Introduction

Note: Infoblox recommends that NetMRI deployments conform to data center security SAS 70 guidelines.

Infoblox NetMRI™ is a network automation and management software that automatically analyzes and detects network configuration vulnerabilities, changes, and health issues. NetMRI collects configuration and performance data for nodes throughout the network. NetMRI then analyzes that data to generate information for network managers to address problems and improve network reliability and performance. The NetMRI offers a set of specialized network management products to provide solutions to specific requirements in managed networks based on a few licensing options. For more information about, see NetMRI Licensing.

What's New

Note: For additional information about improvements and updates in NetMRI 7.2.1, see the Release Notes.

The following features are new or provide significant updates for this version of NetMRI:

- **Licensing enhancements**: Starting with NetMRI 7.2.1, you can apply a new license or modify the existing license using the license generate administrative shell command on a NetMRI physical appliance. To use this command on a NetMRI virtual appliance, contact Infoblox Technical Support at the following URL http://support.infoblox.com to generate a license file or enable this command, so you can generate a license file on your own. You can continue to use the License Management page as well. For more information about NetMRI licensing, see NetMRI Licensing.
- **Cisco APIC Support**: NetMRI expands its support to discover Cisco API Controllers. You can configure Cisco APIC (Application Policy Infrastructure Controller) on NetMRI and discover Cisco APIC components, such as SDN Controller and Elements, including spine switches, leaf switches, EPG (End Point Group). For more information, see Configuring Cisco APIC.
- **Python Scripting Support**: NetMRI is now supporting python scripting as well. For information, refer to the Python Scripting section in the online help.

Integrating With NetMRI

NetMRI collects, organizes and displays information in an array of customizable tables, graphs and reports covering virtually every aspect of network operations. Infoblox dedicates its efforts to allowing its customers to make effective use of this data, as easily as possible. Infoblox provides several ways to integrate with NetMRI, with varying degrees of simplicity, flexibility and power.

User Interface Exports

Many NetMRI information and results displays can be exported as CSV files, Microsoft Excel spreadsheets and PDF documents. Before developing a program to extract data from the NetMRI database using the API, determine whether it is easier to obtain the needed information through the GUI.

Notifications

When significant events occur, notifications allow external users and systems to receive e-mail, Syslog, or SNMP traps from NetMRI. This method of integration is the simplest for most one-way, system-to-system solutions. You can use the NetMRI user interface to configure the notifications of interest, filter out those that are not important, and set delivery time-windows and destinations. See the NetMRI online Help topics under Event Notifications and System Health Monitoring for more details.

NetMRI Application Programming Interface

The NetMRI Application Programming Interface (API) enables external programs to retrieve information about devices, interfaces, VLANs and other network entities from the NetMRI database. It also enables programs to retrieve information about neighbor relationships between devices, and send commands to NetMRI. This is the most powerful method of integrating with NetMRI, and the most difficult. API integration requires knowledge of Perl or other programming languages. For more information, see the NetMRI API Developer's Guide under Additional Documentation in the Online Help and the NetMRI API under Tools → Network → API Documentation.

About NetMRI

Beyond monitoring traffic flow and generating alarms every time thresholds are passed, NetMRI periodically analyzes the contents of all router and switch tables to detect device-level problems, such as router and VLAN instability. Beyond reporting that a given serial link has an excessive error rate, NetMRI analyzes the configuration of the interfaces on both sides of the link to determine what is causing the excessive error rate. NetMRI also tracks changes in status and configuration for all managed devices and displays the Detected Changes and Most Changed Devices listings in an accessible dashboard view.

NetMRI is a network management interface to analyze and monitor devices and enterprise networks, their protocols and their configurations from a convenient Web browser window. The primary browser pages are called the NetMRI Dashboards. The Dashboards are your home pages for managing devices on the network. The Dashboards provide easy access to tasks and to the status of the networks.

NetMRI provides a layered system of tabs to access and operate features of the software. The top layer of the NetMRI tabbed interface provides the six key functional areas of the software, consisting of the following pages.
The NetMRI Dashboards

The Dashboard tab provides three high-level Dashboard summaries of information and network analytics, selectable from the Select Dashboard menu at the top of the page.

