BROCADE

USER GUIDE

Brocade Visibility Manager User Guide

53-1004090-03
15 February 2016

Contents

Copyright Statement

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 NetIron Command Reference
- Brocade MLXe Series Installation Guide
- StableNet® Version 7.5 Admin Manual
- StableNet® Version 7.5 Back Office Manual
- StableNet® Version 7.5 User Manual

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.

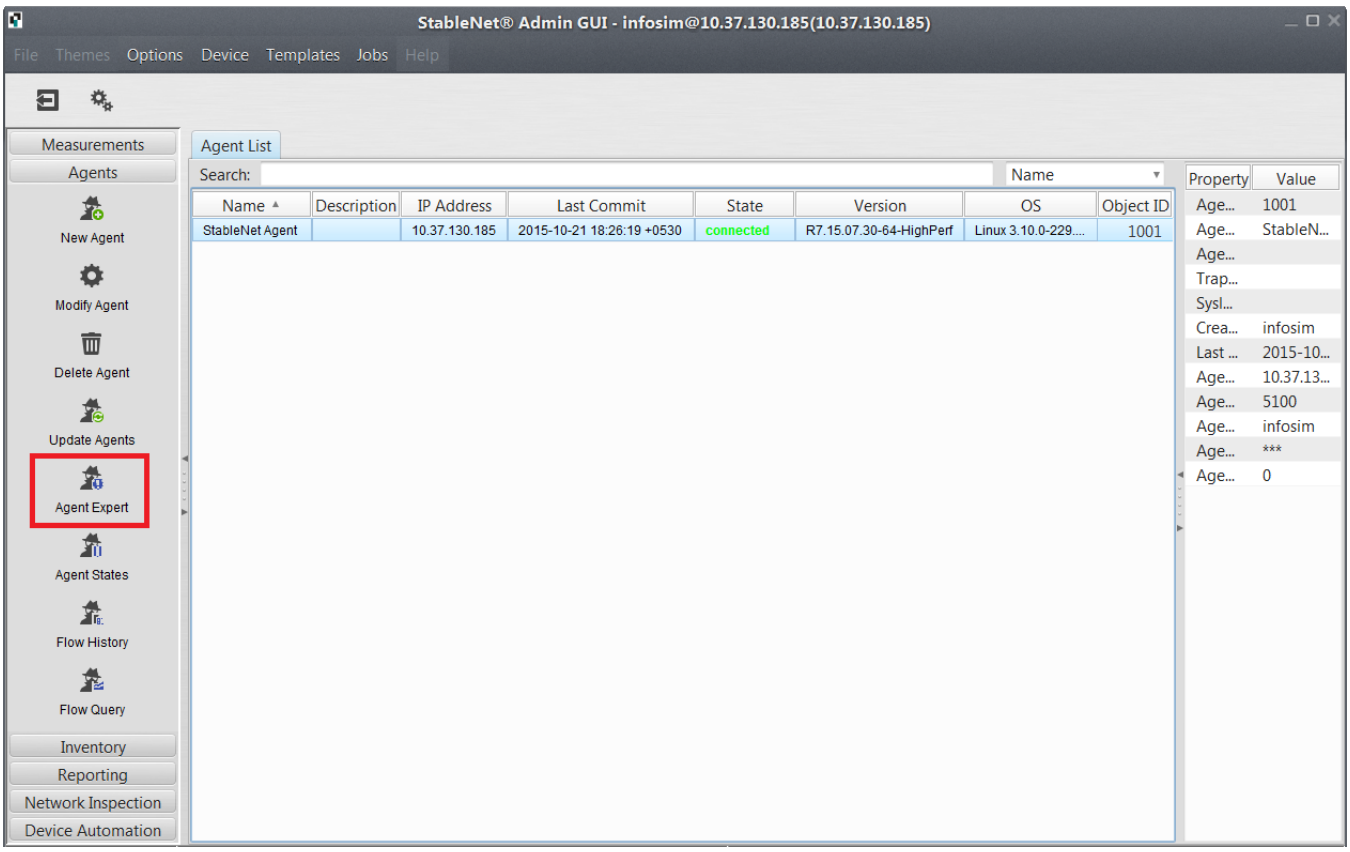
After signing in to StableNet®, perform the following steps:

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**.

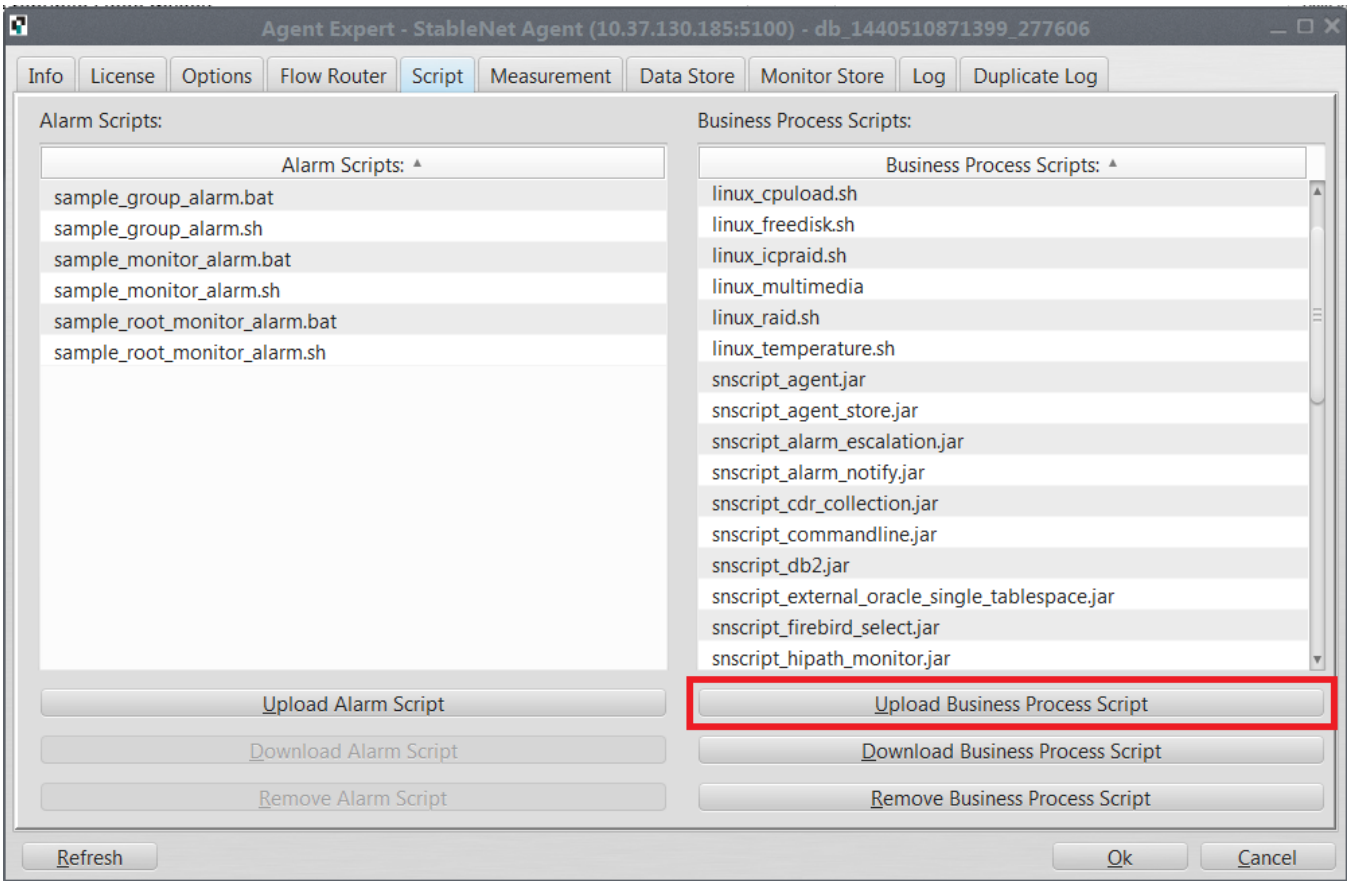
   The **Agent Expert - StableNet Agent** window appears.

FIGURE 1 Agent Expert



4. Click the **Script** tab.

FIGURE 2 Script tab

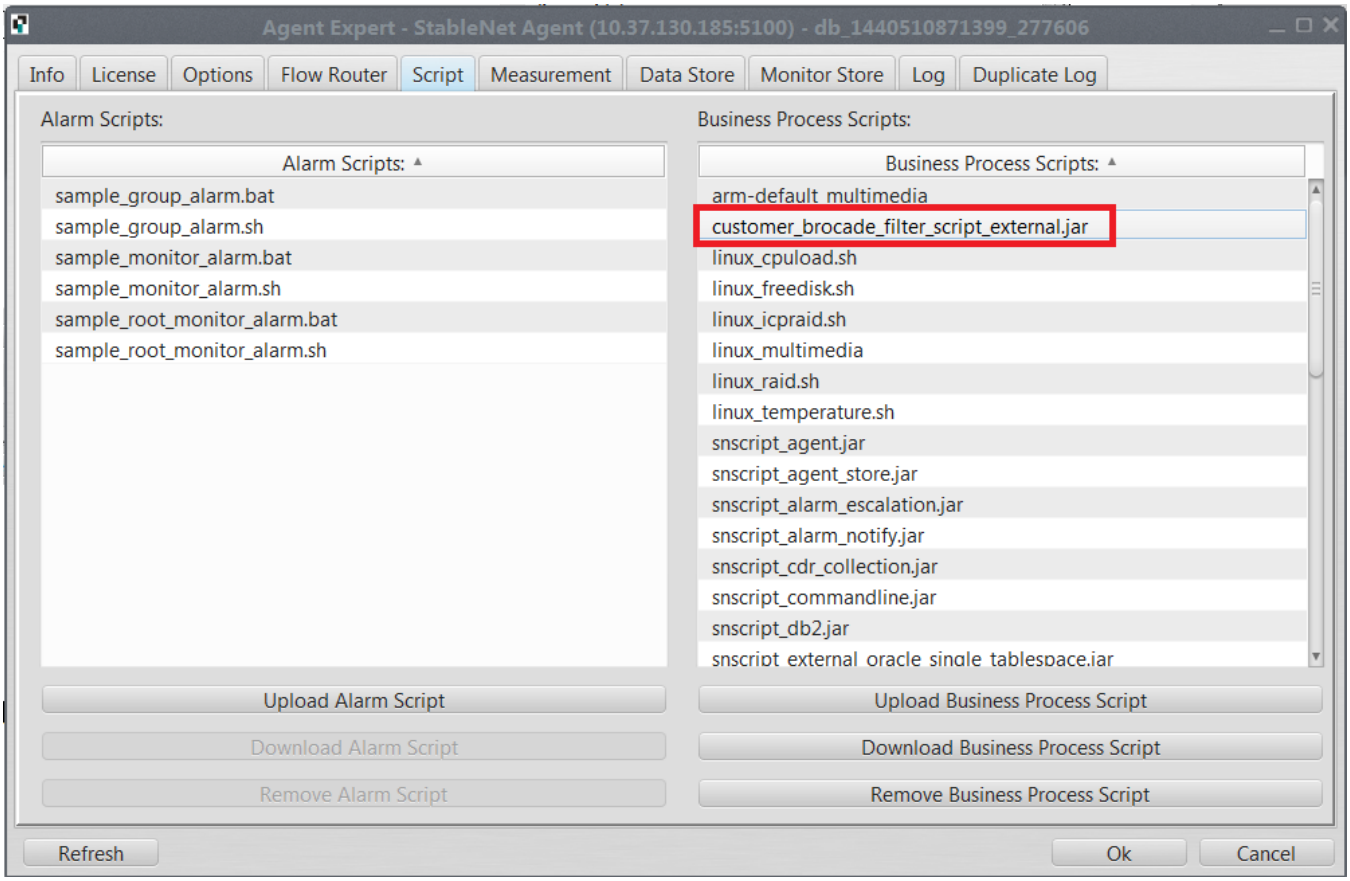


5. Click **Upload Business Process Script**.

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 3 Brocade-specific script



7. Click **Ok**.

Groups and users

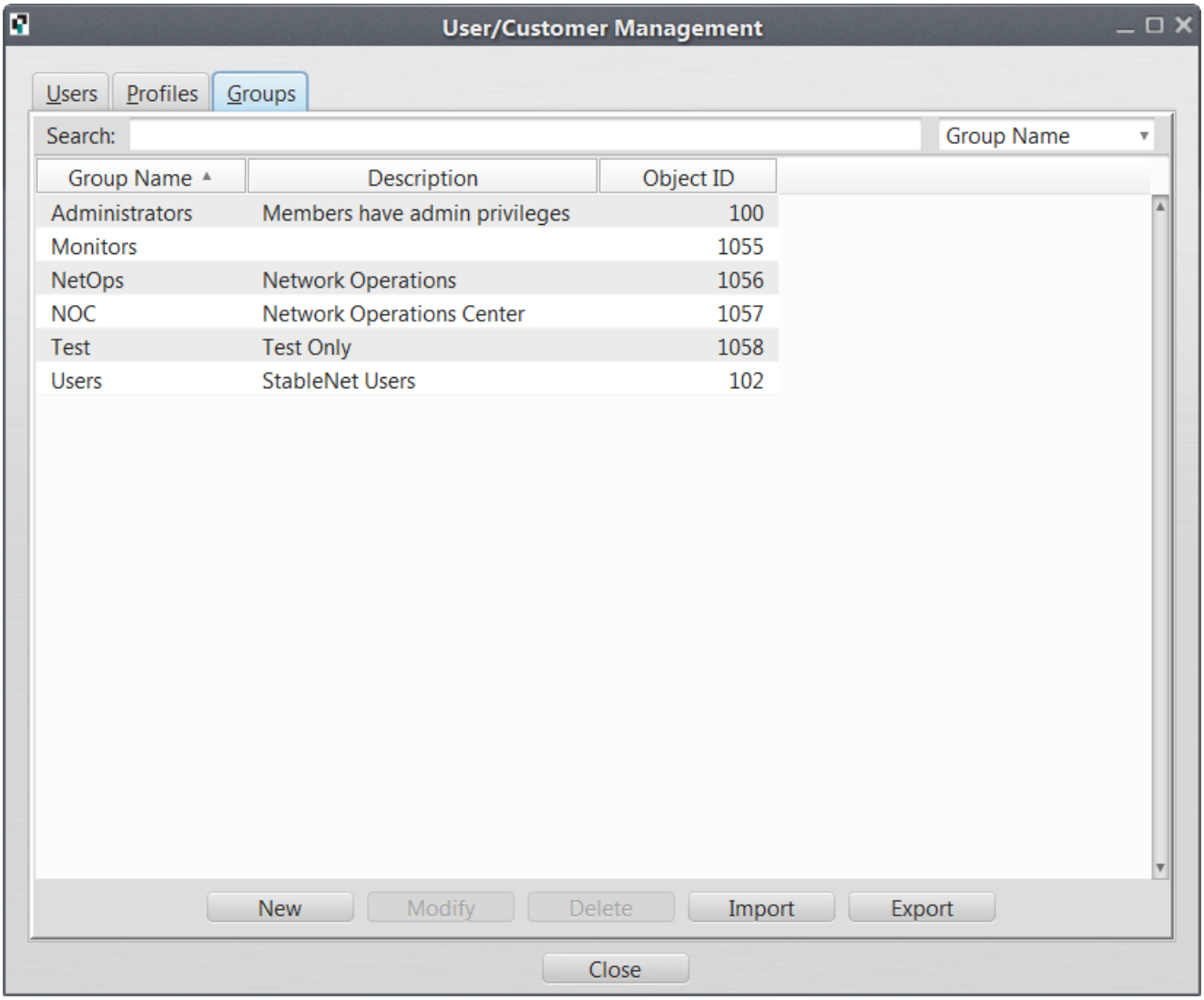
In StableNet® devices can be structured into groups. In addition, groups can contain other groups.

