BROCADE

USER GUIDE

Brocade Visibility Manager User Guide

Supporting ICX 7750 with FastIron 08.0.30f
Supporting Brocade SDN Controller 2.3.0
Brocade Visibility Manager 1.2.0 is a specific release to support OpenFlow-enabled ICX using SDN Controller. This release does not support MLXe and StableNet®.

53-1004090-06
30 March 2016

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables Identifies document titles
`Courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.

Convention	Description
x | y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About this guide

Audience

If you are using a Brocade device, you should be familiar with Layer 2 and Layer 3 switching and routing.

Related publications

The following documents supplement the information in this guide:

- Brocade Visibility Manager Release Notes
- Brocade SDN Controller Software Installation Guide

Part A - Brocade Visibility Manager App for ICX

Getting Started with Brocade Visibility Manager App for ICX

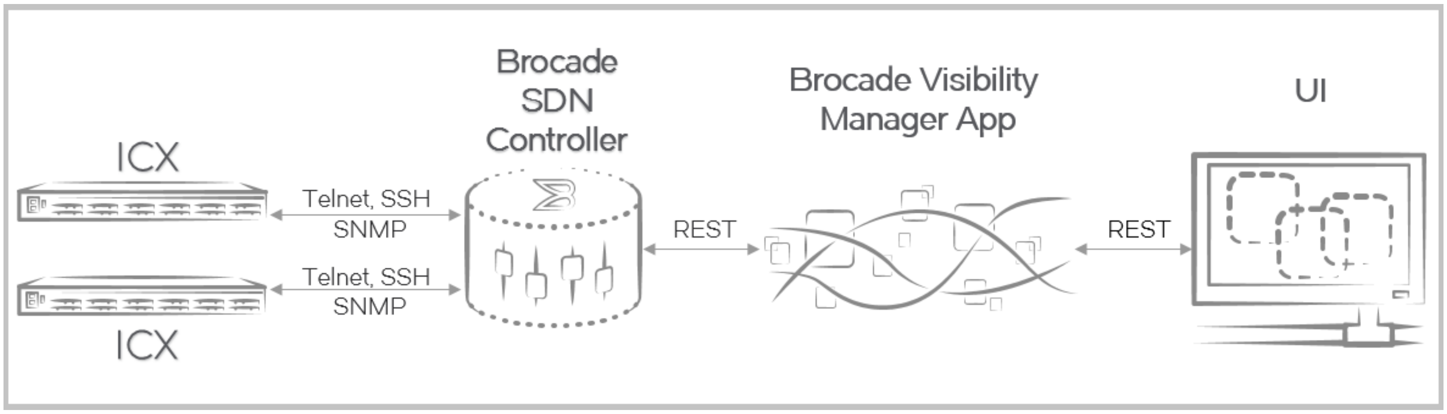
Introduction

Brocade Visibility Manager App for ICX is a Web application that provides several options for configuring Brocade network packet brokers.

The Brocade Visibility Manager App for ICX can be used to:

- Enable and disable ports
- Configure ports as Ingress or Egress
- Create Port Groups for Load Balance
- Create filter rule definitions based on L2-L4 criteria
- View device configuration

FIGURE 1 Brocade Visibility Manager App Flow



Brocade Visibility Manager App Installation

This section provides information about installing Brocade Visibility Manager App.

System Requirements

Brocade Visibility Manager is hosted on the same server as Brocade SDN Controller. For information about the System Requirements, see the section 'Prerequisites for installing the controller' in *Brocade SDN Controller Software Installation Guide*.

Downloading the Distribution

Perform the following steps to download the distribution for Brocade Visibility Manager from the My Brocade website:

1. Go to the MyBrocade website at https://my.brocade.com and log in with your username and password.
2. If you are visiting MyBrocade for the first time, click **Register Now** instead and follow the prompts to register.
3. On the top navigation bar, click **downloads**.
4. In the Product Downloads section, click **Download by** and click **Network Visibility and Analytics** in the drop-down list.
   A list of distributions is displayed in the **Product Name** section.
5. Click **Brocade Visibility Manager** -> **Brocade Visibility Manager 1.x** -> **Brocade Visibility Manager 1.2.0**.
   A list of all the relevant files for this release is displayed.
6. Click a file to download.
7. Accept the terms of the Export Compliance statement and the End User Terms and Conditions statement to initiate the download.
   If you have any concerns about the Export Compliance statement or the End User Terms and Conditions statement, consult Brocade Technical Support.
8. Save the file to a local directory on your system.
9. Click **back to downloads** to download the remaining files.

Pre-installation Steps

Before installing Brocade Visibility Manager App, perform the following pre-installation steps:

1. **Install JRE 1.8.0 and JDK 1.7.0**

   NOTE
   Remove all previous versions of Java before performing the steps below.

   a) Download the file `jre-8u51-linux-x64.rpm` from http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html.

   b) Run the following command to install JRE 8u51:

   ```
   rpm -ivh jre-8u51-linux-x64.rpm
   ```

   c) Download the file `jdk-7u80-linux-x64.rpm` from http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html.

   d) Run the following command to install JDK 7u80:

   ```
   rpm -ivh jdk-7u80-linux-x64.rpm
   ```

   e) Set `JAVA_HOME` to `jdk1.7.0_80`, and run the `java -version` command to ensure that the Java version is `jdk1.7.0_80`.

2. **Install MySQL**

   NOTE
   Remove all previous versions of MySQL before performing the steps below.

   a) Run the following commands to download the yum repo rpm package:

   ```
   wget http://repo.mysql.com/mysql-community-release-el6-5.noarch.rpm
   ```

   b) Install the downloaded rpm package:

   ```
   rpm -ivh mysql-community-release-el6-5.noarch.rpm
   ```

   c) Run the following command to install MySQL server:

   ```
   yum install mysql-server
   ```

   d) After the installation is complete, start the MySQL server:

   ```
   /etc/init.d/mysqld start
   ```

   e) Run the following command to perform a secure installation of MySQL:

   ```
   /usr/bin/mysql_secure_installation
   ```

   NOTE
   Make a note of the root password that you set during the installation of MySQL.

Example

```
# /usr/bin/mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.
```

```
Disallow root login remotely? [Y/n] y
... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
ERROR 1008 (HY000) at line 1: Can't drop database 'test'; database doesn't exist
... Failed!  Not critical, keep moving...
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

Installing and Configuring Brocade SDN Controller

Brocade SDN Controller is a prerequisite for Brocade Visibility Manager. Perform the following steps to install and configure Brocade SDN Controller:

1. Install Brocade SDN Controller version 2.3.0.
   For more information, see *Brocade SDN Controller Software Installation Guide*.

2. After installing Brocade SDN Controller, login to ICX and perform the following steps:

   a) Run the following commands in Global Configuration command mode. This is to configure the ICX to connect to the Brocade SDN Controller:

   ```
   openflow enable ofv130
   openflow controller passive no-ssl port 6633
   openflow controller ip-address <SDN_Controller_IP_address> no-ssl port 6633
   ```

   Where: 6633 is the default controller port.

   Example

   ```
   ICX-7750-1(config)#
   openflow enable ofv130
   openflow controller passive no-ssl port 6633
   openflow controller ip-address 10.18.236.252 no-ssl port 6633
   ```

   b) Run the following command to verify ICX connectivity to Brocade SDN Controller:

   ```
   sh openflow controller
   ```

   Example

   ```
   #sh openflow controller
   Openflow controller information

   --------------------------------------------------------------------------------
     Controller    Mode      TCP/SSL    IP-address         Port    Status
   --------------------------------------------------------------------------------
     1  (Equal)    passive   TCP        0.0.0.0            6633    TCP_LISTENING
     2  (Equal)    active    TCP        10.18.236.252      6633    OPENFLOW_ESTABLISHED
   ```

   c) Run the following command to clear all flows from the flow table:

   ```
   clear openflow all
   ```

Installing Brocade Visibility Manager App

Perform the following steps to install Brocade Visibility Manager App:

NOTE

- It is recommended that you do not download or install the installation files in the `/root` folder.
- If you are reinstalling the Brocade Visibility Manager App, make sure to backup the Brocade Visibility Manager database before reinstalling the App. For more information, see the section Brocade Visibility Manager App Database Backup and Restore on page 23.

1. Go to the location where the Brocade Visibility Manager App installation files were downloaded.
2. Run the following command:

   ```
   rpm -ivh bvm-1.2.0-0.el6.x86_64.rpm
   ```

   Example

   ```
   Preparing...                          ################################# [100%]
   Updating / installing...
      1:bvm-1.2.0-0.el6                  ################################# [100%]
   Created symlink from /etc/systemd/system/bvm.service to /usr/lib/systemd/system/bvm.service.
   Created symlink from /etc/systemd/system/multi-user.target.wants/bvm.service to /usr/lib/systemd/
   system/bvm.service.sh
   ```

3. Go to the `/opt/brocade/bin` directory.

4. Open the file `configuration.properties` and verify the following:
   - Make sure that the value of `java_home` is set to the correct path.
   - Make sure that MySQL configuration is configured correctly.

   Example

   ```
   mysql_root_username="root"
   mysql_username="bvm"
   mysql_password="Password1"
   mysql_db="bvm"
   mysql_ip="localhost"
   mysql_port="3308"
   backup_location="/tmp/backup"
   restore_location="/tmp/backup"
   java_home=/usr/java/jre1.8.0_51
   ```
5. Save file and exit.
6. At the same location, execute the following command:

   ```
   sh install_bvm.sh
   ```

   NOTE
   During the installation, you will be prompted for MySQL root password. This is the same password that you set while installing MySQL.

   Example

   ```
   # sh install_bvm.sh
   Enter MySQL root password: ****

   *******************************************************
   Creating the BVM database username and password...
   *******************************************************
   mysql: [Warning] Using a password on the command line interface can be insecure.
   bvm database creation complete.
   mysql: [Warning] Using a password on the command line interface can be insecure.
   mysql: [Warning] Using a password on the command line interface can be insecure.
   *******************************************************
   ```

Brocade Visibility Manager App installation is now complete.

Post-installation Steps

After Brocade Visibility Manager installation is complete, perform the following steps:

1. Login to ICX and run the following commands to add Telnet support:

   ```
   aaa authentication login default local
   enable telnet authentication
   ```
2. Run the following commands to change the administrator username and password, and to write the changes to the memory:

   ```
   username <admin> password <admin>
   wr mem
   ```

   NOTE
   The username and password should match the credentials provided for Brocade SDN Controller.

   These steps allow ICX to communicate with Brocade SDN Controller and Brocade Visibility Manager.
3. Next, login to the Brocade Visibility Manager machine and go to `/opt/brocade/bvm/current/config/bems-api` directory.

4. Open the file `application-production.properties` and change the following parameter:

   ```
   bsc.rest.base-url=http://<SDN_Controller_IP_address>:8181/restconf
   ```

   Example

   ```
   #app settings
   https.enabled=false

   #db
   spring.datasource.url=jdbc:mysql://localhost/bvm
   spring.datasource.username=bvm
   spring.datasource.password=Password1

   #logs
   spring.jpa.show-sql=false
   logging.level.com.brocade=DEBUG
   logging.level.org.flyway=DEBUG
   logging.file=/var/log/bvmapp.log

   #dependencies
   bsc.rest.base-url=http://10.37.130.178:8181/restconf
   bsc.resource-url.max.flows=2000
   #bsc.queue-id=0
   ```

Verifying Installation of Brocade Visibility Manager App

Run the following command to verify the installation of the Brocade Visibility Manager App:

```
rpm -qa | grep bvm
```

If the installation is successful, full version of the Brocade Visibility Manager App RPM is displayed.

Example

```
# rpm -qa | grep bvm
bvm-1.2.0-0.el6.x86_64
```

Starting Brocade Visibility Manager App Processes

After configuring Brocade Visibility Manager App, perform the following steps:

> **NOTE**
> Ensure that the Brocade SDN Controller is running before performing the following steps.

1. Run the following command to start Brocade Visibility Manager App processes:

   ```
   service bvm start
   ```

   Example

   ```
   # service bvm start
   Redirecting to /bin/systemctl start bvm.service
   ```

   > **NOTE**
   > The Brocade Visibility Manager App processes must be started whenever the system is rebooted.

2. Run the following command to verify if all processes are running:

   `service bvm status`

   Example

```
# service bvm status
Redirecting to /bin/systemctl status  bvm.service
● bvm.service - BVM
   Loaded: loaded (/usr/lib/systemd/system/bvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2016-02-18 04:47:38 EST; 55s ago
  Process: 5671 ExecStart=/usr/lib/systemd/scripts/bvm.sh start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/bvm.service
           ├─5689 /opt/tools/jdk1.8.0_73/bin/java -jar /opt/brocade/bvm/current/app/bems-api/libs/
bems-api-1.0.0.jar --spring.config.locat...
           └─5704 /opt/brocade/oss/node-v0.12.7-linux-x64/bin/node start-ux.js

Feb 18 04:47:38 bsc2.3 systemd[1]: Starting BVM...
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: *******************************************************
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: Starting the BVM 1.2.0-2 Application
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: *******************************************************
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: Starting BVM API Application
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: Starting BVM UI Application
Feb 18 04:47:38 bsc2.3 bvm.sh[5671]: *******************************************************
Feb 18 04:47:38 bsc2.3 systemd[1]: Started BVM.
```

   NOTE

   - For information about accessing the Brocade Visibility Manager App, see the section Accessing Brocade Visibility Manager App on page 25.
   - To stop Brocade Visibility Manager App processes, run the `service bvm stop` command.
   - To restart Brocade Visibility Manager App processes, run the `service bvm restart` command.

Brocade Visibility Manager App Configuration

This section provides information about configuring Brocade Visibility Manager App.

Changing Default Port for Brocade Visibility Manager App

NOTE
This step is optional.

The default port for accessing Brocade Visibility Manager App is 9286. If you want to change the port, perform the following steps:

1. Run the following command to stop Brocade Visibility Manager App processes:

   `service bvm stop`

2. Run the following command to change the port:

   `export GRK_UX_HTTP_PORT=`*`<port_number>`*

   Example

```
export GRK_UX_HTTP_PORT=9002
```

3. Go to the `/opt/brocade/bvm/current/config/bems-api` directory.

4. Open the file `application.properties` and change the value of `access.control.allow.origin` to the new port number.

   Example

   ```
   access.control.allow.origin=http://localhost:9002
   ```

5. Run the following command to start Brocade Visibility Manager App processes:

   ```
   service bvm start
   ```

Brocade Visibility Manager App Database Backup and Restore

This section provides information about backing up and restoring Brocade Visibility Manager App database.

This section contains the following subsections:

- Backing up Brocade Visibility Manager Database on page 23
- Restoring Brocade Visibility Manager Database on page 24

Backing up Brocade Visibility Manager Database

Perform the following steps to backup Brocade Visibility Manager App database.

1. Run the following command to stop all Brocade Visibility Manager App processes:

   ```
   service bvm stop
   ```

2. Go to the `/opt/brocade/bin` directory.
3. Run the following command to backup the Brocade Visibility Manager database:

   ```
   sh bvm_db_manager.sh backup
   ```

   NOTE
   You will be prompted for MySQL root password.

   Example

   ```
   sh bvm_db_manager.sh backup
   Enter MySQL root password: *********

   *******************************************************
   Performing BVM DB backup...
   *******************************************************
   Warning: Using a password on the command line interface can be insecure.
   bvm.sql.20160205 created in /tmp/backup.
   -rw-r--r-- 1 root root 18683 Feb  5 11:51 bvm.sql.20160205
   *******************************************************
   BVM DB backup compeleted.
   *******************************************************
   ```

   NOTE

   - The backup files are stored in the `/tmp/backup` directory. To change the location, open the file `configuration.properties` located at `/opt/brocade/bin` and change the value of the parameter `backup_location`.
   - Run the `sh bvm_db_manager.sh cleanup` command to cleanup the Brocade Visibility Manager database.

Restoring Brocade Visibility Manager Database

Perform the following steps to restore the Brocade Visibility Manager App database.

> **NOTE**
> Use restore as a disaster recovery option only. Restoring the database can cause issues if there is a mismatch between device data and Brocade Visibility Manager App database.

1. Run the following command to stop all Brocade Visibility Manager App processes:

   ```
   service bvm stop
   ```

2. Go to the `/opt/brocade/bin` directory.
3. Run the following command to restore the Brocade Visibility Manager database:

   ```
   sh bvm_db_manager.sh restore
   ```

   > **NOTE**
   > You will be prompted for MySQL root password.

   Example

   ```
   sh bvm_db_manager.sh restore
   Enter MySQL root password: *********

   Please enter the backup file name to be restored (bvm.sql.yyyymmdd):bvm.sql.20160205
   bvm.sql.20160205
   Warning: Using a password on the command line interface can be insecure.
   *******************************************************
   Creating and restoring the BVM database from the bvm.sql.20160205
   *******************************************************
   sh: /usr/brocade/bin/create_bvm_db.sh: No such file or directory
   Warning: Using a password on the command line interface can be insecure.
   ERROR 1049 (42000): Unknown database 'bvm'
   *******************************************************
   Restoring the BVM database from bvm.sql.20160205 completed.
   *******************************************************
   ```

   > **NOTE**
   > The backup files used for restoring the Brocade Visibility Manager database are stored in the `/tmp/backup` directory. To change the location, open the file `configuration.properties` located at `/opt/brocade/bin` and change the value of the parameter `restore_location`.

Uninstalling Brocade Visibility Manager App

Perform the following steps to uninstall the Brocade Visibility Manager App:

1. Run the following command to stop all Brocade Visibility Manager App processes:

   ```
   service bvm stop
   ```

2. Run the following commands to verify if all the processes have stopped:

   ```
   ps -ef | grep bvm
   ```

   ```
   ps -ef | grep start-ux
   ```

3. Next, run the following command to uninstall the Brocade Visibility Manager App:

   ```
   rpm -e bvm
   ```

   Example

   ```
   Enter MySQL root password: *********