- The Timeline Status Summary displays the Network Scorecard (seen here), a numeric metric that provides an at-a-glance overall assessment of the current state of the network. The Timeline Status Summary also provides graphs showing most-changed devices, a policy compliance breakdown, and historical graphs of percent compliance, issue variation and changes:
  - Under Timeline Status Summary, the Policy Compliance chart shows the daily percentage of all managed devices, as a pie chart, that match against Policy Compliance Rules from the defined Policy Compliance criteria in the NetMRI system. The Percent Policy Compliance bar chart shows the same daily data as a progression from one day to the next;
  - The Issue Variation chart lists the following data points for the overall daily issue status in the NetMRI system or the Operations Center: the daily Overall Score in yellow, the total issue count and Delta (change in number of Issues; this value can be positive or negative for the time period measurement) in blue; and the number of Added and Deleted Issues in blue. A yellow trendline shows the Overall Score trend over the chart's time period. Green dots at the bottom of the chart are the activity indicators for the measurement time period, showing the number of added or deleted issues. Clicking the trendline opens the Network Analysis → Issues page, showing the corresponding Overall Score History stacked bar chart;
  - The Change Summary dashboard provides a bar chart and trendline for specified time increments, with the bar chart indicating the total number of changes, breaking out the administrative and hardware changes for the time period, and the trendline showing the average rate of changes across the entire chart time period.
- The useful Issue Summary also replicates the Network Scorecard, shows a Top Issue Types bar chart and a Top Affected Devices bar chart, and displays historical graphs of Issue type and instance trends.
  - Two important bar charts, Top Issue Types and Top Affected Devices, show at a glance the issues that appear most frequently in the managed network; and the devices exhibiting the largest number of Issues;
  - The New Issue Types table lists all new Issues of specific types that appear for the current time period (corresponds to the #New column in the main Network Analysis → Issues page);
  - The New Issue Instances table provides the number of devices affected by each issue type (this value corresponds to the #Affected value in the main Issues page);
  - The Type Issue Trend area chart combines sections for severity Info (blue), severity Warning (yellow) and severity Error (red), each of which are links to the main Issues page showing a table only for the issues of the chosen severity type.
  - The Type Instance Trend area chart combines sections for severity Info (blue), severity Warning (yellow) and severity Error (red), each of which are links to the main Issues page showing a table only for the issues of the chosen severity type.
  - The Change Summary shows most-changed types, most-changed models, most-changed devices, number of changes detected over time, and most-active change makers.

Note: In the Timeline Status Summary dashboard, the zero value in the Issue Variations chart's Y axis corresponds to the average number of issues for the shown time period.

The main Dashboard page and Network Analysis → Issues pages display the Network Scorecard, which is a quick-guide to the overall status of all Issues in the managed network. (See About the Network Scorecard for more information about this tool.)

- To select among the dashboard types: Open the Select Dashboard list, then click the desired type.
- To change the date or period for information displayed in the Dashboard: See Setting the Date and Period.
- To change the scope of information displayed in the Dashboard: Select an item in the Select Device Groups panel.
- To view supporting data: Hover the cursor over various elements in graphs and charts.
- To zoom in the Timeline Status Summary graphs: Drag to select the section you want to see zoomed in. When you release the mouse button, all three graphs will zoom in.
- To zoom out the Timeline Status Summary graphs (after zooming in): Click Show All below the center graph.

Network Analysis

Network Analysis also features the Network Scorecard on its front page. Information is organized in four tabs within the Network Analysis page:

- The Issues tab summarizes current network status, showing the same scorecard that appears on the main Dashboard; a flexible Network History chart; and an overview of current problems and possible problems in the network;
- The Changes tab summarizes all recent changes made to the network, and provides features to change the information displayed in the summary table;
- The Policy Compliance tab summarizes the results of Policies developed in the Policy Compliance features for device groups and active devices in the network;
- The Performance tab summarizes active device operations in charts and tables.

Network Explorer

The Network Explorer tab displays everything NetMRI learns about the network. Network Explorer is a good starting point for inspecting the results of a Network Discovery process, viewing the topology of the discovered network, viewing the operational state of individual network devices (through a feature called the Device Viewer), and obtaining views of how the network is behaving in different locations in the topology.