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 4 Groups



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

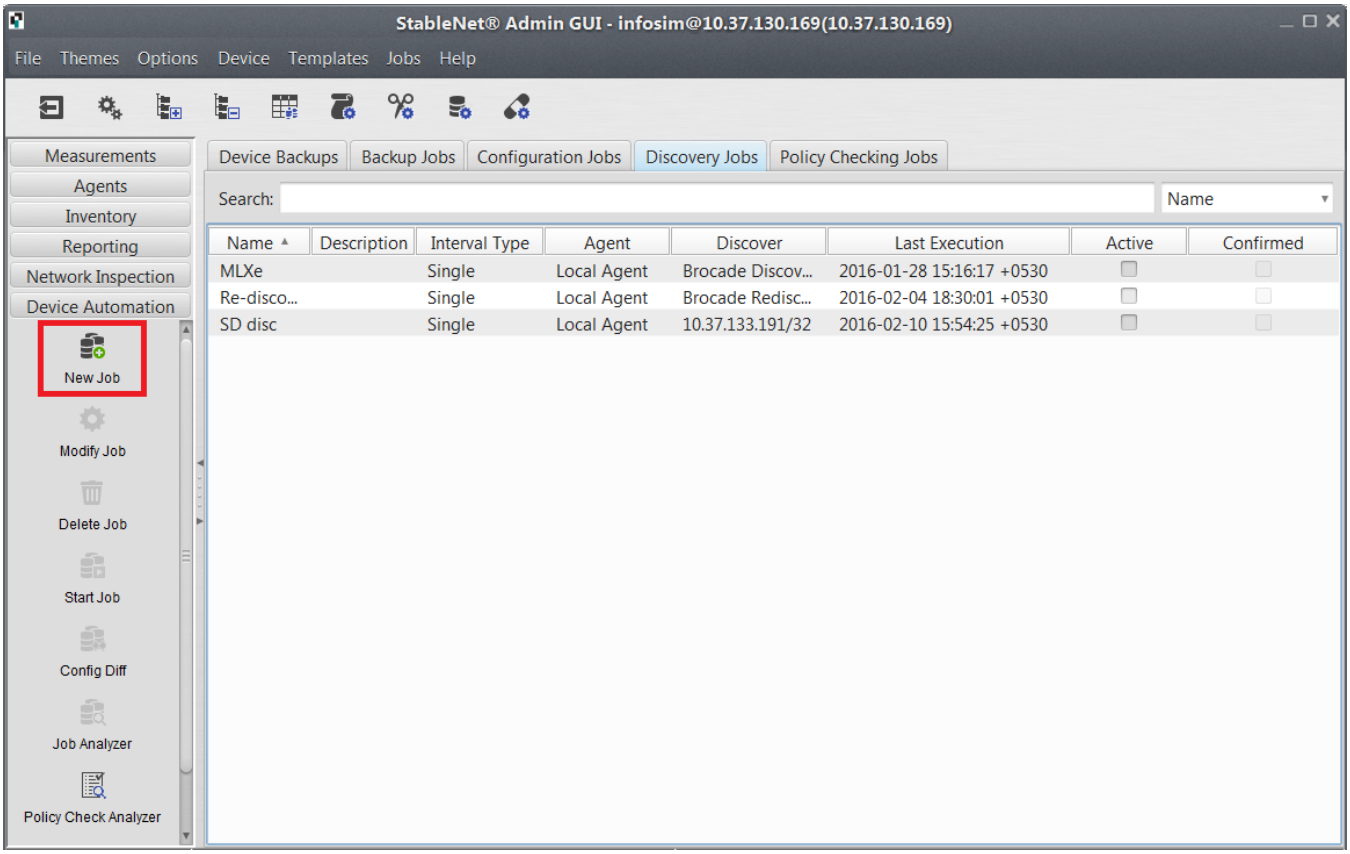
There are several methods that can be used to discover devices. During the discovery process, StableNet® performs a network scan based on the discovery input and queries device information from the available devices.

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.

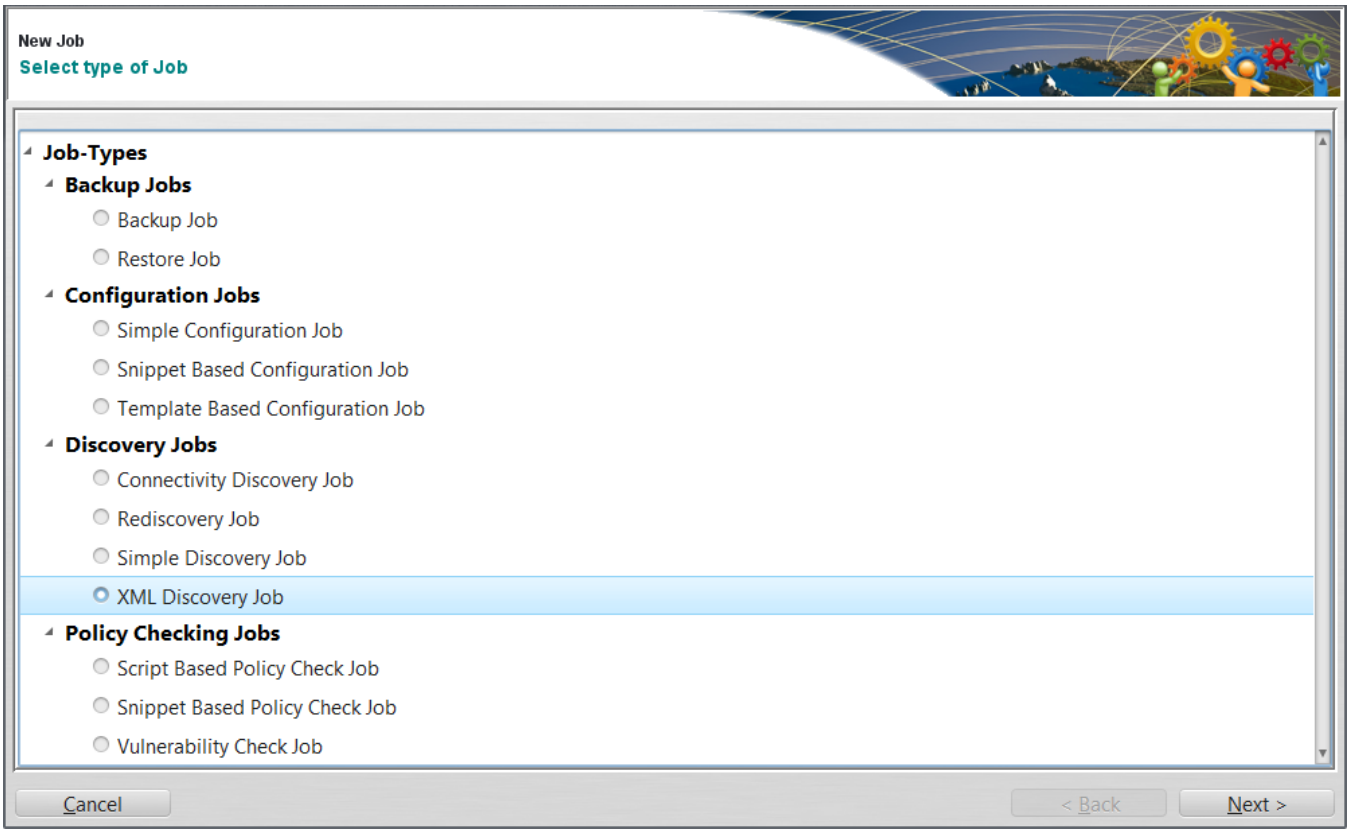
FIGURE 5 Discovery Jobs



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

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

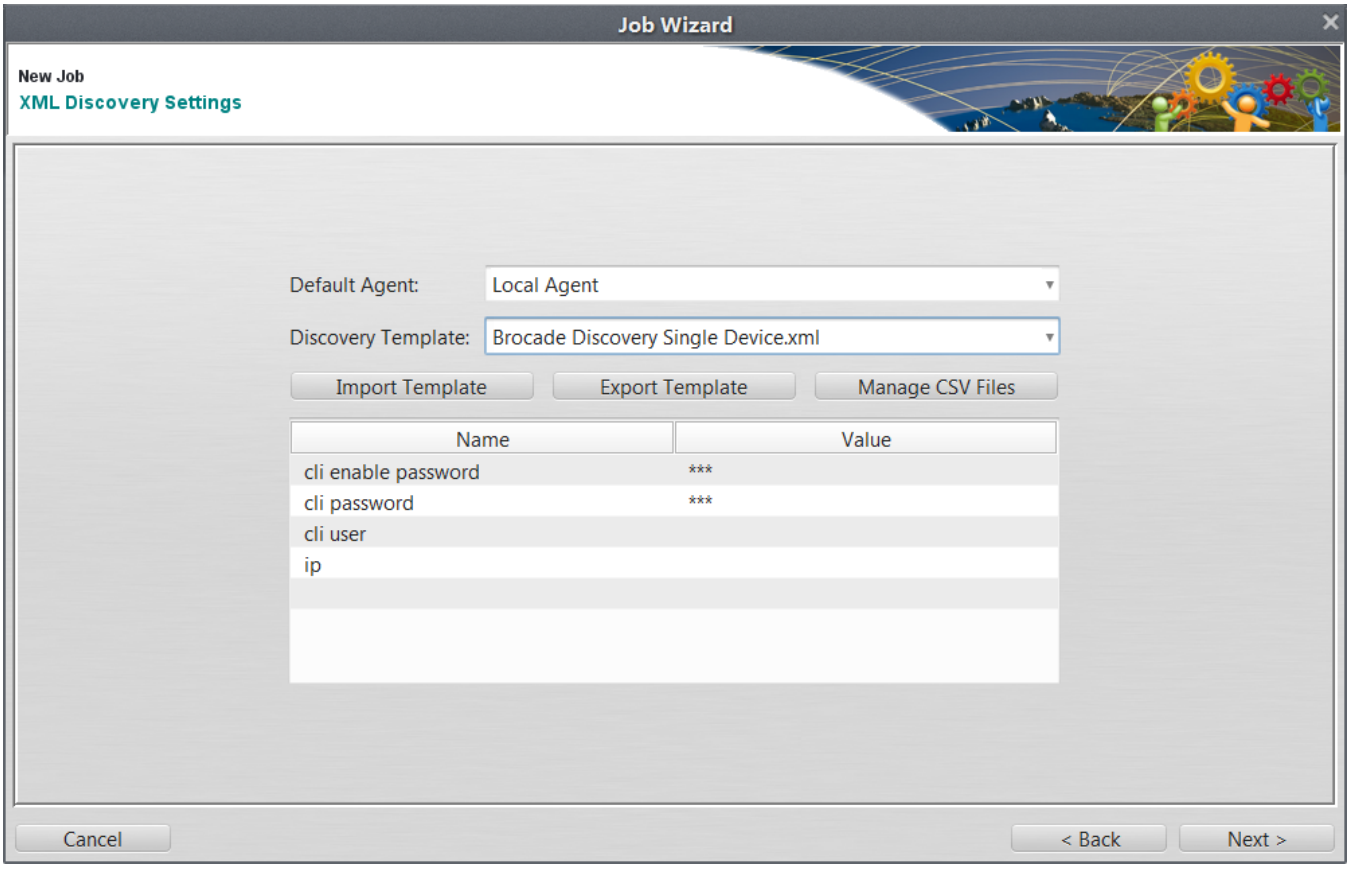
FIGURE 6 XML Discovery Job



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 7 XML Discovery Settings

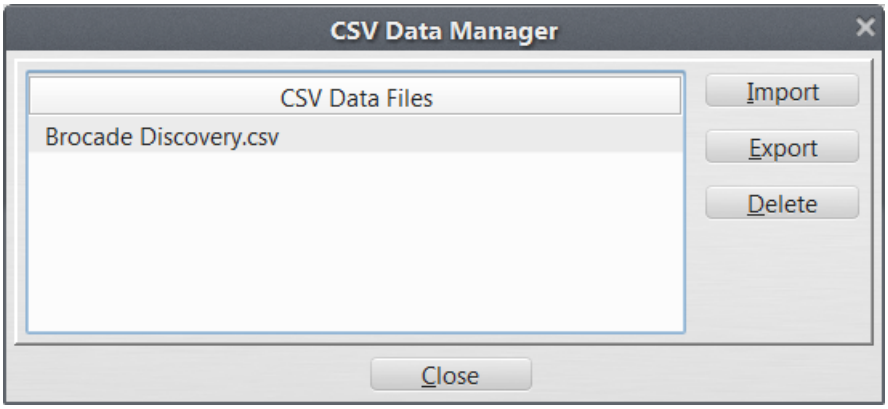


8. On the XML Discovery Settings window, click to select either **Brocade Discovery Multiple Devices.xml** or **Brocade Discovery Single Device.xml** and configure it as follows:
   - **Brocade Discovery Single Device.xml**: Use this option to discover a single device.

     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 8 CSV Data Manager

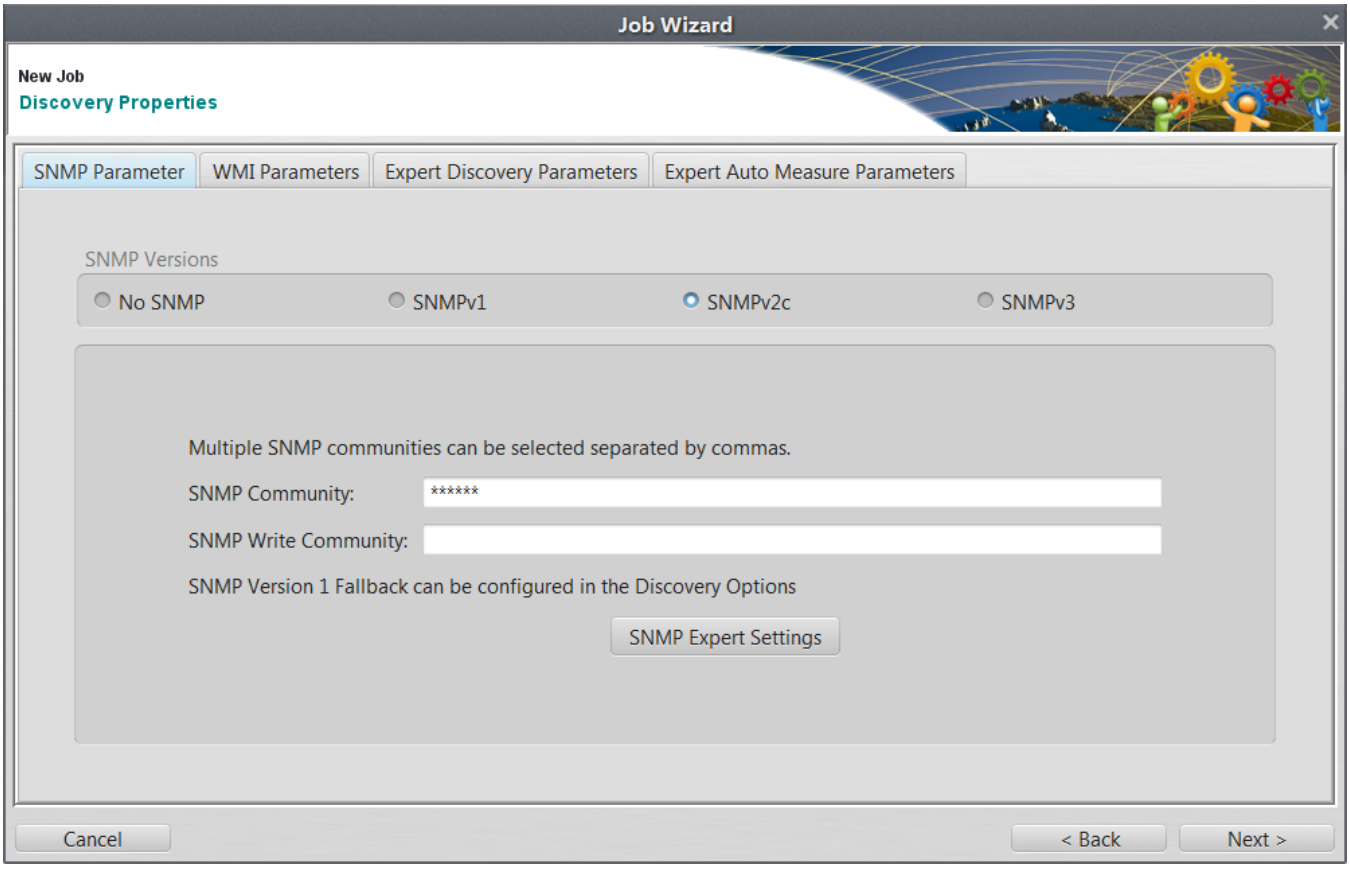
     2. On the **CSV Data Manager window**, select **Brocade Discovery.csv**, click **Export** and save the file to a local directory.
     3. Open **Brocade Discovery.csv**. This file allows you to add information about all the devices that need to discovered.
     4. Add information about the devices in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

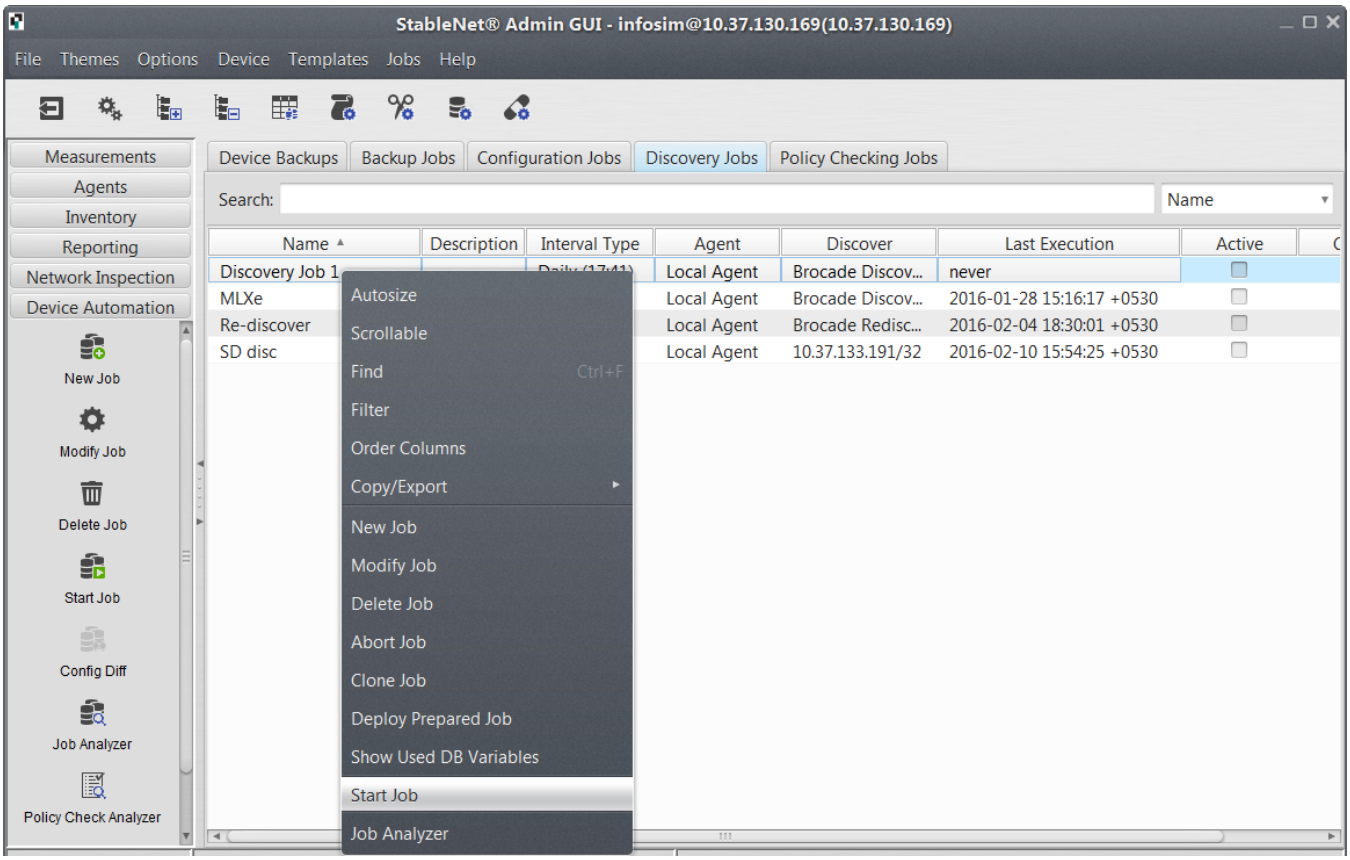
   FIGURE 9 Discovery Properties



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.