   Existing bvm database will be deleted. Please backup if you need to retain data. Do you want to
   continue delete (y/n)?
   Warning: Using a password on the command line interface can be insecure.
   *******************************************************
   Starting the cleanup and deleting the BVM database...
   *******************************************************
   Warning: Using a password on the command line interface can be insecure.
   *******************************************************
   Cleanup and deletion of BVM database complete.
   *******************************************************
   BVM DB Cleanup is completed successfully,BVM RPM uninstallation success.
   rm '/etc/systemd/system/multi-user.target.wants/bvm.service'
   rm '/etc/systemd/system/bvm.service'
   ```

Accessing Brocade Visibility Manager App

NOTE

This version of Brocade Visibility Manager App supports the following Web browsers:

- Chrome 48.0.2564.82 m and above
- Firefox 43.0.4 and above

Perform the following steps to access the Brocade Visibility Manager App:

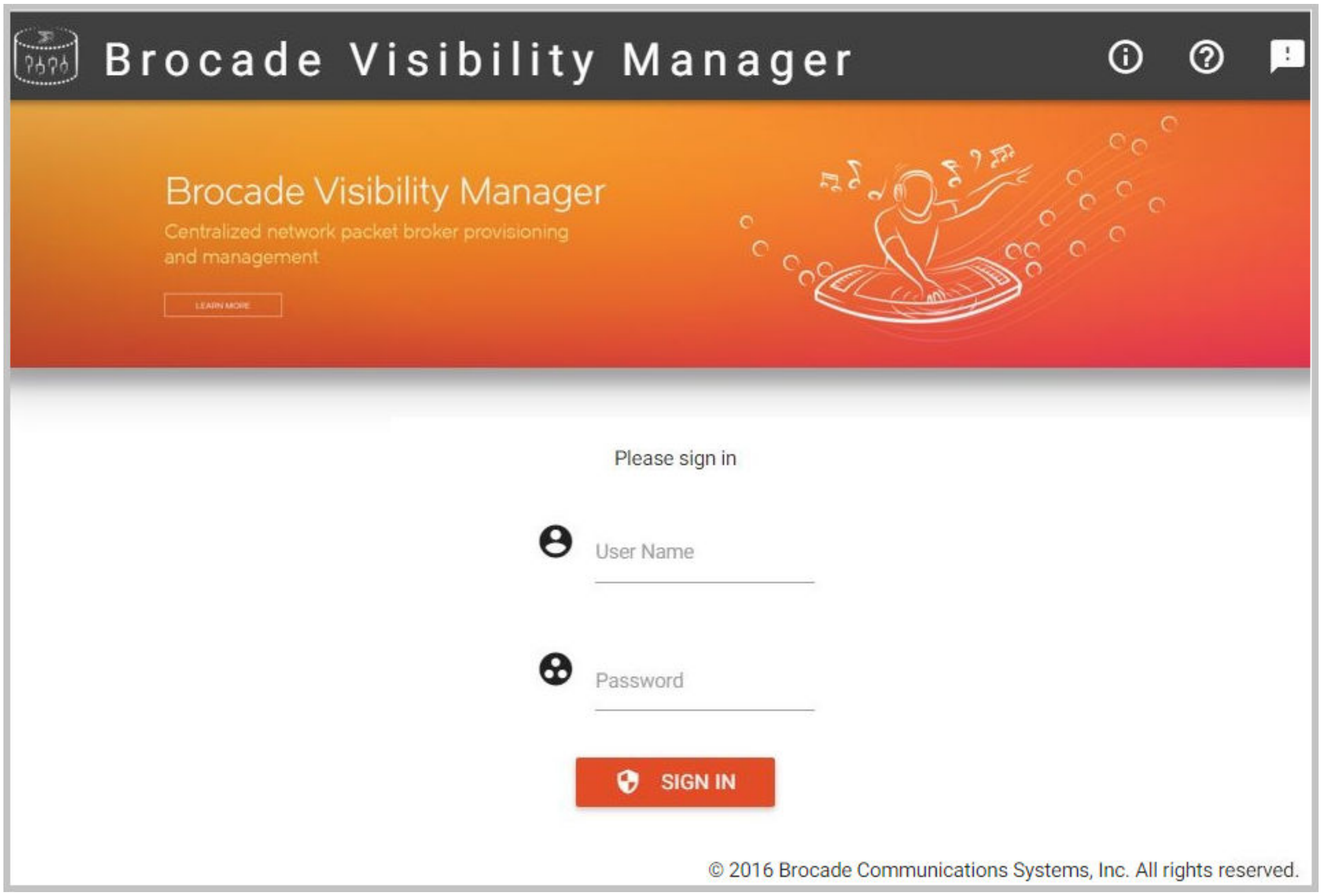
1. Open a Web browser and enter the Brocade SDN Controller IP address with 9286 as the port number.

   Example

   ```
   http://10.37.130.178:9286
   ```

2. The Brocade Visibility Manager App login screen appears.

FIGURE 2 Brocade Visibility Manager App login page

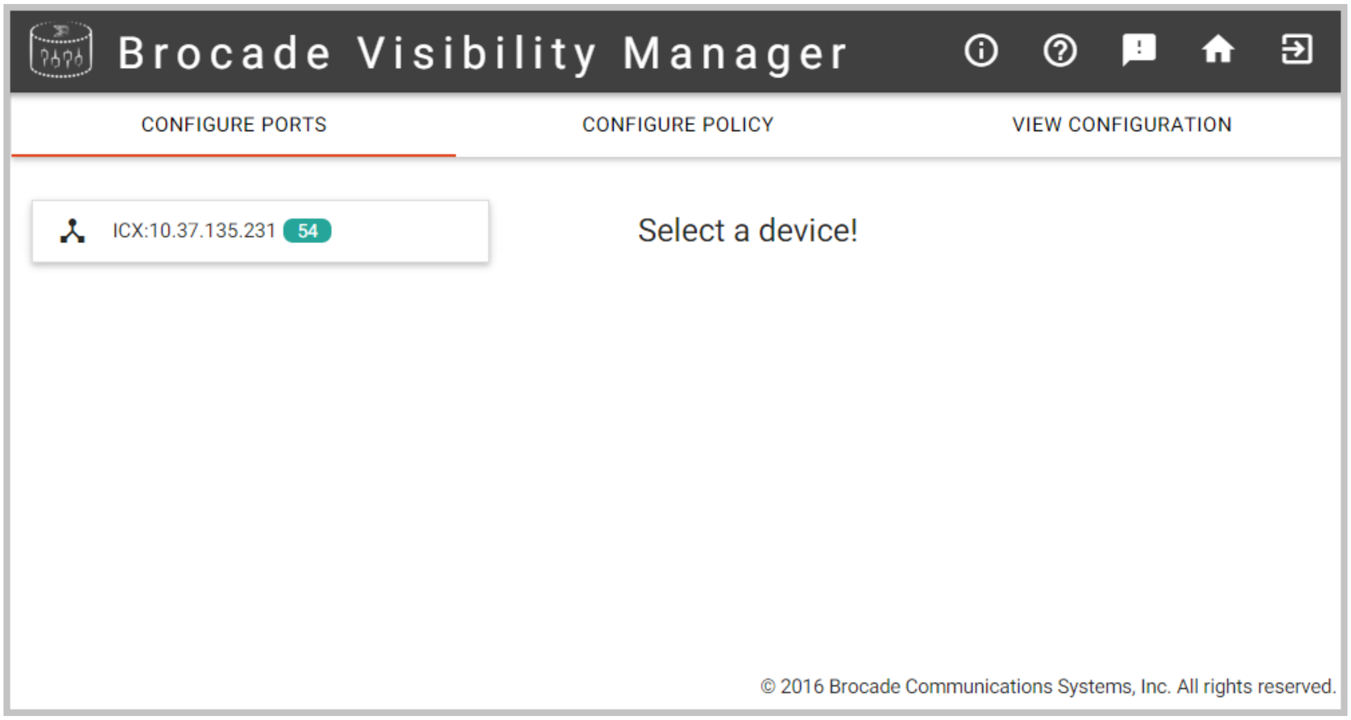


Centralized network packet broker provisioning and management

© 2016 Brocade Communications Systems, Inc. All rights reserved.

3. Enter your user name and password, and click **SIGN IN**.
4. The Brocade Visibility Manager App home page appears.

FIGURE 3 Brocade Visibility Manager App home page



Brocade Visibility Manager

Select a device!

© 2016 Brocade Communications Systems, Inc. All rights reserved.

Ports Configuration

Introduction

This chapter provides information about enabling and disabling ports, configuring ports as ingress, egress, or Port Groups.

Enabling and Disabling Ports

Perform the following steps to enable or disable a port:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure. Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the ports that you want to enable or disable.
4. Click the menu icon.

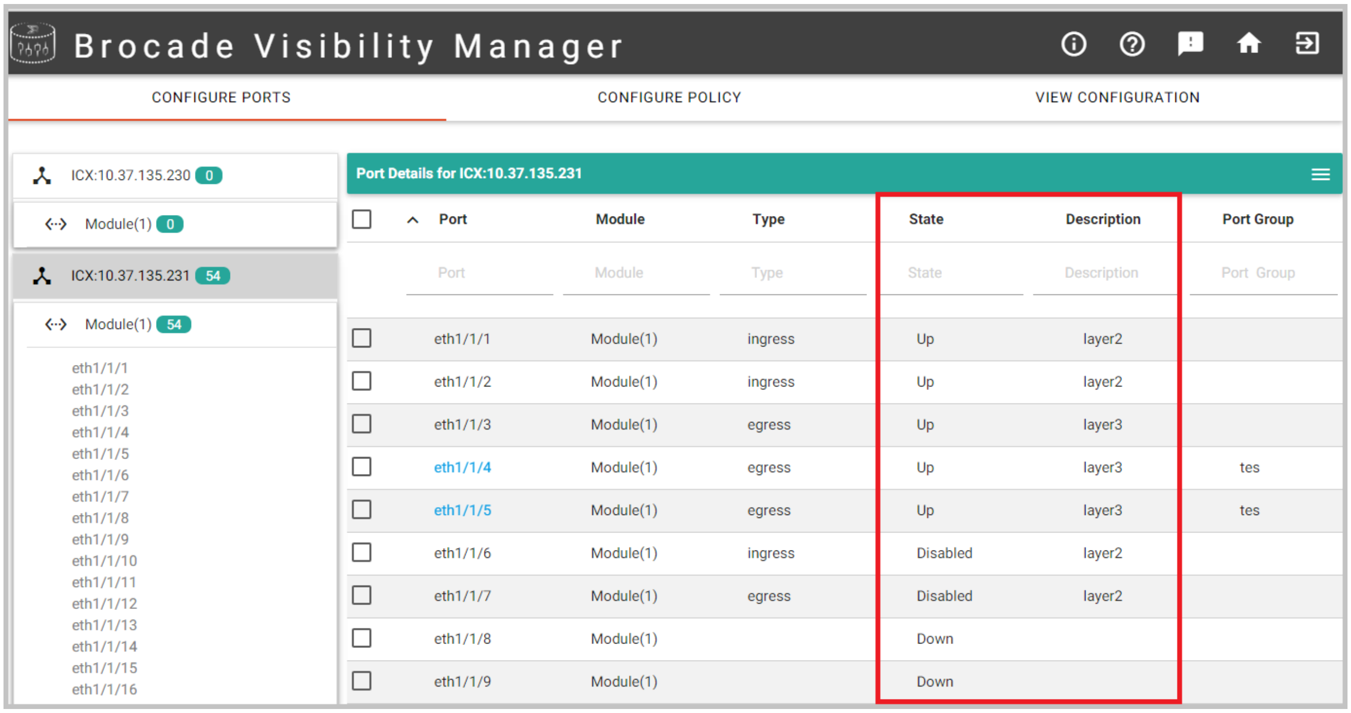
   ☰
5. From the drop-down list, click one of the following options:
   - **Enable as L2**: Enable port as L2.
   - **Enable as L3**: Enable port as L3.
   - **Enable as L23**: Enable port as L23.
   - **Disable**: Disable port.

   A confirmation window appears.

   NOTE
   When a port is enabled, the state changes to either Up or Down depending on the current link state of the port.

6. Click **Yes** to confirm the change.
   The **State** and **Description** columns are updated as per the change.

FIGURE 4 Ports enabled/disabled



Port Details for ICX:10.37.135.231

□	Port	Module	Type	State	Description	Port Group
	Port	Module	Type	State	Description	Port Group
□	eth1/1/1	Module(1)	ingress	Up	layer2	
□	eth1/1/2	Module(1)	ingress	Up	layer2	
□	eth1/1/3	Module(1)	egress	Up	layer3	
□	eth1/1/4	Module(1)	egress	Up	layer3	tes
□	eth1/1/5	Module(1)	egress	Up	layer3	tes
□	eth1/1/6	Module(1)	ingress	Disabled	layer2	
□	eth1/1/7	Module(1)	egress	Disabled	layer2	
□	eth1/1/8	Module(1)		Down		
□	eth1/1/9	Module(1)		Down		

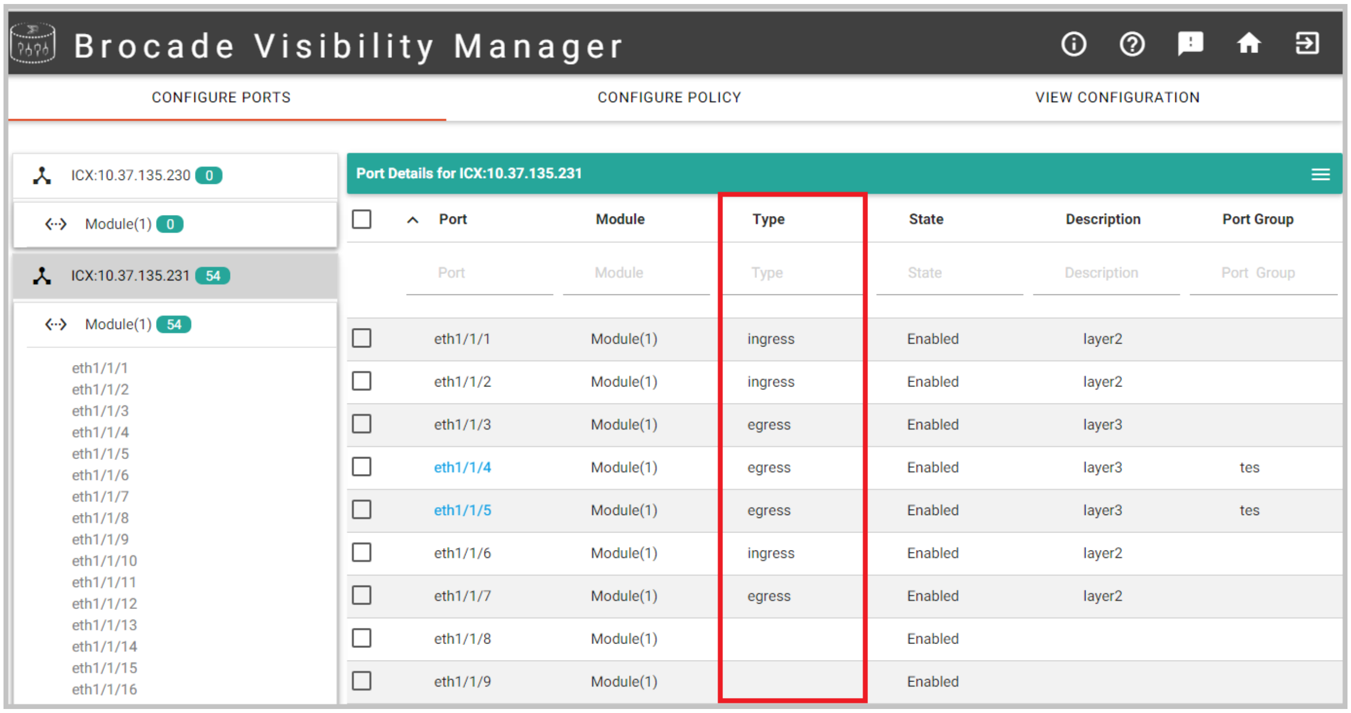
Configuring Ports as Ingress or Egress

Perform the following steps to configure a port as either Ingress or Egress:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the ports that you want to configure as Ingress or Egress.
4. Click the menu icon.
   ≡
5. From the drop-down list, click **Mark as Ingress** to configure the selected port as Ingress or **Mark as Egress** to configure the selected port as Egress.
   A confirmation window appears.

6. Click **Yes** to confirm the change.
   The **Type** column for the selected port is updated to either Ingress or Egress.

FIGURE 5 Ports Ingress/Egress



☐	Port	Module	Type	State	Description	Port Group
	Port	Module	Type	State	Description	Port Group
☐	eth1/1/1	Module(1)	ingress	Enabled	layer2	
☐	eth1/1/2	Module(1)	ingress	Enabled	layer2	
☐	eth1/1/3	Module(1)	egress	Enabled	layer3	
☐	eth1/1/4	Module(1)	egress	Enabled	layer3	tes
☐	eth1/1/5	Module(1)	egress	Enabled	layer3	tes
☐	eth1/1/6	Module(1)	ingress	Enabled	layer2	
☐	eth1/1/7	Module(1)	egress	Enabled	layer2	
☐	eth1/1/8	Module(1)		Enabled		
☐	eth1/1/9	Module(1)		Enabled		

Port Groups

This section describes how to configure Port Groups for Brocade devices.

Port Groups are used for load balancing. A port can be a member of only one Port Group. After a Port Group is created, it will appear in the egress list while creating a policy. Users can choose Port Groups and egress ports to create policies. If a Port Group is selected as the egress, the traffic will be load balanced across the ports in the Port Group.

Creating a Port Group

Perform the following steps to create a Port Group:

NOTE
To create a Port Group, at least of the selected ports should be in 'Up' state.

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the egress ports that you want to configure as a Port Group. Make sure that at least one of the selected ports is in 'Up' state.

4. Click the menu icon.

   ☰

   The **Create Port Group** window appears.
5. From the drop-down list, click **Create Port Group**.
6. In the **Group Name** field, enter a name for the Port Group.
7. To add other egress ports, click the **All Ports** field and click to select egress ports from the drop-down list.
8. Click **COMMIT**.
   The Port Group appears in the port list.

Deleting a Port Group

Perform the following steps to delete a Port Group:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.

   Port details for the selected module is displayed on the right side pane.
3. Click the Port Group you want to delete.
   The **Edit Port Group** window appears.
4. Click the **DELETE** button to delete the Port Group.

Editing a Port Group

Perform the following steps to edit a Port Group:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. Click the Port Group you want to edit.
   The **Edit Port Group** window appears.
4. Make the required changes and click **SAVE**.

Policy Configuration

Introduction

The Policy Configuration tab can be used to create filter rules for incoming or outgoing traffic on an interface. Users can select an ingress ports, egress ports, and Port Groups, and author filters for a device.

While creating a policy:

- If multiple Port Groups are selected as the egress, the traffic will be replicated to those Port Groups and load balanced independently within the ports of the Port Groups.
- If both egress ports and Port Groups are selected in a policy, the traffic will be replicated to the egress ports and the Port Groups, and load balanced independently within the ports of the Port Groups.

Adding a Policy

This section provides information about adding a policy.

Perform the following steps to add a policy:

1. Click the **CONFIGURE POLICY** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
3. Click the menu icon.

   ☰
4. Click **Create Filter(s)**.
   The **Policy Configuration** page appears.

5. Configure the fields as follows:

Option	Description
Policy Name	Name of the policy.
VLAN Tagging	VLAN Id is used to identify the flow from ingress ports to egress ports within ICX. VLAN Id must be a number between 1 and 4094.
Network Port [Ingress]	Select one or more ingress ports from the drop-down menu.
Tool Ports [Egress]	Select one of more egress ports from the drop-down menu.
Filters	Click **Apply** to configure and apply the following filters: • L2: Layer 2 filter • L3-L4: Layer 3/Layer 4 filter • L23: Combination of Layer 2 and Layer 3 filters

Create L2 Filter

The table below provides information about the fields for creating a Layer 2 filter:

Option	Description
Action	Select one of the following actions for the selected filter: • Permit • Deny
Source MAC	Filter based on source MAC.
Source Mask	Filter based on source Mask.
Destination MAC	Filter based on destination MAC.
Destination Mask	Filter based on destination Mask.
Ether Type	Select one of the following options from the drop-down list: • Any • ARP • IPv4 • IPv6
VLAN Id	VLAN Id must be a number between 2 and 4095.
List of Rules	All the rules that are added will appear here.

After adding the filters, click **ADD**. The filters will be added to the **List of Rules** field.

Click **CLEAR** to clear all fields.

Create L3/L4 Filter

The table below provides information about the fields for creating a Layer 3/Layer 4 filter:

Option	Description
Type	Select one of the following options:

Option	Description
	• IPv4 • IPv6
Action	Select one of the following actions: • Permit • Deny
Protocol	Filter based on one of the following protocols: • TCP • UDP • SCTP • ICMP • IGMP
VLAN Id	VLAN Id must be a number between 2 and 4095.
Source Port	Filter based on source port.
Destination IP	Filter based on destination IP.
Destination Port	Filter based on destination port.
List of IPv4 Rules	All the IPv4 rules that are added will appear here.
List of IPv6 Rules	All the IPv6 rules that are added will appear here.

After adding the filters, click **ADD**. Depending on the selected type, the filters will be added to the List of Rules for either IPv4 or IPv6.

Click **CLEAR** to clear all fields.

Create L23 Filter

The table below provides information about the fields for creating a Layer 23 filter:

Option	Description
Type	Select one of the following types: • IPv4 • IPv6
Action	Select one of the following actions for the selected ACL: • Permit • Deny
Protocol	Filter based on one of the following protocols: • TCP • UDP • SCTP • ICMP • IGMP

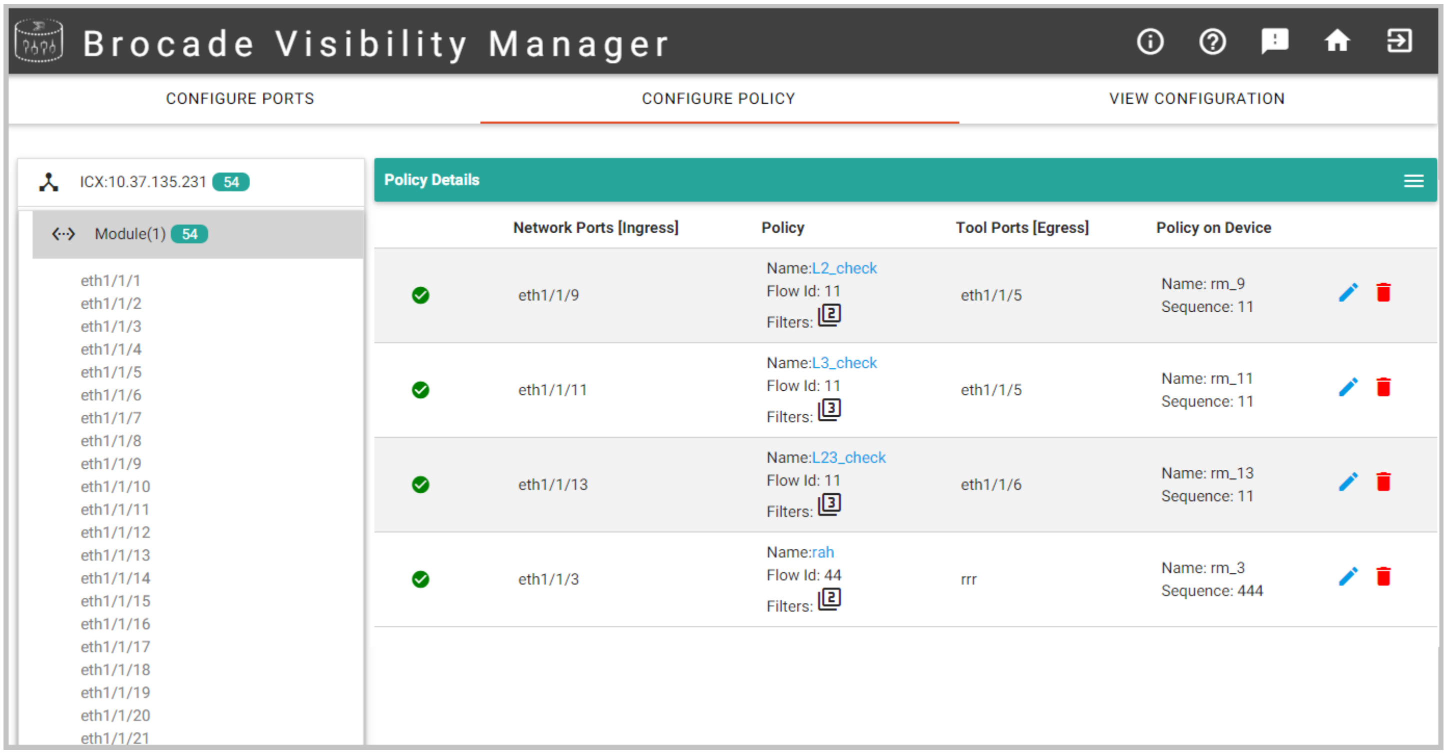
Option	Description
VLAN Id	VLAN Id must be a number between 2 and 4095.
Source Port	Filter based on source port.
Destination IP	Filter based on destination IP.
Destination Port	Filter based on destination port.
Source MAC	Filter based on source MAC.
Source Mask	Filter based on source Mask.
Destination MAC	Filter based on destination MAC.
Destination Mask	Filter based on destination Mask.
Ether Type	Select one of the following options from the drop-down list: • Any • ARP • IPv4 • IPv6
List of IPv4 Rules	All the IPv4 rules that are added will appear here.
List of IPv6 Rules	All the IPv6 rules that are added will appear here.

After adding the filters, click **ADD**. Depending on the selected type, the filters will be added to the List of Rules for either IPv4 or IPv6.

Click **CLEAR** to clear all fields.

6. Click **OK**.
7. Click one of the following buttons:
   - **Save**: Saves to the database, but the changes are not applied to the device.
   - **Commit**: Saves to the database and the changes are applied to the device.

FIGURE 6 Policy



	Network Ports [Ingress]	Policy	Tool Ports [Egress]	Policy on Device
✓	eth1/1/9	Name:L2_check Flow Id: 11 Filters: 2	eth1/1/5	Name: rm_9 Sequence: 11
✓	eth1/1/11	Name:L3_check Flow Id: 11 Filters: 3	eth1/1/5	Name: rm_11 Sequence: 11
✓	eth1/1/13	Name:L23_check Flow Id: 11 Filters: 3	eth1/1/6	Name: rm_13 Sequence: 11
✓	eth1/1/3	Name:rah Flow Id: 44 Filters: 2	rrr	Name: rm_3 Sequence: 444

Handling Errors

This section provides information about some of the common error scenarios that you might encounter while configuring ports or policies. These errors can be caused by various issues, such as an issue with the Brocade Visibility Manager database, issue connecting to SDN or a Brocade device, and so on.

Perform the following steps to determine the exact cause of an error and to fix the error:

1. Whenever there is an error, a notification icon is displayed in the bottom right corner of the page.

   Click the notification icon.

   The **Alerts** window is displayed. This window provides a brief overview of the message.

2. Similarly, an error icon appears next to the port or policy that has an issue.

   Click the error icon.

   The **Job Result** window appears. This window provides detailed information about the issue.

3. To fix an error, delete the configuration. When a configuration is deleted, it cleans up the device for that particular policy. It is then moved to saved state.

View Configuration

Introduction

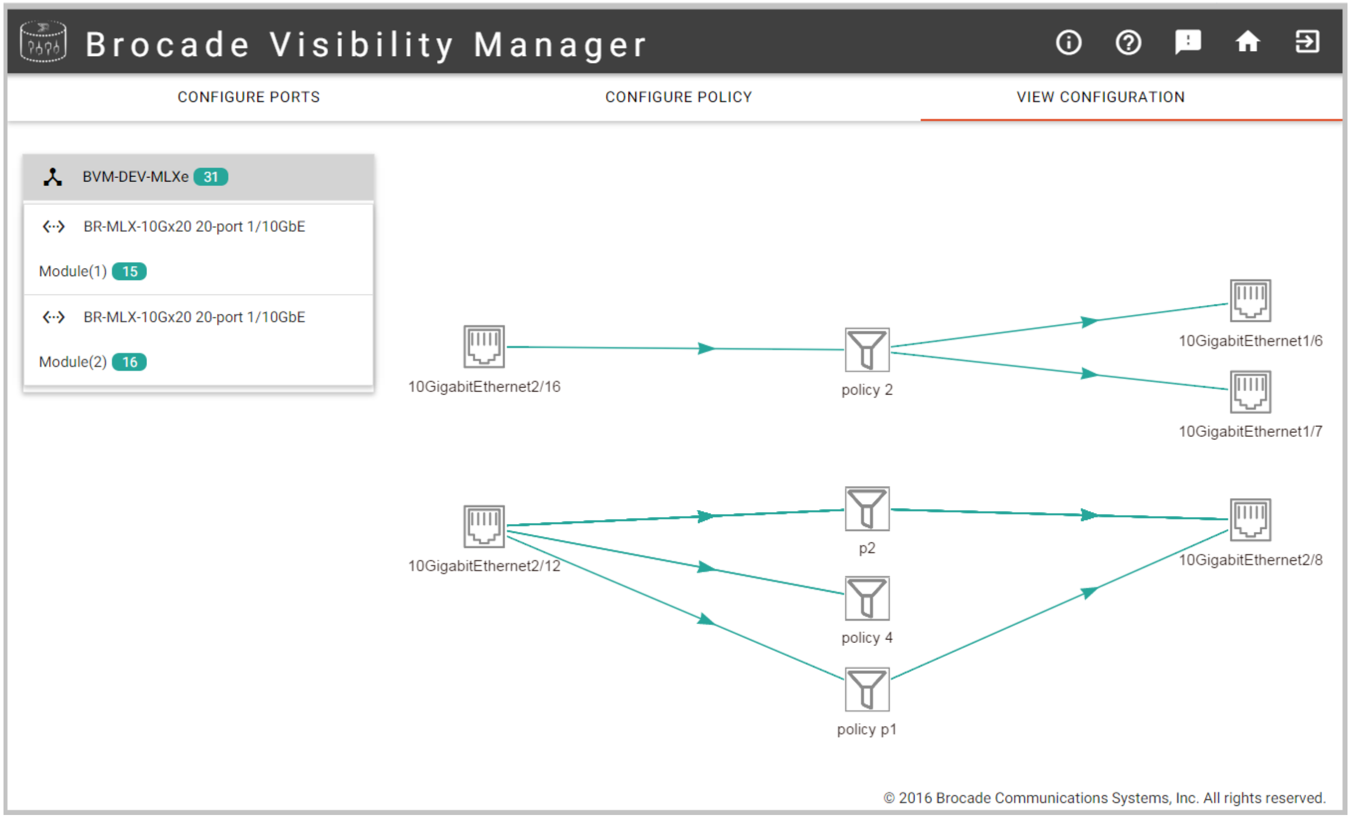
The View Configuration tab provides a visual representation of how each device is configured. It shows the traffic flow for each device and includes information about the policies configured on the device.

Viewing a configuration

Perform the following steps to view the configuration for a device:

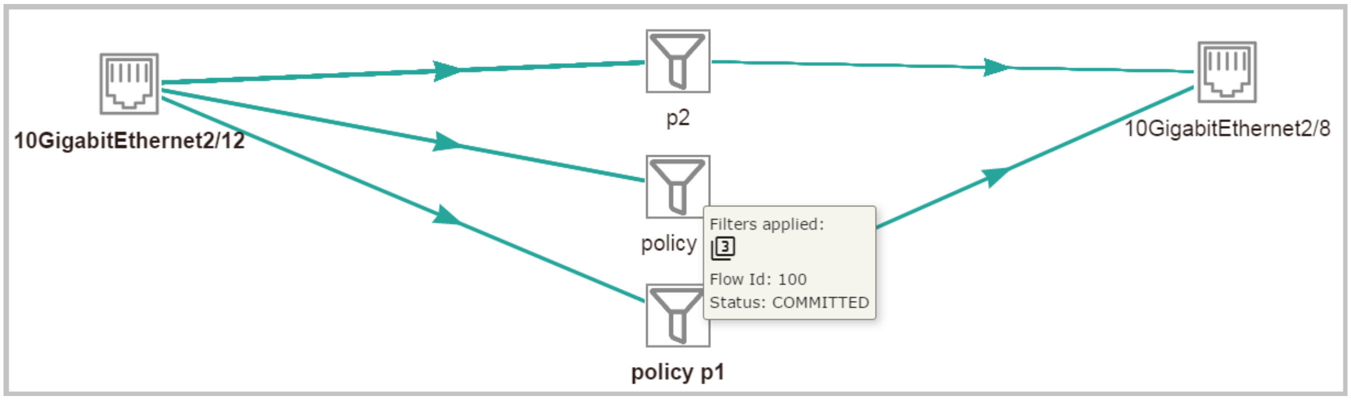
1. Click the **VIEW CONFIGURATION** tab.
2. From the list of devices on the navigation pane on the left side, click a device.
   The configuration details for the selected module is displayed on the right side pane.

FIGURE 7 View configuration



3. Hover the mouse pointer over a policy to view more details.

FIGURE 8 Policy details



Filters applied:
3
Flow Id: 100
Status: COMMITTED

Part B - Brocade Visibility Manager for StableNet®

Getting started with Brocade Visibility Manager

Introduction

Brocade Visibility Manager[1] is an Element Management System (EMS) powered by StableNet®. Brocade Visibility Manager provides centralized provisioning and management of the Brocade MLXe and ICX series packet brokers. In addition, Brocade Visibility Manager provides several customized templates that are specific to these devices.

Installing StableNet®

There are several installation and configuration steps that must be performed before you start using StableNet® GUI. This includes installing the Database and configuring memory. For more information, see 'Chapter 3, Installation' in *StableNet® Version 7.5 Admin Manual.*

Installing Brocade Visibility Manager

This section provides information about the steps that must be performed to use and access Brocade-specific functions in StableNet®.

Perform the following steps:

1. SSH to the StableNet® server.
2. Go to the `/opt/stablenet/snmw/config/imports` folder.
3. Copy the `imports.zip` file, provided by Brocade, to this folder.

   This file includes Brocade-specific job templates, measurement templates, policy job templates, user groups and so on.
4. After copying the file, restart the SNMW service by running the following command:

   ```
   service snmw restart
   ```

   Example

   ```
   service snmw restart
   Stopping StableNet Server: .
   Starting StableNet Server:
   ```

5. Check the status of the service by running the following command:

   ```
   service snmw status
   ```

   Example

   ```
   service snmw status
   StableNet Server is running (pid 5081)
   ```

Accessing StableNet® GUI

For information about accessing and signing in to the StableNet® GUI, see 'Chapter 2, First Steps' in *StableNet® Version 7.5 User Manual*.

> NOTE
> The Brocade plugin requires a Brocade-specific license for Infosim®.

Uploading Brocade-specific custom filter measurement script

This section provides information about uploading Brocade-specific custom filter measurement script.

> NOTE
> Make sure to perform the steps below before the devices are discovered.

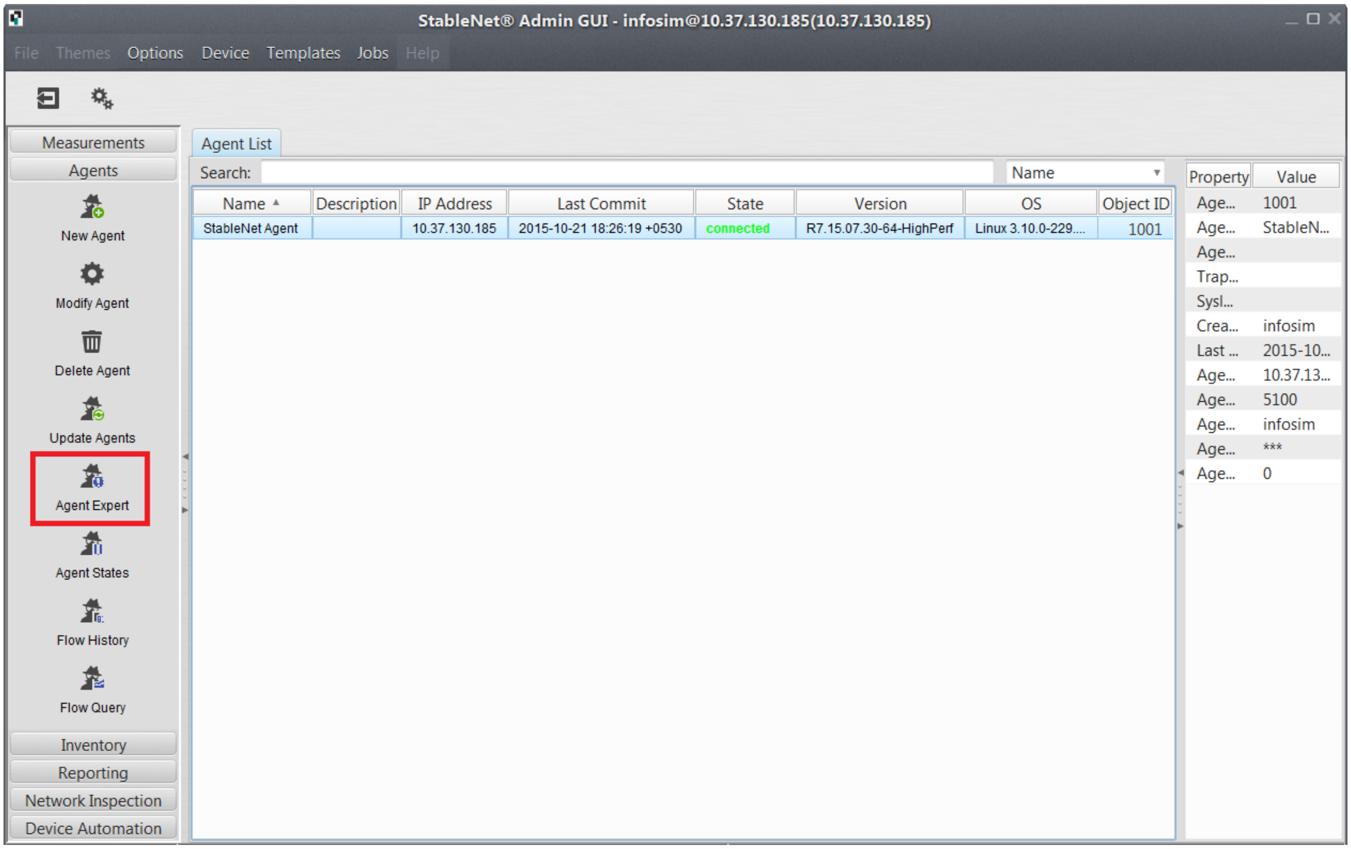
After signing in to StableNet®, perform the following steps:

1. Go to the **Agents** Theme.
2. In the Agent List tab, click to select the agent that is associated with MLXe and ICX devices.

3. Click **Agent Expert**.

   The **Agent Expert - StableNet Agent** window appears.

FIGURE 9 Agent Expert

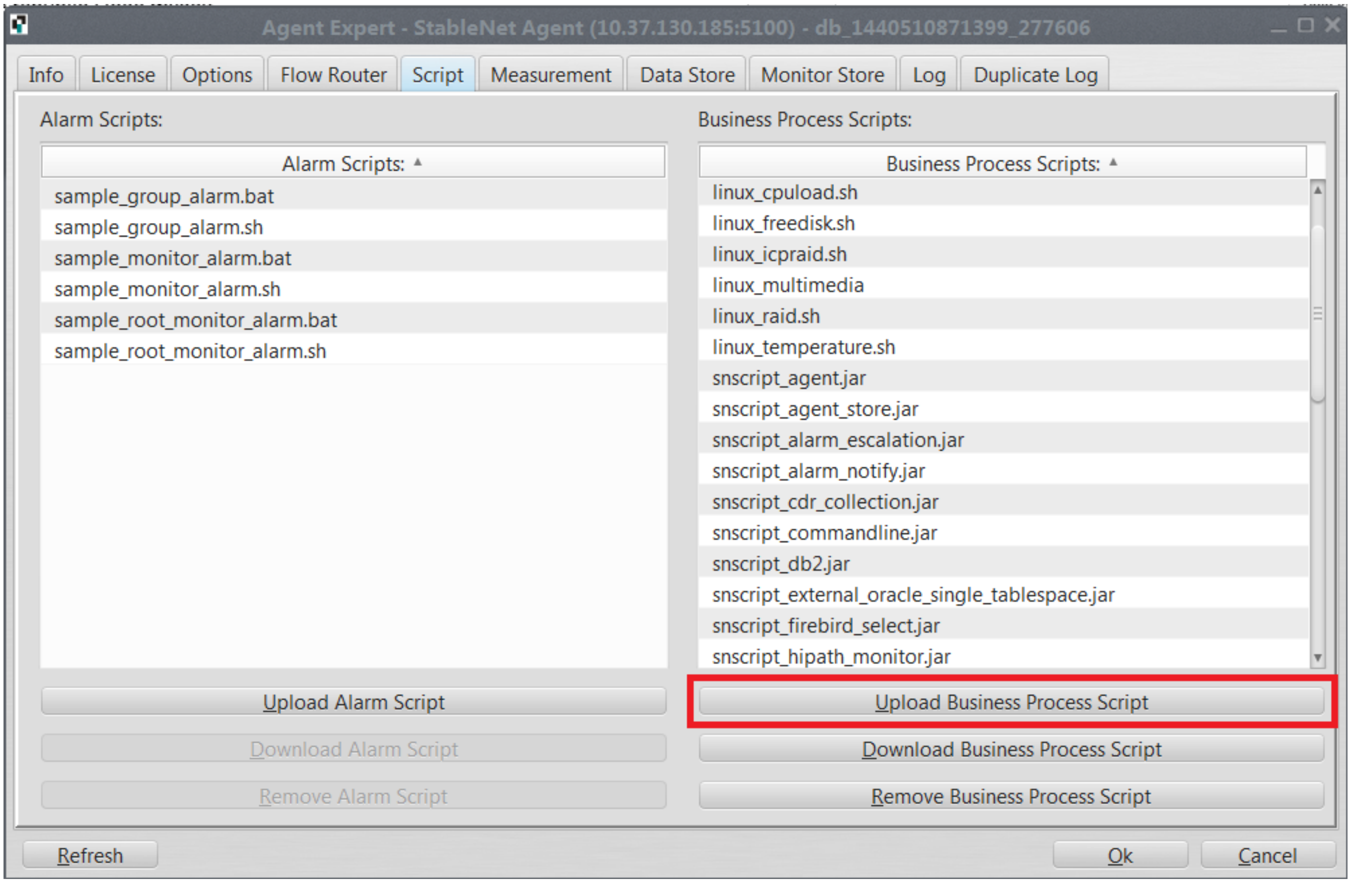


Name ▲	Description	IP Address	Last Commit	State	Version	OS	Object ID
StableNet Agent		10.37.130.185	2015-10-21 18:26:19 +0530	connected	R7.15.07.30-64-HighPerf	Linux 3.10.0-229....	1001

Property	Value
Age...	1001
Age...	StableN...
Age...	
Trap...	
Sysl...	
Crea...	infosim
Last ...	2015-10...
Age...	10.37.13...
Age...	5100
Age...	infosim
Age...	***
Age...	0

4. Click the **Script** tab.

FIGURE 10 Script tab


Agent Expert - StableNet Agent (10.37.130.185:5100) - db_1440510871399_277606
Info
License
Options
Flow Router
Script
Measurement
Data Store
Monitor Store
Log
Duplicate Log
Upload Alarm Script
Download Alarm Script
Remove Alarm Script
Upload Business Process Script
Download Business Process Script
Remove Business Process Script
Refresh
Ok
Cancel

Alarm Scripts:

Alarm Scripts: ▲
sample_group_alarm.bat
sample_group_alarm.sh
sample_monitor_alarm.bat
sample_monitor_alarm.sh
sample_root_monitor_alarm.bat
sample_root_monitor_alarm.sh

Business Process Scripts:

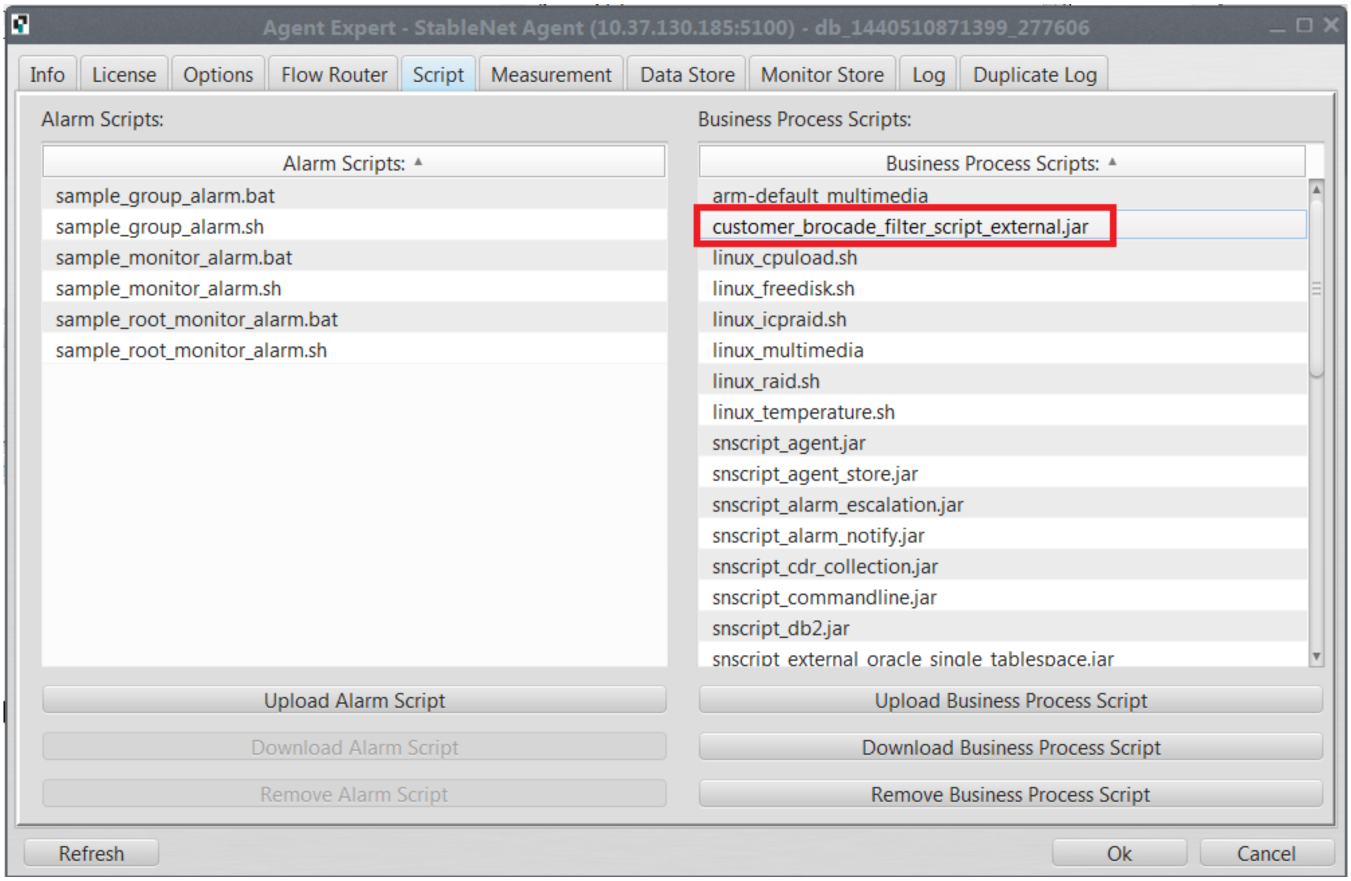
Business Process Scripts: ▲
linux_cpuload.sh
linux_freedisk.sh
linux_icpraid.sh
linux_multimedia
linux_raid.sh
linux_temperature.sh
snscript_agent.jar
snscript_agent_store.jar
snscript_alarm_escalation.jar
snscript_alarm_notify.jar
snscript_cdr_collection.jar
snscript_commandline.jar
snscript_db2.jar
snscript_external_oracle_single_tablespace.jar
snscript_firebird_select.jar
snscript_hipath_monitor.jar

5. Click **Upload Business Process Script**.

6. In the window that appears, browse to the folder that contains the `customer_brocade_filter_script_external.jar` file. Select the file and click **Open**.

   The Brocade-specific script appears in the **Business Process Scripts** list.

   FIGURE 11 Brocade-specific script


Agent Expert - StableNet Agent (10.37.130.185:5100) - db_1440510871399_277606
Info
License
Options
Flow Router
Script
Measurement
Data Store
Monitor Store
Log
Duplicate Log
Upload Alarm Script
Download Alarm Script
Remove Alarm Script
Upload Business Process Script
Download Business Process Script
Remove Business Process Script
Refresh
Ok
Cancel

Alarm Scripts:

Alarm Scripts: ▲
sample_group_alarm.bat
sample_group_alarm.sh
sample_monitor_alarm.bat
sample_monitor_alarm.sh
sample_root_monitor_alarm.bat
sample_root_monitor_alarm.sh

Business Process Scripts:

Business Process Scripts: ▲
arm-default_multimedia
customer_brocade_filter_script_external.jar
linux_cpuload.sh
linux_freedisk.sh
linux_icpraid.sh
linux_multimedia
linux_raid.sh
linux_temperature.sh
snscript_agent.jar
snscript_agent_store.jar
snscript_alarm_escalation.jar
snscript_alarm_notify.jar
snscript_cdr_collection.jar
snscript_commandline.jar
snscript_db2.jar
snscript_external_oracle_single_tablespace.jar

7. Click **Ok**.

Groups and users

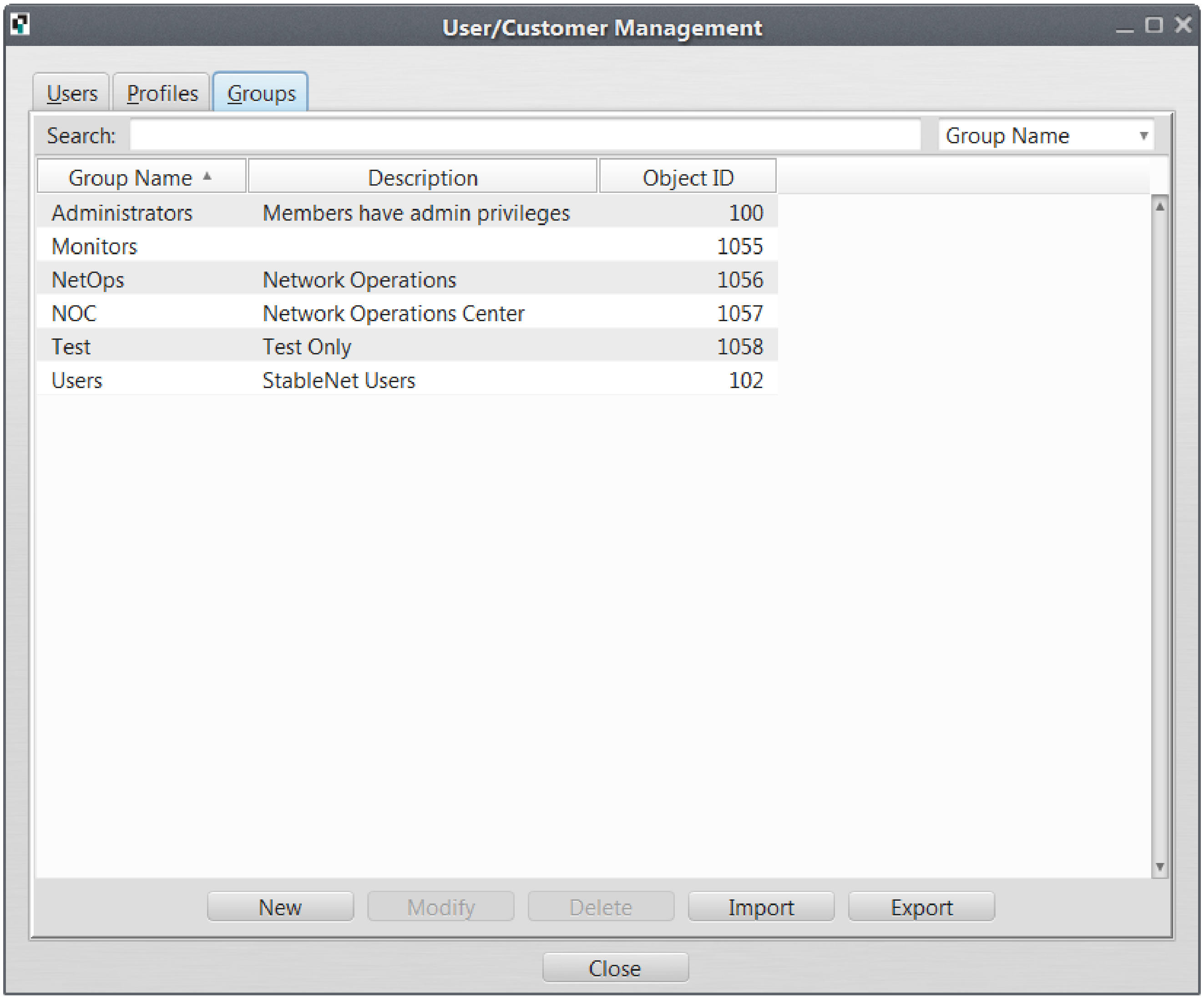
In StableNet® devices can be structured into groups. In addition, groups can contain other groups.

Brocade Visibility Manager includes the following Groups by default:

- **Administrators**: This group includes all the roles and privileges.
- **Read-only user**: Users in this group have read-only access to the assigned devices.
- **System Admin**: Users in this group have configuration privileges to configure assigned devices.
- **Tech Support**: Users of this group can collect logs and debug information from the system.

To view and manage Users and Groups, click **Options** and then click **User/Customer Management**. On the User/Customer Management window, click the **Groups** tab to view the Groups.

FIGURE 12 Groups



Group Name	Description	Object ID
Administrators	Members have admin privileges	100
Monitors		1055
NetOps	Network Operations	1056
NOC	Network Operations Center	1057
Test	Test Only	1058
Users	StableNet Users	102

NOTE
While the Brocade Visibility Manager-specific groups are available by default, a user must be added to each group.

Modifying User Group Rights

After creating users and groups, it is possible to configure user group rights for each device.

To modify user group rights for a device, perform the following steps:

1. Go to the **Measurements** theme.
2. In the list of devices, right-click the Interface you want to modify and click **Modify**.
3. The **Modify Measurement Group** window appears.
4. Click the **Group/Customer Selection** tab.

5. In the **All Groups** column, select the Group you want to add and click **Add**. Alternatively, click **Add all** to add all available groups.
6. Click **Ok**.

Role Based Access Control

Role Based Access Control (RBAC) allows granting access to users on StableNet® components (measurements, devices, reports, and so on). For more information, see ‘Chapter 4, Role Based Access Control’ in *StableNet® Version 7.5 Back Office Manual.*

Device Discovery

Introduction

This chapter provides information about discovering MLXe and ICX devices. Devices that are discovered by StableNet® can be managed using the inventory. You can view device information, modify device attributes or delete devices. Right-click a device to view all the available operations for that device.

Initial Configuration

Before using StableNet® to discover MLXe and ICX devices, the following configuration steps must be performed on each device:

1. Telnet to the device.
2. Run the following command to configure the SNMP community string and access privileges:

   ```
   snmp-server community community-string { ro | rw } [ acl-name | acl-num | ipv6 ipv6-acl-name | view
   [ mib-view ] ]
   ```

   The host-ipaddr parameter is the IP address of the StableNet server.

   Example

   ```
   snmp-server host 10.37.130.185 version v1
   ```

   For more information about this command, see the section 'snmp-server host' in *Brocade NetIron Command Reference*.
3. Run the following command to save the current running configuration information to the startup configuration file:

   ```
   write memory
   ```

   For more information about this command, see the section 'write memory' in *Brocade NetIron Command Reference*.
4. If required, run the following command to organize the machine based on location:

   ```
   snmp-server location text
   ```

   Example

   ```
   snmp-server location blr|6
   ```

Discovering Devices

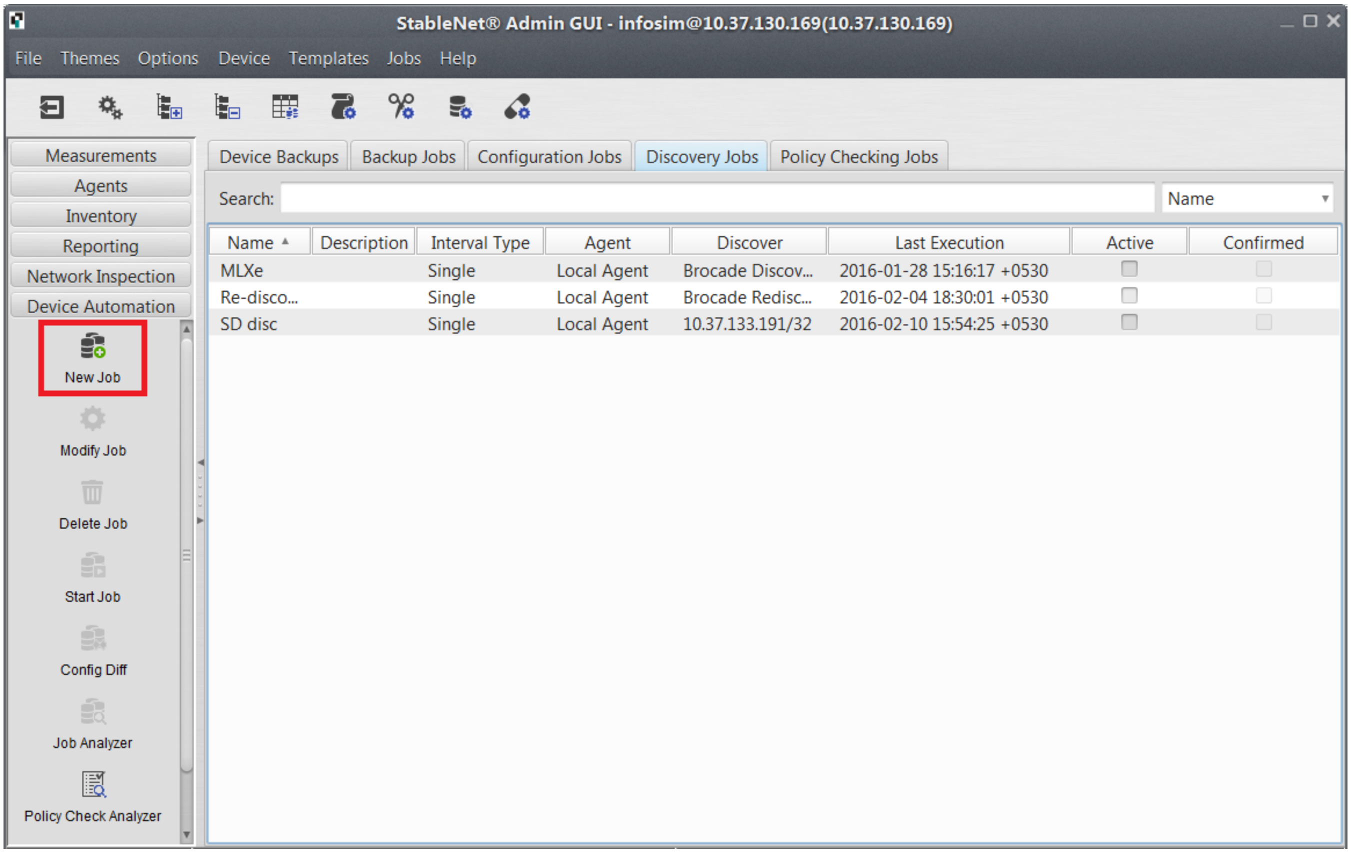
There are several methods that can be used to discover devices. During the discovery process, StableNet® performs a network scan based on the discovery input and queries device information from the available devices.

NOTE
Before devices are discovered, ensure that all devices have login and password information configured. StableNet® will not be able to discover devices that do have this information configured.

Perform the following steps to discover devices:

1. Go the **Device Automation** theme.
2. Click **Discovery Jobs** tab.

FIGURE 13 Discovery Jobs

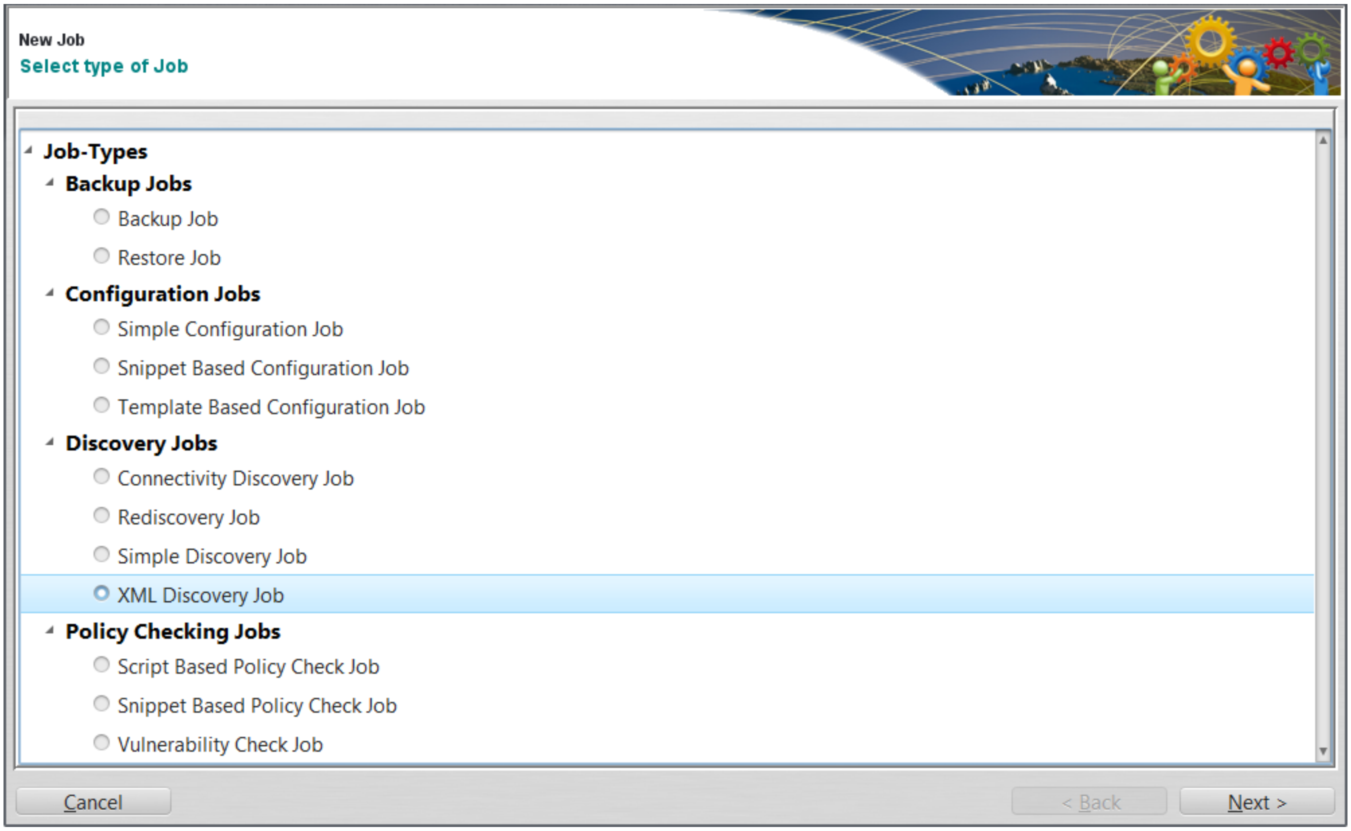


Name ▲	Description	Interval Type	Agent	Discover	Last Execution	Active	Confirmed
MLXe		Single	Local Agent	Brocade Discov...	2016-01-28 15:16:17 +0530	☐	☐
Re-disco...		Single	Local Agent	Brocade Redisc...	2016-02-04 18:30:01 +0530	☐	☐
SD disc		Single	Local Agent	10.37.133.191/32	2016-02-10 15:54:25 +0530	☐	☐

3. Click **New Job**.
Job Wizard window appears.

4. Click to select **XML Discovery Job**.

FIGURE 14 XML Discovery Job



New Job

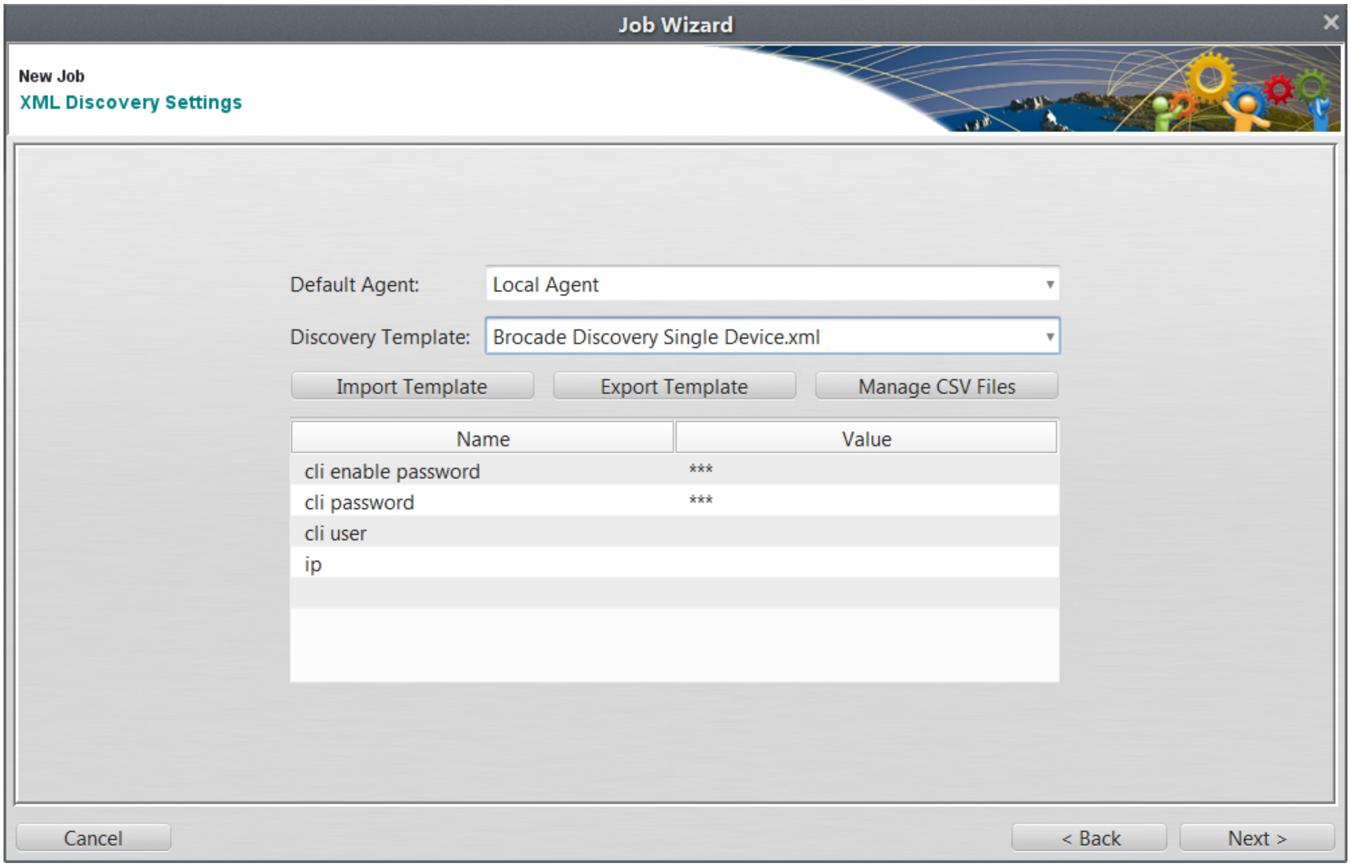
Select type of Job

- Job-Types
  - Backup Jobs
    - ○ Backup Job
    - ○ Restore Job
  - Configuration Jobs
    - ○ Simple Configuration Job
    - ○ Snippet Based Configuration Job
    - ○ Template Based Configuration Job
  - Discovery Jobs
    - ○ Connectivity Discovery Job
    - ○ Rediscovery Job
    - ○ Simple Discovery Job
    - ● XML Discovery Job
  - Policy Checking Jobs
    - ○ Script Based Policy Check Job
    - ○ Snippet Based Policy Check Job
    - ○ Vulnerability Check Job

5. Click **Next**.
   Name window appears.
6. Provide a name in the **Name** field, for example Discovery Job 1, and click **Next**.
   Schedule Settings window appears.

7. Configure the Trigger Types as per your requirement and click **Next**.
   XML Discovery Settings window appears.

FIGURE 15 XML Discovery Settings



Job Wizard

New Job

XML Discovery Settings

Default Agent: Local Agent

Discovery Template: Brocade Discovery Single Device.xml

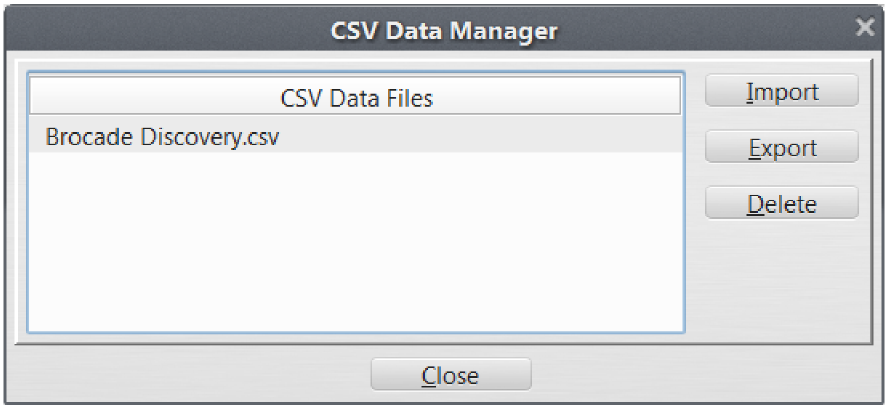
Name	Value
cli enable password	***
cli password	***
cli user	
ip	

8. On the XML Discovery Settings window, click to select either **Brocade Discovery Multiple Devices.xml** or **Brocade Discovery Single Device.xml** and configure it as follows:
   - **Brocade Discovery Single Device.xml**: Use this option to discover a single device.

     Provide the CLI enable password, password, username and IP address for the device that needs to be discovered.
   - **Brocade Discovery Multiple Devices.xml**: Use this option to discover multiple devices.
     1. Click **Manage CSV Files**.

        CSV Data Manager window appears.

        FIGURE 16 CSV Data Manager



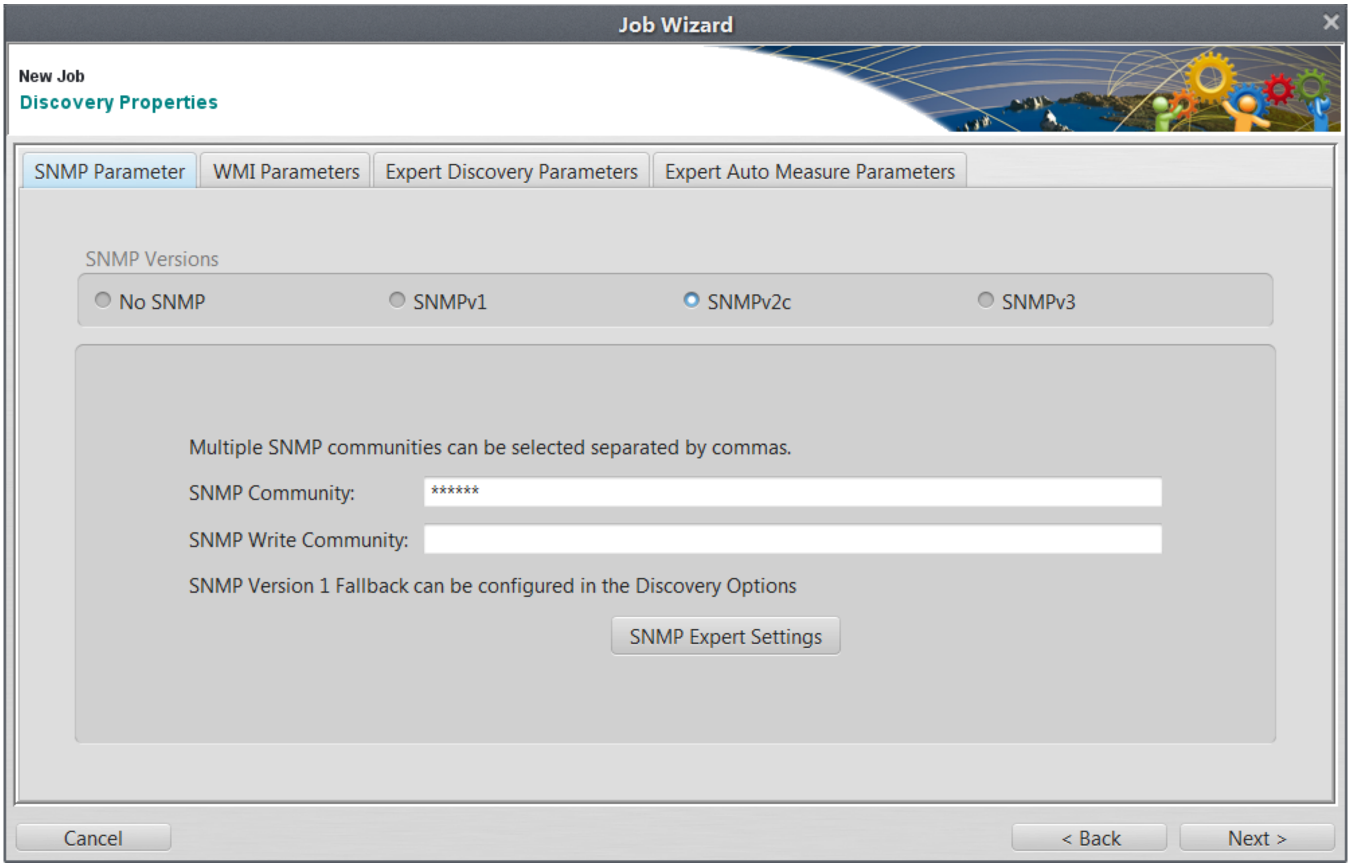
     2. On the **CSV Data Manager window**, select **Brocade Discovery.csv**, click **Export** and save the file to a local directory.
     3. Open **Brocade Discovery.csv**. This file allows you to add information about all the devices that need to discovered.
     4. Add information about the devices in the following format:

