating a DPM task

You can execute a DPM task to activate the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or existing portlet.
2. Select the tasks you want to activate.
3. Click the **Activate Task(s)** icon.
4. Click **OK** to confirm.

Result

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

Note:

Task properties cannot be edited for an active task.

Deleting a DPM task

You can delete a DPM task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or an existing portlet.
2. Select the task you want to delete.
3. Click the **Delete Task(s)** icon.
4. Click **Yes** to confirm.

Result

The DPM task is removed.

Viewing progress of a DPM task

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Device Password Manager** to open a new or an existing portlet.
2. View the **Status** and **Progress** columns.

   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 status results are establishing connection to device, changes successfully applied, and error. Possible reasons for errors are also displayed. You can view the table only in maximized view.

Log Browser tasks

You can use the Log Browser to log all your interactions with devices to a common file. You can browse a maximum of two files to access recent logs.

The following section provides information about Log Browser tasks.

Filtering logs

You can filter the logs view to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a new or existing portlet.
2. Click the **Filter Log** icon.
3. From the Filter log window, complete the fields as needed.

   Tip:

   Click **Clear** if you need to remove the filters.
4. Click **Save**.

Result

The filtered information appears in the Log Browser table.

Configuring log settings

Perform the following procedure to configure the log settings.

Procedure

1. From the 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**.

Configuring the Log Browser view

You can configure the Log Browser view to add or remove columns from view.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a new or existing portlet.
2. From a column header, click the down arrow and navigate to **Columns**.

3. Select the columns to show or hide.
4. Click **Save**.

Result

The column names checked appear in the Log Browser table.

Exporting Log Browser information

Bulk Provisioning stores the information that appears in the Log Browser portlet in a file called BCM_audit.log. When this file reaches 10MB, 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

1. Select **Backup & Restore** > **Device Software Management** > **Log Browser** to open a new or an existing portlet.
2. Click the **Export Logs** icon.
3. From the View log files window, select the file you want to export.
4. Select **Open** or **Save**.
5. Click **OK**.

Result

The log file you selected for export is opened or saved on your local system.

Scheduler tasks

You can create schedules using the Scheduler.

Note:

Scheduler uses the server time for Scheduler tasks. Client time is not used.

The following section provides information about Scheduler tasks.

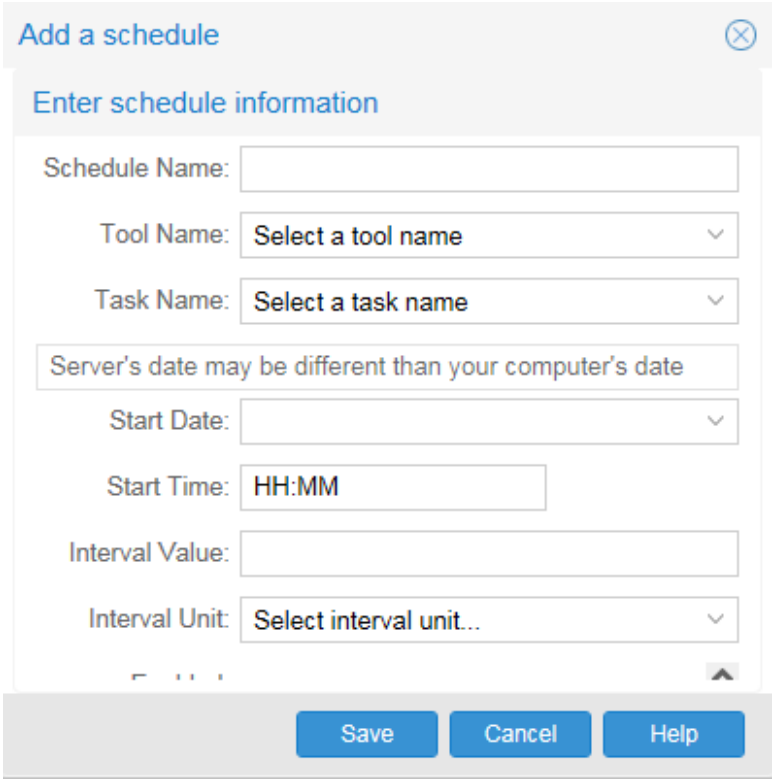
Adding a schedule

You can add a schedule to run tasks at regular or scheduled intervals.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Scheduler** to open a new or existing portlet.
2. Click the **Add Schedule** icon.