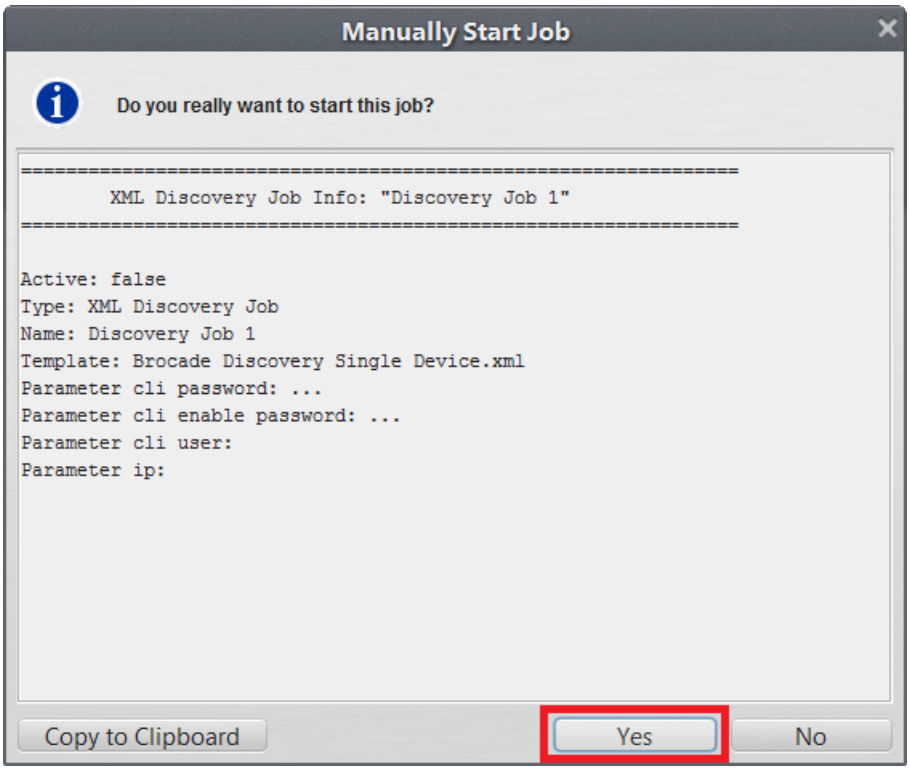
13. Right-click the job you created and click **Start Job**.

FIGURE 10 Discovery Properties



Manually Start Job window appears.

FIGURE 11 Manually Start Job



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*.

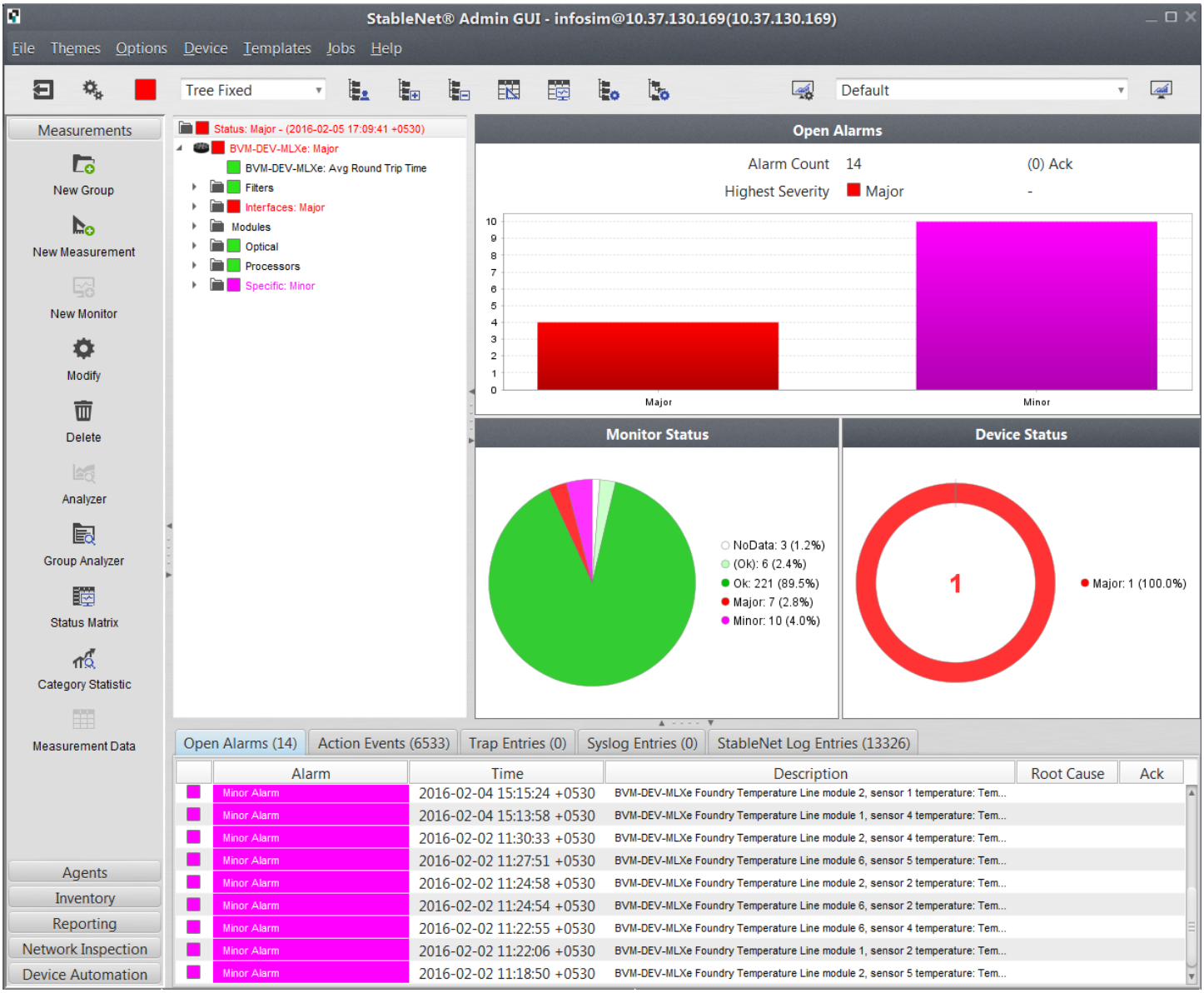
Devices

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 12 Discovered devices



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 40
- XML discovery job on page 45

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.

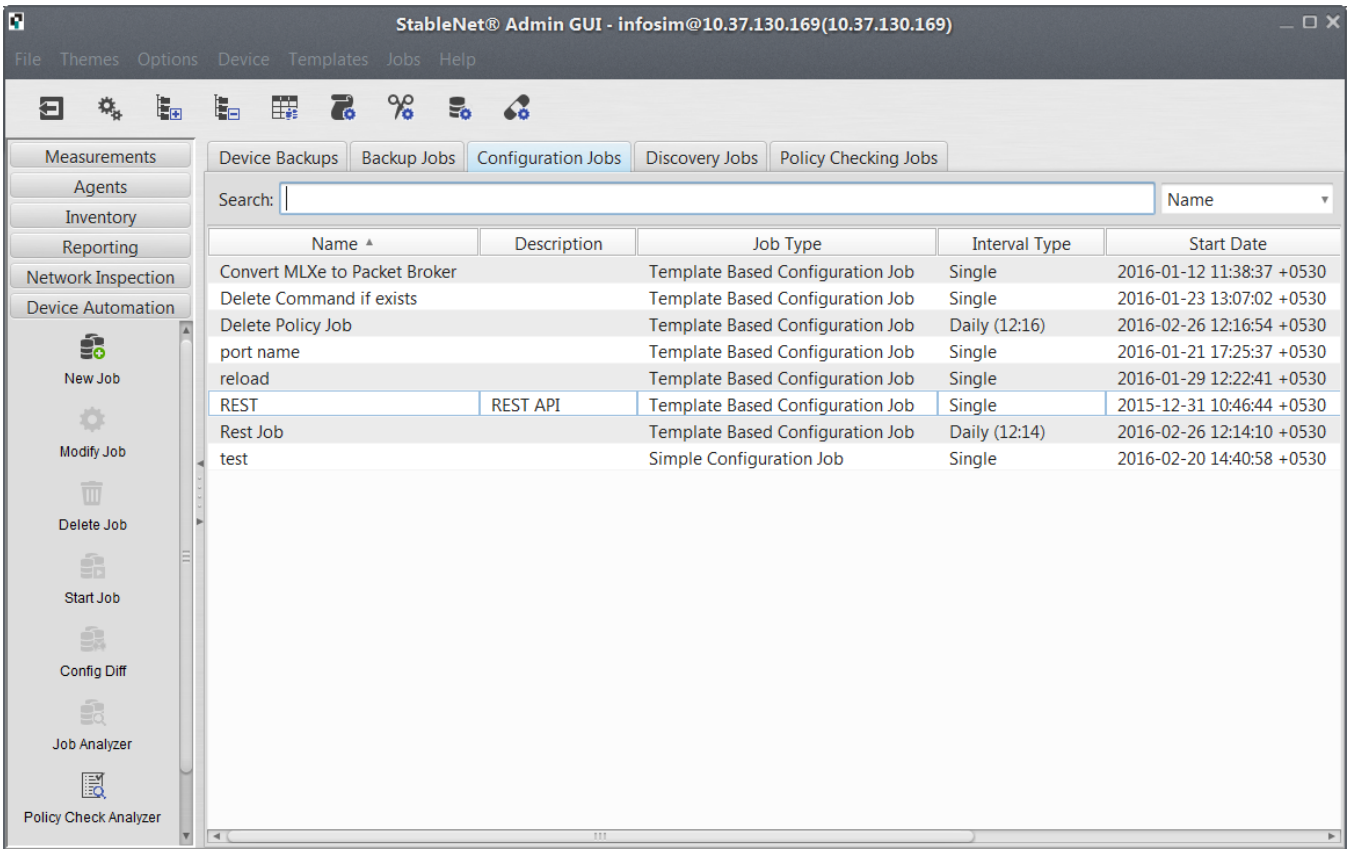
NOTE

- 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 13 Configuration Jobs

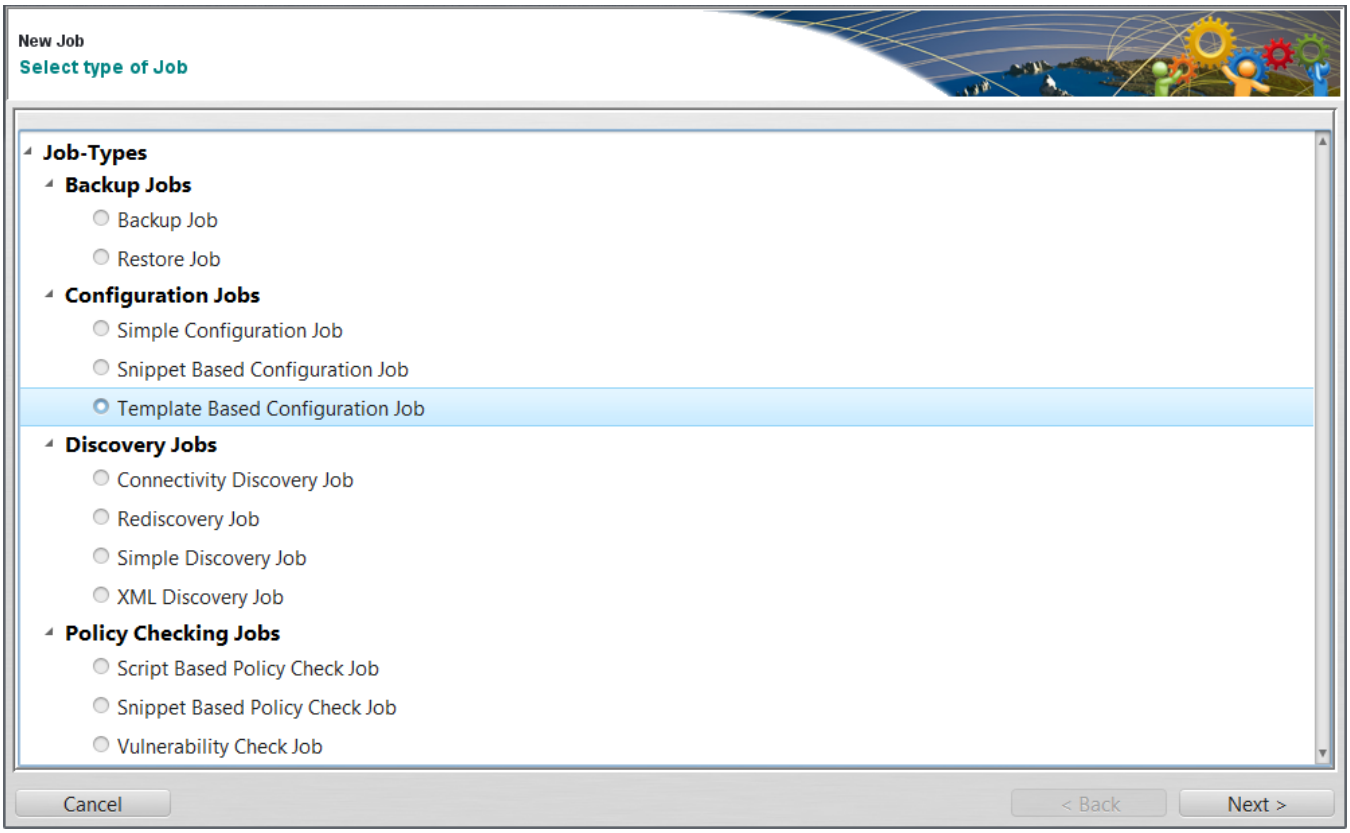


3. Click **New Job**.

Job Wizard window appears.