```
ip;cliuser;clipassword;clienable;clitype
```

        For each device that needs to be discovered, provide the IP address, CLI username, password, enable password, and type.
     5. Save the file.
     6. On the **CSV Data Manager** window, click **Import**.
     7. Select the saved **Brocade Discovery.csv** file and click **Open**
     8. Click **Close** to the close the CSV Data Manager window.

9. Click **Next**.
   Discovery Properties window appears.

FIGURE 17 Discovery Properties



Job Wizard

New Job

Discovery Properties

SNMP Versions

○ No SNMP ○ SNMPv1 ● SNMPv2c ○ SNMPv3

Multiple SNMP communities can be selected separated by commas.

SNMP Community: ******

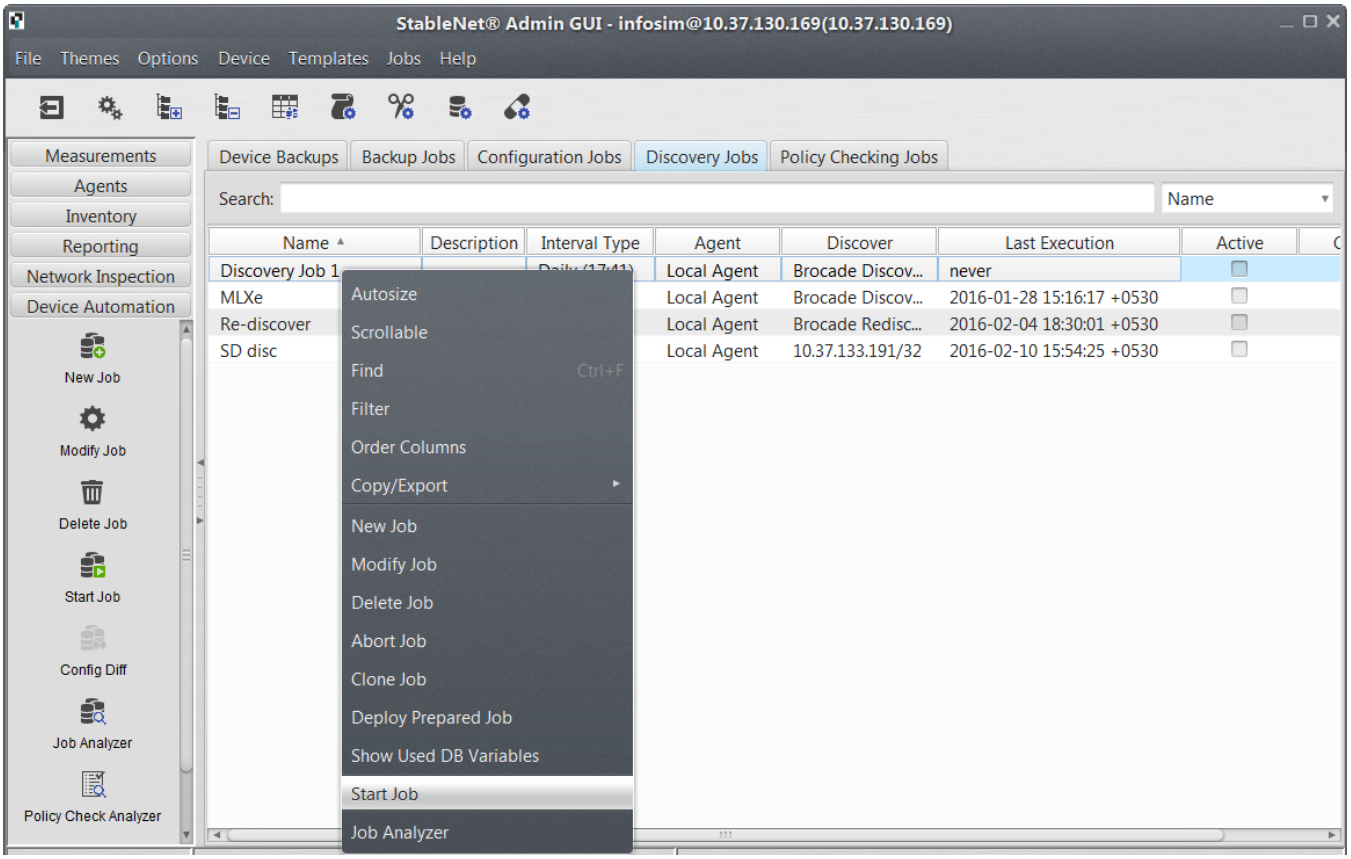
SNMP Write Community:

SNMP Version 1 Fallback can be configured in the Discovery Options

10. Click the **SNMP Parameter** tab and ensure that **SNMPv2c** is selected. In addition, provide the SNMP community string set on the MLXe in the **SNMP Community** field.
11. Click **Next**.
    Group/Customer Selection window appears.
12. Select the appropriate users and groups, and click **Finish**.
    The job you just created appears in the list of Discovery Jobs.

13. Right-click the job you created and click **Start Job**.

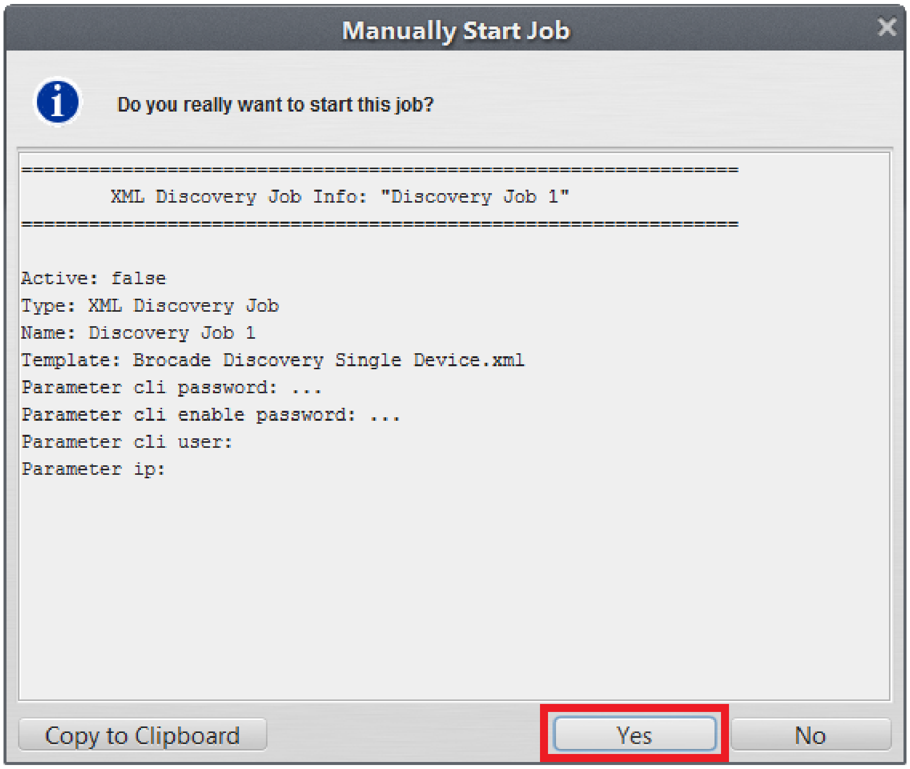
FIGURE 18 Discovery Properties



Name ▲	Description	Interval Type	Agent	Discover	Last Execution	Active
Discovery Job 1		Daily (17:41)	Local Agent	Brocade Discov...	never	□
MLXe			Local Agent	Brocade Discov...	2016-01-28 15:16:17 +0530	□
Re-discover			Local Agent	Brocade Redisc...	2016-02-04 18:30:01 +0530	□
SD disc			Local Agent	10.37.133.191/32	2016-02-10 15:54:25 +0530	□

Manually Start Job window appears.

FIGURE 19 Manually Start Job



Do you really want to start this job?