Tabs within the Network Explorer tab offer different ways to examine network data:

- The Inventory tab provides basic information about devices, interfaces, operating systems and models in the network.
- The Summaries tab lists routes (for all routing protocols), subnetworks, Route Targets, Network Views, VRFs (Virtual Routing and Forwarding instances), VLANs, HSRPs/VRPPs and TCP/UDP port usage in the network.
- The Topology tab provides an interactive viewer for exploring your network's structure.
• The **Discovery** tab provides detailed information about NetMRI's discovery processes, including the ability to affect Discovery settings for individual devices, perform/repeat Discovery on a single device, set licensing for a managed device and remove a device from NetMRI management. (For more information on device-related Discovery functions, see Viewing Device Discovery Status and Re-Discovering a Device.)

**Configuration Management**

Configuration Management provides a powerful set of features for managing, normalizing and editing configurations for all devices managed by NetMRI, including the following:

• The **Config Archive** tab lists all devices in each Device Group, and is the front end for browsing, viewing, and editing configuration files from any active device, or comparing two devices in the managed network. Configuration files drive the operation of higher-end routers, switches, firewalls and other device types across the network. You can read, edit and compare similar-device configuration files across the network;

• The **Config Search** tab lets you search devices in the network for a particular configuration string, an IP address or other specific device specification such as a MAC address, device model or other phenomena, using many different types of search criteria and even regular expressions;

• The **Job Management** tab enables creation, scheduling, approval and execution of Job Management scripts in the Perl and CCS languages, and the definition of custom issues to extend the library of issue types that NetMRI uses for reporting and monitoring of adverse events in the network. **Job Management** is used to automate common network administration tasks, and efficiently enforce normalization and best-practices configuration across the managed network. A critical feature set classified under Job Management is the Automation Change Manager (ACM), that leverages NetMRI's scripting capabilities to support a set of Infoblox NIOS network automation utilities. Subcategories of Job Management include the following tabbed pages:
  • The **Scripts** tab lists all scripts in the NetMRI system;
  • The **Library** tab provides a location for CCS and Perl subroutines that can be called by other scripts;
  • The **Config Templates** tab, a location for templates containing configuration snippets and variables for easier job automation;
  • The **Lists** tab, a second library page, for lists of spreadsheet-type list data for use in automation jobs;
  • The **Scheduled Jobs** tab, showing the current list of scheduled automation jobs;
  • The **Triggered Jobs** tab, showing the current list of recently triggered jobs;
  • The **Job History**, showing the complete history of automation jobs run in the NetMRI managed network;
  • The **Custom Issues**, that allows definition of custom issues based on job execution;

• The **Policy Design Center**, to create rules and policies, and deploy policies on the network. Policies are a tool for ensuring all devices in the network meet minimum standards of readiness and security. Rules are the building blocks that form a policy. You deploy policies against devices and groups of devices.
  • The **Summary** tab provides features for quick creation of Policy Rules, build a new Policy or schedule and deploy Policies;
  • The **Rules** tab allows exploring of the entire library of Policy Rules and the ability to create, edit, copy, import and export Rules;
  • The **Policies** tab provides general Policy management features, such as editing, printing and import/export, and to test Policies against devices, configuration files and configuration templates;
  • The **Policy Deployment** tab is where admins enable policies against individual devices or device groups.

**Reports**

The Reports page provides features to run publishable reports, from providing device information in a report, to reports across device groups or types of devices, to network-wide reports indicating trends across the network.

• The **Reports Gallery** lists standard and custom reports that are available in the current instance of NetMRI, and provides the interface to run and create new reports. Related Report types are gathered into categories where similar data sets can be compared and analyzed. See Scheduling and Running Reports for more;

• The **Scheduled Reports** tab lists reports that are currently scheduled to run from the NetMRI appliance, and allows the editing of scheduled reports to change their timing and configuration. See Scheduling and Running Reports for more;

The **Report Manager** tab provides listings of all Active and Inactive Reports for the current NetMRI appliance, and enables monitoring of currently running and active reports. See Opening the Report Manager for more information.

**Icons and Popup Windows**

NetMRI uses sets of popup windows to organize software configuration settings and provide detailed viewing for devices and networks. Clicking certain icons or links will bring up separate browser windows. Popup windows you will frequently work with include the following:

**Tools** — Provides a set of networking tools for inspecting and testing parts of the managed network. Included are **Ping/Traceroute** for verifying basic connectivity; **SNMP Walk** for retrieving SNMP variable information from a device on the network; **SNMP Credential Test**, for verifying whether a set of community string credentials will work for a given device; **Cisco Command Tool** for issuing a configuration command to a Cisco device; **CLI Credential Test** for testing admin login credentials; and **Discovery Diagnostics** for enabling troubleshooting by Infoblox Technical Support.