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

FIGURE 14 Template Based Configuration Job

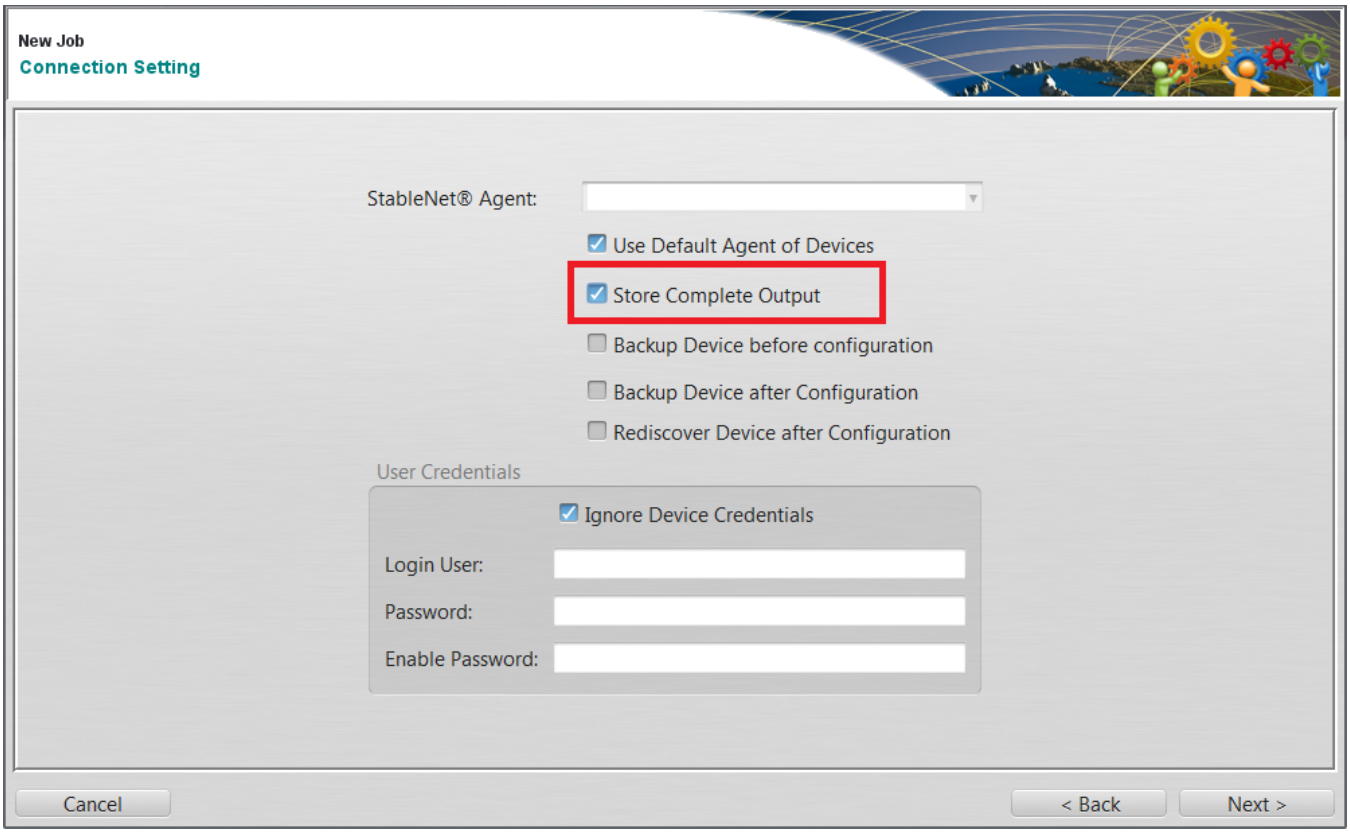


5. Click **Next**.
   Name window appears.
6. Provide a name in the **Name** field and click **Next**.
   Schedule Settings window appears.
7. Configure the Trigger Types as per your requirement and click **Next**.
   Connection Setting window appears.

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 15 Connection Setting

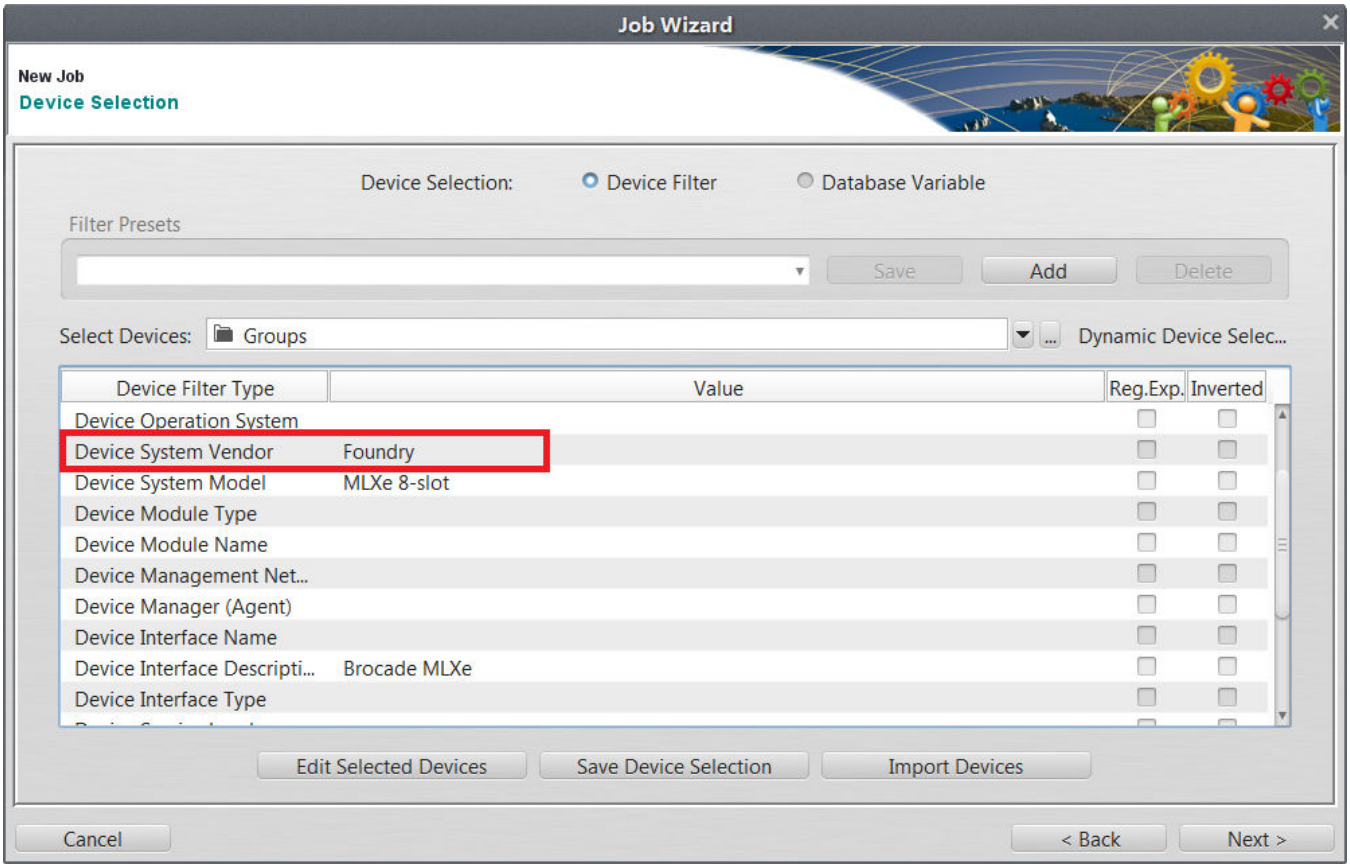


9. After making the appropriate selections on the Connection Setting window, click **Next**.
   Device Selection window appears.

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.

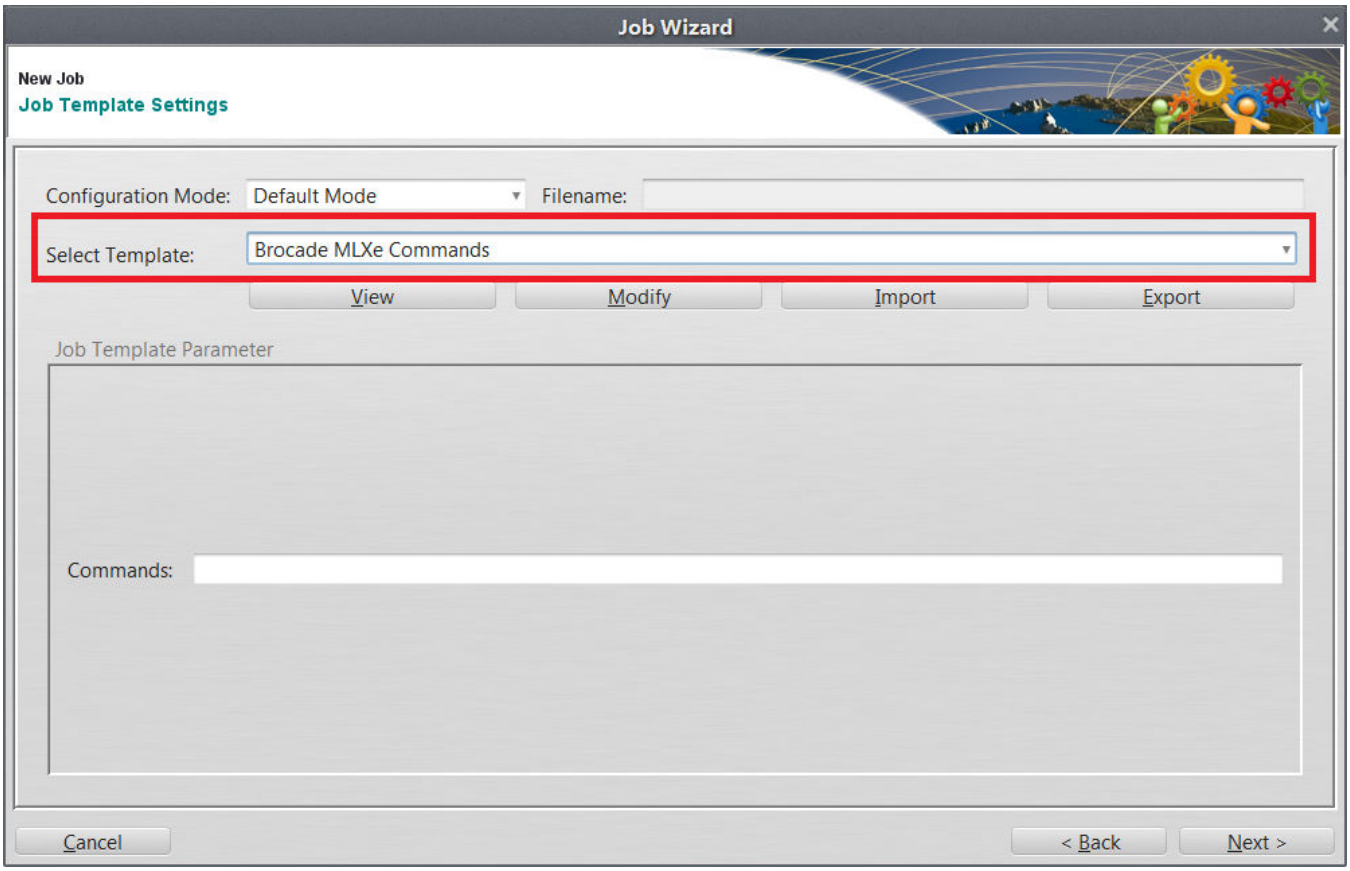
FIGURE 16 Device Selection



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

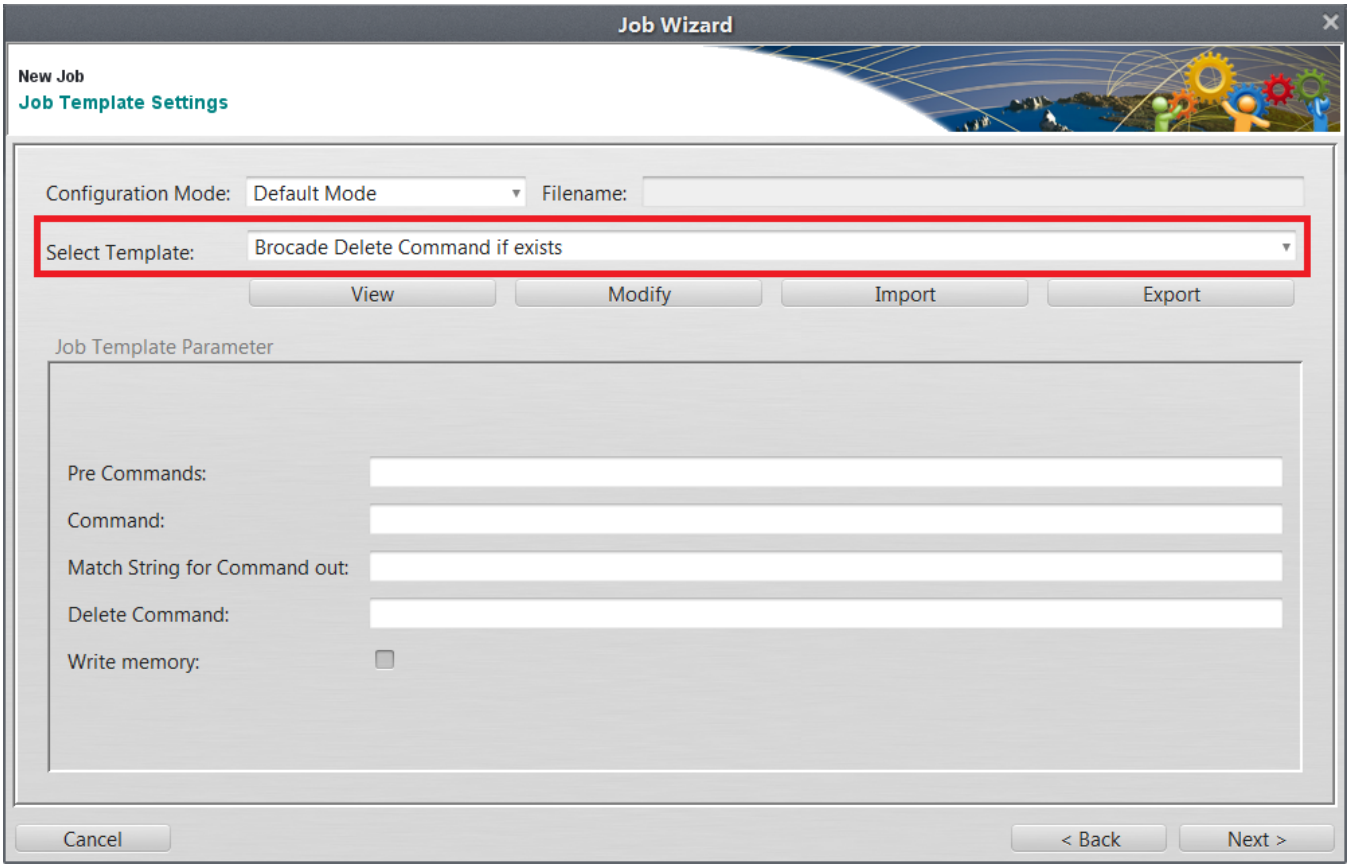
12. While creating the first job, click the **Select Template** drop-down menu and select **Brocade MLXe Commands** as the template.

FIGURE 17 Select Template - Brocade MLXe Commands



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

FIGURE 18 Select Template - Brocade Delete Command if exists



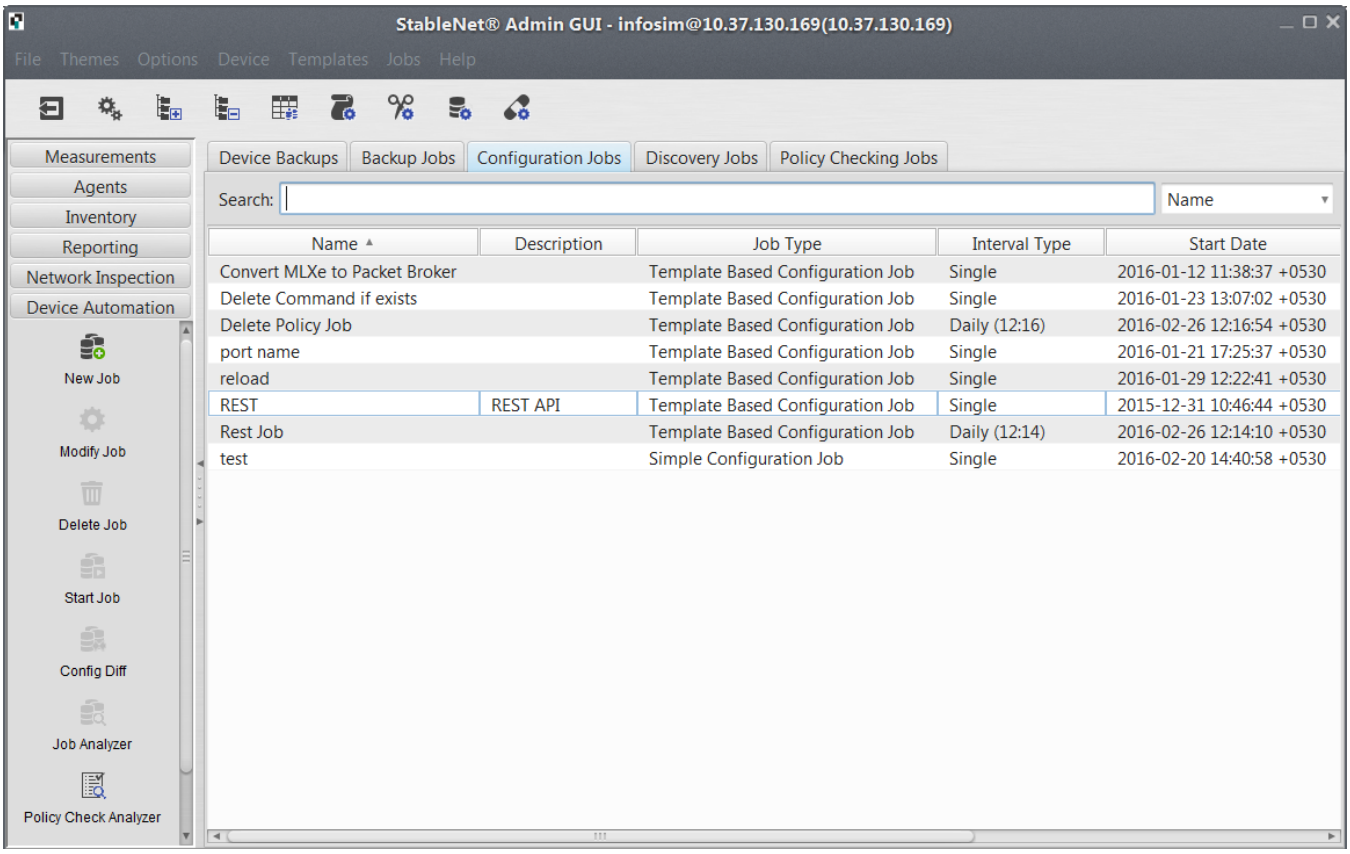
13. Click **Next**.
    Group/Customer Selection window appears.
14. Select the appropriate users and groups, and click **Finish**.