```
================================================================
        XML Discovery Job Info: "Discovery Job 1"
================================================================

Active: false
Type: XML Discovery Job
Name: Discovery Job 1
Template: Brocade Discovery Single Device.xml
Parameter cli password: ...
Parameter cli enable password: ...
Parameter cli user:
Parameter ip:
```

14. Click **Yes** to start the job and click close on the **Close** on the window that appears.

NOTE
For more information about discovering devices, see the sections ‘Network Discovery’ and ‘Automated Discovery’ in *StableNet® Version 7.5 Back Office Manual*.

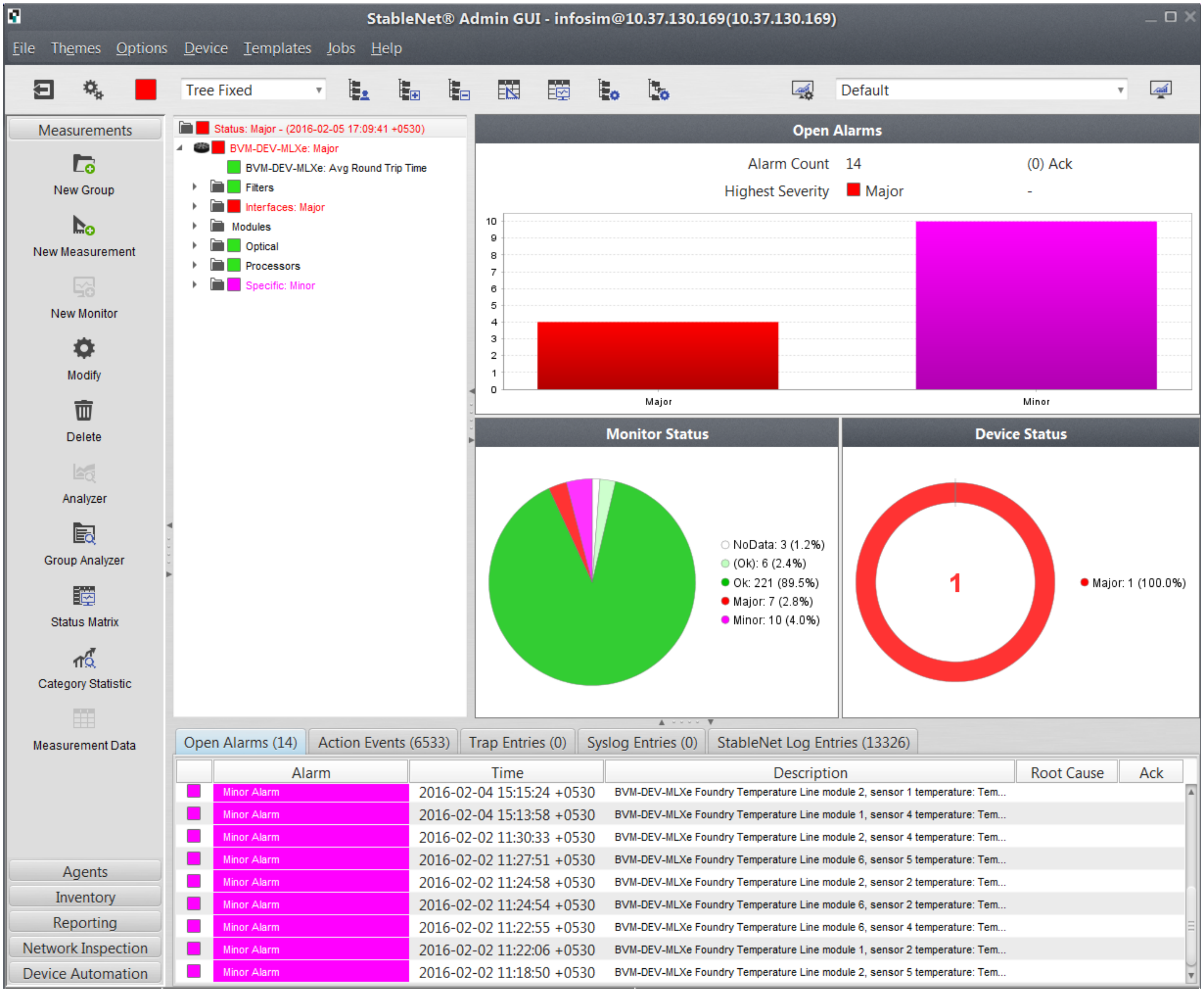
Devices

All discovered devices are displayed in the Measurements view. Here you can check status of all interfaces, check alarms and so on.

Discovered devices are automatically organized into groups. In addition, the following groups are added for MLXe and ICX devices:

- Filters: Lists all the programmed rules per interface.
- Modules: Lists all the Cards. Available for MLXe devices only.
- Optical: Lists all Optical levels of each interfaces.
- Interfaces: Lists all interfaces.

FIGURE 20 Discovered devices



Alarm Count 14 (0) Ack

Highest Severity 🟥 Major -

	Alarm	Time	Description	Root Cause	Ack
■	Minor Alarm	2016-02-04 15:15:24 +0530	BVM-DEV-MLXe Foundry Temperature Line module 2, sensor 1 temperature: Tem...		
■	Minor Alarm	2016-02-04 15:13:58 +0530	BVM-DEV-MLXe Foundry Temperature Line module 1, sensor 4 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:30:33 +0530	BVM-DEV-MLXe Foundry Temperature Line module 2, sensor 4 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:27:51 +0530	BVM-DEV-MLXe Foundry Temperature Line module 6, sensor 5 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:24:58 +0530	BVM-DEV-MLXe Foundry Temperature Line module 2, sensor 2 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:24:54 +0530	BVM-DEV-MLXe Foundry Temperature Line module 6, sensor 2 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:22:55 +0530	BVM-DEV-MLXe Foundry Temperature Line module 6, sensor 4 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:22:06 +0530	BVM-DEV-MLXe Foundry Temperature Line module 1, sensor 2 temperature: Tem...		
■	Minor Alarm	2016-02-02 11:18:50 +0530	BVM-DEV-MLXe Foundry Temperature Line module 2, sensor 5 temperature: Tem...		

Deleting Devices

Perform the following steps to delete a device:

1. Go to **Inventory Theme**.
2. Select the device and use the Delete button of the theme bar or the context menu.
   This removes the device from the Inventory, but the measurements related to the device are not removed. These are still available for reports and have to be deleted separately in the Measurements Theme.
3. Go the **Measurements** Theme.
4. Select the device and use the **Delete** button of the theme bar or the context menu.

Jobs and Measurements

Introduction

This chapter provides information about adding various jobs, checking measurements, and creating backup and restore jobs for the devices discovered using StableNet®.

Jobs

StableNet® provides the ability to start and run several operations periodically. A scheduler is used to control the continuous activities. These scheduled activities are called jobs in StableNet®. Jobs are categorized by job types depending on the task of the job. For more information, see 'Chapter 5, Device Automation' in *StableNet® Version 7.5 User Manual.*

NOTE
Jobs specific to the Brocade plugin can be created using the following options:

- Template Based Configuration Job on page 70
- XML discovery job on page 75

Creating Jobs for Brocade Visibility Manager App

This section provides information about the two template jobs that must be created for configuring Brocade Visibility Manager App.

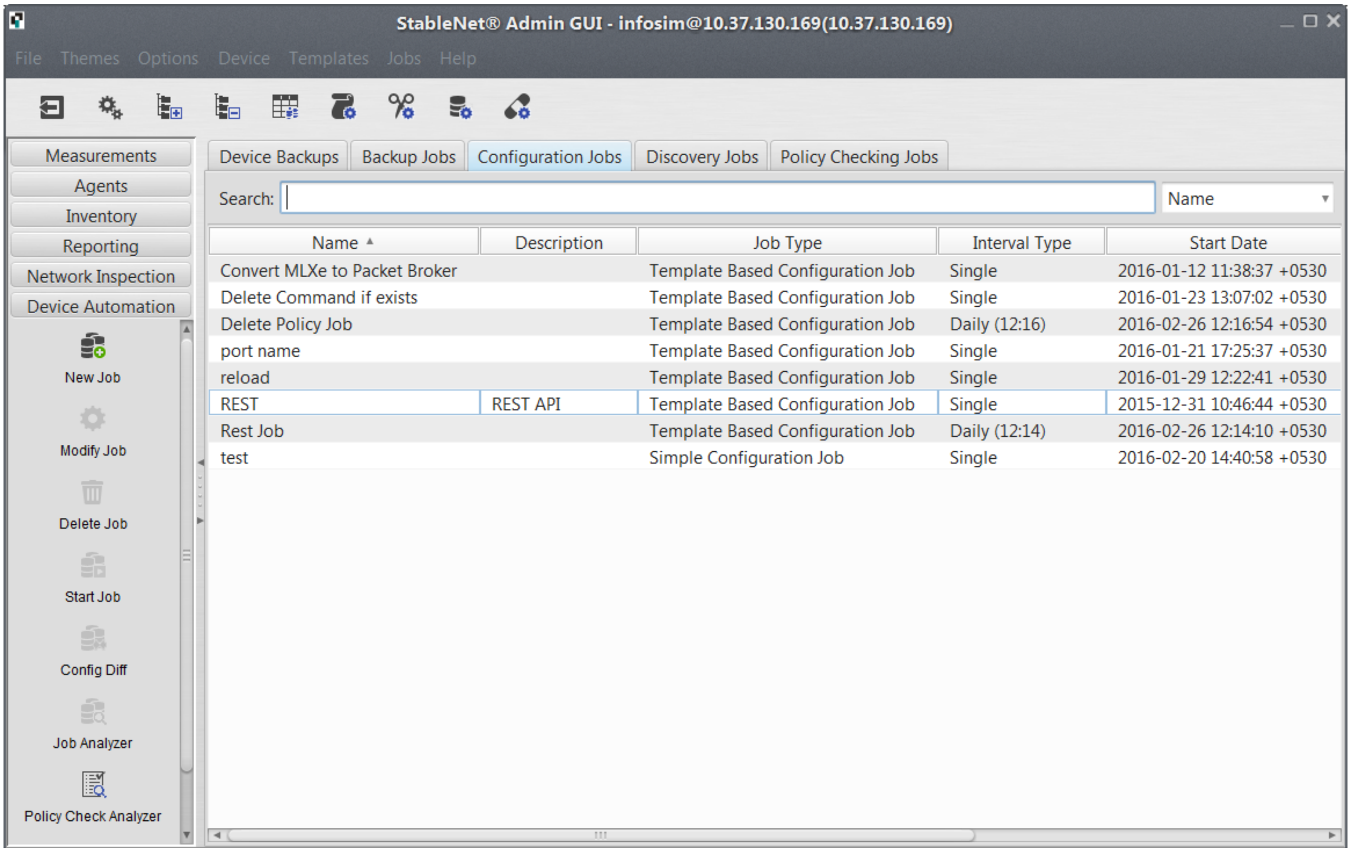
NOTE

- For information about the Brocade Visibility Manager App, see the section Getting Started with Brocade Visibility Manager App.
- After creating the first job, repeat the steps below to create a second job.

1. Go to **Device Automation** theme.

2. Click **Configuration Jobs** tab.

FIGURE 21 Configuration Jobs



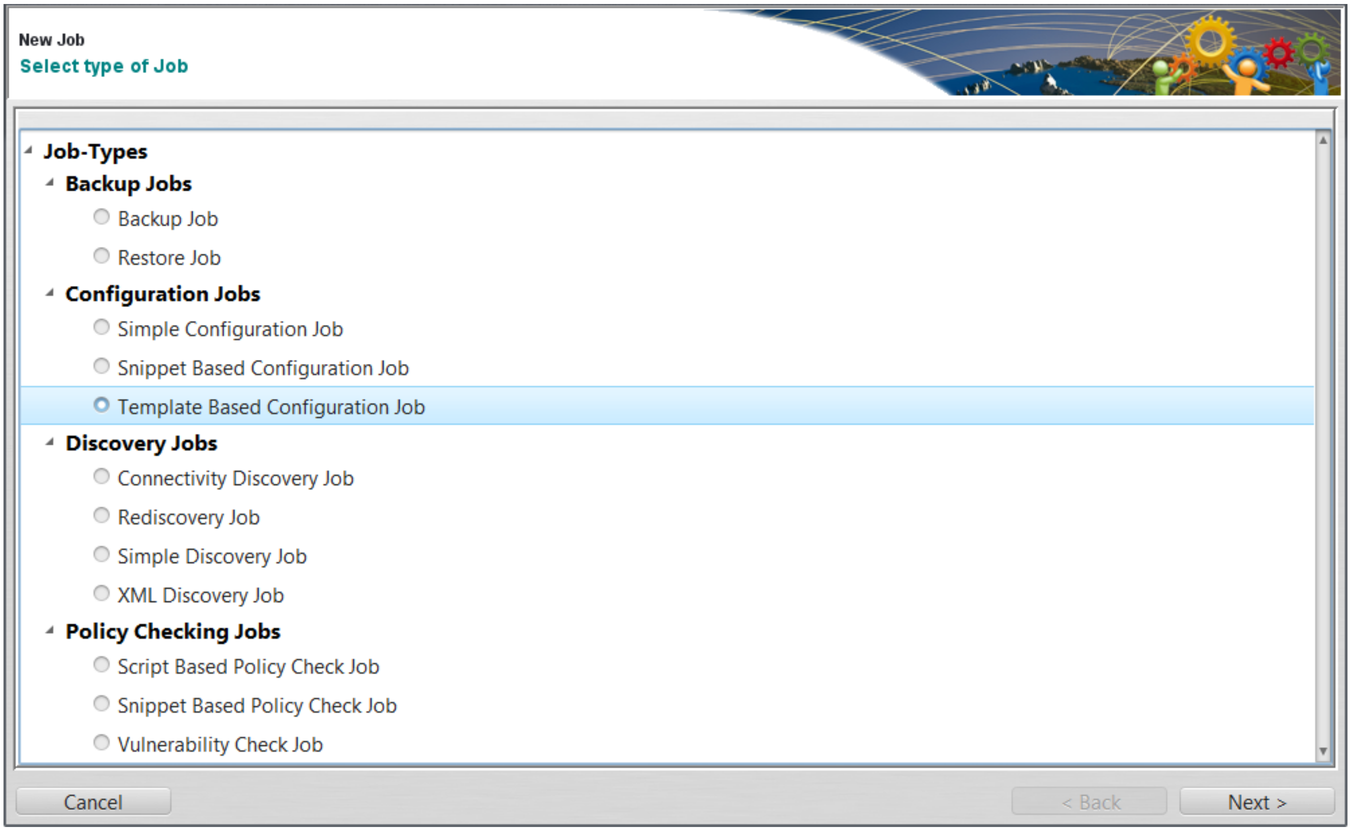
Name ▲	Description	Job Type	Interval Type	Start Date
Convert MLXe to Packet Broker		Template Based Configuration Job	Single	2016-01-12 11:38:37 +0530
Delete Command if exists		Template Based Configuration Job	Single	2016-01-23 13:07:02 +0530
Delete Policy Job		Template Based Configuration Job	Daily (12:16)	2016-02-26 12:16:54 +0530
port name		Template Based Configuration Job	Single	2016-01-21 17:25:37 +0530
reload		Template Based Configuration Job	Single	2016-01-29 12:22:41 +0530
REST	REST API	Template Based Configuration Job	Single	2015-12-31 10:46:44 +0530
Rest Job		Template Based Configuration Job	Daily (12:14)	2016-02-26 12:14:10 +0530
test		Simple Configuration Job	Single	2016-02-20 14:40:58 +0530

3. Click **New Job**.

   Job Wizard window appears.

4. Click to select **Template Based Configuration Job**.

FIGURE 22 Template Based Configuration Job

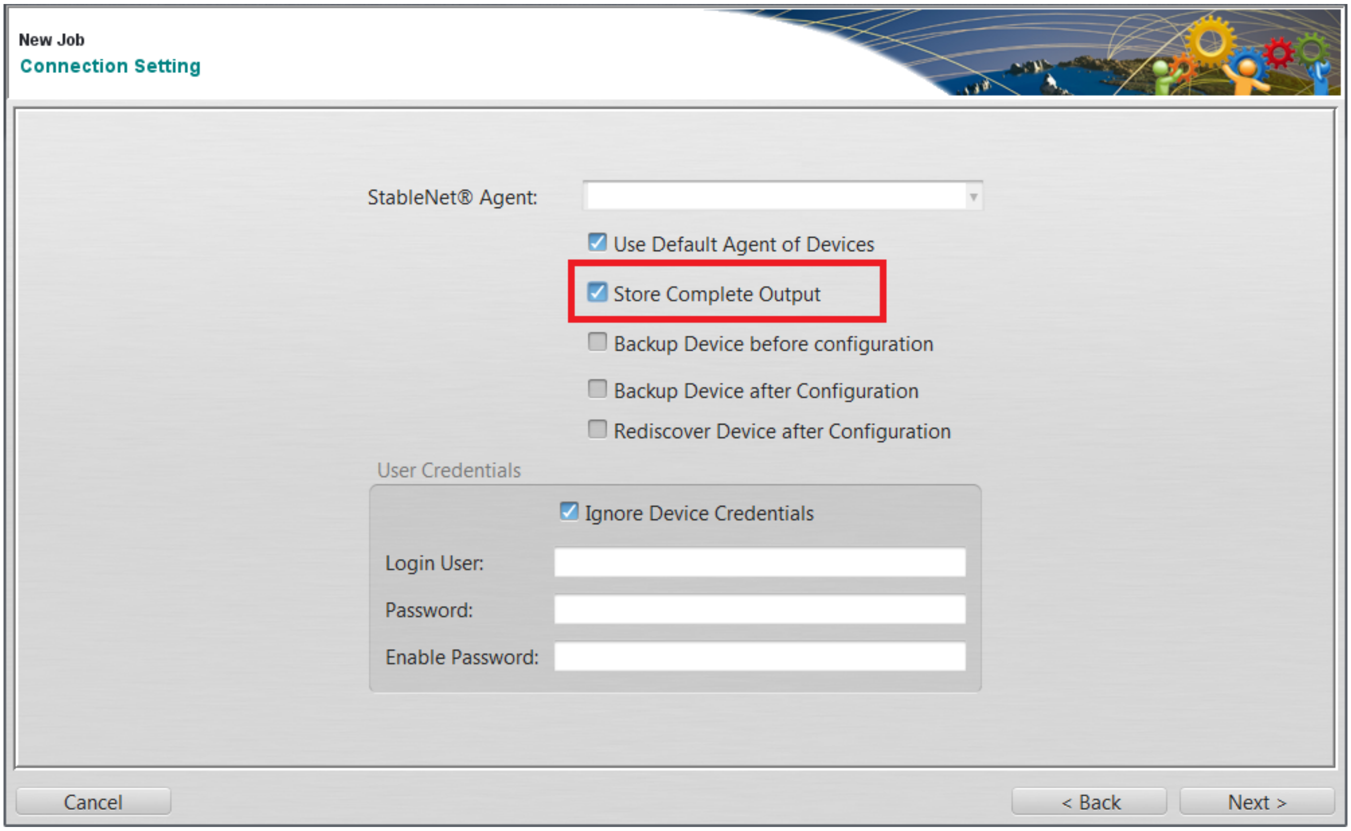

New Job
Select type of Job
Job-Types
Backup Jobs
○ Backup Job
○ Restore Job
Configuration Jobs
○ Simple Configuration Job
○ Snippet Based Configuration Job
○ Template Based Configuration Job
Discovery Jobs
○ Connectivity Discovery Job
○ Rediscovery Job
○ Simple Discovery Job
○ XML Discovery Job
Policy Checking Jobs
○ Script Based Policy Check Job
○ Snippet Based Policy Check Job
○ Vulnerability Check Job
Cancel
< Back
Next >

5. Click **Next**.
   Name window appears.
6. Provide a name in the **Name** field and click **Next**.
   Schedule Settings window appears.
7. Configure the Trigger Types as per your requirement and click **Next**.
   Connection Setting window appears.

8. On the Connection Setting window, perform the following tasks:
   - Click to select **Store Complete Output**. This is useful for getting detailed output for the job.
   - If you want to bypass the user credentials on the device and provide new credentials, deselect **Ignore Device Credentials** and provide the username, password and enable password.

     Do not uncheck the **Ignore Device Credentials** check box if you want to continue using the user credentials currently set on the device.

FIGURE 23 Connection Setting



New Job

Connection Setting

StableNet® Agent:

☑ Use Default Agent of Devices

☑ Store Complete Output

☐ Backup Device before configuration

☐ Backup Device after Configuration

☐ Rediscover Device after Configuration

User Credentials

☑ Ignore Device Credentials

Login User:

Password:

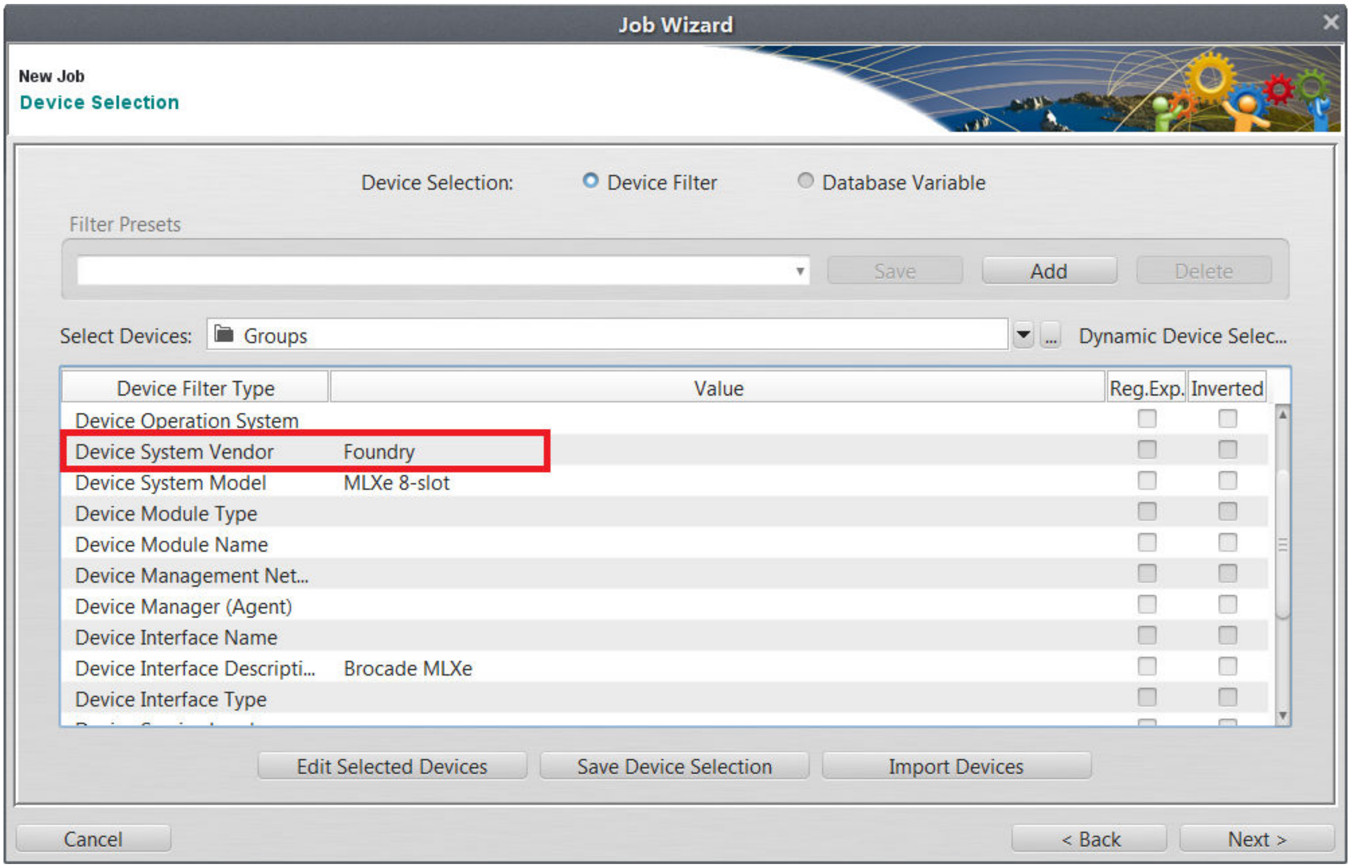
Enable Password:

9. After making the appropriate selections on the Connection Setting window, click **Next**.
   Device Selection window appears.

10. Change the value of the **Device System Vendor** field to **Foundry**.

    NOTE
    Leaving this field empty or providing a different value for this field can cause issues with MLXe device detection.

FIGURE 24 Device Selection



Device Selection: ● Device Filter ○ Database Variable

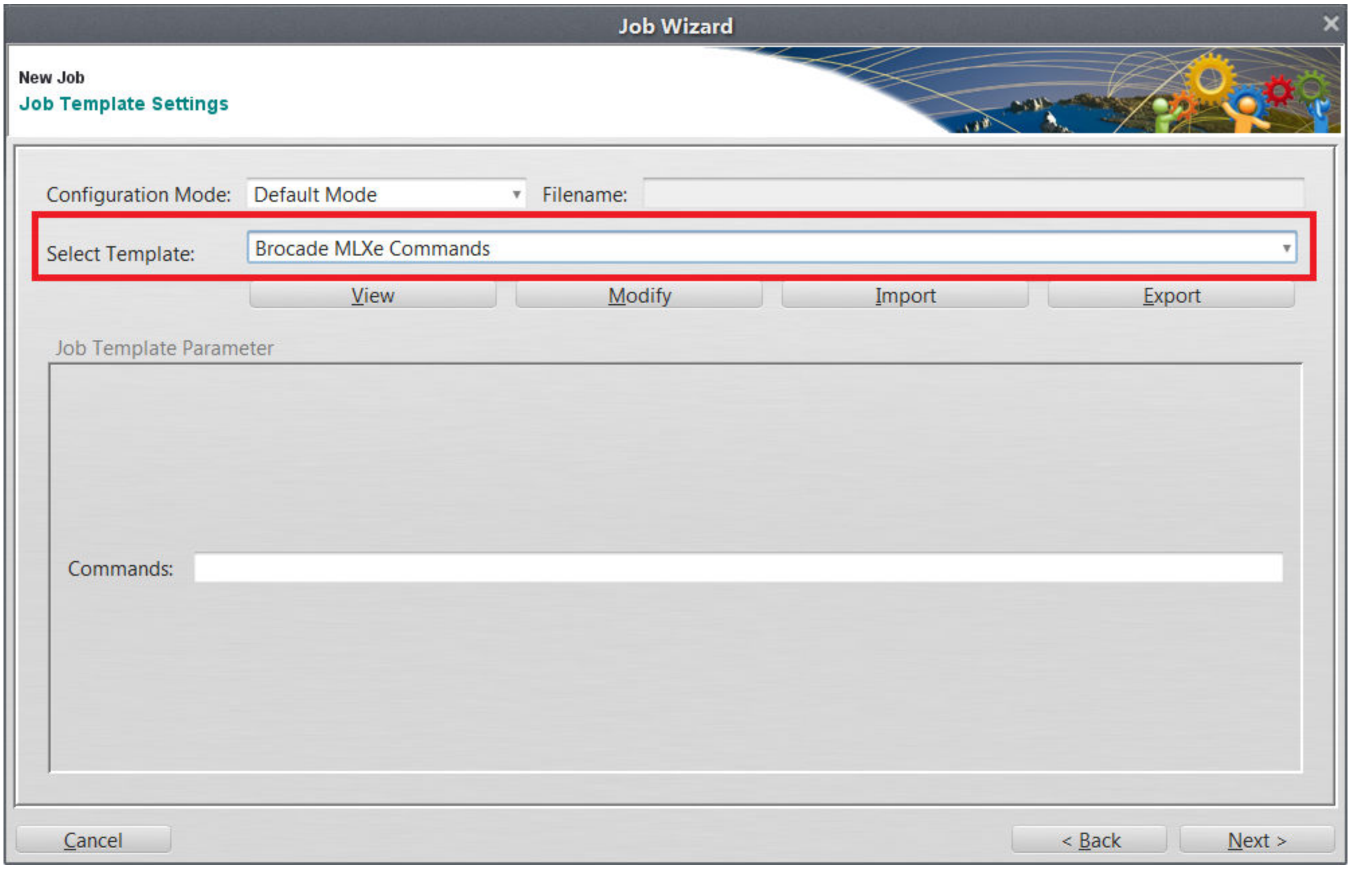
Select Devices: Groups

Device Filter Type	Value	Reg.Exp.	Inverted
Device Operation System		□	□
Device System Vendor	Foundry	□	□
Device System Model	MLXe 8-slot	□	□
Device Module Type		□	□
Device Module Name		□	□
Device Management Net...		□	□
Device Manager (Agent)		□	□
Device Interface Name		□	□
Device Interface Descripti...	Brocade MLXe	□	□
Device Interface Type		□	□

11. Click **Next**.
    Job Template Settings window appears.

12. While creating the first job, click the **Select Template** drop-down menu and select **Brocade MLXe Commands** as the template.

FIGURE 25 Select Template - Brocade MLXe Commands



New Job

Job Template Settings

Configuration Mode: Default Mode

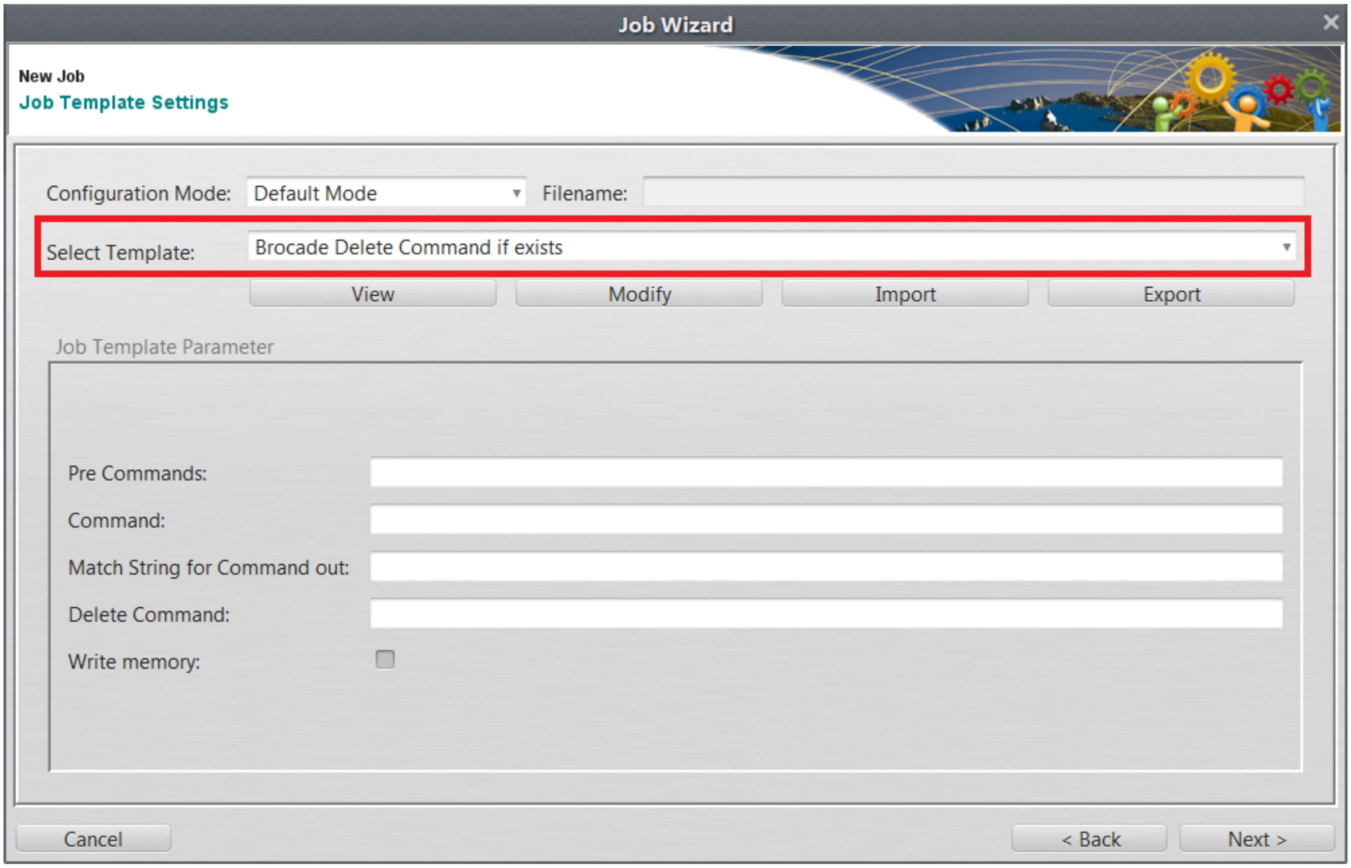
Filename:

Select Template: Brocade MLXe Commands

Commands:

While creating the second job, select **Brocade Delete Command if exists** as the template.

FIGURE 26 Select Template - Brocade Delete Command if exists



Configuration Mode: Default Mode

Filename:

Select Template: Brocade Delete Command if exists

Pre Commands:

Command:

Match String for Command out:

Delete Command:

Write memory: □

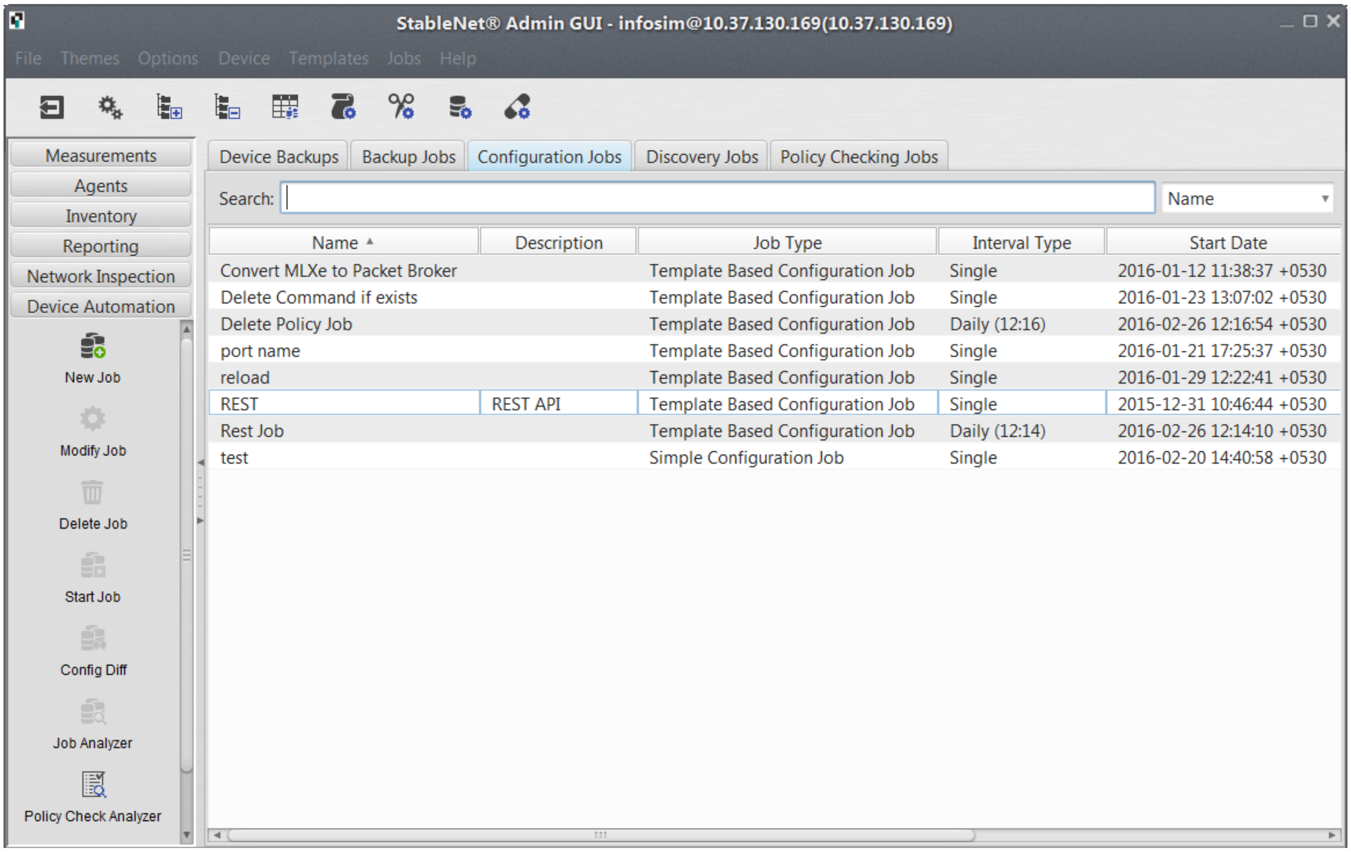
13. Click **Next**.
    Group/Customer Selection window appears.
14. Select the appropriate users and groups, and click **Finish**.

> NOTE
> After creating the first job, repeat the steps above to create a second job. While creating the second job, on the Job Template Settings window (step 12), click the **Select Template** drop-down menu and select **Brocade MLXe Delete Command if exists**.

The two jobs you just created appear in the list of Discovery Jobs.

15. After creating the two jobs, click the **Configuration Jobs** tab.

FIGURE 27 Configuration Jobs

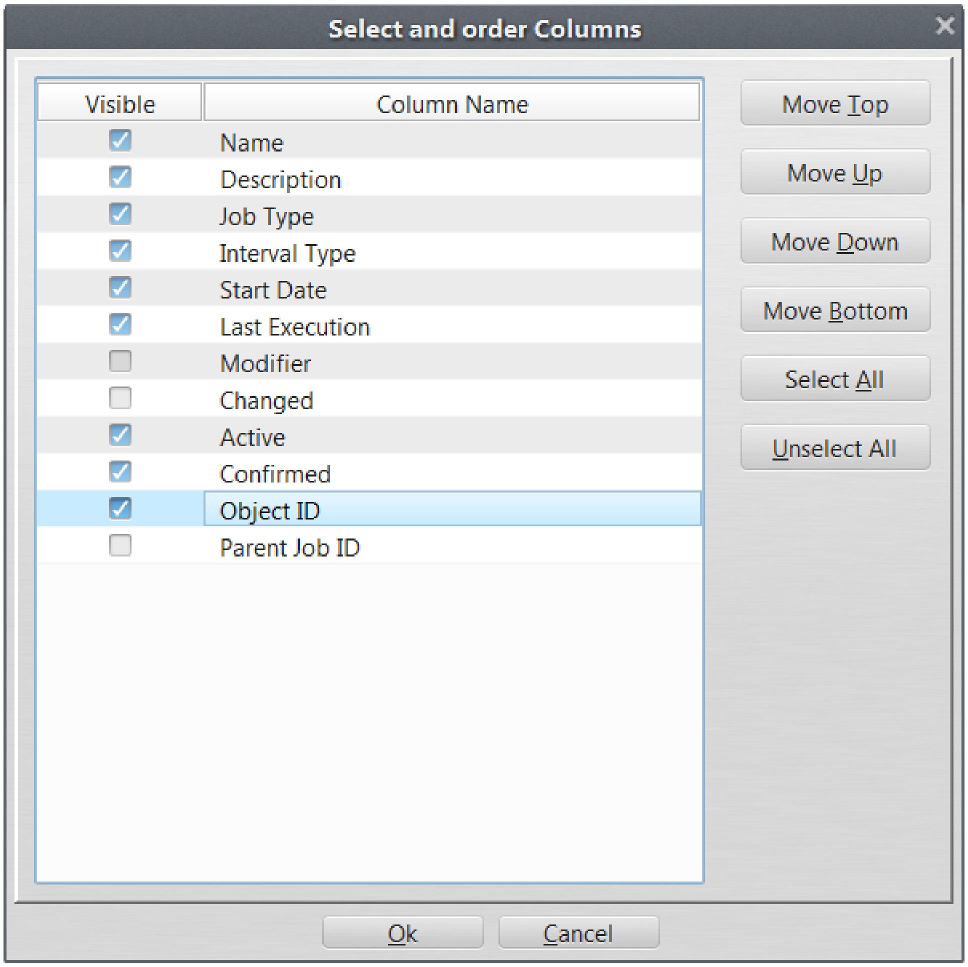


Name ▲	Description	Job Type	Interval Type	Start Date
Convert MLXe to Packet Broker		Template Based Configuration Job	Single	2016-01-12 11:38:37 +0530
Delete Command if exists		Template Based Configuration Job	Single	2016-01-23 13:07:02 +0530
Delete Policy Job		Template Based Configuration Job	Daily (12:16)	2016-02-26 12:16:54 +0530
port name		Template Based Configuration Job	Single	2016-01-21 17:25:37 +0530
reload		Template Based Configuration Job	Single	2016-01-29 12:22:41 +0530
REST	REST API	Template Based Configuration Job	Single	2015-12-31 10:46:44 +0530
Rest Job		Template Based Configuration Job	Daily (12:14)	2016-02-26 12:14:10 +0530
test		Simple Configuration Job	Single	2016-02-20 14:40:58 +0530

16. Right-click any one of the jobs in the list and click **Order Columns**.
The **Select and order Columns** window appears.

17. Click to select the **Object ID** check box and click **Ok**.

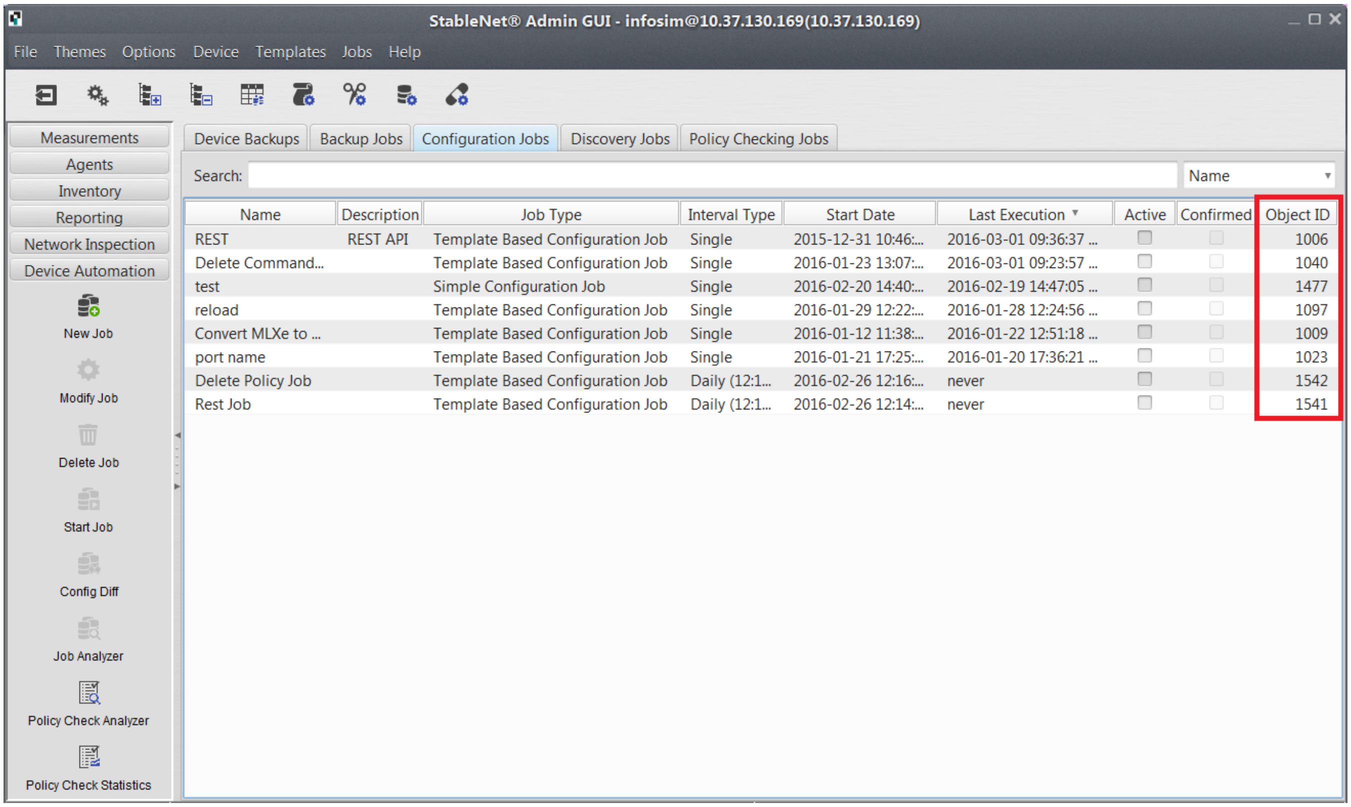
FIGURE 28 Job Template Settings



Visible	Column Name
☑	Name
☑	Description
☑	Job Type
☑	Interval Type
☑	Start Date
☑	Last Execution
□	Modifier
□	Changed
☑	Active
☑	Confirmed
☑	Object ID
□	Parent Job ID

The Configuration Jobs tab now includes the Object ID column.

FIGURE 29 Object ID column



Name	Description	Job Type	Interval Type	Start Date	Last Execution ▼	Active	Confirmed	Object ID
REST	REST API	Template Based Configuration Job	Single	2015-12-31 10:46:...	2016-03-01 09:36:37 ...	□	□	1006
Delete Command...		Template Based Configuration Job	Single	2016-01-23 13:07:...	2016-03-01 09:23:57 ...	□	□	1040
test		Simple Configuration Job	Single	2016-02-20 14:40:...	2016-02-19 14:47:05 ...	□	□	1477
reload		Template Based Configuration Job	Single	2016-01-29 12:22:...	2016-01-28 12:24:56 ...	□	□	1097
Convert MLXe to ...		Template Based Configuration Job	Single	2016-01-12 11:38:...	2016-01-22 12:51:18 ...	□	□	1009
port name		Template Based Configuration Job	Single	2016-01-21 17:25:...	2016-01-20 17:36:21 ...	□	□	1023
Delete Policy Job		Template Based Configuration Job	Daily (12:1...	2016-02-26 12:16:...	never	□	□	1542
Rest Job		Template Based Configuration Job	Daily (12:1...	2016-02-26 12:14:...	never	□	□	1541

Make a note of the Object ID for the two jobs you just created. These values are required while configuring Brocade Visibility Manager App. For more information, see the section Configuring Brocade Visibility Manager App on page 89.

Template Based Configuration Job

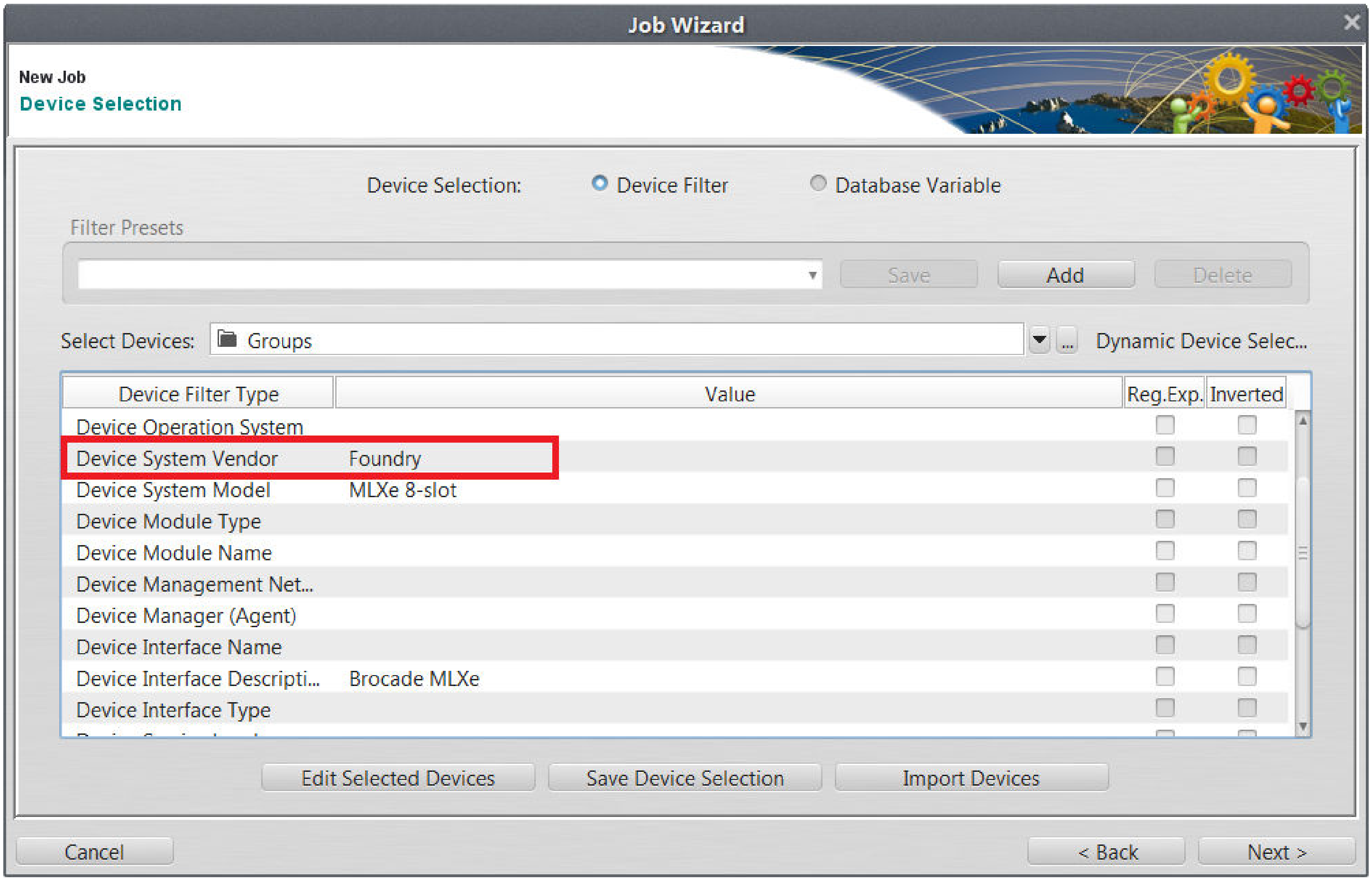
When creating a Template Based Configuration Job, it is possible to filter the devices on which a job will be executed. The job can be applied on a single device or multiple devices based on how the job is created.

To filter devices:

1. On the **Device Selection** window, select **Groups** or a specific device from the **Select Devices** drop-down list.
2. Provide value for various Device Filter Types, such as Device System Model, Device Module Type and so on.

   NOTE
   Change the value of the **Device System Vendor** field to **Foundry**. Leaving this field empty or providing a different value for this field can cause issues with MLXe device detection.

FIGURE 30 Device Selection window



Device Selection: ● Device Filter ○ Database Variable

Filter Presets

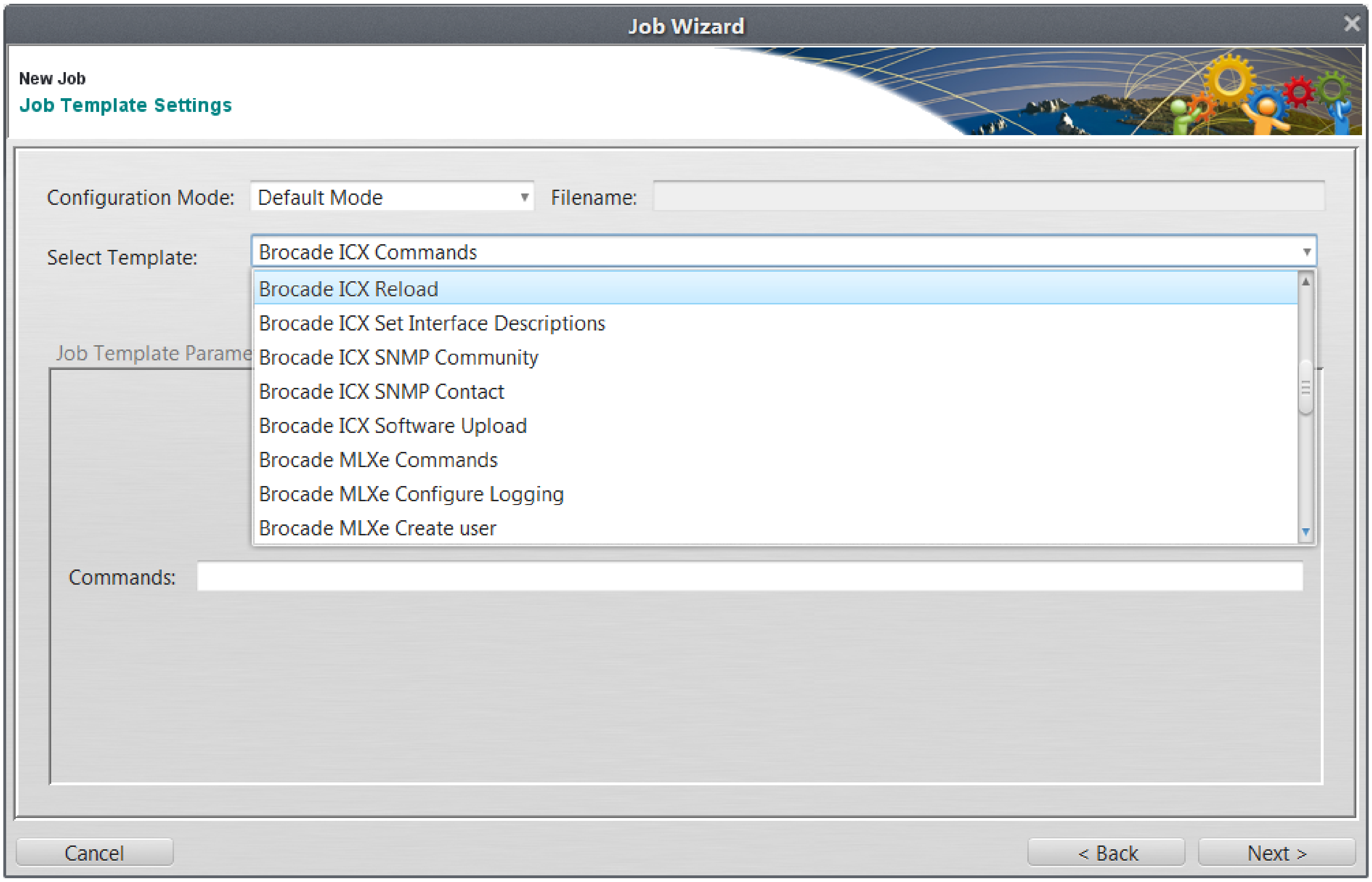
Select Devices: Groups

Dynamic Device Selec...

Device Filter Type	Value	Reg.Exp.	Inverted
Device Operation System		□	□
Device System Vendor	Foundry	□	□
Device System Model	MLXe 8-slot	□	□
Device Module Type		□	□
Device Module Name		□	□
Device Management Net...		□	□
Device Manager (Agent)		□	□
Device Interface Name		□	□
Device Interface Descripti...	Brocade MLXe	□	□
Device Interface Type		□	□

The Job Template Settings window allows you to select a pre-defined template for a job that you would like to perform on the ICX or MLXe devices.

FIGURE 31 Job Template Settings window



Job Wizard

New Job

Job Template Settings

Configuration Mode: Default Mode

Filename:

Select Template: Brocade ICX Commands

Commands:

NOTE

Perform all the remaining steps as outlined in *StableNet® Version 7.5 Back Office Manual*.

List of Brocade-specific templates

Table 1 provides information about all the Brocade-specific templates:

TABLE 1 List of Brocade-specific Templates

Template	Use this template to...
Brocade ICX Commands	Run multiple CLI commands on a specific ICX device or multiple ICX devices. The commands must be separated by semicolons.
Brocade ICX Configure Logging	Enable/disable logging. Provide the following information: • Logging on/off: Use the drop-down menu to enable or disable logging for the options provided. • IP Address: IP address of the machine where logs are to be stored. Logging can be enabled or disabled for the following options: • Enable bfd • CFM

TABLE 1 List of Brocade-specific Templates (continued)

Template	Use this template to...
	- Config Changed - Fan Speed Change - Fan State Change - Link State Change - MGMT Redundance State Change - Module Hot Swap - MPLS Events - MVRP Events - NTP Events - OSPF Events - RSTP Events - SNMP Failure Events - Temperature Error Events - User Login Events - VRRP State Events **Example** - Enabling logging: To enable logging for **Enable bfd**, **CFM**, **Fan Speed Change** and **MVRP Events**, use the drop-down menu to select **On** for **Logging on/off**. Next click to select the check boxes for the relevant options. - Modifying/Disabling logging: To disable logging for an option that was previously enabled, for example **Fan Speed Change**, first use the drop-down menu to select **Off** for **Logging on/off**. Next click to deselect the check boxes for **Enable bfd**, **CFM**, and **MVRP Events**. Ensure that **Fan Speed Change** is selected.
Brocade ICX Create User	Create a new user by providing the following information: - Name - Password - User Privilege Level: – PORT-CONFIG – READ-ONLY – READ-WRITE
Brocade ICX Delete User	Delete a user on the ICX device.
Brocade ICX Enable/Disable an Interface	Enable or disable an Interface, and add the name of the Interface. Use the **Enable** check box to enable or disable the interface.
Brocade ICX Interface Configuration	Enable or disable an interface, add the name and provide a description for the Interface. Use the **Enable** check box to enable or disable the interface.
Brocade ICX Interface IP	Set the Interface IP by providing the following information: - Interface - IP Address - Subnet Mask