   The Add a schedule window displays.



3. From the Add a schedule window, enter the schedule information as needed.
4. Click **Save**.

Result

A schedule is added and saved.

Filtering Scheduler tasks

You can filter the Scheduler tasks to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Scheduler** to open a new or existing portlet.
2. Click the **Filter Tasks** icon.
3. From the Add a filter window, enter the task name or first letter of the task nameto be filtered.

   Tip:

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

Result

The filtered information appears in the Scheduler table.

Editing a schedule

You can edit a schedule to modify the Scheduler.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Scheduler** to open a new or an existing portlet.
2. Select the schedule task you want to edit.
3. Click the **Edit Schedule** icon.
4. From the Edit Schedule window, edit the information as needed.
5. Click **Save**.

Result

The schedule is edited and saved.

Deleting a schedule

You can delete a schedule task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Scheduler** to open a new or an existing portlet.
2. Click the **Refresh** icon to update the scheduler list.
3. Select the schedule task you want to delete.
4. Click the **Delete Schedule(s)** icon.
5. Click **Yes** to confirm.

Result

The schedule task is removed.

Software Version Updater tasks

With the Software Version Updater (SVU) tool, you can perform software upgrade tasks for multiple devices.

Important:

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

The following sections describe SVU tasks.

Adding an image package to the file 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

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Packages** > **Add Package**.
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

You can use the following procedure to remove an image package from the file server.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Packages**, and select the image package you want to delete.
3. Click **Delete Package(s)**.
4. Click **Yes** to confirm.

Result

The image package you selected is deleted from the file server.

Editing files from an image package

You can edit an image package to add or delete files.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Packages**, and select the package you want to edit.
3. Click **Edit Package**.
4. From the Edit Package window, select the files you want to delete from the **Files in package** area.
5. Click **Delete selected files**, then click **Yes** to confirm.

Result

The selected files are deleted from the image package.