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.

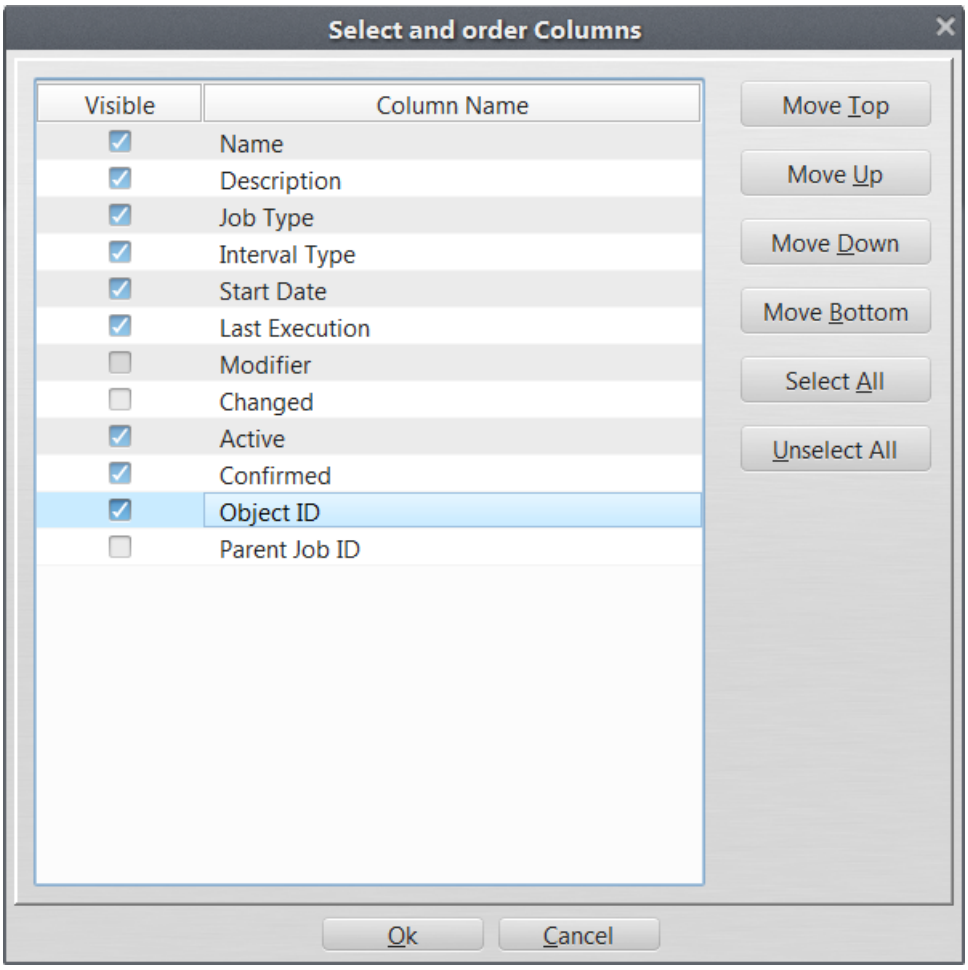
FIGURE 19 Configuration Jobs



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

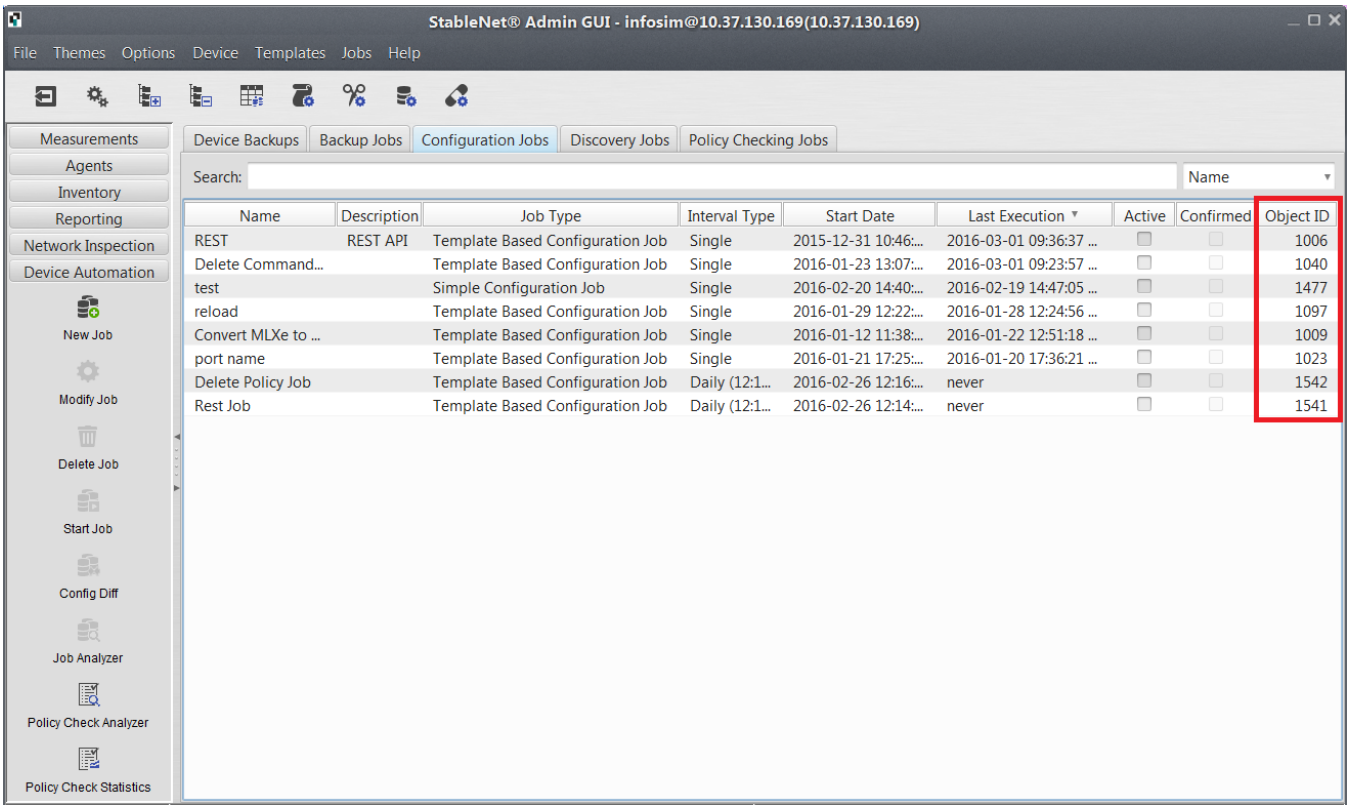
17. Click to select the **Object ID** check box and click **Ok**.

FIGURE 20 Job Template Settings



The Configuration Jobs tab now includes the Object ID column.

FIGURE 21 Object ID column



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 57.

Template Based Configuration Job

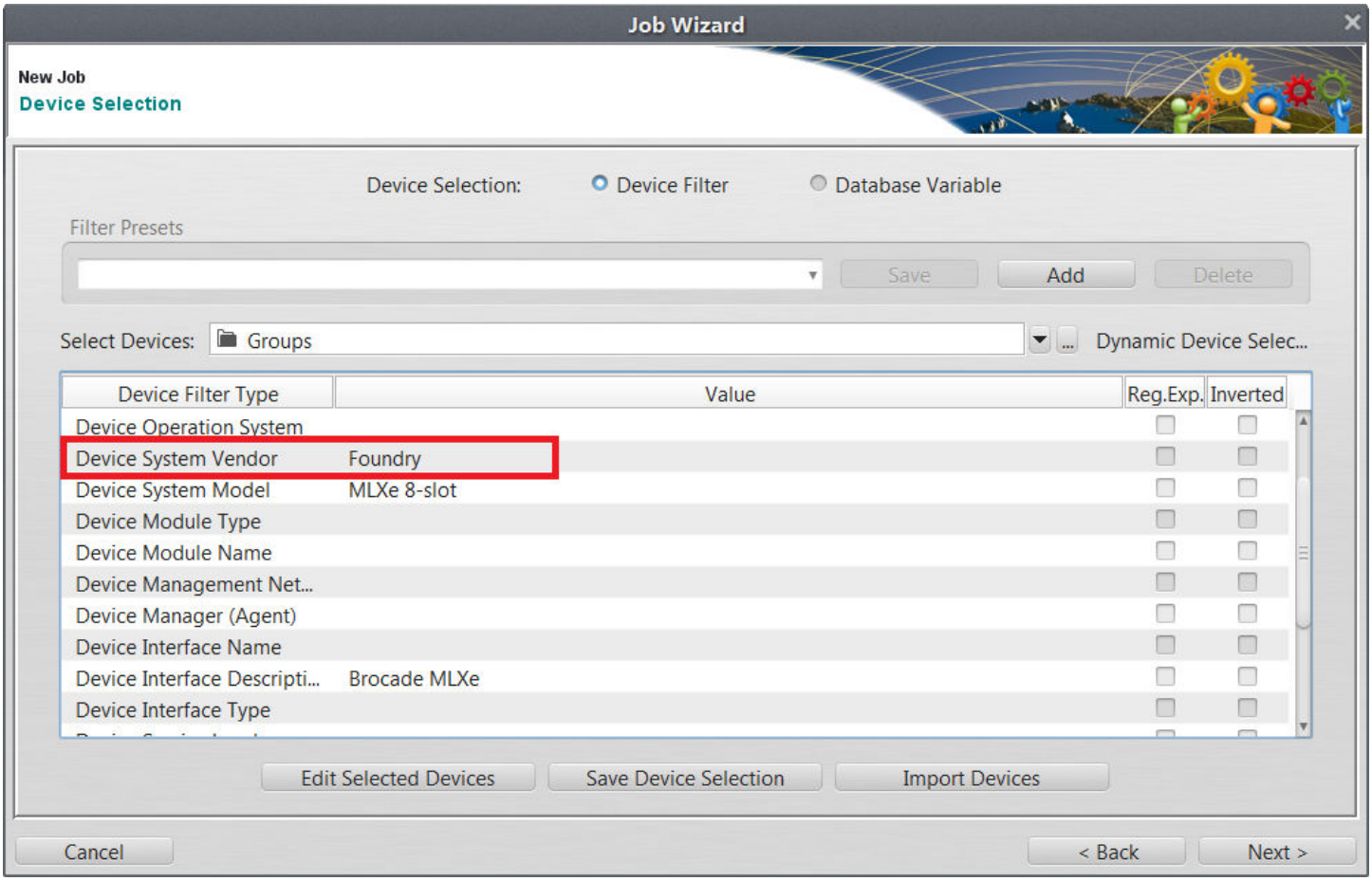
When creating a Template Based Configuration Job, it is possible to filter the devices on which a job will be executed. The job can be applied on a single device or multiple devices based on how the job is created.

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.

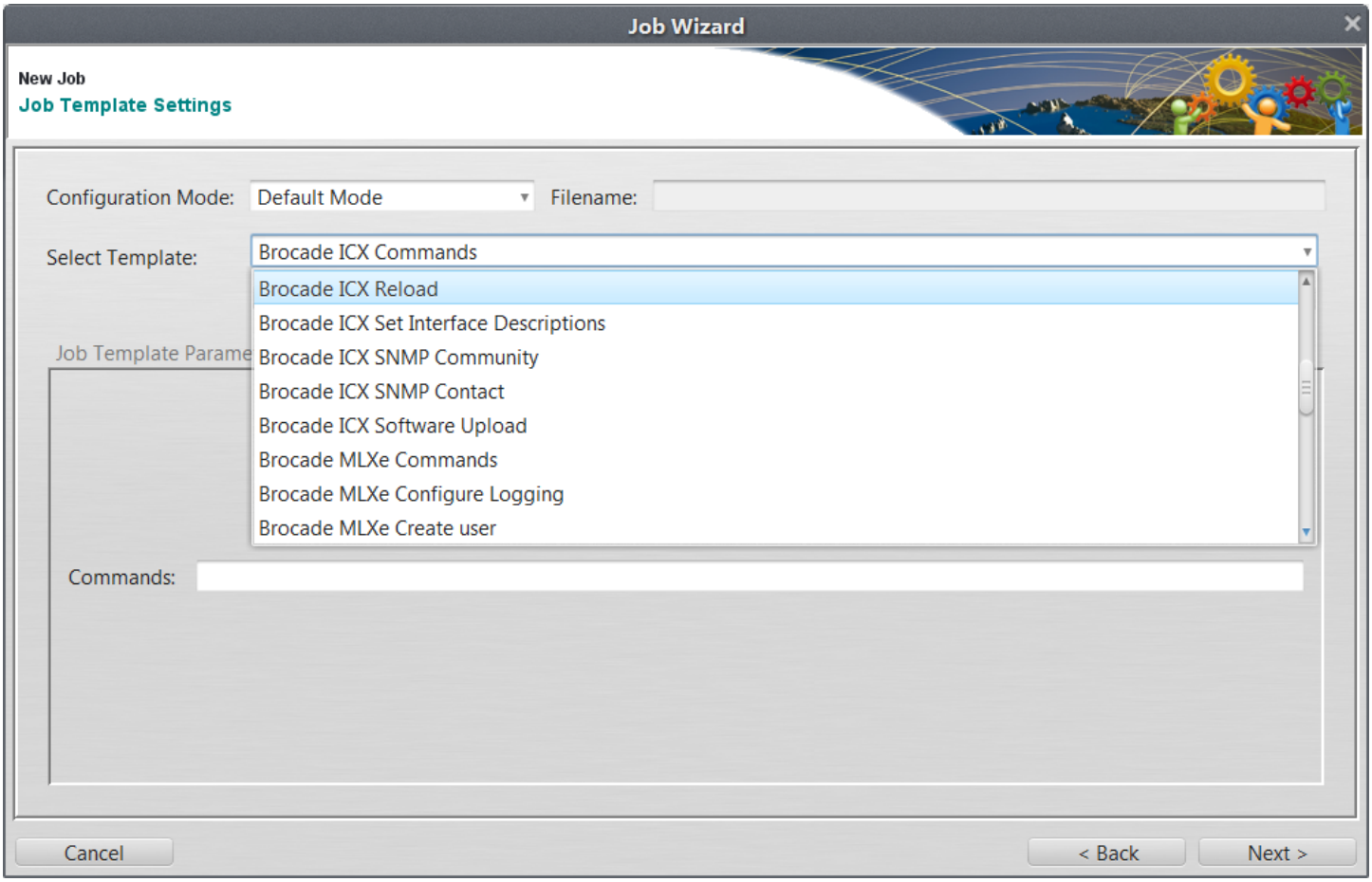
   NOTE
   Change the value of the **Device System Vendor** field to **Foundry**. Leaving this field empty or providing a different value for this field can cause issues with MLXe device detection.

FIGURE 22 Device Selection window



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 23 Job Template Settings window



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

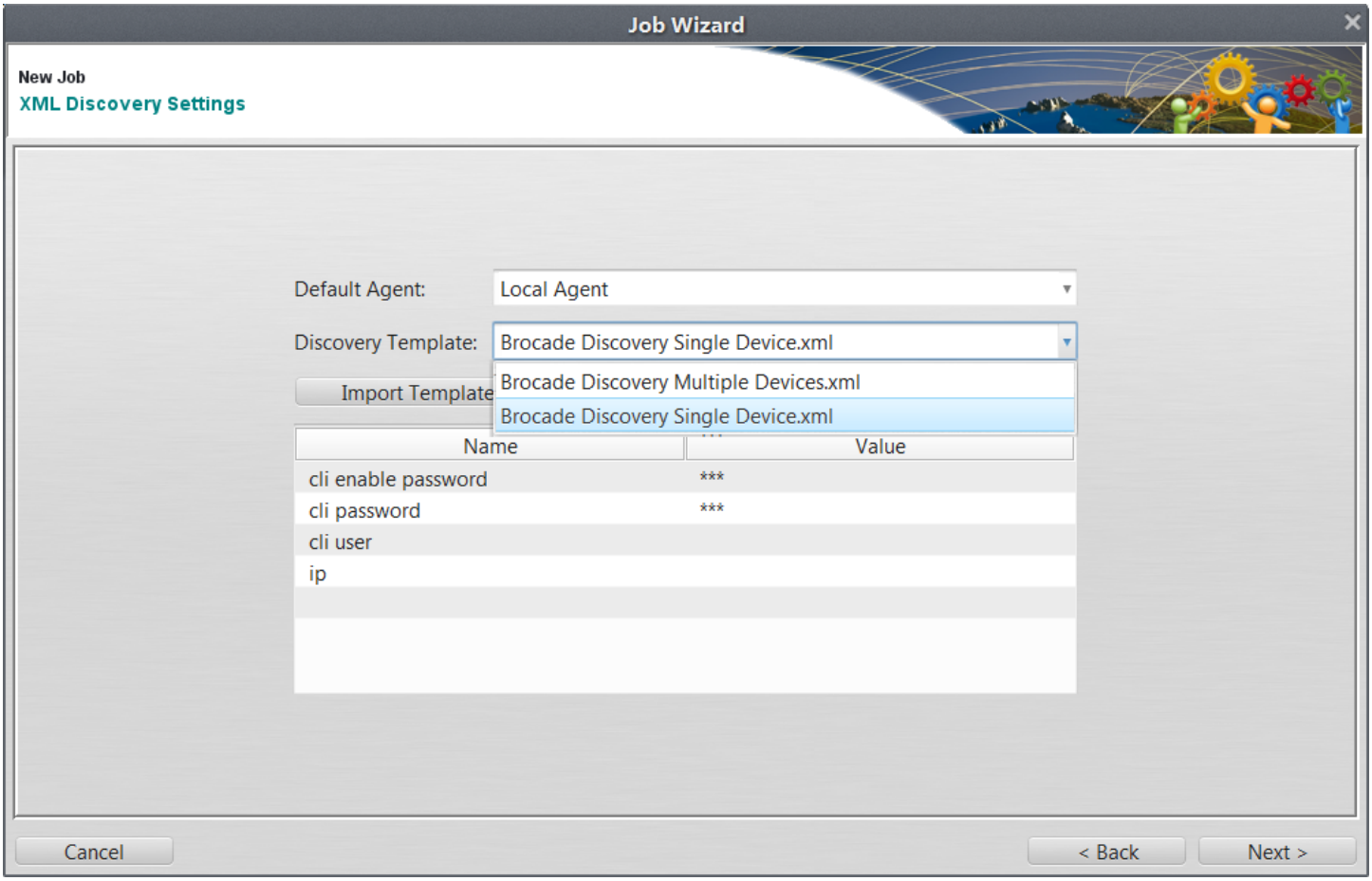
TABLE 1 List of Brocade-specific Templates (continued)

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 24 XML Discovery Settings



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**.