**Settings** — Provides several categories of important NetMRI software configuration settings governing how the appliance operates: **User Admin** (see Configuring Admin and User Accounts), for defining administrator accounts for the NetMRI appliance; **Setup**, a crucial block of settings for information collection; **Issue Analysis** (see Evaluating Issues in NetMRI), for configuring Issue Group settings and defining suppression of issues; **Notifications**, for defining user event notifications (see Event Notifications and System Health Monitoring); **Settings** for a diverse block of NetMRI-specific configuration elements including license management, system security protocols and Custom Fields definition; and **Database Settings** for copying, restoring and archiving (see etMRI Database Management).

**Define and Configure Network Editor** — Enables the assignment of unassigned VRFs to network views, and reassignment of VRFs to different views.

**Device Viewer** — The Device Viewer (see Device Viewer topic) is a popup window that provides many details about any single router, switch, firewall or other device, including interface configurations, device identification and location, functioning network services, neighboring devices in the network and other information.
**Interface Viewer** – Provides information on individual interface connectivity, performance and configuration settings.

**Network Viewer** – Lists VRFs that route traffic for the currently selected network, and VRFs imported from other VRF-aware devices that route traffic for the virtual network.

**Issue Viewer** — Shows detailed information about device Issues detected by NetMRI.

**Job Viewer** — Provides execution and error information about job scripts written and run through NetMRI.

The following table provides explanations about the various icons you will encounter in the NetMRI graphical user interface, including icons that appear in many tables in the system.

<table>
<thead>
<tr>
<th>Table Sample...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Created By</strong></td>
</tr>
<tr>
<td>admin</td>
</tr>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>

- **Copy** – copies a selected record.
- **Edit** – Click here to edit a record in a table.
- **Schedule** – Where applicable, schedules the item in the table for execution.
- **Run Now/Actions** – Where applicable, Run Now immediately executes the directives in the current table record. The Actions icon contexts provide features to execute against individual records in data tables throughout the entire NetMRI system.
- **Test Policy** – Where applicable, tests the currently selected Policy.
- **CSV Export** – Where applicable, exports the contents of the current record to a tab-delimited file suitable for viewing in Excel.
- **Delete** – Deletes a selected record from a NetMRI table.
- **Add** – adds a new record to a table of NetMRI items.
- **Tools** – Opens a set of networking utilities for network admins to perform troubleshooting and device communication tasks, such as Ping, Traceroute, SNMP Walks and other operations.

- **Background Task indicator bar** – Indicates NetMRI is performing a background task. Appears on the NetMRI toolbar and disappears when the task completes.
- **Settings** – An important icon providing a hierarchical list of configuration settings such as User Admin, Issue Analysis configuration, general Setup, Notifications setup, Database setup and other fundamental areas that define how NetMRI operates.
- **General online Help feature**, providing the entire online Help information window without specificity to the currently displayed feature page in NetMRI.
- **Context-sensitive online Help**, from which the currently displayed UI page can show Help for that feature in a separate popup window.
- **Refresh Grid** – allows refreshing of a complete table list or ‘grid’ of information. NetMRI collects the same body of related information for the table, including any possible changes that may have occurred since the table was last compiled.
- **Refine View** – a tool to change and filter the data reflected in graphical Topology views under Network Explorer.
- **Zoom In and Zoom Out** – Tools to magnify or shrink the view in graphical Topology views under Network Explorer.
- **Fit Content** – a tool to resize a large map or a small view of a map to fit the entire graphic pane in graphical Topology views under Network Explorer.

**Working with Table Information**

**Note:** Table rows in NetMRI frequently provide sets of icons for editing, exporting and deleting relevant table records, among other functions. For a closer look at record editing functions in NetMRI tables, see the **Icons and Popup Windows** topic.

Most NetMRI tables are highly customizable. You can do the following functions with tables:
• Select multiple table rows for modification or deletion, select multiple pages from a table, and select all rows/table records for any table.
• Sort, reorder and resize columns, and show/hide columns.
• Refresh to display changed data.
• Filter tables to sift through quantities of data and locate desired data records.
• Create and apply views, so you can quickly recreate a particular table layout.
• In tables listing issues, you can filter by issue activity type.
• Perform a quick search in a table, and jump from IP address hyperlinks to frequently-accessed destinations.