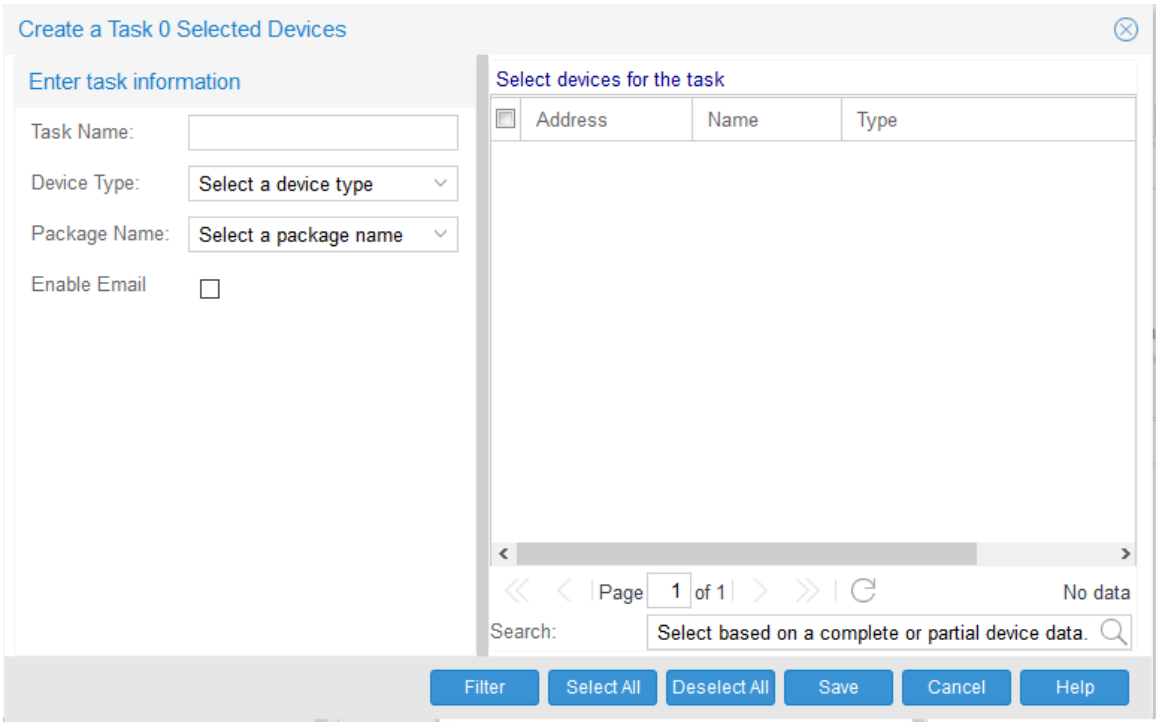
Adding a SVU task

You can add a SVU task to group devices for updates.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Tasks**.
3. Click the **Add Task** icon.

   The Create a Task window displays.



4. From the Add a task window, complete the fields as needed.

   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].

   Note:

   For Extreme Networks Ethernet Routing Switch 8600 and 8800, you can select an option to save the upgraded image on a PCMCIA card.

   For ERS devices, you can select the options to reboot after image download and diag download.

For VOSS, and APLS devices, you can select an option to reboot after image download.

5. **(Optional)** Click **Filter** to filter the list of devices based on IP Address, Name, Type, and Description.
6. **(Optional)** Enter the required device data in the **Search** field to auto select devices from the list of devices.
7. Select the list of devices to update from the **Select devices for the task** area.
8. Click **Save**.

Result

A SVU task is added and saved.

Filtering the SVU tasks

You can filter the SVU tasks view to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Tasks**.
3. Click the **Filter Tasks** icon.
4. From the Add a filter window, in the **Task Name** field enter the first letter or full name of the task you want to filter.

   Tip:

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

Result

The filtered information appears in the SVU tasks table.

Duplicating a SVU task

You can duplicate a SVU task in SVU tasks table. 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

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater**.
2. Click **Tasks**, and select the tasks you want to duplicate.
3. Click the **Duplicate Task** icon.
4. Click **Yes** to confirm the duplication.

Result

The duplicate task appears in the SVU tasks table.

Activating a SVU task

You can execute a SVU task to activate the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open a new or existing portlet.
2. Click **Tasks**.
3. Select the tasks you want to activate.
4. Click the **Activate Task(s)** icon.
5. Click **OK** to confirm.

Result

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

Note:

Task properties cannot be edited for an active task.

Editing a SVU task

You can edit a SVU task to modify the device list for the task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open a new or an existing portlet.
2. Click **Tasks**, and select the task to be edited.
3. Click the **Edit Task** icon.
4. From the Edit Task window, edit the information as needed.
5. Click **Save**.

Result

The SVU task is edited and saved.

Deleting a SVU task

You can delete a SVU task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Version Updater** to open a new or an existing portlet.

2. Click **Tasks**, and select the files to be deleted.
3. Click the **Delete Task** icon.
4. Click **Yes** to confirm.

Result

The SVU task is removed.

Viewing progress of a SVU task

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **Software Device Updater** to open a new or an existing portlet.
2. Click **Tasks**.
3. View the **Status** and **Progress** columns.

   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 status results are establishing connection to device, deploying file, completed successfully, and error. Possible reasons for errors are also displayed.

TunnelGuard Distributor tasks

With the TunnelGuard Distributor (TGD) tool, you can copy a TunnelGuard rule from one device to multiple devices and activate the rule on an associated domain group.

Note:

TunnelGuard rules can only be applied to Secure Network Access Switch (SNAS) devices.

The following sections provide information for TGD policies and tasks.