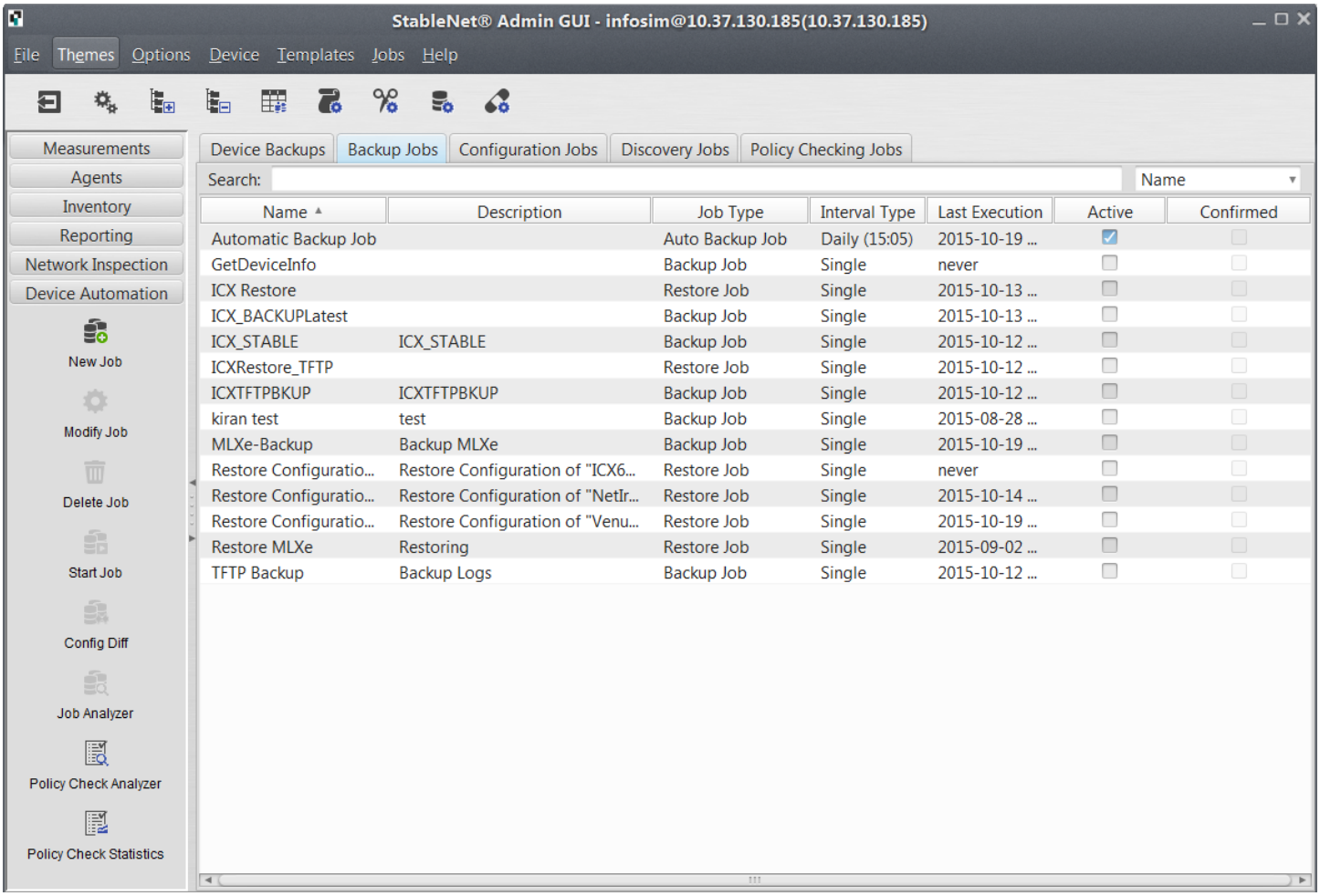
   NOTE
   For discovering newly added ACLs/Filters on MLXe or ICX devices, follow step 5 to step 9.

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 25 Automatic Backup Job



Measurements

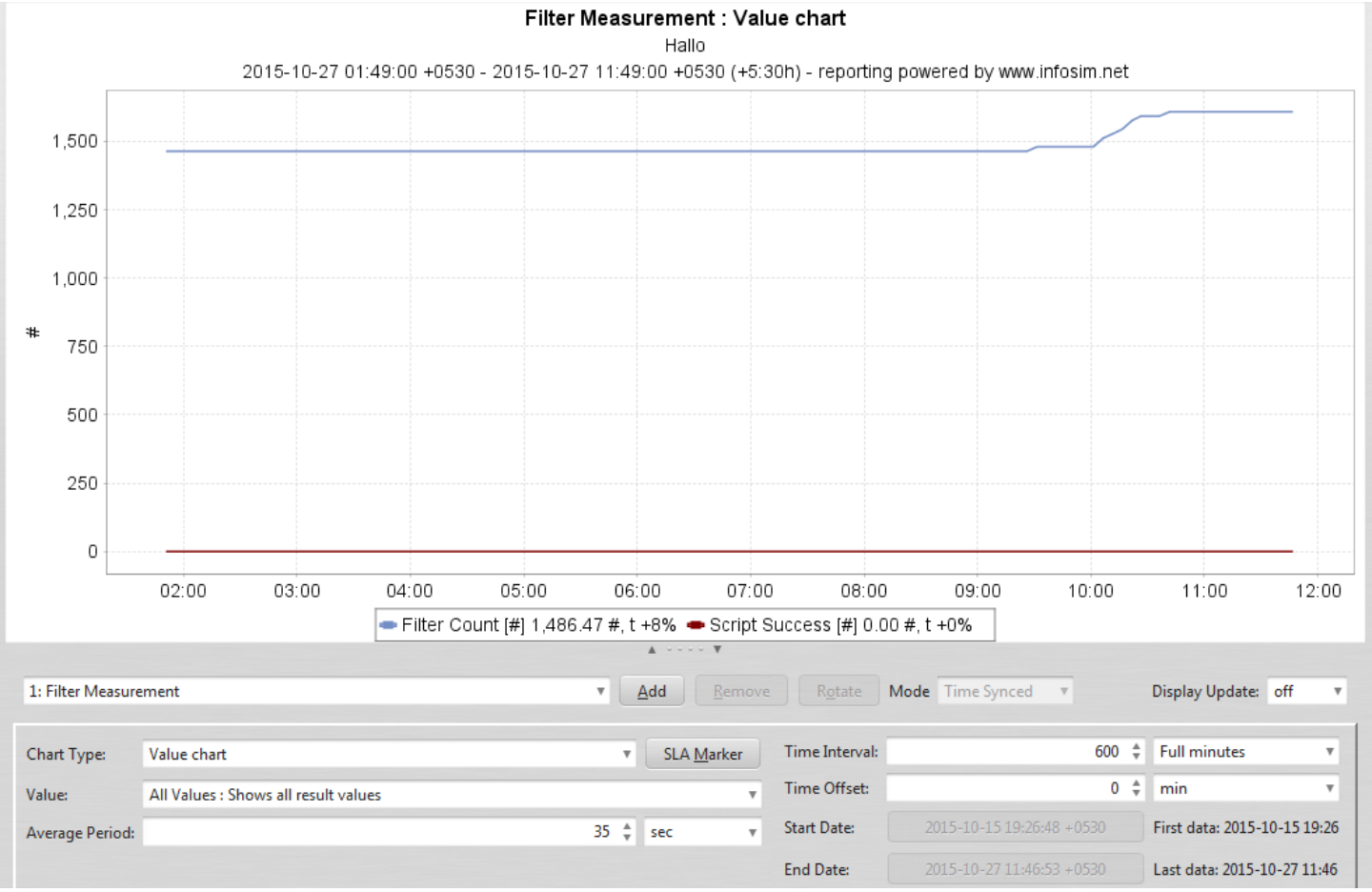
A measurement is a recurring measurement job that is configured to acquire data from one of the devices. Measurements collect data that can be used later, for example, for performance analysis or to get notified if the system is not working as expected.

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.

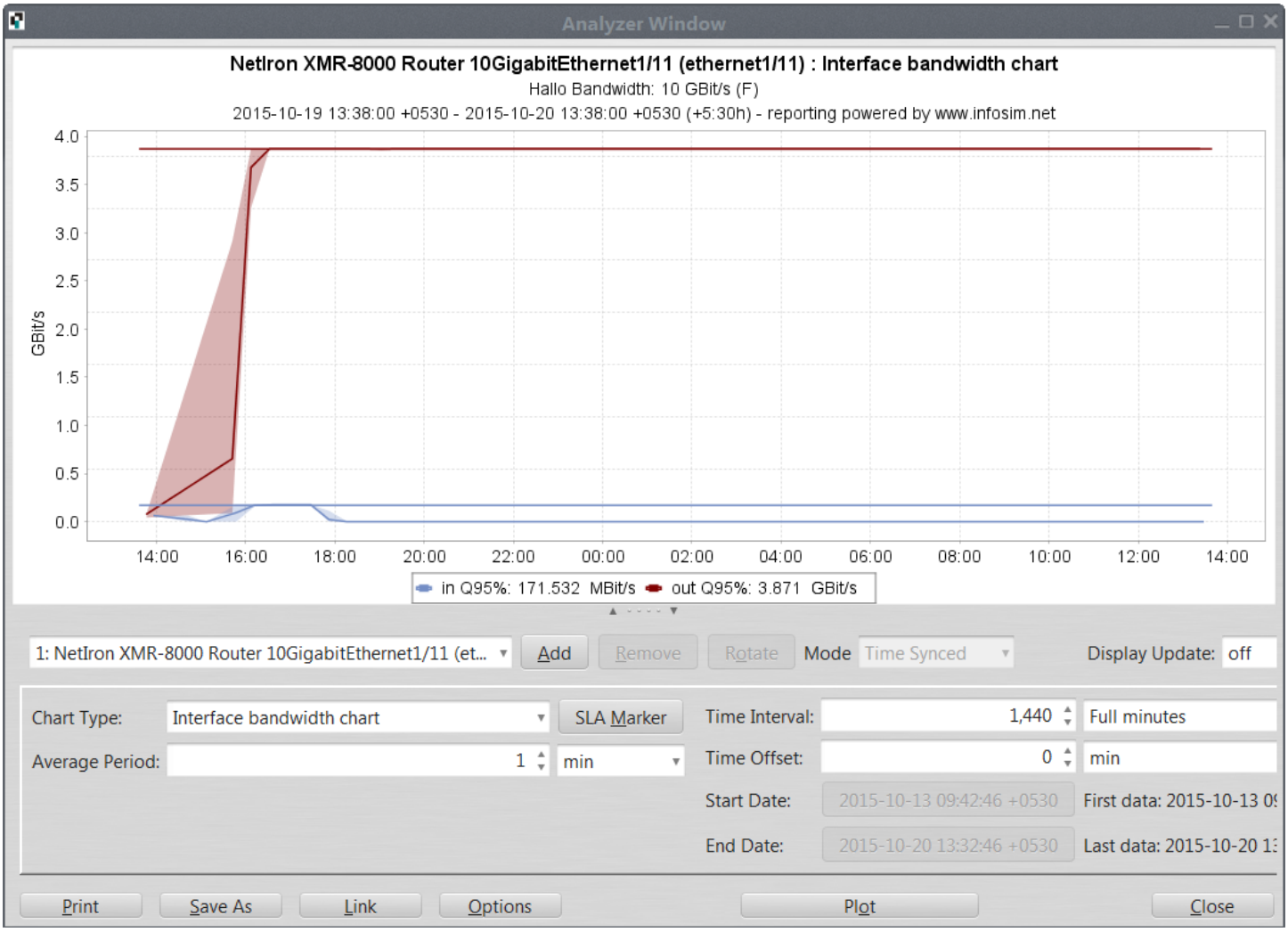
The figure below shows an sample chart plotted for a module:

FIGURE 26 Filter - Chart



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

FIGURE 27 Module - Chart



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.*

Getting Started with Brocade Visibility Manager App

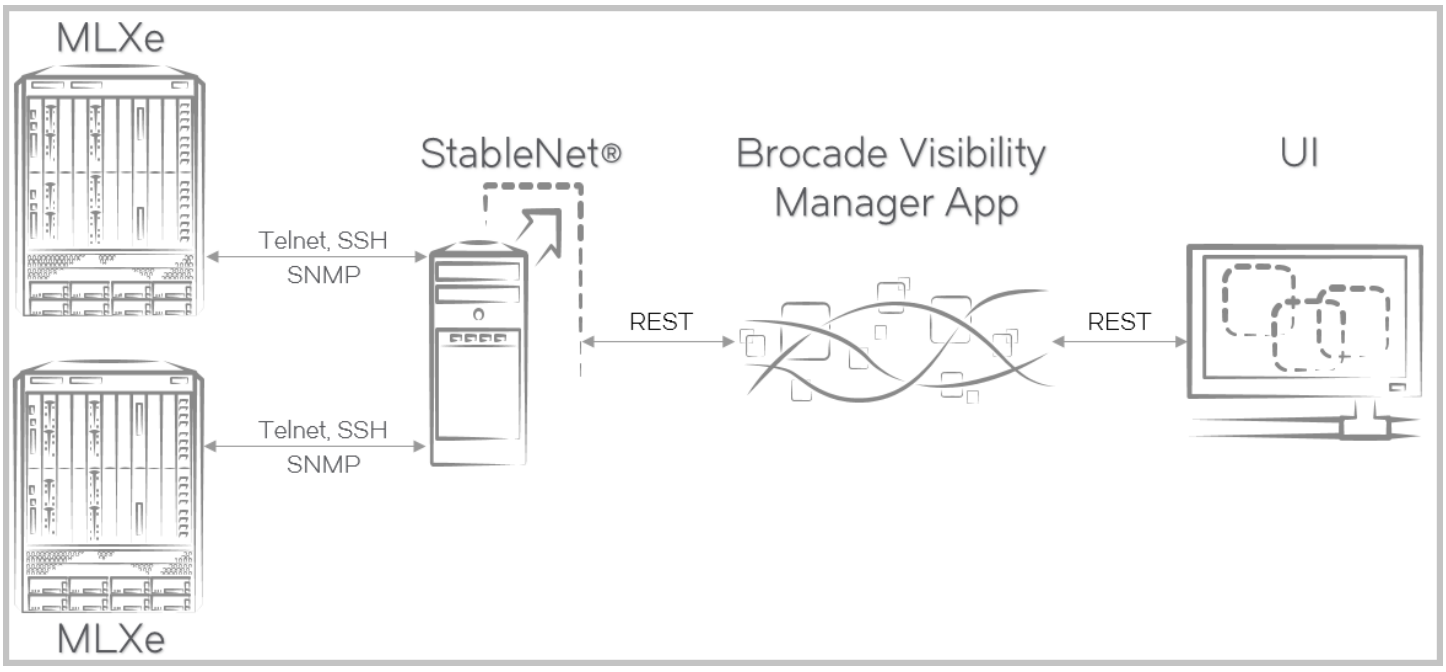
Introduction

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 28 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

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 59.

   To perform a fresh installation of the Brocade Visibility Manager database, skip to the section Installing Brocade Visibility Manager App on page 54.

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 31.

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 31.

   - 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 17.