To resize a column: In the table heading row, hover over the column border, then drag the border left or right.

To reorder a column: In the table heading row, drag the column heading. (Blue arrows indicate where the column is inserted.)

Sorting Table Data

To sort rows based on the contents of a column (method 1): Click the column heading. Click the heading again to sort in the other direction.
The sorted column will have an arrow indicating sort direction.

To sort rows based on the contents of a column (method 2), do the following:
1. Hover over the heading for the column to sort, then click the down arrow at the right end of the column heading.
2. In the drop-down menu, click Sort Ascending or Sort Descending, as desired.

One column at a time can be sorted.

To hide or show columns, do the following:
1. Hover over any column heading, then click the down arrow at the right end of the column heading.
2. In the drop-down menu, hover over Columns.
3. In the Columns submenu:

To hide a column: Uncheck the chosen column.

To show a column: Click the checkbox for the chosen column. At least one column must remain visible in any table.

Selecting Table Data

In a table, NetMRI displays data on multiple pages when the number of items to be displayed exceeds the maximum number of items that can appear on one page. Use the navigational buttons at the bottom of the table to page through the display.

You can select multiple rows in a table. For example, in a Windows browser, you can do the following to select multiple rows:

• Click check boxes adjacent to each other to select contiguous rows.
• Click check boxes for any row, separated by any number of rows, to select multiple non-contiguous rows.
• Click the check box in the Select column of the table header to select all rows on a page, as shown in the figure.

When you click the check box in the Select column of the table header, in a table that contains multiple pages, only the rows on the current page are selected. All selected rows are greyed out on the table page, denoting their selection. After you select all rows on a page, you can deselect a specific row by clearing the check box for the row; the remaining table rows remain selected.

Note: The table will not preserve selected rows when you navigate to the next page in the table and then return to the current page.

For some tables, the Select check box is to the left of an Action icon. When you select multiple rows of a table, the Action icons are disabled and the Delete button activates. The Delete list option is the only available option after selecting multiple rows. Doing so enables you to delete all selected records from the table. Exercise caution when performing this action, as you may unintentionally delete rows of data that you did not wish to select. NetMRI user accounts with read-only privileges will not be able to perform this action.

Filtering Table Data

Use a filter to restrict a table to items of most interest. Filtering operates on specific table columns using operators (such as "=" and "<" for numbers, and "doesn't contain" and "starts with" for strings) and values you specify. You can simultaneously filter multiple columns using terms unique to each column.

To filter a table, do the following:
1. Click the Filters button (above the column headings). The Filters dialog box appears.
2. Open the Select a new field list, and click the name of the column you want to filter. This creates a new row in the dialog box.
3. In the new row, open the Operator field, then click the desired operator.
4. In the Value field, type the value for the filter (values are case-sensitive).
5. To see how the filter affects the table: Click Apply.
6. Click OK. The table is now filtered according to your specifications.

Filter terms can include regular expressions. Any characters between two forward slashes (/) are interpreted as a regular expression.

To edit or delete a filter, do the following:
1. Click Filter.
2. In the Filters dialog:, click the delete button for the term you want to delete (there is no confirmation).

Note: To fully remove a filter, and return the table to its unfiltered state, you must delete all filter terms.
3. To see how the change affects the table: Click **Apply**.

4. Click **OK**.

**Saving Table Views**

You can save customized table views for future use. A table view saves the current state of a table, including column show/hide state, column order, column size, sort order and filter (but not quick searches).

**Note:** All NetMRI users share the same views. New views, for example, are available to all users, and deleting a view makes it unavailable to all users.

To save a table view:

1. Set up the table the way you want by applying a filter and/or showing/hiding columns.
2. Click the **Views** button (above the column headings), then click **Add view** in the drop-down menu. The **Add View** dialog appears.
3. Enter a name for the view (required).
4. Enter a description of the view (optional).
5. To designate this view as the default for the table: Click the Default check box.
6. Click **OK**. The view is now listed in the Views menu.

To apply a view, click **Views**, then choose the desired view in the drop-down menu.

**Note:** If you apply a view, then modify the table (e.g., rearrange columns), the changes are not saved for that view. To save the changes, you must create a new view.