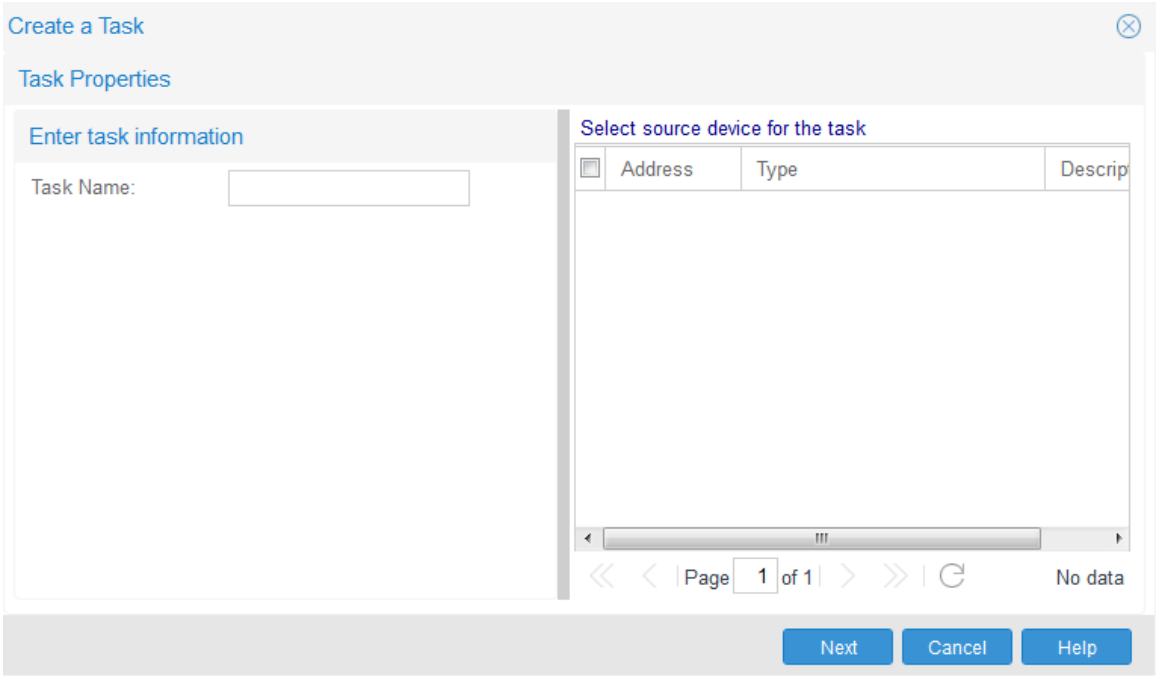
Adding existing TunnelGuard policies

You can create a TGD task to copy an existing policy from one device to many devices.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor**.
2. Click the **Add Task** icon.

   The Create a Task window displays.



3. Enter a task name and select the source device from which the policy requires to be transferred.

   The task name may include numbers, letters with spaces, underscores (_) hyphens (-), colons (:), left and right parenthesis ( ), and square brackets [ ].
4. Select the source device from which the policy requires to be transferred.
5. Click **Next**.
6. Enter the domain information and click **Next**.
7. Select the group to be transferred. Complete the other fields as appropriate.
8. Click **Next**.
9. Select the devices to which the policy requires to be transferred.
10. **Finish**.

Filtering the TGD tasks

You can filter the TGD tasks view to reduce the amount of information that appears.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a new or existing portlet.
2. Click the **Filter Tasks** icon.
3. From the Add a filter window, in the **Task Name** field enter the first letter or full name of the task you want to filter.

Tip:

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

4. Click **Find**.

Result

The filtered information appears in the TGD tasks table.

Duplicating a TGD task

You can duplicate a TGD task in TGD tasks table. 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

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a new or existing portlet.
2. Select the tasks you want to duplicate.
3. Click the **Duplicate Task** icon.
4. Click **Yes** to confirm the duplication.

Result

The duplicate task appears in the TGD tasks table.

Editing a TGD task

You can edit a TGD task to change the domain, the group, or the tunnelguard rule from the source device and the destination device.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a new or an existing portlet.
2. Select the task to be edited.
3. Click the **Edit Task** icon.
4. Edit the task information as needed, then click **Next**.
5. Edit the domain information as needed, then click **Next**.
6. Edit the group information as needed, then click **Next**.
7. Select the devices to which the policy is going to apply.
8. Click **Finish**.

Result

The TGD task is edited and saved.