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

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

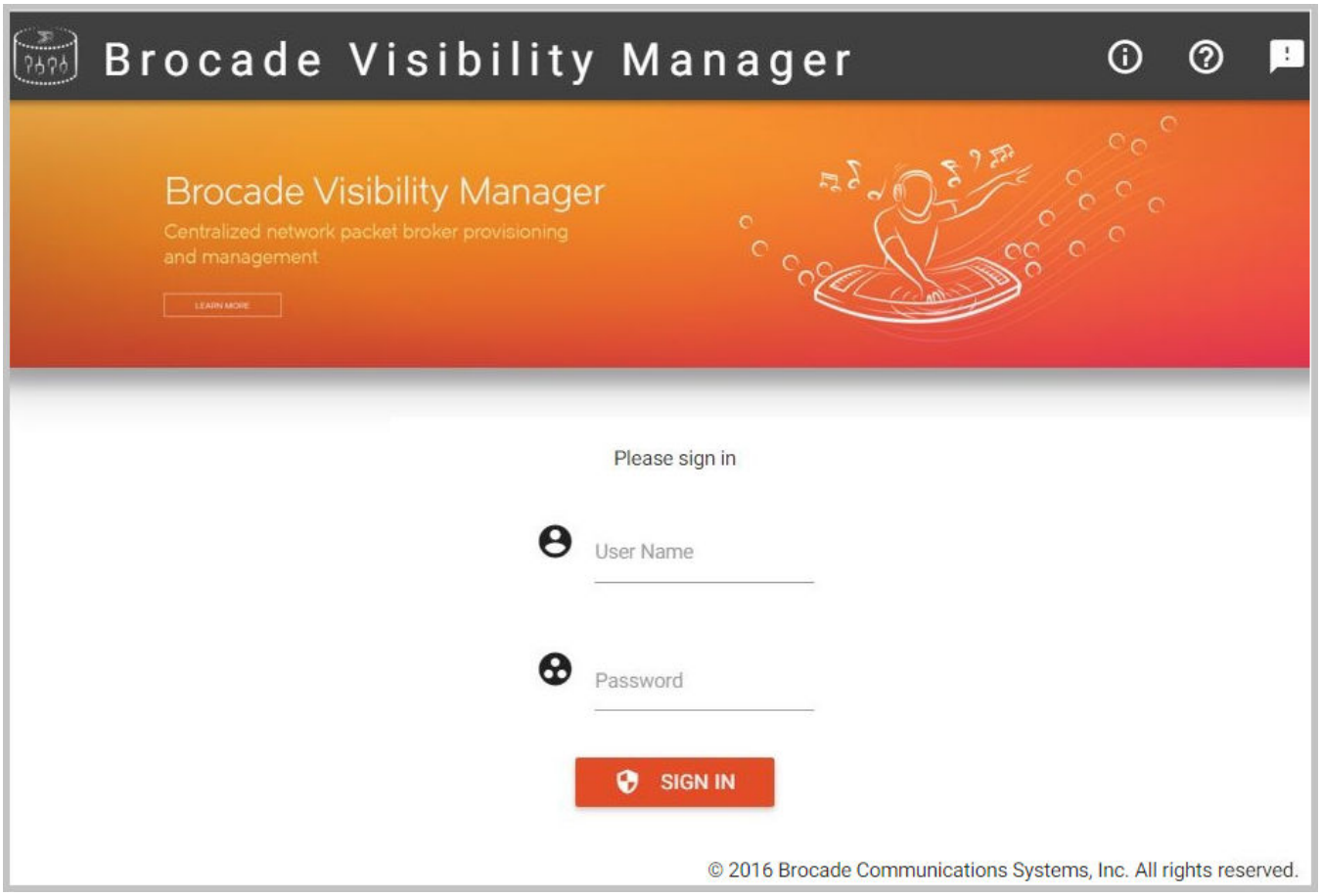
Perform the following steps to access Brocade Visibility Manager App:

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 57.

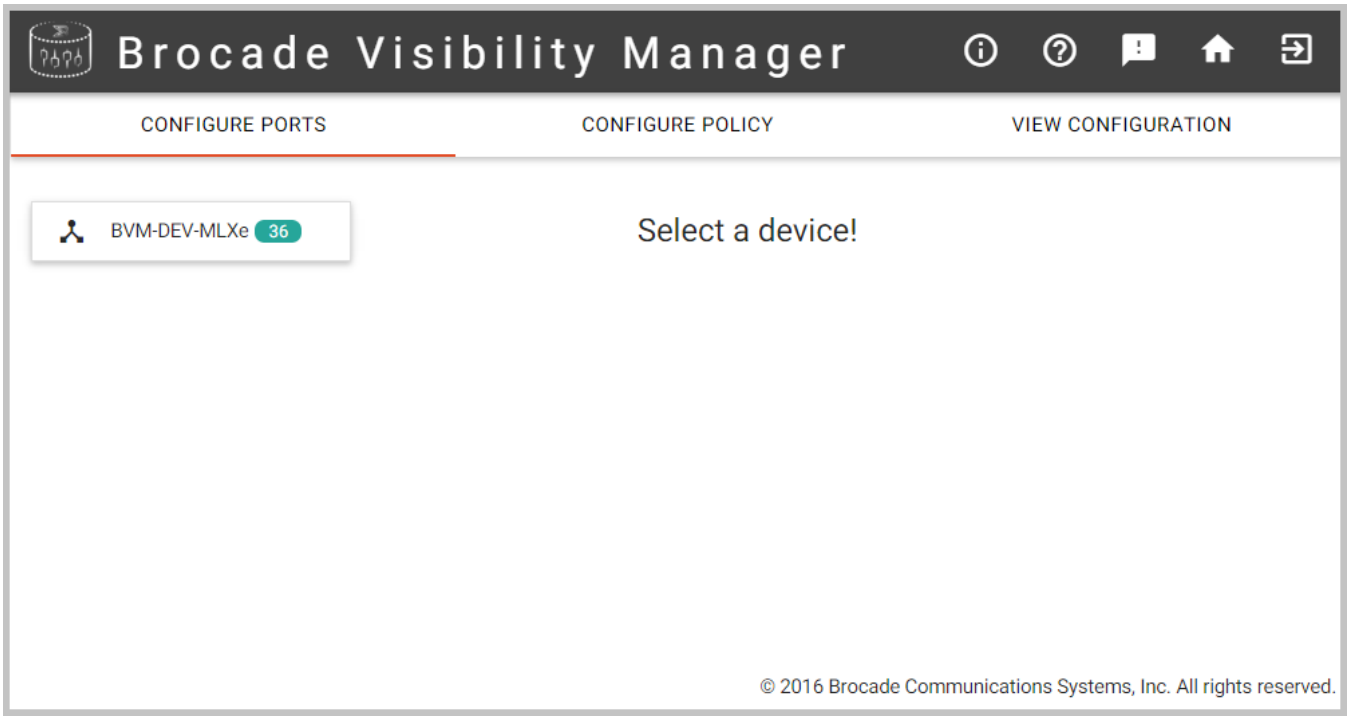
2. The Brocade Visibility Manager App login screen appears.

FIGURE 29 Brocade Visibility Manager App login page



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

FIGURE 30 Brocade Visibility Manager App home page



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®:

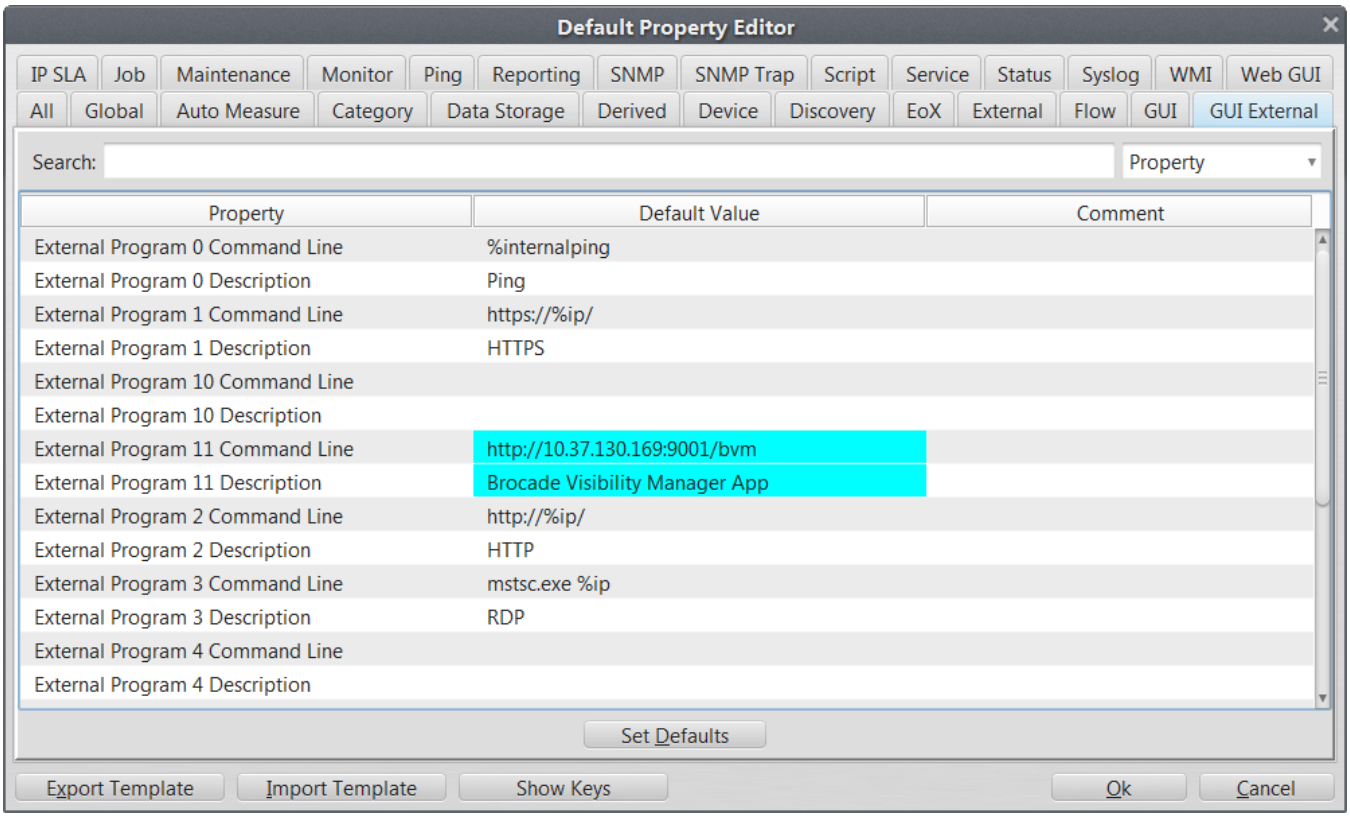
1. Login to StableNet® using thick client.
2. Click the **Default Property Editor** icon.

   The **Default Property Editor** window appears.

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

FIGURE 31 Default Property Editor - GUI External tab



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®

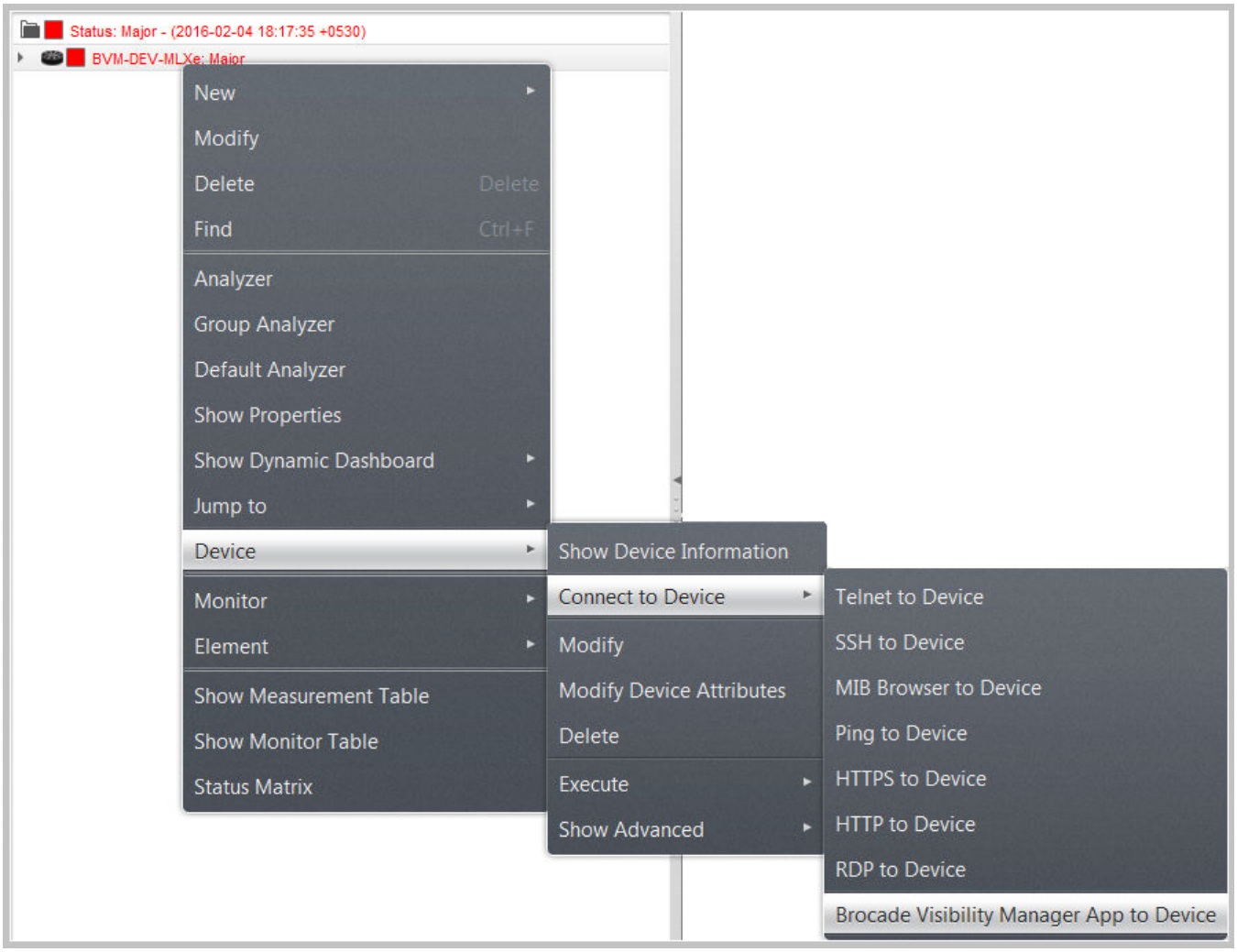
After creating a link to Brocade Visibility Manager App from StableNet®, perform the following steps to access Brocade Visibility Manager App using StableNet® .

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 32 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.