Brocade ICX License Update	Update the license using TFTP. Provide the following information: - License Filename - Server IP: IP address of the machine where the license file is located. - Unit: Number of units to apply.
Brocade ICX Reload	Reload the ICX device. Before restarting the ICX device, if you want to save the configuration running on the device, click the **Save Running Config** drop-down menu. and select **Yes**.

TABLE 1 List of Brocade-specific Templates (continued)

Template	Use this template to...
Brocade ICX Set Interface Descriptions	Add the name and provide a description for an Interface.
Brocade ICX SNMP Community	Set or update an SNMP community. Provide the following information: • SNMP Community: This is the community string. • Access: Select **ro** or **rw** from the drop-down menu.
Brocade ICX SNMP Contact	Set or change the SNMP contact information for the ICX device.
Brocade ICX Software Upload	Set or update an SNMP community. Provide the following information: • Manifest Filename • IP TFTP Server: IP address of the machine where the file is located.
Brocade MLXe Commands	Run multiple CLI commands on a specific MLXe device or multiple MLXe devices. The commands must be separated by semicolons.
Brocade MLXe Configure Logging	Enable/disable logging. Provide the following information: • Logging on/off: Use the drop-down menu to enable or disable logging for the options provided. • IP Address: IP address of the machine where logs are to be stored. Logging can be enabled or disabled for the following options: • Enable bfd • CFM • Config Changed • Fan Speed Change • Fan State Change • Link State Change • MGMT Redundance State Change • Module Hot Swap • MPLS Events • MVRP Events • NTP Events • OSPF Events • RSTP Events • SNMP Failure Events • Temperature Error Events • User Login Events • VRRP State Events **Example** • Enabling logging: To enable logging for **Enable bfd**, **CFM**, **Fan Speed Change** and **MVRP Events**, use the drop-down menu to select **On** for **Logging on/off**. Next click to select the check boxes for the relevant options. • Modifying/Disabling logging. To disable logging for an option that was previously enabled, for example **Fan Speed Change**, first use the drop-down menu to select **Off** for **Logging on/off**. Next click to deselect the check boxes for **Enable bfd**, **CFM**, and **MVRP Events**. Ensure that **Fan Speed Change** is selected.
Brocade MLXe Create User	Create a new user by providing the following information: • Name • Password • User Privilege Level: – PORT-CONFIG – READ-ONLY

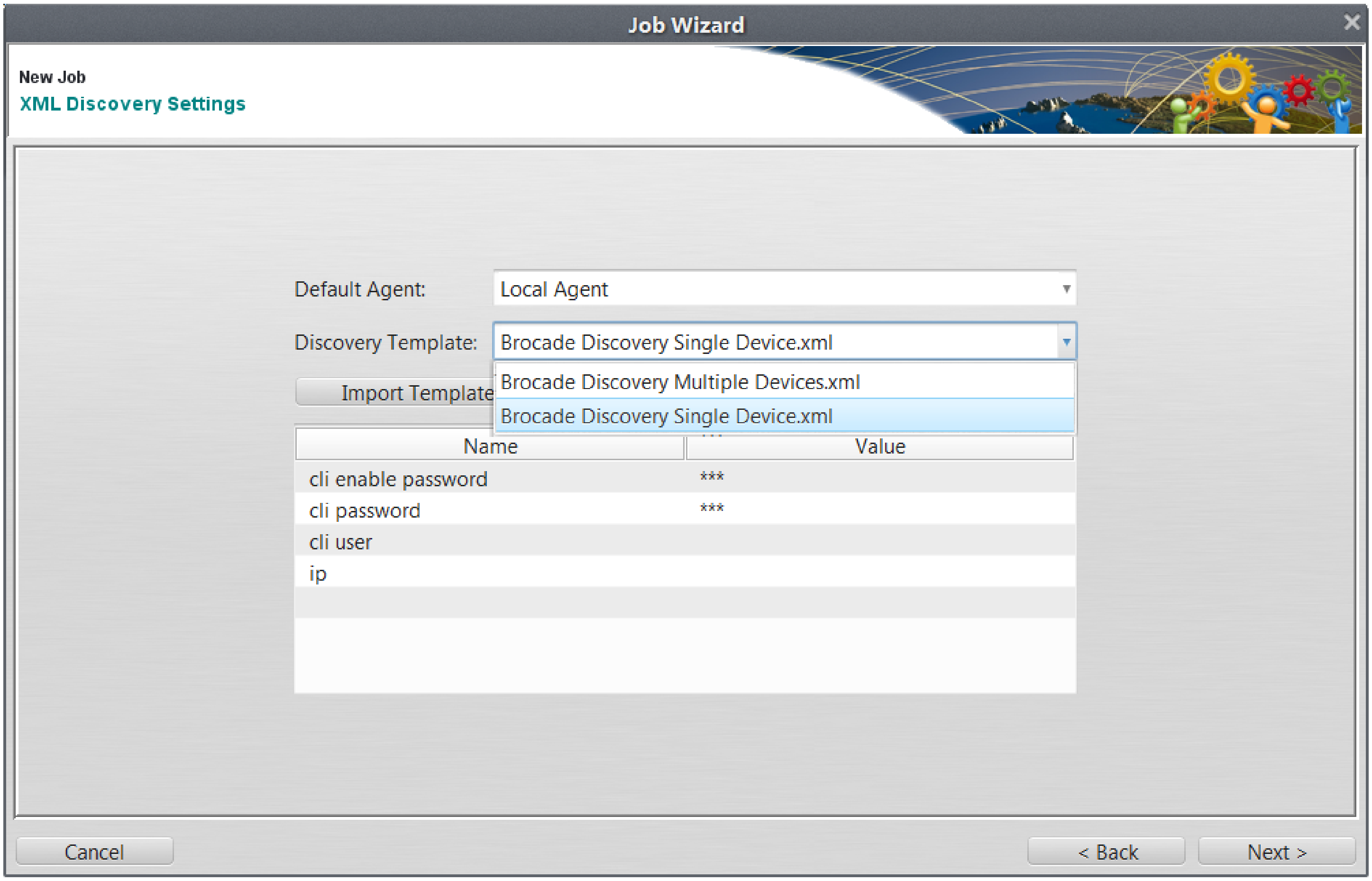
TABLE 1 List of Brocade-specific Templates (continued)

Template	Use this template to...
	– READ-WRITE
Brocade MLXe Delete User	Delete a user.
Brocade MLXe Enable/Disable an Interface	Enable or disable an Interface, and add the name of the Interface. Use the **Enable** check box to enable or disable the interface.
Brocade MLXe Interface Configuration	Enable or disable an interface, add the name and provide a description for the Interface. Use the **Enable** check box to enable or disable the interface.
Brocade MLXe Interface IP	Set the Interface IP by providing the following information: • Interface • IP Address • Subnet Mask
Brocade MLXe License Update	Update the license using TFTP. Provide the following information: • License Filename • Server IP: IP address of the machine where the license file is located. • Unit: Number of units to apply.
Brocade MLXe Modify Interface Description	Modify an interface description by providing the following information: • Interface: Name of the interface • Prefix • Postfix
Brocade MLXe Reload	Reload the MLXe device. Before restarting the MLXe device, if you want to save the configuration running on the device, click the **Save Running Config** drop-down menu. and select **Yes**.
Brocade MLXe Set Interface Descriptions	Add the name and provide a description for an Interface.
Brocade MLXe SNMP Community	Set or update an SNMP community. Provide the following information: • SNMP Community: This is the community string. • Access: Select **ro** or **rw** from the drop-down menu.
Brocade MLXe SNMP Contact	Set or change the SNMP contact information for the MLXe device.
Brocade MLXe Software Upload	Set or update an SNMP community. Provide the following information: • Manifest Filename • IP TFTP Server: IP address of the machine where the file is located.
Brocade MLXe Delete Command if exists	This is a Brocade Visibility Manager-specific custom template. Do not configure this template.
Configure MLXe as Packet Broker	Configure an MLXe as a Packet Broker. This template performs some basic configuration on the MLXe to configure it as a Packet Broker.

XML discovery job

XML Discovery Job option allows you to select a pre-defined template for a job that you would like to perform on the ICX or MLXe devices.

FIGURE 32 XML Discovery Settings



Job Wizard

New Job

XML Discovery Settings

Default Agent: Local Agent

Discovery Template: Brocade Discovery Single Device.xml

Brocade Discovery Multiple Devices.xml
Brocade Discovery Single Device.xml
Import Template
Cancel
< Back
Next >

Name	Value
cli enable password	***
cli password	***
cli user	
ip	

List of Brocade-specific XML discovery templates

To run an XML Discovery, it is necessary to create an XML Discovery Job in the Device Automation theme.

Table 1 provides information about all the Brocade-specific XML Discovery Templates:

TABLE 2 List of Brocade-specific XML Discovery Templates

Template	Use this template to...
Brocade Discovery Single Device	Discover a single device. Provide the following information: • CLI Enable Password • CLI Password • CLI User • IP: IP address of the device to be discovered
Brocade Discovery Multiple Devices	Discover multiple devices. Modify the `Brocade Discovery.csv` file to add all IP addresses.

TABLE 2 List of Brocade-specific XML Discovery Templates (continued)

Template	Use this template to...
	To add multiple devices for discovery: 1. After adding the job, on the **Device Automation** theme, click the **Discovery Jobs** tab. 2. Select the job you just created and click **Modify Job**. 3. On the **Job Wizard** window, click the **XML Discovery Settings** tab. 4. Click **Manage CSV Files** button. 5. On the **CSV Data Manager** window, ensure that Brocade Discovery.csv file is selected and click **Export** to save the file to a local directory. 6. After exporting the CSV file, open the file and add the following information for each device: • IP: IP address of the device to be discovered • CLI User • CLI Password • CLI Enable Password Ensure that the information is in the following format: `ip;cliuser;clipassword;clienable;clitype` 7. Save the file. 8. On the **CSV Data Manager** window, click **Import** to import the CSV file you just modified. 9. Click **Yes** to overwrite the existing file. 10. Click **Close** to close the CSV Import window. 11. Click **Close** to close the CSV Data Manager.

Network discovery

A simple XML Discovery Job can be created using the Network Discovery wizard available in the Inventory Theme. A job created using this wizard is added to Discovery Job tab in the Device Automation Theme, and the CSV and XML file is added to the config/discovery directory of the StableNet® Server.

To create a new discovery job, go the Inventory theme and click **Create Discovery Job**. Select the StableNet® Client Agent that will execute the discovery, and provide a name and description for the job. In addition, select one of the following discovery types:

- **Subnet Discovery**: This option discovers a network based on an IP address and a subnet mask. Multiple networks can be discovered in one Discovery Job.

  NOTE
  The selected StableNet® Agent must be able to access the specified networks.

- **Range Discovery**: This option discovers a given IP address range. Multiple ranges can be discovered in one Discovery Job.

  NOTE
  The selected StableNet® Agent must be able to access the specified ranges.

- **CSV File**: This option discovers IP addresses imported from a CSV file. The CSV file needs a header and values separated by ";".
- **Host File**: This options discovers IP addresses imported from an ASCII file (such as, hosts file).

For more information about Network Discovery, see the section 'Network Discovery and Re-Discovery' in *StableNet® Version 7.5 Back Office Manual.*

Rediscovering devices

Rediscovering devices is useful for updating measurements and to keep track of changing hardware on the devices. Executing rediscovery job is mandatory in the following cases:

- ACL/Filter added on MLXe or ICX devices.
- SNMP location update/removed.

If there are changes to the SNMP location, perform the following steps:

1. Telnet to the ICX or MLXe device.
2. Run the following command to remove the old system location string:

   ```
   no snmp-server location text
   ```

   Example

   ```
   snmp-server location blr|6
   ```

3. Run the following command to set the new system location string:

   ```
   snmp-server location text
   ```

   Example

   ```
   snmp-server location blr|7
   ```

4. Run the following command to save the current running configuration information to the startup configuration file:

   ```
   write memory
   ```

   For more information about this command, see the section ‘write memory’ in *Brocade NetIron Command Reference.*
5. Login to StableNet®.
6. Go to **Device Automation** Theme.
7. Click **Discovery Job**
8. Click to select on of the following options:
   - **ICX Discovery** for ICX devices.
   - **MLXe Discovery** for MLXe devices.
9. Click **Start Job**.

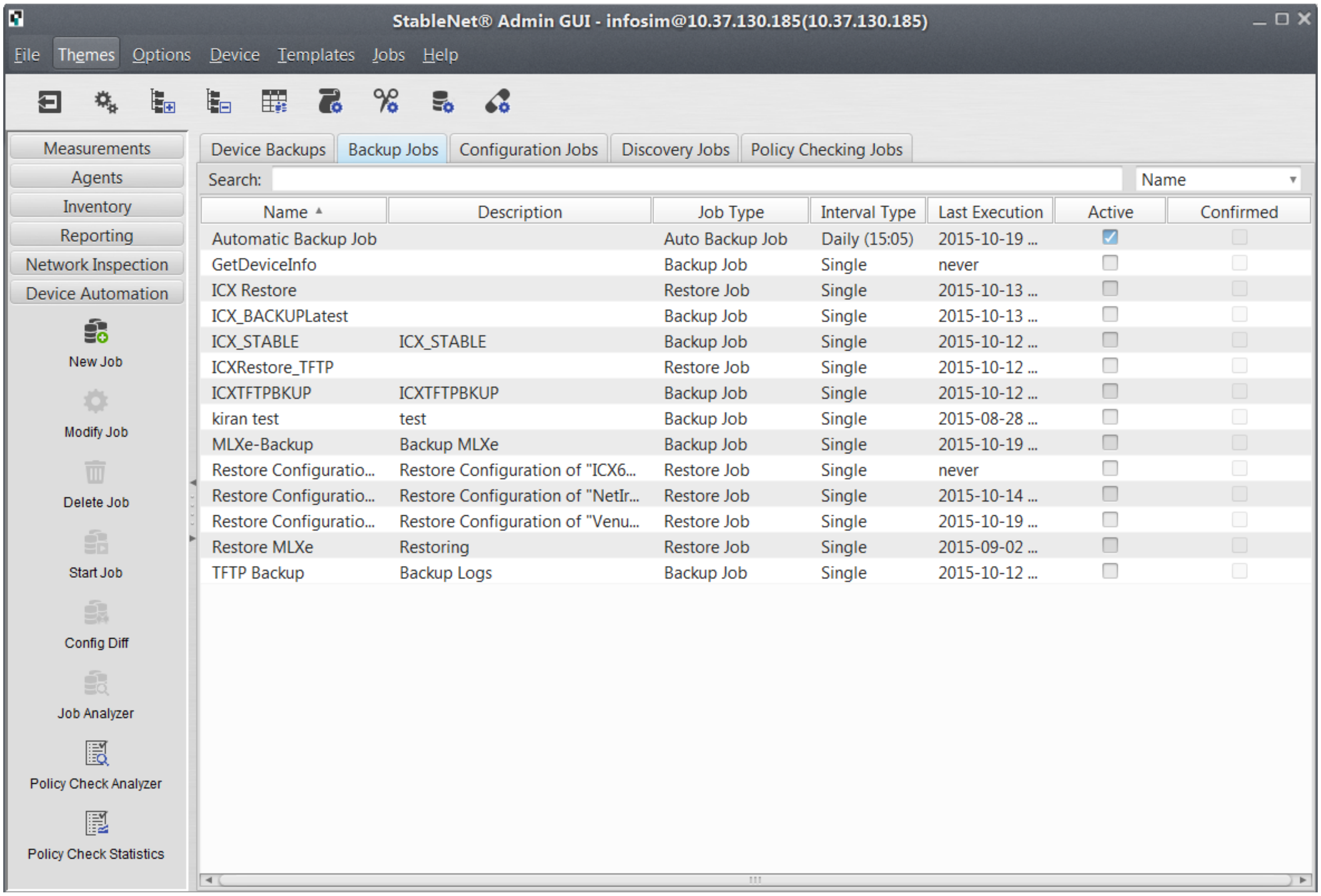
NOTE
For discovering newly added ACLs/Filters on MLXe or ICX devices, follow step 5 to step 9.

Backup and restore

The configuration of MLXe and ICX devices can be backed up in StableNet® by running a Backup Job. In addition, it is possible to restore a backup to a device. Backup Jobs and Restore Jobs are created using the Device Automation theme in the StableNet® GUI. For more information, see the section ‘Backup and Restore’ in *StableNet® Version 7.5 Back Office Manual.*

Note that to execute backup jobs on MLXe and ICX devices, the Automatic Backup Job option in the Backup Jobs tab must be set to Active.

FIGURE 33 Automatic Backup Job



Name ▲	Description	Job Type	Interval Type	Last Execution	Active	Confirmed
Automatic Backup Job		Auto Backup Job	Daily (15:05)	2015-10-19 ...	☑	□
GetDeviceInfo		Backup Job	Single	never	□	□
ICX Restore		Restore Job	Single	2015-10-13 ...	□	□
ICX_BACKUPLatest		Backup Job	Single	2015-10-13 ...	□	□
ICX_STABLE	ICX_STABLE	Backup Job	Single	2015-10-12 ...	□	□
ICXRestore_TFTP		Restore Job	Single	2015-10-12 ...	□	□
ICXTFTPBKUP	ICXTFTPBKUP	Backup Job	Single	2015-10-12 ...	□	□
kiran test	test	Backup Job	Single	2015-08-28 ...	□	□
MLXe-Backup	Backup MLXe	Backup Job	Single	2015-10-19 ...	□	□
Restore Configuratio...	Restore Configuration of "ICX6...	Restore Job	Single	never	□	□
Restore Configuratio...	Restore Configuration of "NetIr...	Restore Job	Single	2015-10-14 ...	□	□
Restore Configuratio...	Restore Configuration of "Venu...	Restore Job	Single	2015-10-19 ...	□	□
Restore MLXe	Restoring	Restore Job	Single	2015-09-02 ...	□	□
TFTP Backup	Backup Logs	Backup Job	Single	2015-10-12 ...	□	□

Measurements

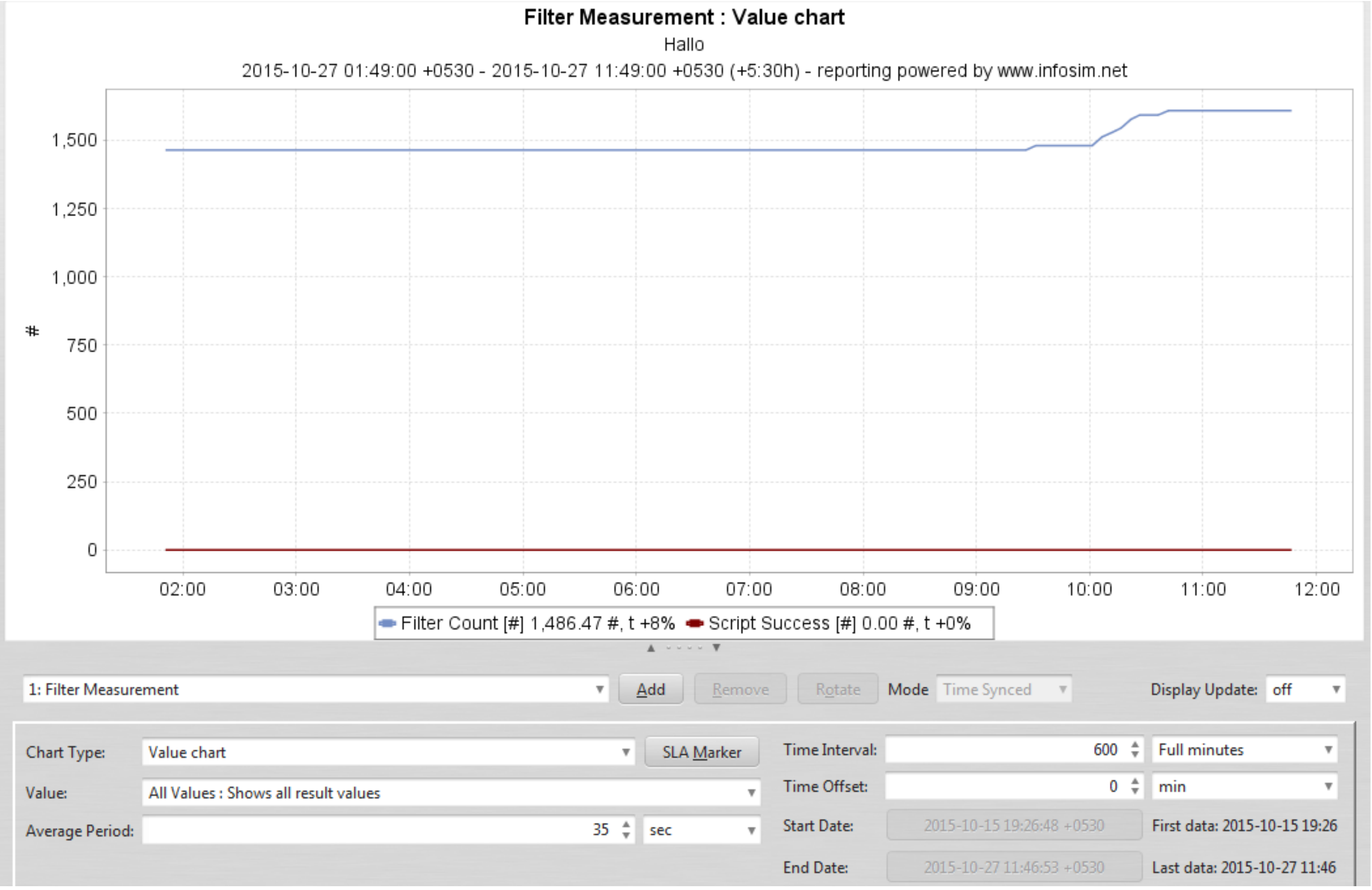
A measurement is a recurring measurement job that is configured to acquire data from one of the devices. Measurements collect data that can be used later, for example, for performance analysis or to get notified if the system is not working as expected.

The Brocade plugin includes specific measurements for the following groups:

- **Filters**: Plot measurements for traffic, and run analyzer jobs on hit rates and miss rates.
- **Modules**: Plot measurements and graphs for various modules (see “Modules - Chart”).
- **Optical**: Analyze temperature and power for each device. Check the levels at which a device is working.
- **Interfaces**: Plot measurements and graphs for all the listed interfaces.

The figure below shows an sample chart plotted for a module:

FIGURE 34 Filter - Chart


Filter Measurement : Value chart
Hallo
2015-10-27 01:49:00 +0530 - 2015-10-27 11:49:00 +0530 (+5:30h) - reporting powered by www.infosim.net
#
1,500
1,250
1,000
750
500
250
0
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
Filter Count [#] 1,486.47 #, t +8%
Script Success [#] 0.00 #, t +0%
Add
Remove
Rotate
SLA Marker

1: Filter Measurement

Mode: Time Synced

Display Update: off

Chart Type: Value chart

Value: All Values : Shows all result values

Average Period: 35 sec

Time Interval: 600 Full minutes

Time Offset: 0 min

Start Date: 2015-10-15 19:26:48 +0530

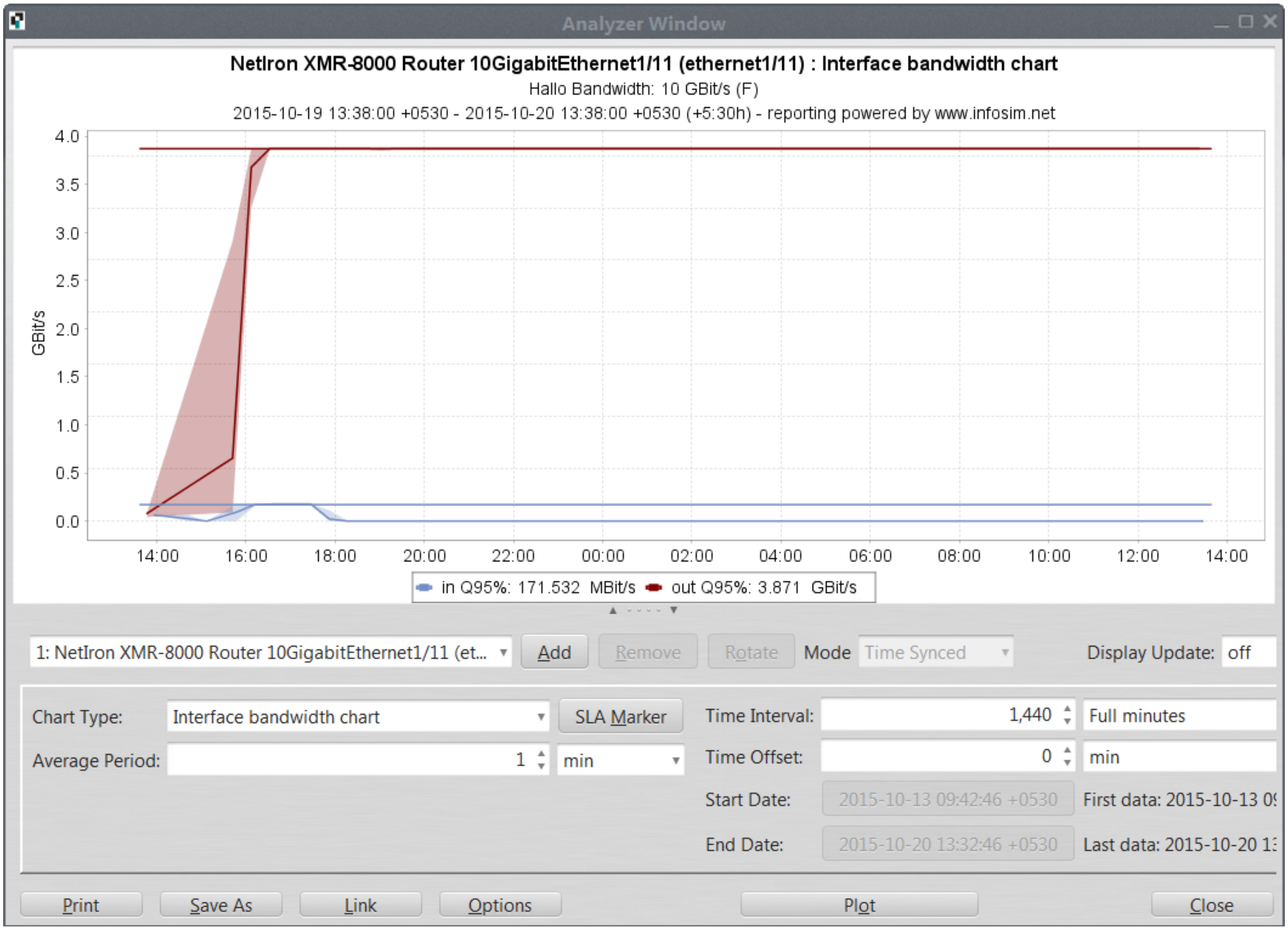
First data: 2015-10-15 19:26

End Date: 2015-10-27 11:46:53 +0530

Last data: 2015-10-27 11:46

The figure below shows an sample chart plotted for a module:

FIGURE 35 Module - Chart



NetIron XMR-8000 Router 10GigabitEthernet1/11 (ethernet1/11) : Interface bandwidth chart

Hallo Bandwidth: 10 GBit/s (F)

2015-10-19 13:38:00 +0530 - 2015-10-20 13:38:00 +0530 (+5:30h) - reporting powered by www.infosim.net

in Q95%: 171.532 MBit/s out Q95%: 3.871 GBit/s

1: NetIron XMR-8000 Router 10GigabitEthernet1/11 (et...

Mode: Time Synced

Display Update: off

Chart Type: Interface bandwidth chart

Average Period: 1 min

Time Interval: 1,440 Full minutes

Time Offset: 0 min

Start Date: 2015-10-13 09:42:46 +0530 First data: 2015-10-13 0

End Date: 2015-10-20 13:32:46 +0530 Last data: 2015-10-20 1

NOTE

By default it takes about 25 minutes to plot a graph.

For more information about measurements, see the section 'Measurements Theme' in *StableNet® Version 7.5 User Manual.*

Part C - Brocade Visibility Manager App for MLXe

Getting Started with Brocade Visibility Manager App

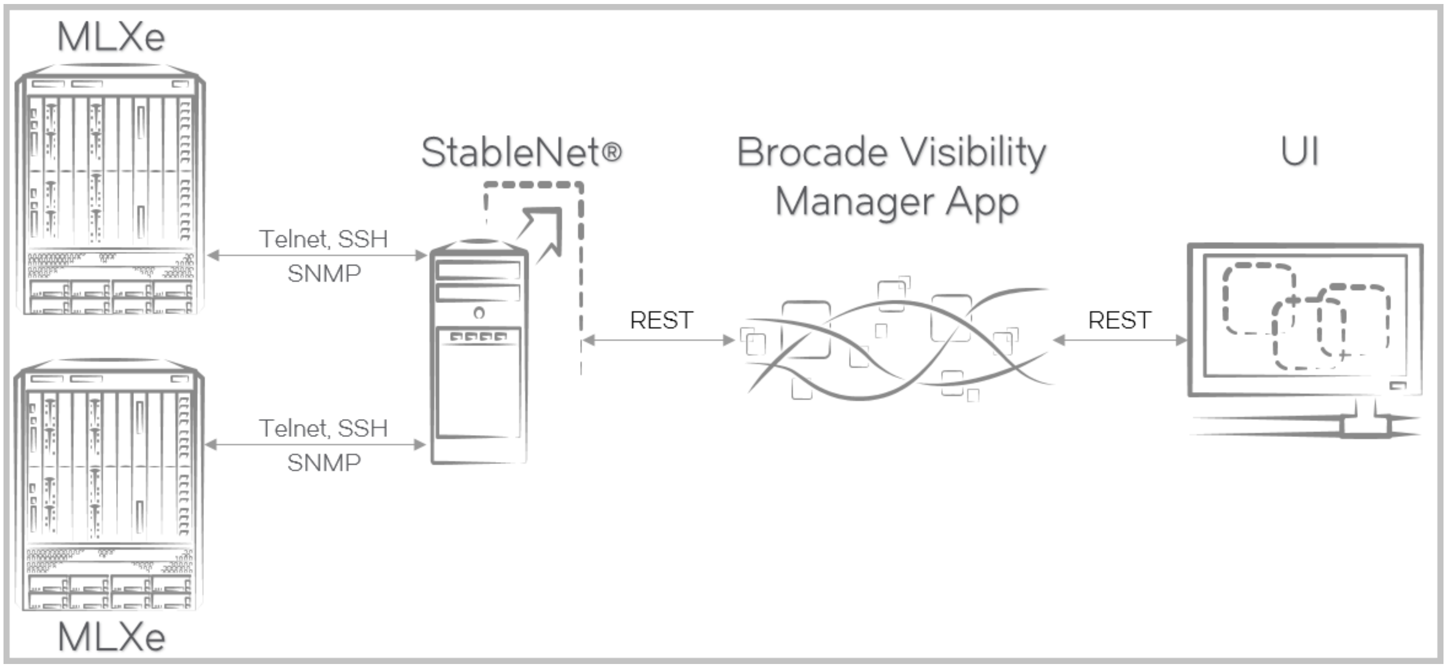
Introduction

Brocade Visibility Manager App is a Web application that provides several options for configuring Brocade network packet brokers.

Brocade Visibility Manager App can be used to:

- Enable and disable ports
- Configure ports as Ingress or Egress
- Create Port Groups for Load Balance
- Create filter rule definitions based on L2-L4 criteria
- Create Load Balance policies
- View device configuration

FIGURE 36 Brocade Visibility Manager App Flow



Brocade Visibility Manager App Installation

This section provides information about installing Brocade Visibility Manager App.

This section includes the following subsections:

- Pre-installation Steps on page 86
- Installing Brocade Visibility Manager App on page 86
- Verifying Installation of Brocade Visibility Manager App on page 87
- Uninstalling Brocade Visibility Manager App on page 88

Pre-installation Steps

Before installing Brocade Visibility Manager App, perform the following pre-installation steps:

> NOTE
> Brocade Visibility Manager App is hosted on the same server as StableNet®[1]. For information about the system requirements for installing and running StableNet®, see *StableNet® Version 7.5 Admin Manual*.

1. Install and configure the StableNet® server and agent. For more information, see *StableNet® Version 7.5 Admin Manual*.
2. Install Java Runtime Environment (JRE):
   a) Download the file `jre-8u51-linux-x64.rpm` from http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html.
   b) Run the following command to install JRE:

```
rpm -ivh jre-8u51-linux-x64.rpm
```

> NOTE
> After installing Java, make sure to set default Java version. For more information, click the following URL: https://access.redhat.com/documentation/en-US/JBoss_Enterprise_Web_Platform/5/html/Installation_Guide/sect-use_alternatives_to_set_default_JDK.html

   c) Run the `java -version` command to verify if the Java version is `jre1.8.0_51`.
3. If you are reinstalling the Brocade Visibility Manager App, make sure to backup the Brocade Visibility Manager database before reinstalling the App. For more information, see the section Brocade Visibility Manager App Database Backup and Restore on page 23.

   To perform a fresh installation of the Brocade Visibility Manager database, skip to the section Installing Brocade Visibility Manager App on page 86.

Installing Brocade Visibility Manager App

Perform the following steps to install Brocade Visibility Manager App:

> NOTE
> It is recommended that you do not download or install the installation files in the `/root` folder.

1. Go to the location where the Brocade Visibility Manager App installation files were downloaded.

2. Run the following command:

   ```
   rpm -ivh bvm-1.1.1-0.el6.x86_64.rpm
   ```

   Example

   ```
   # rpm -ivh bvm-1.1.1-0.el6.x86_64.rpm
   Preparing...                          ################################# [100%]
   Updating / installing...
      1:bvm-1.1.1-0.el6                 ################################# [100%]
   Created symlink from /etc/systemd/system/bvm.service to /usr/lib/systemd/system/bvm.service.
   Created symlink from /etc/systemd/system/multi-user.target.wants/bvm.service to /usr/lib/systemd/
   system/bvm.service.
   ```

3. Go to the `/opt/brocade/bin` directory and execute the following command:

   ```
   sh install_bvm.sh
   ```

   NOTE
   During the installation, a new database/schema called `bvm` is created in the MySQL server. You will be prompted for MySQL root password.

   Example

   ```
   sh install_bvm.sh
   Enter MySQL root password: *********