Deleting a TGD task

You can delete a TGD task.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a new or an existing portlet.
2. Select the task you want to delete.
3. Click the **Delete Task** icon.
4. Click **Yes** to confirm.

Result

The TGD task is removed.

Activating a TGD task

You can activate a TGD task to copy a TunnelGuard rule from one device to multiple devices.

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor**.
2. Select the task you want to activate.
3. Click the **Activate Task** icon.
4. Click **Yes** to confirm activation.

Viewing progress of a TGD task

Procedure

1. Select **Backup & Restore** > **Device Software Management** > **TunnelGuard Distributor** to open a new or an existing portlet.
2. View the **Status** and **Progress** columns.

   Status and progress are automatically updated while the task is running. Each row in the table reflects the selected source and destination devices, and displays the status of the transfer.

   You can click **Refresh** to retrieve the current status of the listed tasks. If an error status occurs, the possible reasons for the error are shown.

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 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**.

Appendix A: Device types and limitations

Device types and limitations

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

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

- Contivity VPN routers cannot have # or > in the prompt.
- Extreme Networks 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 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 Bulk Provisioning supported devices, and shows how approved vendor device names appear on the Bulk Provisioning interface.

Device name	Label on Bulk Provisioning interface
APLS	APLS
Secure Router 1000/3100	Secure Router 1000/3100
Secure Router 4134	Secure Router 4000
VPN Router 600-5000	VPN Router
Secure Network Access Switch 4050/4070	Secure Network Access Switch 4050/4070
Ethernet Routing Switch (5600 Series)	Ethernet Routing Switch (5600 Series)
Ethernet Switch 460/470	Ethernet Switch 460/470
Business Secure Router 222	Business Secure Router 222
Business Secure Router 252	Business Secure Router 252
Ethernet Routing Switch (8800 Series)	Ethernet Routing Switch (8600 Series)
Ethernet Routing Switch (8600 Series)	Ethernet Routing Switch (8600 Series)

Table continues…

Device name	Label on Bulk Provisioning interface
Ethernet Routing Switch (8300 Series)	Ethernet Routing Switch (8300 Series)
Ethernet Routing Switch (5900 Series)	Ethernet Routing Switch (5900 Series)
Ethernet Routing Switch (5500 Series)	Ethernet Routing Switch (5500 Series)
Ethernet Routing Switch (5000 Series)	Ethernet Routing Switch (5000 Series)
Ethernet Routing Switch (4900 Series)	Ethernet Routing Switch (4900 Series)
Ethernet Routing Switch (4800 Series)	Ethernet Routing Switch (4800 Series)
Ethernet Routing Switch (4500 Series)	Ethernet Routing Switch (4500 Series)
Ethernet Routing Switch (3600 Series)	Ethernet Routing Switch (3600 Series)
Ethernet Routing Switch (3500 Series)	Ethernet Routing Switch (3500 Series)
Ethernet Routing Switch (2500 Series)	Ethernet Routing Switch (2500 Series)
VPN Gateway 3050/3070	VPN Gateway 3050/3070
VSP (7000 and 9000 Series)	VSP (9000 Series)
VSP (8000 Series)	VSP (8000 Series)
VSP (4000 Series)	VSP (4000 Series)
Wireless LAN 8180	Wireless LAN 8180

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
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 supported devices, see *Network Management Supported Devices, Device MIBs, and Legacy Devices Reference*, NN48100–701.

Sample configuration scripts

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

VPN router configuration scripts

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, Bulk Provisioning executes the following commands by default:

```
enable

configure terminal
```

After 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
```

CUG script examples

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 scripts

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, Bulk Provisioning executes the following commands by default:

```
apply
```

The preceding 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
```

CUG script examples

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 scripts

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

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

```
enable
configure terminal
```

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
```

CUG script examples

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
```

Ethernet Routing Switch 2500, 4500, and 5500 configuration scripts

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

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

```
enable

configure terminal
```

Note:

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 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
```

CUG example scripts

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
```

Ethernet Routing Switch 8300 and 8600 configuration scripts

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

If you use CUG to execute commands on Ethernet Routing Switches, 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, 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
```

CUG script examples

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
```