To edit or delete table views:

1. Click the **Views** button, then click **Manage view** in the drop-down menu. The **Manage View** dialog appears.
   - To modify a table view: Click the view, then click the Modify button. In the Modify view dialog, change the view parameters (name, description and whether it is the default), then click **OK**.
   - To delete a table view: Click the view, then click the **Delete** button (there is no confirmation).

**Issue Table Filtering**

Issues tables allow filtering by issue activity type.

To filter the issues table by activity type, do the following:

1. Click the **Display** menu (above the column headers).
2. In the submenu, click the activity type you want to see in the table.

- **All** displays all issues that existed during the selected time period. This is an important view for real-time analysis because if an issue existed at one point in the day, but was later automatically cleared by NetMRI, it will be listed by selecting **All**.
- **Current** (default) displays all issues open for the selected time period, or all issues open at the end of the selected time period if before today.
- **New** displays all new issues during the selected time period.
- **Cleared** displays all issues that have cleared instances during the selected time period.
- **Suppressed** displays all issues that have suppressed instances during the selected time period.

**Quick Searching Within a Table**

Quick searching enables you to reduce the number of rows in a table by typing a few characters. NetMRI displays the rows for which it finds a match in any column. Quick searching is dynamic, so you can change the search term and immediately see the results.

To perform a quick search: In the **Quick Search** field, type at least three characters of the search term (or enter one or two characters, then press ENTER).

**Note:** You can enter regular expressions in the Quick Search field. Any characters between two forward slashes (“/”) are interpreted as a regular expression.

To clear quick search results: Delete the entry from the **Quick Search** field.

NetMRI provides an alternative search tool called FindIT, which allows users with limited access rights to search information in the system. For more information, see [Using FindIT for Limited-Access Applications](#).

**Exporting NetMRI Table Data**
You can export data from any NetMRI table displaying the **CSV Export** icon. Exported data is in standard comma-separated values (CSV) format. You can view exported data in a text editor or a spreadsheet program such as MS Excel.

To export data, do the following:

1. Click the **CSV Export** icon.
2. In the resulting dialog, open the file or save it to disk.

MS Excel can display the first 65,536 rows of data in a large data set.

### Using FindIT for Limited-Access Applications

NetMRI FindIT is a search engine for retrieving information about network components. FindIT also provides a special limited-access operational role to users who need to use NetMRI to search for devices across the managed network, such as printers and end host computers.

FindIT displays a single field for entering a search term. Unlike Web searches, results returned by NetMRI FindIT are divided into two categories—exact matches and close matches—to narrow the search.

**Note:** NetMRI FindIT is particularly useful for people who are not regular NetMRI users. They can examine basic component data without having to request information from network or IT personnel. These users can access FindIT using a special login dedicated to that function (this login does not allow access to any other system functions). If a user has only the FindIT privilege, they will see a dedicated FindIT page when they log in, that provides no other access to NetMRI software functions.

The FindIT search field appears in the upper right corner of the main NetMRI browser window, to the right of your user name and the **Logout** hyperlink.

### Performing a FindIT Search

1. In the FindIT search field, enter all or part of any of the following:
   - Device name
   - IP address
   - Network View
   - MAC address
   - Model
   - Software version
   - Vendor name
   - Model name
   - Device type
   - Interface identification

2. Press ENTER, or click the **Submit Search** button. Search results will appear in a new page.

To maintain simplicity, FindIT does not accept multiple search terms or enable definition of complex search mnemonics. For instance, you cannot enter two MAC addresses, or an IP address and a device type, in the same search term. You can enter punctuation and special characters in search terms (such as a "." in an IP address), and if meaningful in the context of the search, FindIT will also use them as part of the term.

### NetMRI Licensing

Any and all NetMRI appliances and virtual appliance platforms can be licensed to run any NetMRI features. Starting with NetMRI 7.2.1, you can apply a new license or modify the existing license on a NetMRI physical appliance through the license generate administrative shell command. To use this command on a NetMRI virtual appliance, contact Infoblox Technical Support at the following URL: [http://support.infoblox.com](http://support.infoblox.com). Infoblox Technical Support will generate a license file for you or enable the License Generate command so you can generate a license on your own. When applying the license file using this command, you can choose to deploy the NetMRI appliance in the standalone or Operations Center mode. For information, see License Generate command. You can continue to use the License Management page (Settings icon → General Settings → License Management) to review your license configuration and upload the customer license or evaluation license file. The Current License Configuration panel displays your license type, expiration date, and license ID. You can use the License Show command and Show License commands to review your license configuration.