   *******************************************************
   Creating the BVM database username and password...
   *******************************************************
   Warning: Using a password on the command line interface can be insecure.
   bvm database creation complete.
   Warning: Using a password on the command line interface can be insecure.
   Warning: Using a password on the command line interface can be insecure.
   *******************************************************
   *******************************************************
   Performing the BVM database setup...
   *******************************************************
   *******************************************************
   BVM database setup complete.
   *******************************************************
   ```

Brocade Visibility Manager App installation is now complete.

Verifying Installation of Brocade Visibility Manager App

Run the following command to verify the installation of Brocade Visibility Manager App:

```
rpm -qa | grep bvm
```

If the installation is successful, full version of the Brocade Visibility Manager App RPM is displayed.

Example

```
# rpm -qa | grep bvm
bvm-1.1.1-0.el6.x86_64
```

NOTE
If the installation is unsuccessful, no message is displayed.

Uninstalling Brocade Visibility Manager App

Perform the following steps to uninstall Brocade Visibility Manager App:

1. Run the following command to stop all the Brocade Visibility Manager App processes:

   ```
   service bvm stop
   ```

2. Run the following commands to verify if all the processes have stopped:

   ```
   ps -ef | grep bvm
   ```

   ```
   ps -ef | grep start-ux
   ```

3. Next, run the following command to uninstall Brocade Visibility Manager App:

   ```
   rpm -e bvm
   ```

   NOTE
   While uninstalling Brocade Visibility Manager App, you will be prompted for MySQL root password.

   Example

   ```
   # rpm -e bvm
   Enter MySQL root password: *********

   Existing bvm database will be deleted. Please backup if you need to retain data. Do you want to
   continue delete (y/n)?
   Warning: Using a password on the command line interface can be insecure.
   bvm database does not exist.
   BVM DB Cleanup is completed successfully,BVM RPM uninstallation success.
   Removed symlink /etc/systemd/system/multi-user.target.wants/bvm.service.
   Removed symlink /etc/systemd/system/bvm.service.
   ```

Brocade Visibility Manager App Configuration

Configuring Brocade Visibility Manager App

After installing Brocade Visibility Manager App, perform the following steps to configure it:

> NOTE
> Before performing the steps below, login to StableNet® and create the two Template Based Configuration Jobs as outlined in the section Creating Jobs for Brocade Visibility Manager App on page 61.

1. Go to the `/opt/brocade/bvm/current/config/bems-api` directory.
2. Open the file `application.properties` and make the following changes:
   - Change the value of `stablenet.resource-url.jobs.jobid` to the Object ID for the job **Brocade MLXe commands**.
   - Change the value of `stablenet.resource-url.jobs.deletejobid` to the Object ID for the job **Brocade MLXe Delete Command if exists**.

     > NOTE
     > For more information about the Object IDs for the two jobs, see steps 15 to 17 in the section Creating Jobs for Brocade Visibility Manager App on page 61.

   - Change the value of `stablenet.rest.base-url` to the StableNet® URL.
3. Save file and exit.

> NOTE
> All Brocade Visibility Manager logs are saved as `bvm.log` and `bvmapp.log` in the `/var/log` directory.

Changing Default Port for Brocade Visibility Manager App

The default port for accessing Brocade Visibility Manager App is 9286 . If you want to change the port, perform the following steps:

> NOTE
> Perform these steps only if you want to change the default port.

1. Run the following command to stop Brocade Visibility Manager App processes:

```
service bvm stop
```

2. Run the following command to change the port:

   ```
   export GRK_UX_HTTP_PORT=<port_number>
   ```

   Example

   ```
   export GRK_UX_HTTP_PORT=9002
   ```

3. Go to the `/opt/brocade/bvm/current/config/bems-api` directory.
4. Open the file `application.properties` and change the value of `access.control.allow.origin` to the new port number.

   Example

   ```
   access.control.allow.origin=http://localhost:9002
   ```

5. Run the following command to start Brocade Visibility Manager App processes:

   ```
   service bvm start
   ```

Starting Brocade Visibility Manager App Processes

After configuring Brocade Visibility Manager App, perform the following steps:

NOTE
Ensure that the StableNet® Server is running before performing the following steps.

1. Run the following command to start Brocade Visibility Manager App processes:

   ```
   service bvm start
   ```

   Example

   ```
   # service bvm start
   Redirecting to /bin/systemctl start  bvm.service
   ```

   NOTE
   The Brocade Visibility Manager App processes must be started whenever the system is rebooted.

2. Run the following command to verify if all processes are running:

   ```
   service bvm status
   ```

   Example

```
# service bvm status
Redirecting to /bin/systemctl status  bvm.service
 bvm.service - BVM
   Loaded: loaded (/usr/lib/systemd/system/bvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2016-02-05 11:40:32 IST; 7s ago
  Process: 3950 ExecStart=/usr/lib/systemd/scripts/bvm.sh start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/bvm.service
           ├─3968 java -jar /opt/brocade/bvm/current/app/bems-api/libs/bems-api-1.0.0.jar --
spring.config.location=/opt/brocade/bvm/current/config/bems-api/application.properties,/opt/br...
           └─3983 /opt/brocade/oss/node-v0.12.7-linux-x64/bin/node start-ux.js

Feb 05 11:40:32 VM-131.210 systemd[1]: Starting BVM...
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: *******************************************************
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: Starting the BVM 1.1.0-0 Application
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: *******************************************************
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: Starting BVM API Application
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: Starting BVM UI Application
Feb 05 11:40:32 VM-131.210 bvm.sh[3950]: *******************************************************
Feb 05 11:40:32 VM-131.210 systemd[1]: Started BVM.
Feb 05 11:40:36 VM-131.210 systemd[1]: Started BVM.
```

   NOTE

   - To stop Brocade Visibility Manager App processes, run the `service bvm stop` command.
   - To restart Brocade Visibility Manager App processes, run the `service bvm restart` command.

Users and Group Rights Management

All user credentials are validated against the StableNet® server. A user with access to a device will have access to all its ports. Brocade Visibility Manager will filter ports for a user based on the measurements that the user can access.

To support port-level RBAC, StableNet® administrator must provide users access to view the measurements for that port. In addition, the administrator can control user group rights for all devices. For more information, see the section Groups and users on page 47.

Brocade Visibility Manager App Database Backup and Restore

This section provides information about backing up and restoring Brocade Visibility Manager App database.

This section contains the following subsections:

- Backing up Brocade Visibility Manager Database on page 23
- Restoring Brocade Visibility Manager Database on page 24

Backing up Brocade Visibility Manager Database

Perform the following steps to backup Brocade Visibility Manager App database.

1. Run the following command to stop all Brocade Visibility Manager App processes:

   ```
   service bvm stop
   ```

2. Go to the `/opt/brocade/bin` directory.
3. Run the following command to backup the Brocade Visibility Manager database:

   `sh bvm_db_manager.sh backup`

   NOTE
   You will be prompted for MySQL root password.

Example

```
sh bvm_db_manager.sh backup
Enter MySQL root password: *********

*******************************************************
Performing BVM DB backup...
*******************************************************
Warning: Using a password on the command line interface can be insecure.
bvm.sql.20160205 created in /tmp/backup.
-rw-r--r-- 1 root root 18683 Feb  5 11:51 bvm.sql.20160205
*******************************************************
BVM DB backup compeleted.
*******************************************************
```

NOTE

- The backup files are stored in the `/tmp/backup` directory. To change the location, open the file `configuration.properties` located at `/opt/brocade/bin` and change the value of the parameter `backup_location`.
- Run the `sh bvm_db_manager.sh cleanup` command to cleanup the Brocade Visibility Manager database.

Restoring Brocade Visibility Manager Database

Perform the following steps to restore the Brocade Visibility Manager App database.

NOTE
Use restore as a disaster recovery option only. Restoring the database can cause issues if there is a mismatch between device data and Brocade Visibility Manager App database.

1. Run the following command to stop all Brocade Visibility Manager App processes:

   `service bvm stop`
2. Go to the `/opt/brocade/bin` directory.

3. Run the following command to restore the Brocade Visibility Manager database:

   `sh bvm_db_manager.sh restore`

   NOTE
   You will be prompted for MySQL root password.

Example