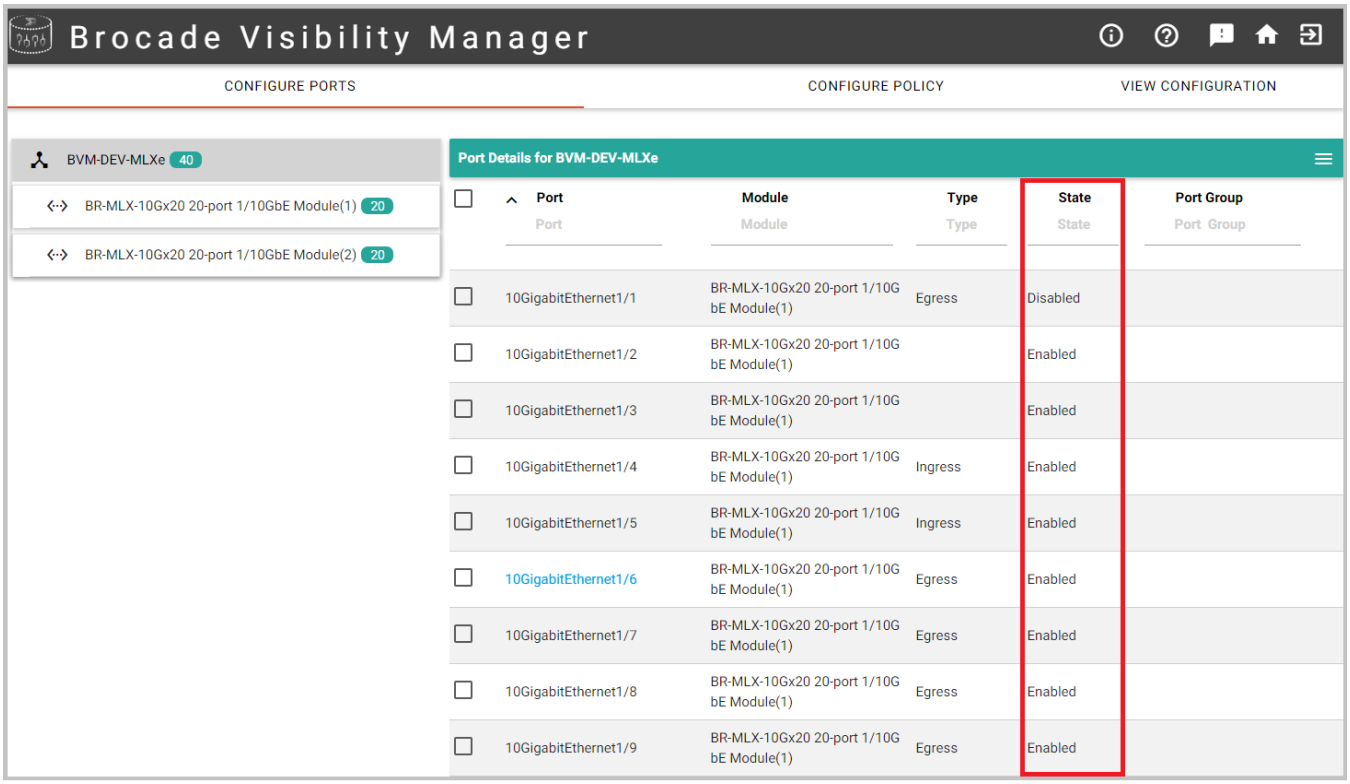
Enabling and Disabling Ports

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 33 Ports enabled/disabled



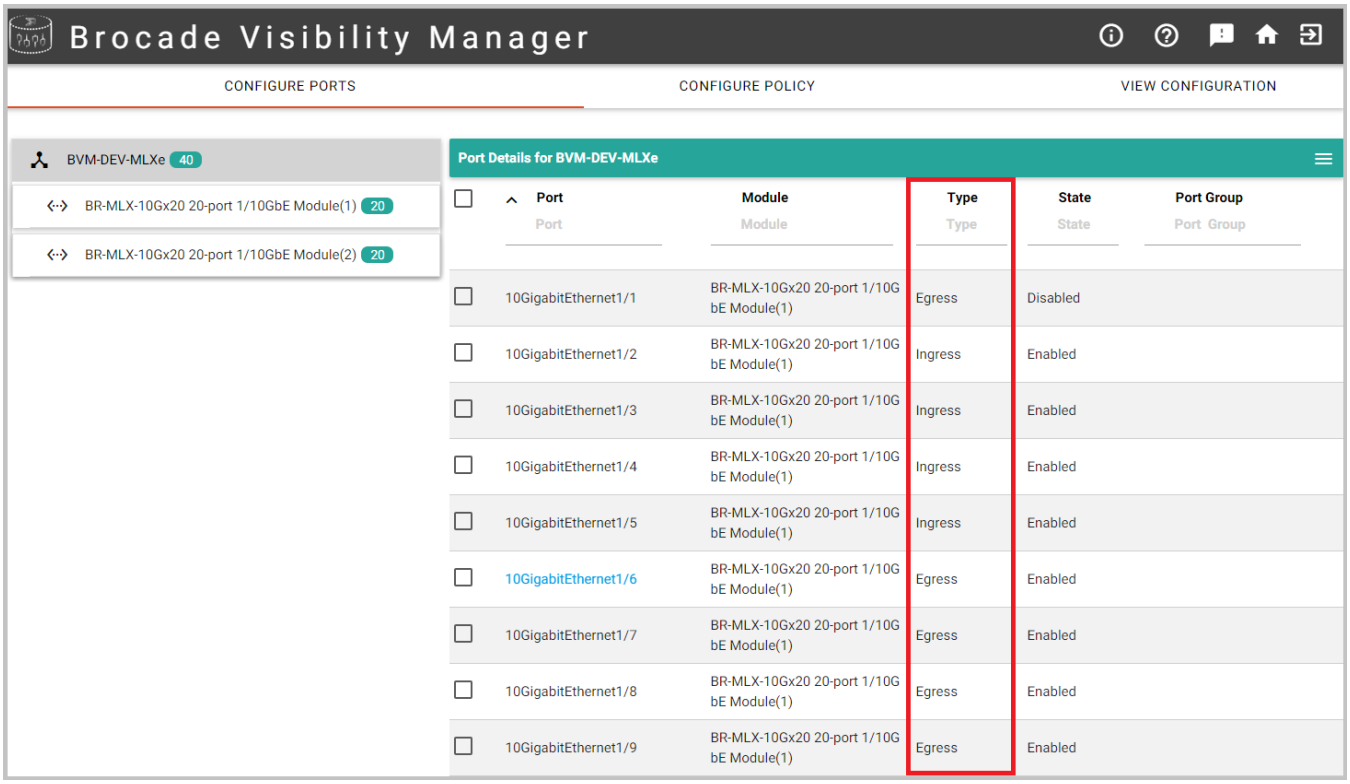
Configuring Ports as Ingress or Egress

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 34 Ports Ingress/Egress



Resetting Port Type

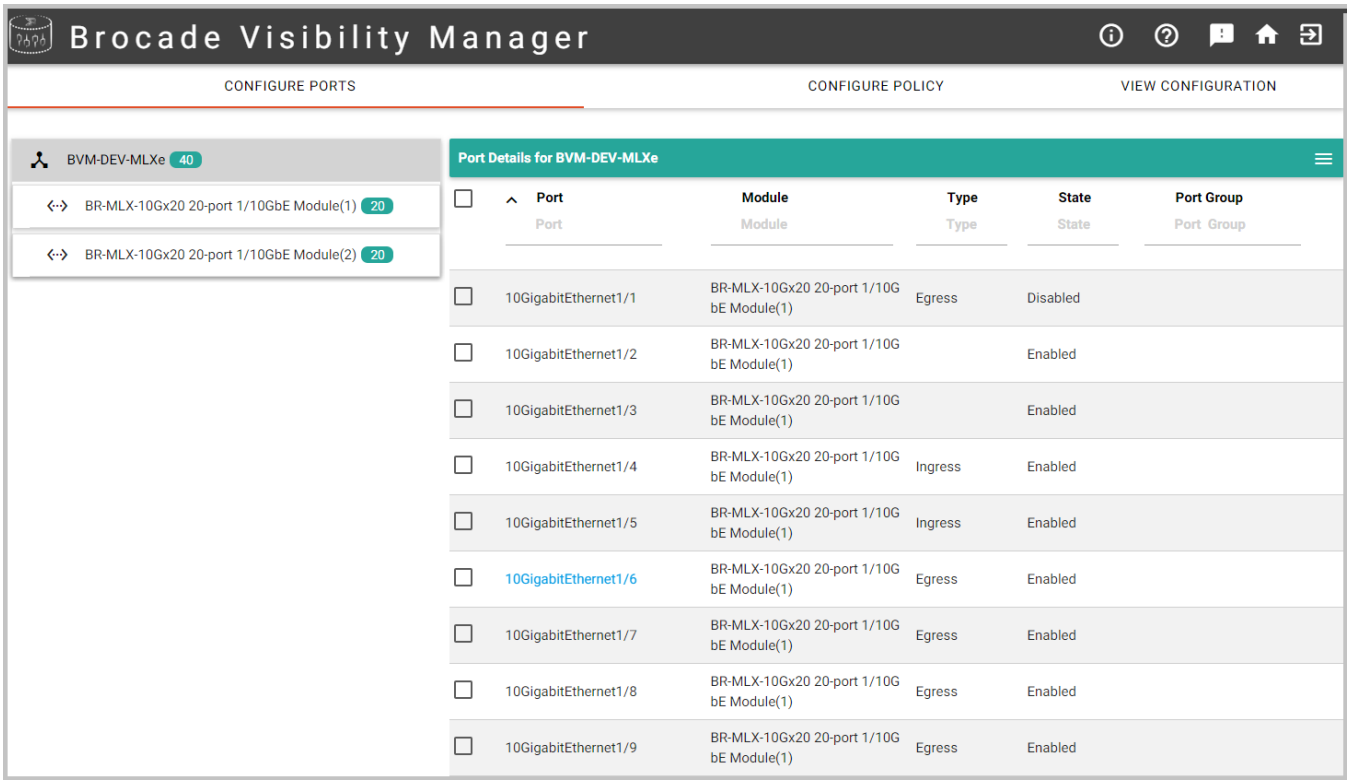
A port's type setting can be reset using the **Port as None** option. This is especially useful for resetting ports that have been set as Egress or Ingress.

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 35 Ports Ingress/Egress



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:

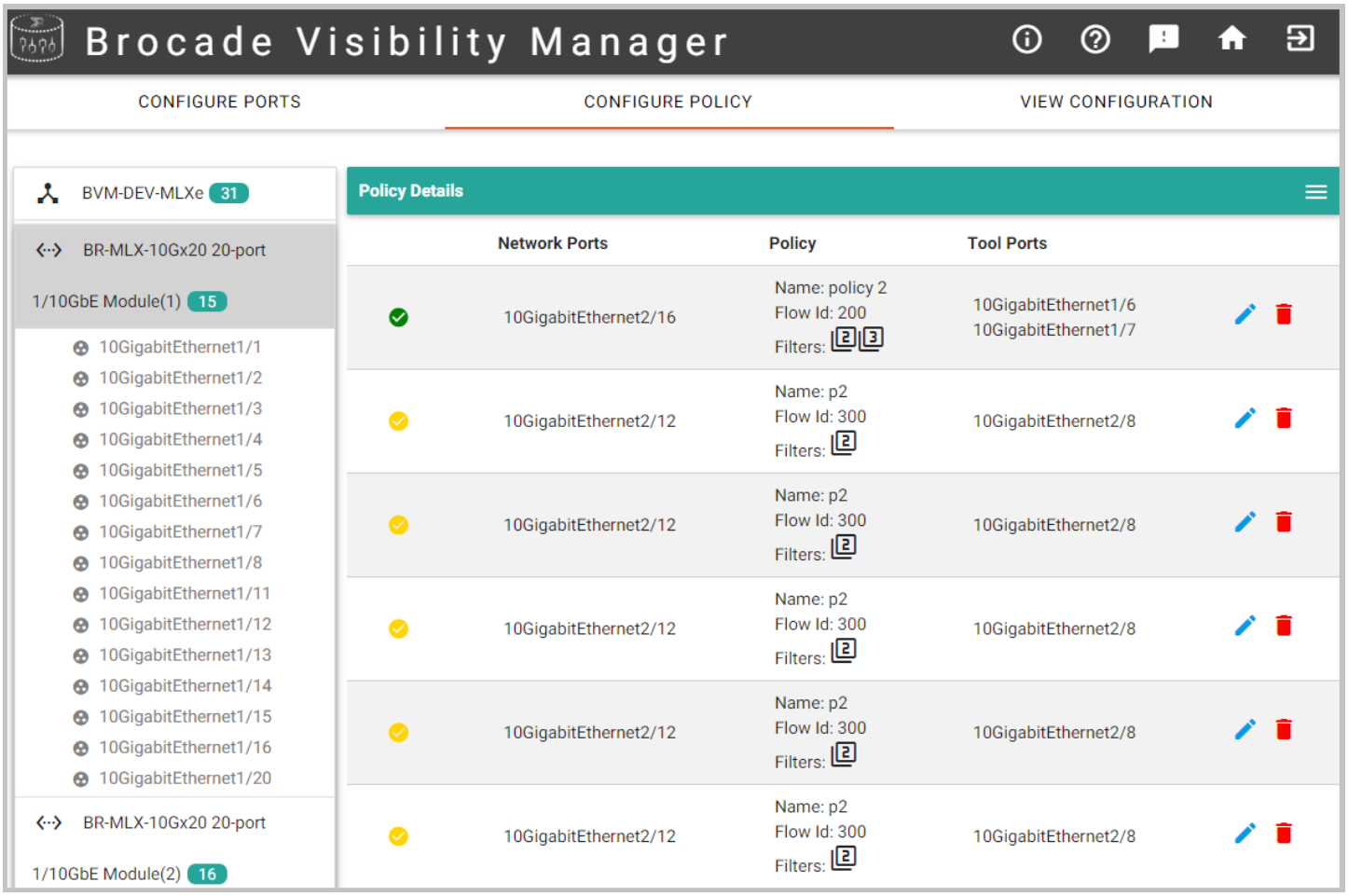
Option	Description
ACL Type	Select one of the following ACL types: • IPv4 • IPv6
Action	Select one of the following actions for the selected ACL: • Permit • Deny
Protocol	Filter based on one of the following protocols: • TCP • UDP • IP • SCTP • ICMP • IGMP • Others
Source IP	Filter based on source IP.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



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.

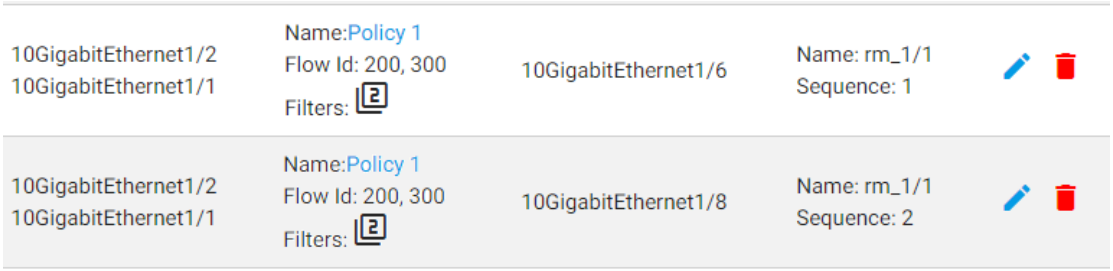
3. To fix an error, delete the configuration. When a configuration is deleted, it cleans up the device for that particular policy. It is then moved to saved state.

Use Cases

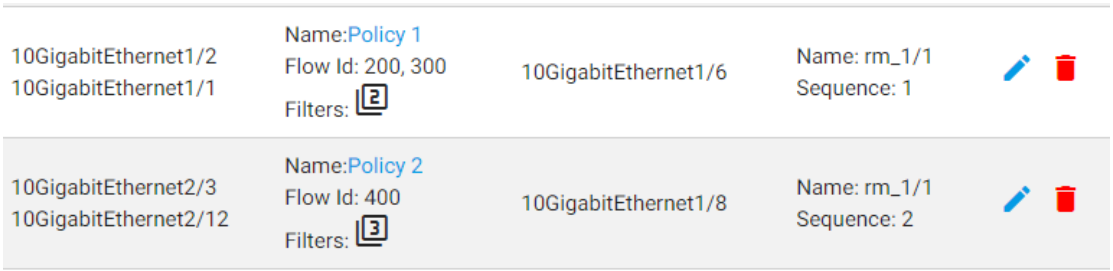
The section includes some common aggregation and replication use cases.

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.



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.



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.

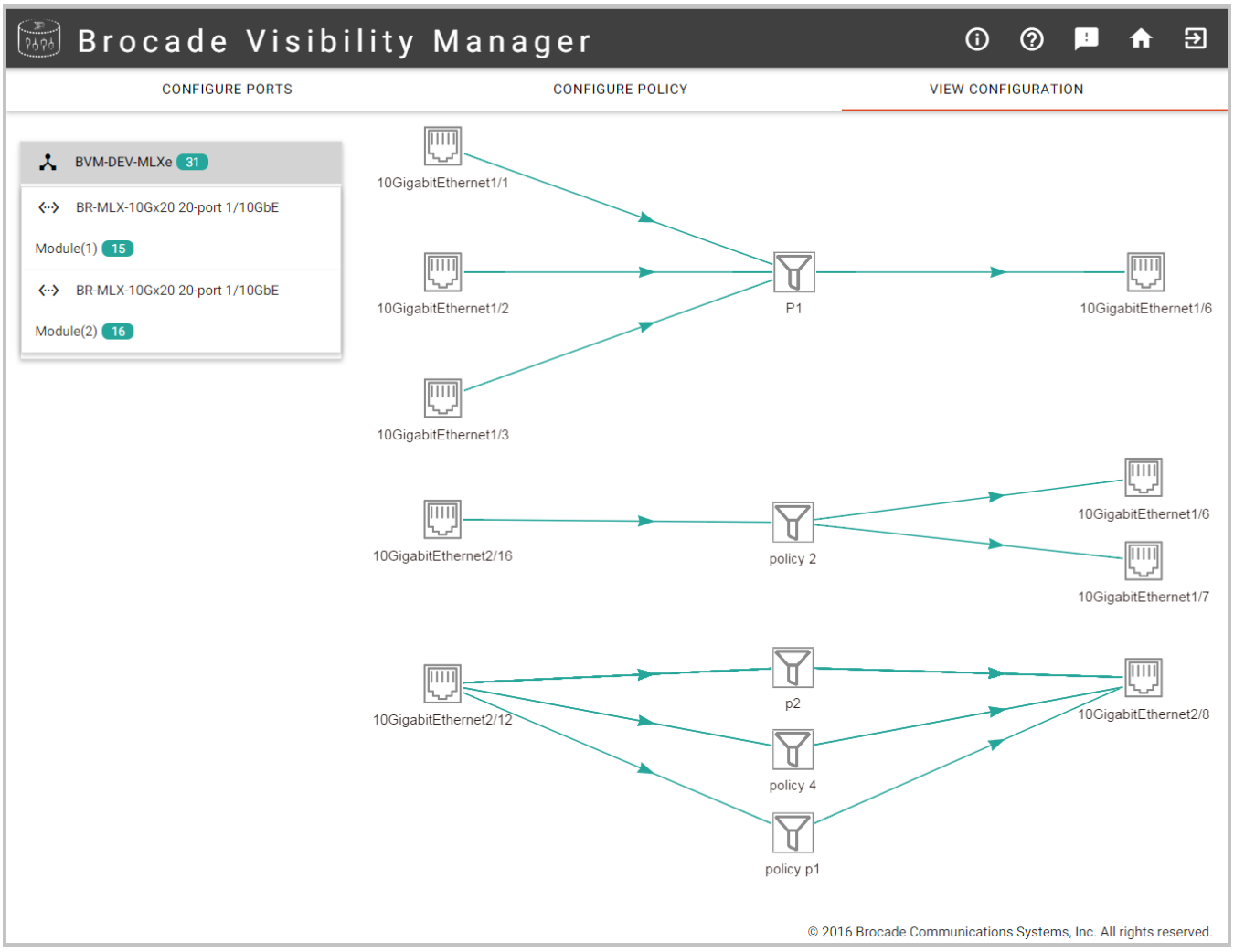
Viewing a configuration

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 37 View configuration



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

FIGURE 38 Policy details