```
sh bvm_db_manager.sh restore
Enter MySQL root password: *********

Please enter the backup file name to be restored (bvm.sql.yyyymmdd):bvm.sql.20160205
bvm.sql.20160205
Warning: Using a password on the command line interface can be insecure.
*******************************************************
Creating and restoring the BVM database from the bvm.sql.20160205
*******************************************************
sh: /usr/brocade/bin/create_bvm_db.sh: No such file or directory
Warning: Using a password on the command line interface can be insecure.
ERROR 1049 (42000): Unknown database 'bvm'
*******************************************************
Restoring the BVM database from bvm.sql.20160205 completed.
*******************************************************
```

NOTE
The backup files used for restoring the Brocade Visibility Manager database are stored in the `/tmp/backup` directory. To change the location, open the file `configuration.properties` located at `/opt/brocade/bin` and change the value of the parameter `restore_location`.

Accessing Brocade Visibility Manager App

NOTE
This version of Brocade Visibility Manager App supports the following Web browsers:

- Chrome 48.0.2564.82 m and above
- Firefox 43.0.4 and above

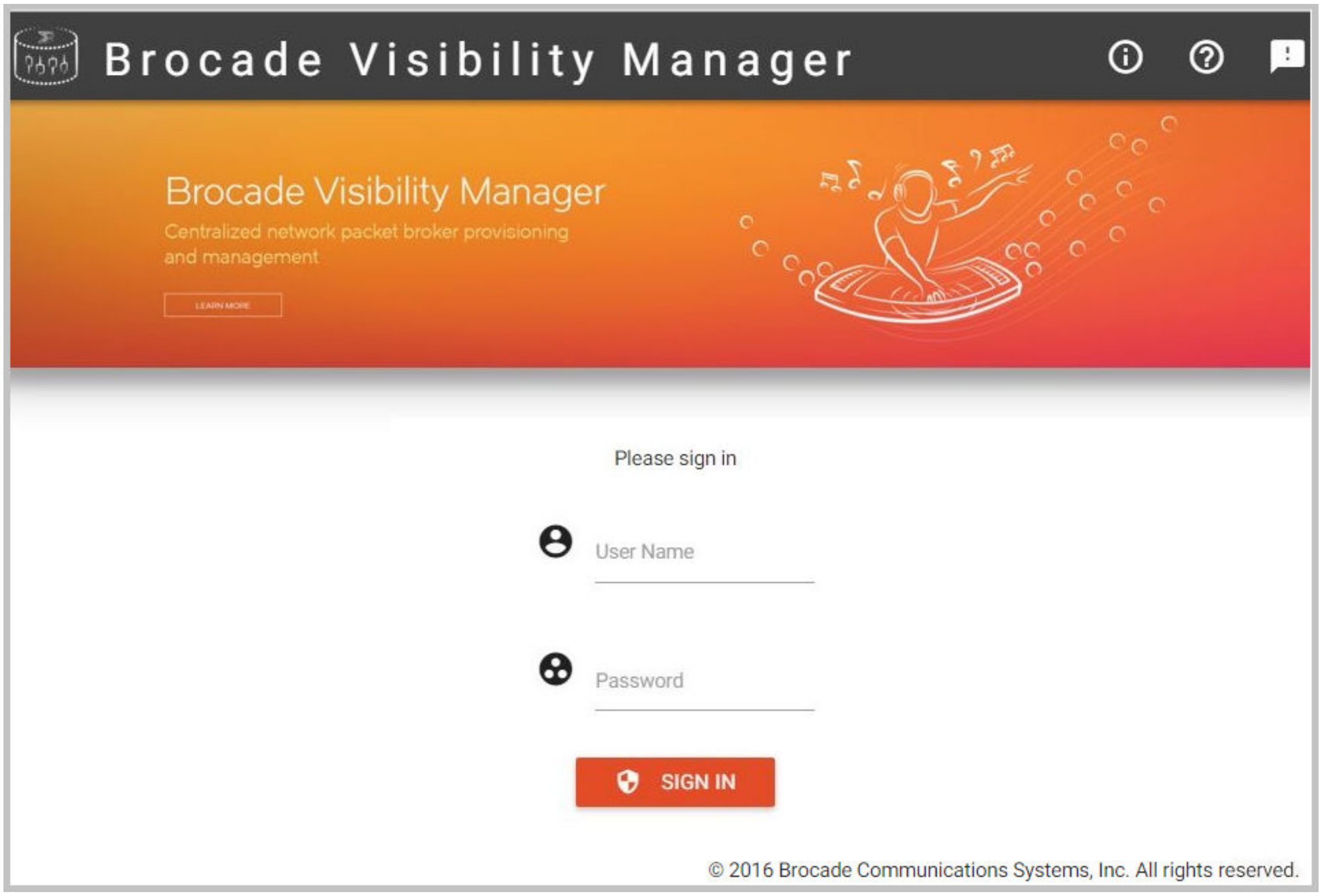
Perform the following steps to access Brocade Visibility Manager App:

1. Open a Web browser and enter the Brocade Visibility Manager App URL.

   NOTE
   For information about configuring this URL to access Brocade Visibility Manager App, see the section Configuring Brocade Visibility Manager App on page 89.

2. The Brocade Visibility Manager App login screen appears.

FIGURE 37 Brocade Visibility Manager App login page



Brocade Visibility Manager

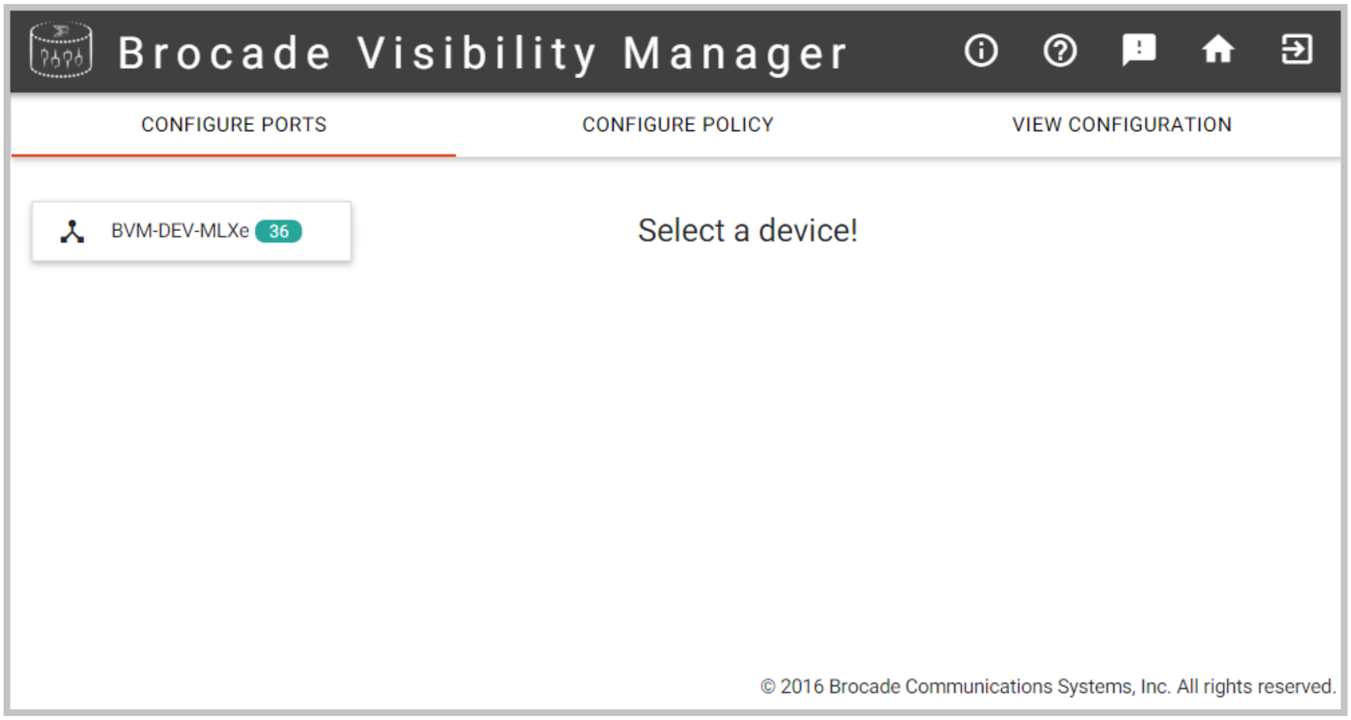
Centralized network packet broker provisioning and management

Please sign in

© 2016 Brocade Communications Systems, Inc. All rights reserved.

3. Enter your StableNet® user name and password, and click **SIGN IN**.
4. The Brocade Visibility Manager App home page appears.

FIGURE 38 Brocade Visibility Manager App home page



Select a device!

© 2016 Brocade Communications Systems, Inc. All rights reserved.

Linking Brocade Visibility Manager App and StableNet®

It is possible to create a link to Brocade Visibility Manager App from StableNet®. This link can be used to access Brocade Visibility Manager App using StableNet® .

Perform the following steps to link Brocade Visibility Manager App and StableNet®:

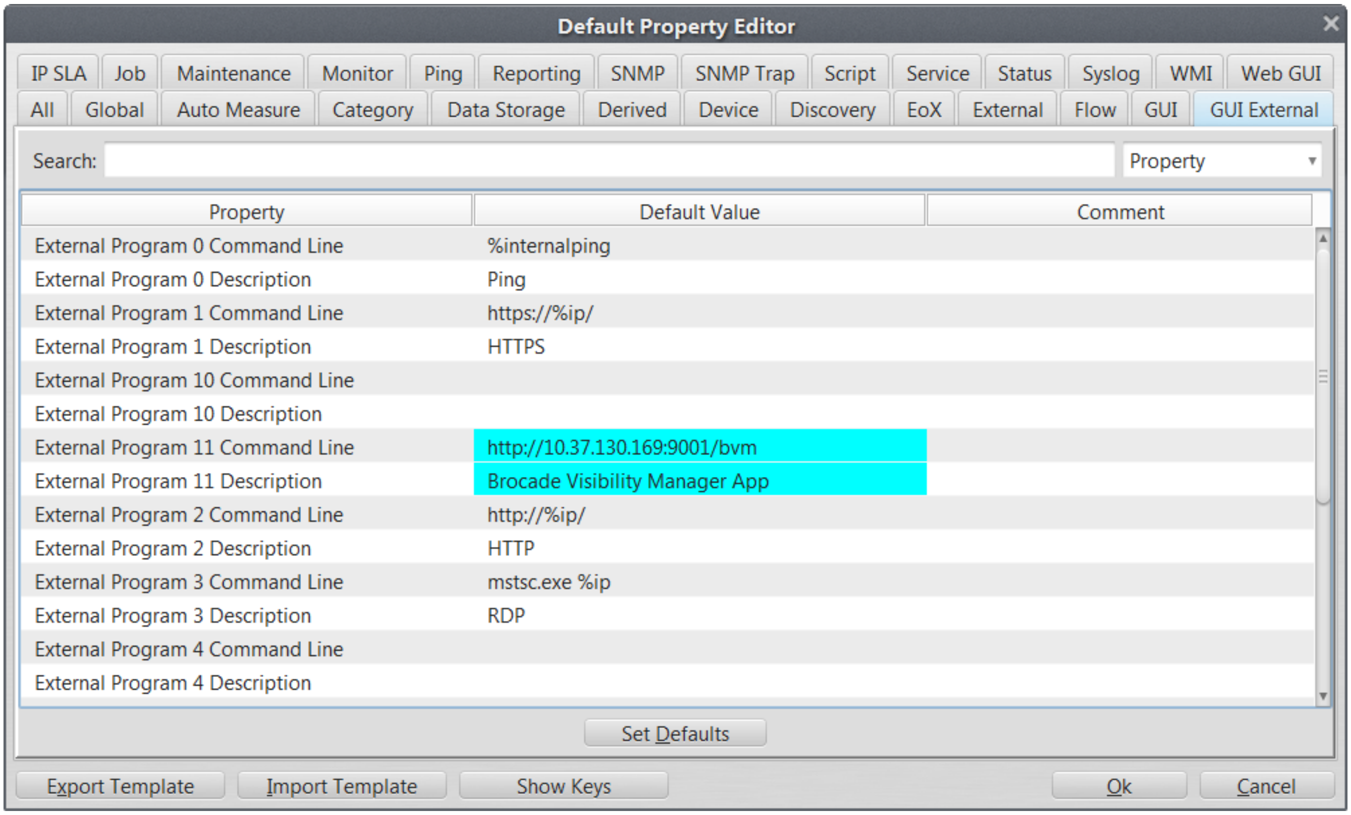
1. Login to StableNet® using thick client.
2. Click the **Default Property Editor** icon.

   ⚙

   The **Default Property Editor** window appears.

3. Click the **GUI External** tab.

FIGURE 39 Default Property Editor - GUI External tab



Property	Default Value	Comment
External Program 0 Command Line	%internalping	
External Program 0 Description	Ping	
External Program 1 Command Line	https://%ip/	
External Program 1 Description	HTTPS	
External Program 10 Command Line		
External Program 10 Description		
External Program 11 Command Line	http://10.37.130.169:9001/bvm	
External Program 11 Description	Brocade Visibility Manager App	
External Program 2 Command Line	http://%ip/	
External Program 2 Description	HTTP	
External Program 3 Command Line	mstsc.exe %ip	
External Program 3 Description	RDP	
External Program 4 Command Line		
External Program 4 Description		

4. Double-click an empty External Program Command Line property field and enter the URL for the BVM App.
5. Next, double-click the associated External Program Description field and provide a description for the URL. For example, Brocade Visibility Manager App.
6. Click **Ok**.
7. Exit StableNet®.

Accessing Brocade Visibility Manager App using StableNet®

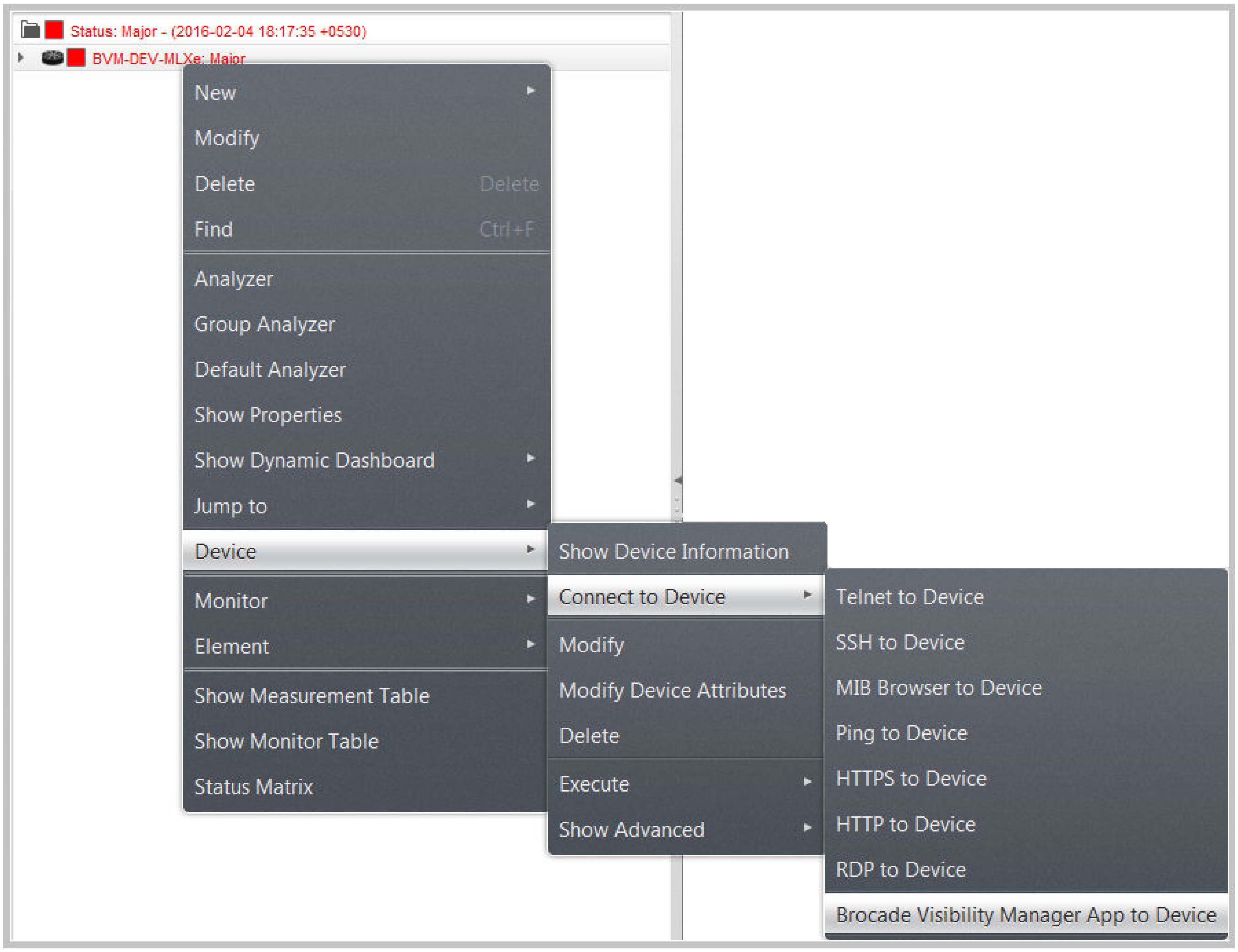
After creating a link to Brocade Visibility Manager App from StableNet®, perform the following steps to access Brocade Visibility Manager App using StableNet® .

1. Login to StableNet® using thick client.
2. Go to the **Measurements** theme.

3. In the list of devices, right-click the device you want to configure using Brocade Visibility Manager App, and go to **Device**, **Connect to Device**.

   The description provided for Brocade Visibility Manager App appears in this list.

   FIGURE 40 Connect to Device



4. Click to access Brocade Visibility Manager App.

Ports Configuration

Introduction

This chapter provides information about enabling and disabling ports, configuring ports as ingress or egress, and configuring ports as Port Groups.

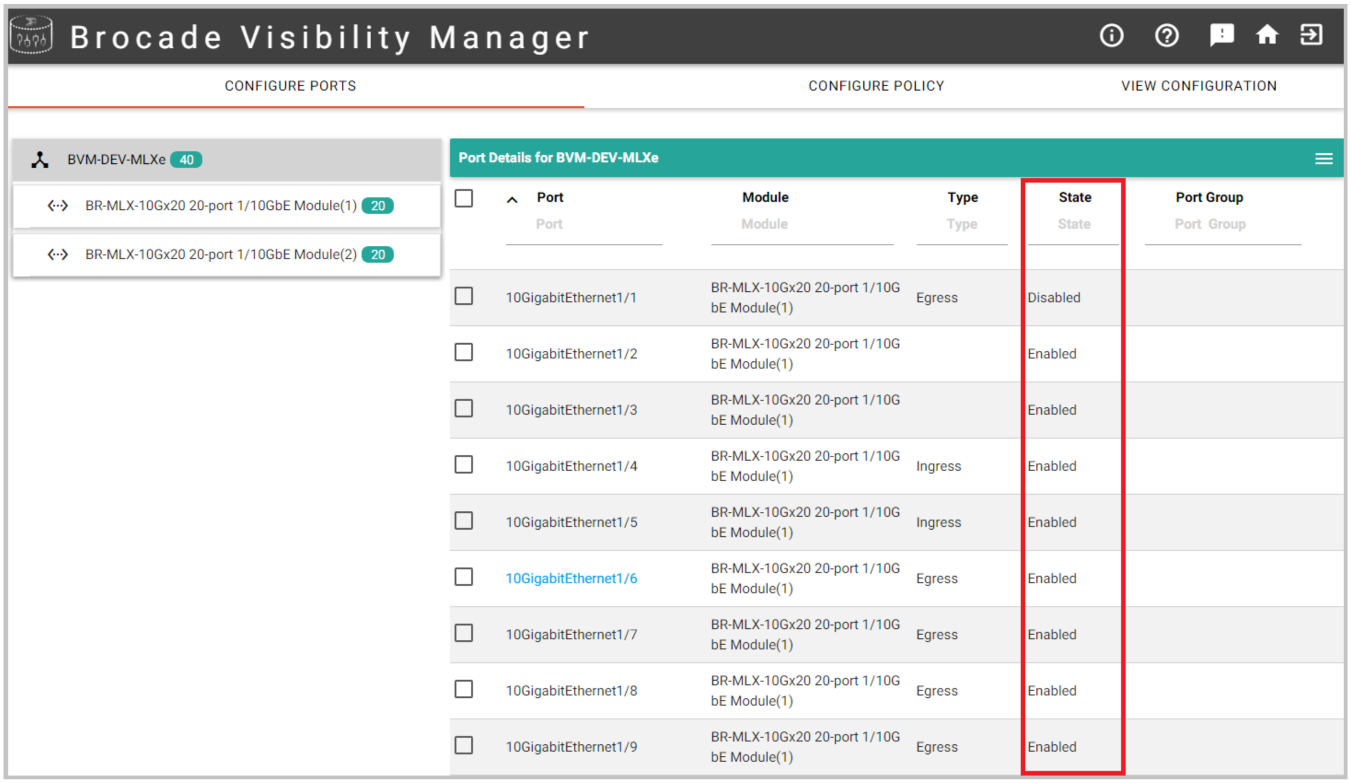
Enabling and Disabling Ports

Perform the following steps to enable or disable a port:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the ports that you want to enable or disable.
4. Click the menu icon ☰.
5. From the drop-down list, click **Enable** to enable the selected port, or **Disable** to disable the selected port.
   A confirmation window appears.
6. Click the **Rediscover** check box if you want the port to be rediscovered after it has been enabled or disabled.

7. Click **Yes** to confirm the change.
   The **State** column for the selected port is updated to Enabled or Disabled.

   FIGURE 41 Ports enabled/disabled



Brocade Visibility Manager
CONFIGURE PORTS
CONFIGURE POLICY
VIEW CONFIGURATION
BVM-DEV-MLXe 40
BR-MLX-10Gx20 20-port 1/10GbE Module(1) 20
BR-MLX-10Gx20 20-port 1/10GbE Module(2) 20

Port Details for BVM-DEV-MLXe

☐	Port	Module	Type	State	Port Group
☐	10GigabitEthernet1/1	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Disabled	
☐	10GigabitEthernet1/2	BR-MLX-10Gx20 20-port 1/10GbE Module(1)		Enabled	
☐	10GigabitEthernet1/3	BR-MLX-10Gx20 20-port 1/10GbE Module(1)		Enabled	
☐	10GigabitEthernet1/4	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/5	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/6	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/7	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/8	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/9	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	

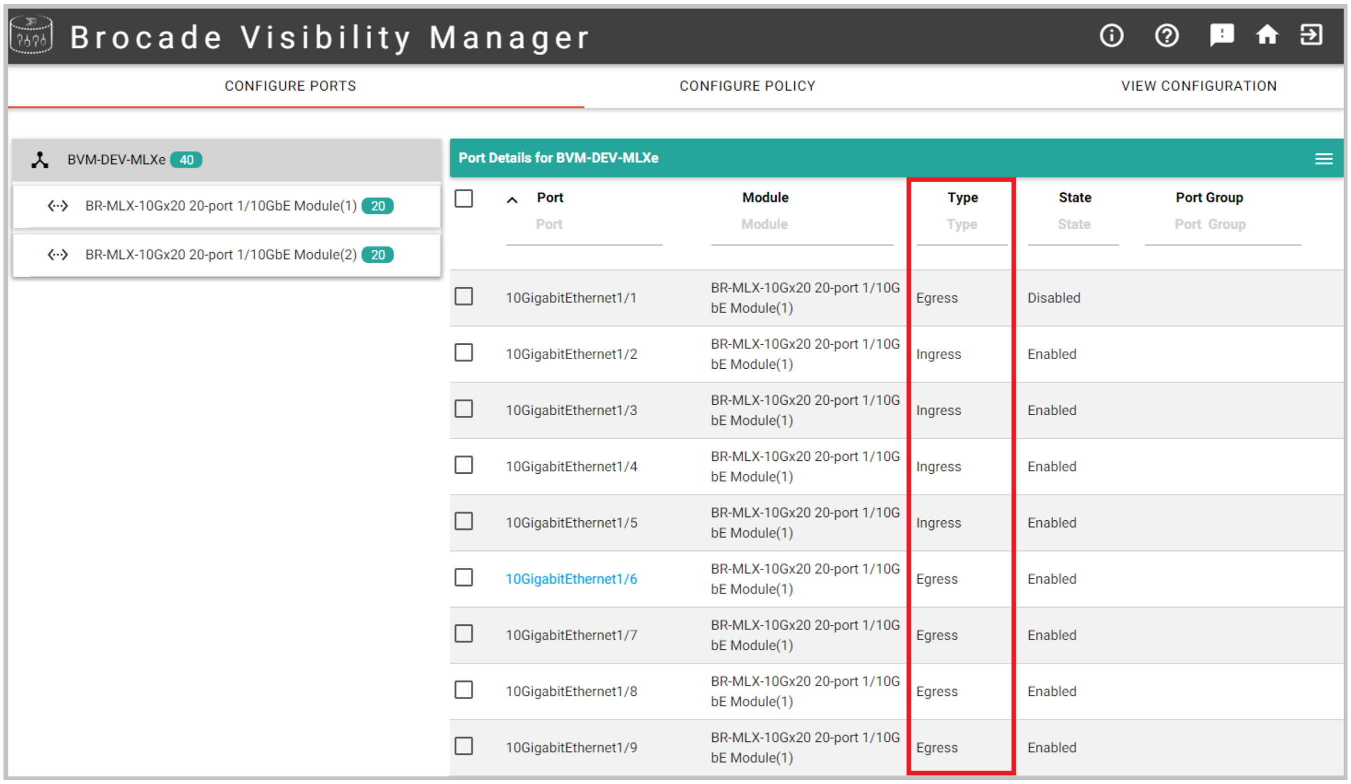
Configuring Ports as Ingress or Egress

Perform the following steps to configure a port as either Ingress or Egress:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the ports that you want to configure as Ingress or Egress.
4. Click the menu icon ☰.
5. From the drop-down list, click **Mark as Ingress** to configure the selected port as Ingress or **Mark as Egress** to configure the selected port as Egress.
   A confirmation window appears.
6. Click the **Rediscover** check box if you want the port to be rediscovered after it has been configured as Ingress or Egress.

7. Click **Yes** to confirm the change.
   The **Type** column for the selected port is updated to either Ingress or Egress.

FIGURE 42 Ports Ingress/Egress


Brocade Visibility Manager
CONFIGURE PORTS
CONFIGURE POLICY
VIEW CONFIGURATION
BVM-DEV-MLXe 40
BR-MLX-10Gx20 20-port 1/10GbE Module(1) 20
BR-MLX-10Gx20 20-port 1/10GbE Module(2) 20
Port Details for BVM-DEV-MLXe

☐	Port	Module	Type	State	Port Group
☐	10GigabitEthernet1/1	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Disabled	
☐	10GigabitEthernet1/2	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/3	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/4	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/5	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
☐	10GigabitEthernet1/6	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/7	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/8	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
☐	10GigabitEthernet1/9	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	

Resetting Port Type

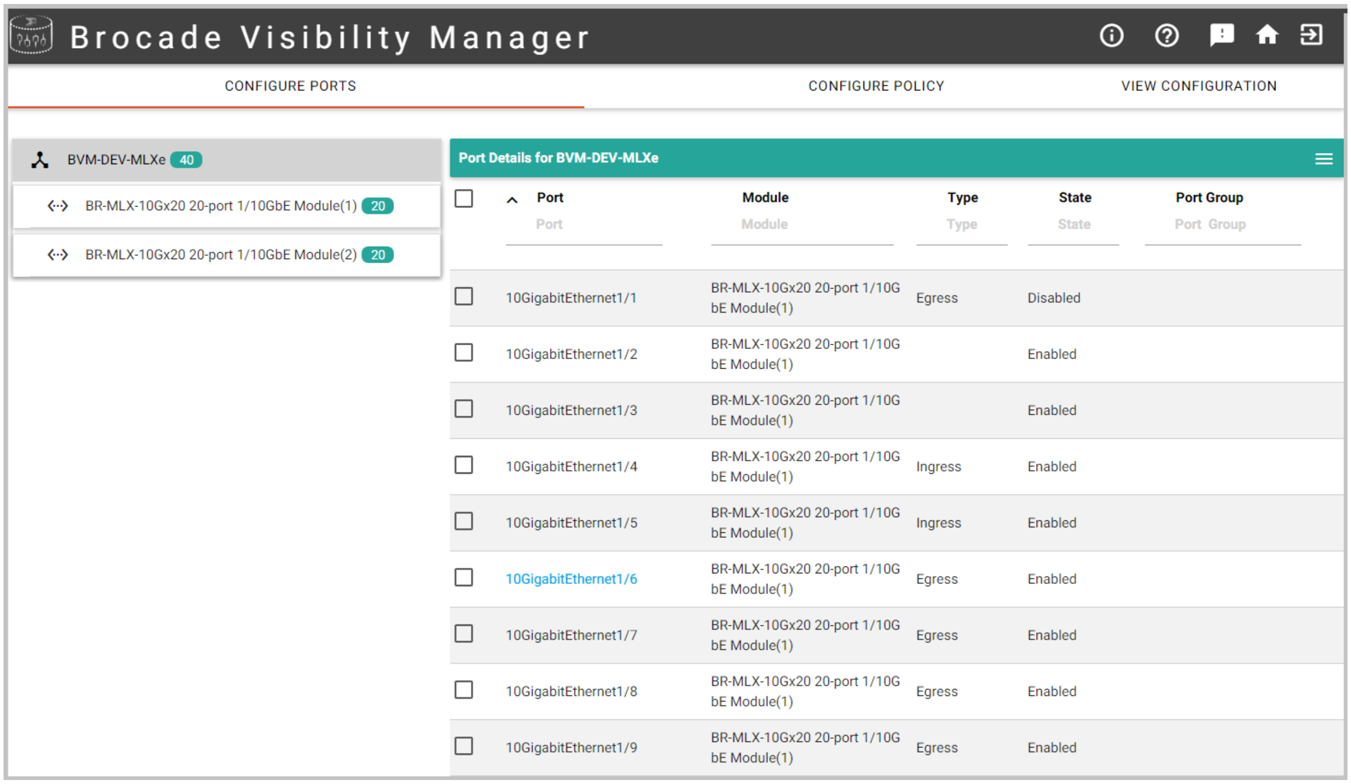
A port's type setting can be reset using the **Port as None** option. This is especially useful for resetting ports that have been set as Egress or Ingress.

Perform the following steps to reset a port:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the ports that you want to configure.
4. Click the menu icon ☰.
5. From the drop-down list, click **Mark as None**.
   A confirmation window appears.
6. Click the **Rediscover** check box if you want the port to be rediscovered after this change.

7. Click **Yes** to confirm the change.
   The **Type** column for the selected port is updated to reflect the change.

FIGURE 43 Ports Ingress/Egress



Brocade Visibility Manager

CONFIGURE PORTS | CONFIGURE POLICY | VIEW CONFIGURATION

BVM-DEV-MLXe 40

BR-MLX-10Gx20 20-port 1/10GbE Module(1) 20

BR-MLX-10Gx20 20-port 1/10GbE Module(2) 20

Port Details for BVM-DEV-MLXe

□	Port	Module	Type	State	Port Group
□	10GigabitEthernet1/1	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Disabled	
□	10GigabitEthernet1/2	BR-MLX-10Gx20 20-port 1/10GbE Module(1)		Enabled	
□	10GigabitEthernet1/3	BR-MLX-10Gx20 20-port 1/10GbE Module(1)		Enabled	
□	10GigabitEthernet1/4	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
□	10GigabitEthernet1/5	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Ingress	Enabled	
□	10GigabitEthernet1/6	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
□	10GigabitEthernet1/7	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
□	10GigabitEthernet1/8	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	
□	10GigabitEthernet1/9	BR-MLX-10Gx20 20-port 1/10GbE Module(1)	Egress	Enabled	

Port Groups

This section describes how to configure Port Groups for Brocade devices.

Port Groups are used for load balancing. Creating a Port Group involves adding egress ports and choosing a primary port. The primary port acts as the anchor for load balancing.

A port can be a member of only one Port Group. After a Port Group is created, it will appear in the egress list while creating a policy. Users can choose Port Groups and egress ports to create policies. If a Port Group is selected as the egress, the traffic will be load balanced across the ports in the Port Group.

Creating a Port Group

Perform the following steps to create a Port Group:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. From the list, click the check box for the egress ports that you want to configure as a Port Group.

4. Click the menu icon ☰.
5. From the drop-down list, click **Create Port Group**.
   The **Add Port Group** window appears.
6. In the Group Name field, enter a name for the Port Group.
7. To add other egress ports, click the **All Ports** field and click the egress ports in the drop-down list.
8. Use the **Primary Port** drop-down menu to select one of the ports in the list as the primary port.

   > NOTE
   > The primary port for a Port Group cannot be changed if the Port Group is used in a policy.

9. Click **SAVE**.
   The Port Group appears in the port list.

Deleting a Port Group

Perform the following steps to delete a Port Group:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.

   Port details for the selected module is displayed on the right side pane.
3. Click the delete icon for the Port Group you want to delete.
4. Click **Yes** to delete the Port Group.

Editing a Port Group

Perform the following steps to edit a Port Group:

1. Click the **CONFIGURE PORTS** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
   Port details for the selected module is displayed on the right side pane.
3. Click the edit icon for the Port Group you want to edit.
   The **Edit Port Group** window appears.
4. Make the required changes and click **SAVE**.

Policy Configuration

Introduction

The Policy Configuration tab can be used to create filter rules for incoming or outgoing traffic on an interface. Users can select an ingress ports, egress ports, and Port Groups, and author filters for a device.

While creating a policy:

- If multiple Port Groups are selected as the egress, the traffic will be replicated to those Port Groups and load balanced independently within the ports of the Port Groups.
- If both egress ports and Port Groups are selected in a policy, the traffic will be replicated to the egress ports and the Port Groups, and load balanced independently within the ports of the Port Groups.

Adding a Policy

This section provides information about adding a policy.

Perform the following steps to add a policy:

1. Click the **CONFIGURE POLICY** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
3. Click the menu icon ☰.
4. Click **Create Filter(s)**.
   The **Policy Configuration** page appears.

5. Configure the fields as follows:

Option	Description
Policy Name	Name of the policy.
Flow Id	Flow Id is also known as Transparent VLAN Flooding (TVF). It is used to identify the flow from ingress ports to egress ports within the MLXe. Flow Id must be a number between 2 and 4090. It can contain multiple VLAN Ids.
Sequence No.	Sequence policies across the same ingress ports.
Network Port [Ingress]	Select one or more ingress ports from the drop-down menu.
Tool Ports [Egress]	Select one of more egress ports from the drop-down menu.
Filters	Click **Apply** to apply the following filters: • L2: Layer 2 ACL • L3-L4: Layer 3/Layer 4 ACL **NOTE** Use the up ▲icon or down ▼ icon to change the order in which individual ACLs need to be applied.

Create L2 Filter

The table below provides information about the fields for creating a Layer 2 ACL:

Option	Description
Action	Select one of the following actions for the selected ACL: • Permit • Deny
Source MAC	Filter based on source MAC.
Source Mask	Filter based on source Mask.
Destination MAC	Filter based on destination MAC.
Destination Mask	Filter based on destination Mask.
Eth Type	Select one of the following options from the drop-down list: • Any • ARP • IPv4 • IPv6 • Others
VLAN Id	VLAN Id must be a number between 2 and 4095.
Rule String	Use this field to add custom ACLs. ACLs added here will override values in all the other fields.
List of ACL Rules	List of ACL rules will appear here.

After adding the ACLs, click **ADD**. The ACLs will be added to the **List of ACL Rules** field.

Click **CLEAR** to clear all fields.

Create L3-L4 Filter

The table below provides information about the fields for creating a Layer 3-Layer 4 ACL:

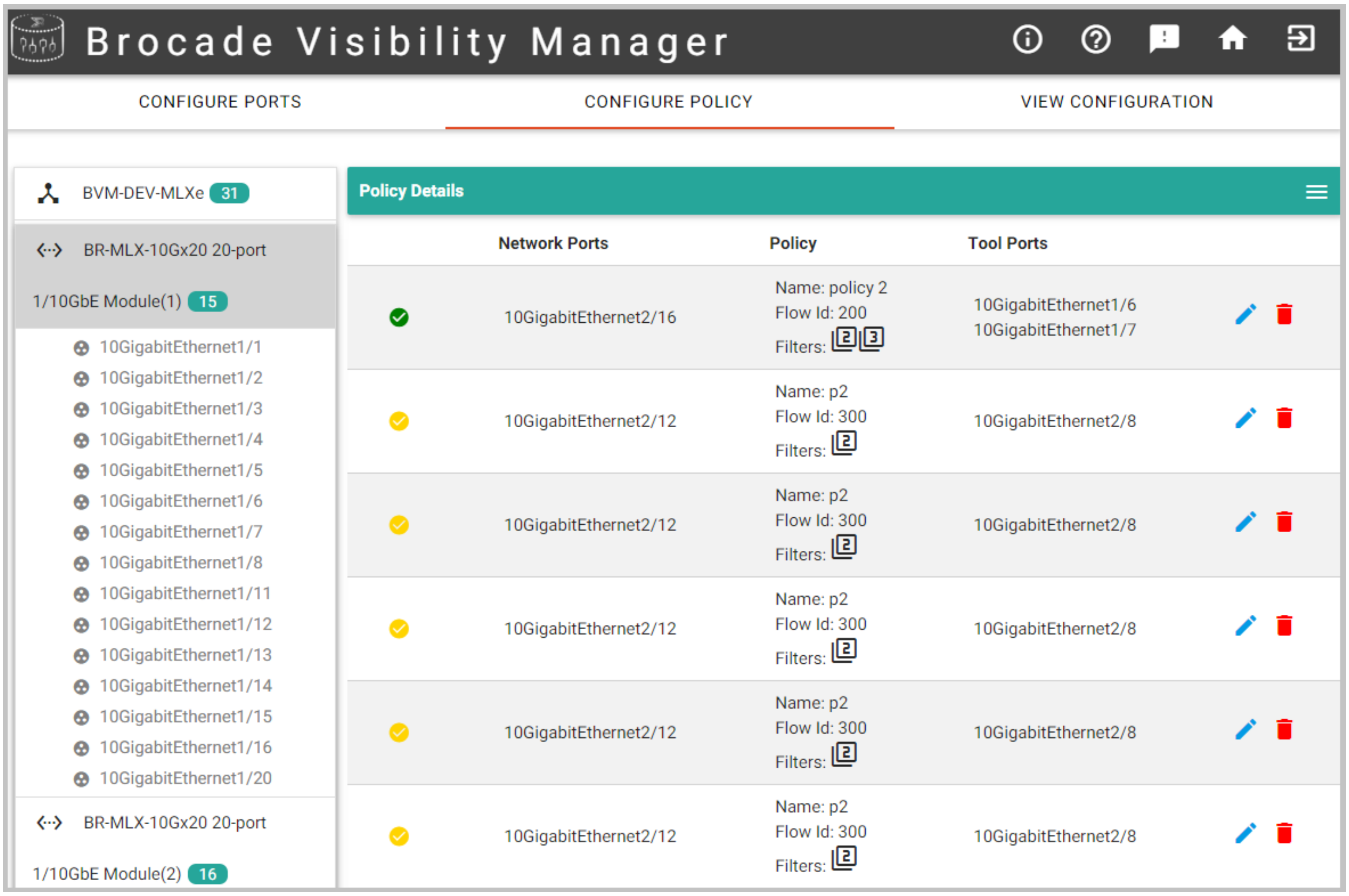
Option	Description
ACL Type	Select one of the following ACL types: • IPv4 • IPv6
Action	Select one of the following actions for the selected ACL: • Permit • Deny
Protocol	Filter based on one of the following protocols: • TCP • UDP • IP • SCTP • ICMP • IGMP • Others
Source IP	Filter based on source IP.
Source Port	Filter based on source port..
Destination IP	Filter based on destination IP.
Destination Port	Filter based on destination port.
Operator	Select an operator for Source Port and Destination Port.
VLAN Id	VLAN Id must be a number between 2 and 4095.
Rule String	Use this field to add ACLs. ACLs added here will override values in all the other fields.
List of ACL Rules IPv4	List of ACL rules for IPv4 will appear here.
List of ACL Rules IPv6	List of ACL rules for IPv6 will appear here.

After adding the ACLs, click **ADD**. Depending on the selected ACL type, the ACLs will be added to the List of ACL Rules for either IPv4 or IPv6.

Click **CLEAR** to clear all fields.

6. Click **OK**.
7. Click one of the following buttons:
   - **Save**: Saves to the database, but the changes are not applied to the device.
   - **Commit**: Saves to the database and the changes are applied to the device.

FIGURE 44 Policies



	Network Ports	Policy	Tool Ports	
🟢	10GigabitEthernet2/16	Name: policy 2 Flow Id: 200 Filters: 2 3	10GigabitEthernet1/6 10GigabitEthernet1/7	✎ 🗑
🟡	10GigabitEthernet2/12	Name: p2 Flow Id: 300 Filters: 2	10GigabitEthernet2/8	✎ 🗑
🟡	10GigabitEthernet2/12	Name: p2 Flow Id: 300 Filters: 2	10GigabitEthernet2/8	✎ 🗑
🟡	10GigabitEthernet2/12	Name: p2 Flow Id: 300 Filters: 2	10GigabitEthernet2/8	✎ 🗑
🟡	10GigabitEthernet2/12	Name: p2 Flow Id: 300 Filters: 2	10GigabitEthernet2/8	✎ 🗑
🟡	10GigabitEthernet2/12	Name: p2 Flow Id: 300 Filters: 2	10GigabitEthernet2/8	✎ 🗑

Editing a Policy

Perform the following steps to edit a policy:

NOTE

Before editing a policy, disable the ingress ports on which the policy is being applied and then re-enable the ports after successfully editing the policy.

1. **Disable Ports**
   a) Click the **CONFIGURE PORTS** tab.
   b) From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
      Port details for the selected module is displayed on the right side pane.
   c) From the list, click the check box for the ports that must be disabled.
   d) Click the menu icon ☰.
   e) From the drop-down list, click **Disable** to disable the selected ports.
      A confirmation window appears.
   f) Click to deselect the **Rediscover** check box.
   g) Click **Yes** to confirm the change.
2. **Edit Policy**
   a) Next, click the **CONFIGURE POLICY** tab.
   b) From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
      Policy details for the selected module is displayed on the right side pane.
   c) Click the **Edit** button for the policy you want to edit.

      ✎

      The **Policy Configuration** window appears.
   d) Make the required changes and click one of the following buttons:
      - **Save**: Saves to the database, but the changes are not applied to the device.
      - **Commit**: Saves to the database and the changes are applied to the device.
3. **Enable Ports**
   a) Click the **CONFIGURE PORTS** tab.
   b) From the list of devices on the navigation pane on the left side, click the device and then click the module you want to configure.
      Port details for the selected module is displayed on the right side pane.
   c) From the list, click the check box for the ports that must be enabled.
   d) Click the menu icon ☰.
   e) From the drop-down list, click **Enable** to enable the selected ports.
      A confirmation window appears.
   f) Click to deselect the **Rediscover** check box.
   g) Click **Yes** to confirm the change.

Configuring a Load Balance Policy

Perform the following steps to configure load balance:

1. Click the **CONFIGURE POLICY** tab.
2. From the list of devices on the navigation pane on the left side, click a device and then click the module you want to configure.
3. Click the menu icon ☰.
4. Click **Create Load Balance**.
   The **Load Balance Policy** window appears.
5. Configure the fields outlined in the following table:

Option	Description
Module	Use the drop-down list to select the module.
Apply to	The load balancing policy can be applied to one of the following: • Outer IP • GTP
Load Balance Fields	Select the following Load Balance fields: • Source IP • Source Port • Destination IP • Destination Port • Protocol • Tied (GTP only)
Bidirectional/ Symmetric	Click this check box to enable symmetric load balancing. This is used to accomplish bidirectional conversations and it is applied to Load Balance hash calculations.

6. After selecting the appropriate fields, click **COMMIT**.

   NOTE
   The options shown on the page is the default setting for MLXe. The **COMMIT** button gets activated only when the default configuration for MLXe is changed.

The Load Balance policy for the selected module is displayed on the right side pane.

Handling Errors

This section provides information about some of the common error scenarios that you might encounter while configuring ports or policies. These errors can be caused by various issues, such as an issue with the Brocade Visibility Manager database, issue connecting to StableNet® or a Brocade device, and so on.

Perform the following steps to determine the exact cause of an error and to fix the error:

1. Whenever there is an error, a notification icon is displayed in the bottom right corner of the page.

   🔔

   Click the notification icon.

   The **Alerts** window is displayed. This window provides a brief overview of the message.

2. Similarly, an error icon appears next to the port or policy that has an issue.

   ❗

   Click the error icon.

   The **Job Result** window appears. This window provides detailed information about the issue.

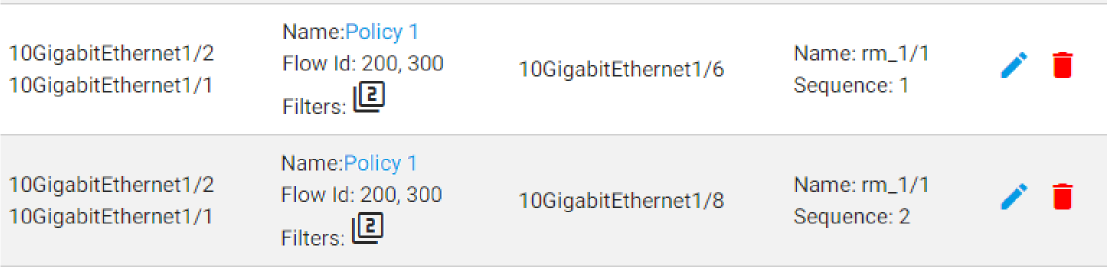
3. To fix an error, delete the configuration. When a configuration is deleted, it cleans up the device for that particular policy. It is then moved to saved state.

Use Cases

The section includes some common aggregation and replication use cases.

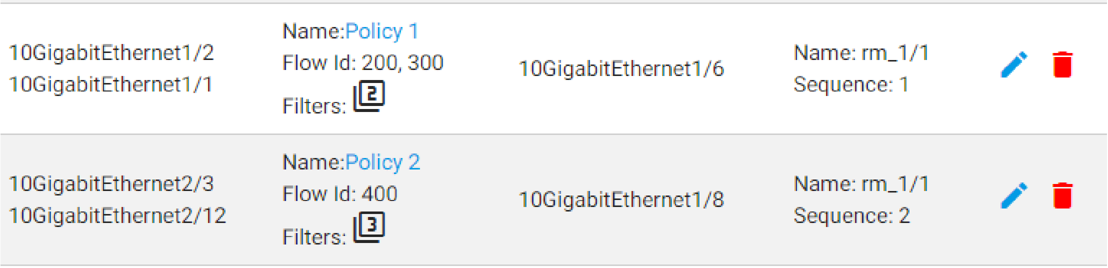
TABLE 3 Use Cases

Scenario	Description
Aggregation - Same policy on multiple ingress ports	Same policy is applied to all the ingress ports, and traffic is aggregated to one or more egress ports.



10GigabitEthernet1/2 10GigabitEthernet1/1	Name:Policy 1 Flow Id: 200, 300 Filters: 2	10GigabitEthernet1/6	Name: rm_1/1 Sequence: 1	✎ 🗑
10GigabitEthernet1/2 10GigabitEthernet1/1	Name:Policy 1 Flow Id: 200, 300 Filters: 2	10GigabitEthernet1/8	Name: rm_1/1 Sequence: 2	✎ 🗑

Scenario	Description
Aggregation - Multiple policies on multiple ingress ports	Multiple policies are applied to multiple ingress ports, and traffic is aggregated to one or more egress ports.



10GigabitEthernet1/2 10GigabitEthernet1/1	Name:Policy 1 Flow Id: 200, 300 Filters: 2	10GigabitEthernet1/6	Name: rm_1/1 Sequence: 1	✎ 🗑
10GigabitEthernet2/3 10GigabitEthernet2/12	Name:Policy 2 Flow Id: 400 Filters: 3	10GigabitEthernet1/8	Name: rm_1/1 Sequence: 2	✎ 🗑

Scenario	Description
Replication - Multiple Port Groups	When multiple Port Groups are selected as the egress, the traffic is replicated to those Port Groups and load balanced independently within the ports of the Port Groups.
Replication - Multiple ports and multiple Port Groups	When multiple egress ports and Port Groups are selected in a policy, the traffic is replicated to the egress ports and the Port Groups, and load balanced independently within the ports of the Port Groups.

View Configuration

Introduction

The View Configuration tab provides a visual representation of how each device is configured. It shows the traffic flow for each device and includes information about the policies configured on the device.

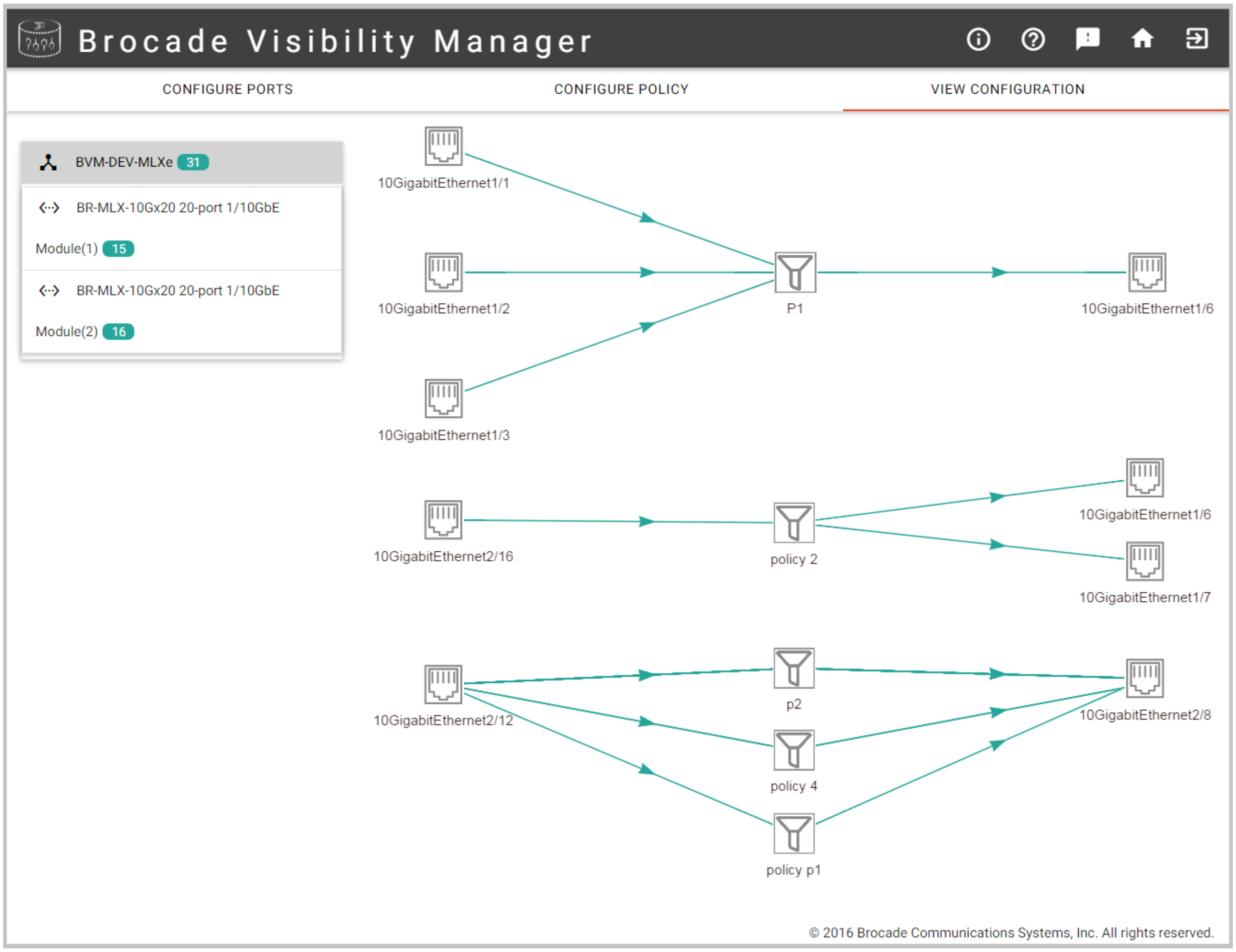
Viewing a configuration

Perform the following steps to view the configuration for a device:

1. Click the **VIEW CONFIGURATION** tab.

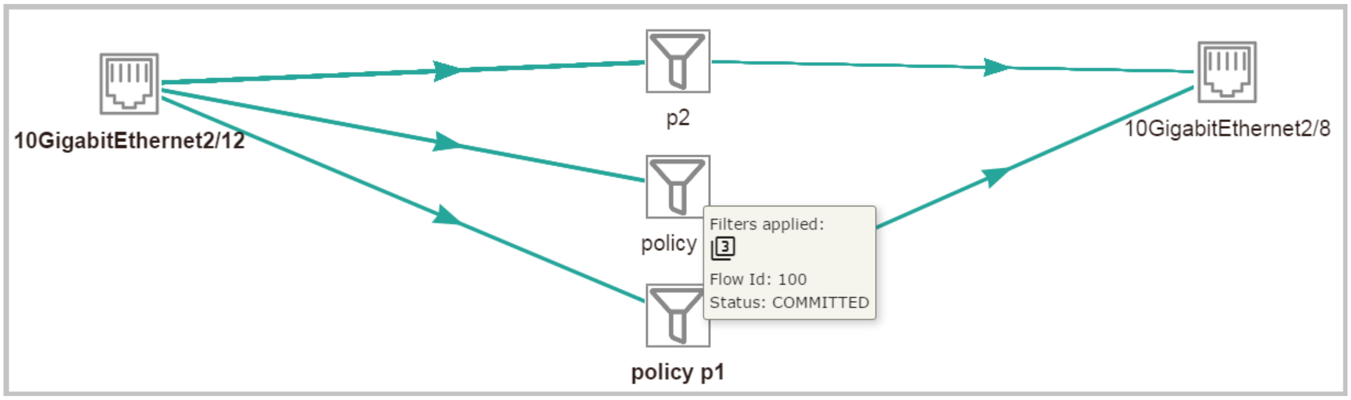
2. From the list of devices on the navigation pane on the left side, click a device.
   The configuration details for the selected module is displayed on the right side pane.

FIGURE 45 View configuration



3. Hover the mouse pointer over a policy to view more information.

FIGURE 46 Policy details



Flow Id: 100
Status: COMMITTED