Infoblox offers the following NetMRI licensing types:

- **Full NetMRI**: The complete NetMRI package excluding the Security Device Controller feature set. It includes all features from Switch Port Manager and Automation Change Manager.
- **SPM2**: Includes all features for the switch port management, except for Configuration Management, Policy Compliance and Performance features, Dashboard, and reports related to disabled features. For more information, see Switch Port Management.
- **Automation Change Manager**: A superset of Switch Port Manager that includes support for the Automation Task Pack functions in NIOS, but excludes a few major features, such as Policy Management and Performance Management. For more information, see Job Management and Automation Change Manager.

### Using Evaluation License
You can obtain a single 60-day evaluation license for the NetMRI license type that is not currently under a purchased license, and if you have not already received a temporary license. For example, you may be currently running the Switch Port Manager as an original purchaser and wish to look at either Automation Change Manager (ACM) or the complete NetMRI package, you can obtain an evaluation license for ACM or Full NetMRI.

To obtain an Evaluation License file, do the following:

1. Go to Settings -> General Settings -> License Management.
2. In the Evaluation License File Generation section, note the serial number.
3. Go to http://support.infoblox.com and complete the license registration form by using the noted serial number. The registration site generates an Evaluation License file, valid for 60 days. Download the license file to your workstation.

To install the Customer License or Evaluation License file through the NetMRI GUI:

1. Go to Settings -> General Settings -> License Management.
2. In the License Installation section, click Choose File, then locate and select the license file.
3. Click OK.

To install the Evaluation License file using the administrative shell command:

1. Open a command line session through SSH to the NetMRI system.
2. Enter the command set temp_license.

```
> set temp_license
```

1. Add Switch Port Manager license
2. Add Automation Change Manager license
3. Add NetMRI license
4. Add Security Device Controller license

Select license (1-4) or q to quit: 2

This action will generate a temporary 60-day Automation Change Manager license.

Are you sure you want to do this? (y or n): y

Automation Change Manager temporary license installed.

Expiration: 2017-10-27

Temporary license installed

Adding Network Devices to the License Count

NetMRI applies all detected and managed devices to the appliance’s license count. After new systems are installed in the network, you Discover the device and can add it to the NetMRI license count.

To license a network device in NetMRI:

1. Under Network Explorer, click a hyperlink for a device. The Device Viewer appears.

3. Click OK after choosing your option for the selected device.
NetMRI gives priority to explicitly licensed devices in determining which devices to manage. Unlicensed devices continue to be managed by NetMRI, but their data sets are limited to basic discovery data.

**Note:** To economize on Switch Port Management device licensing, or on any licensing, be aware that some device types don't warrant allocation of license units from NetMRI. Examples include smart hubs and many PC clients in the network. NetMRI will discover these devices and include them in topologies, but such network devices don't necessarily require frequent change management; thus, simple discovery is sufficient for such devices and licensing is not required.

### Using Evaluation Licenses

You can obtain a single 60-day evaluation license for either NetMRI license type that is not currently under a purchased license, and if you have not already received a temporary license. For example, you may be currently running the Switch Port Manager as an original purchaser and wish to look at either Automation Change Manager (ACM) or the complete NetMRI package.

To obtain an Evaluation License File, do the following:

1. In the Current License Configuration panel, note the serial number.
2. Open a command line session through SSH to the NetMRI system.
3. Enter the command `set temp_license`.

   ```
   > set temp_license
   1. Add Automation Change Manager license
   2. Add NetMRI license
   Select license (1-2) or q to quit: 3
   ```

4. If you are currently running the Switch Port Manager license, enter `2`, `3` or `4` and press Enter.

   `This action will generate a temporary 60-day NetMRI license.
   Are you sure you want to do this? (y or n):`

5. Press **Y** to continue. The registration site will generate an Evaluation License File valid for 60 days. Download the file to your workstation.

To install a license file, do the following:

1. Go to **Settings –> General Settings –> License Management**.
2. In the License Installation section, click **Browse**, then locate and select the license file.
3. Click **OK**.

### NetMRI Security Settings

Use the Security page (Settings icon –> **General Settings** section –> **Security**) to configure certificates, and define HTTPS, SNMP and SSH settings. The settings you define here ensure that communications between NetMRI and managed network devices conform to best-practice security protocols. You must upload X.509 certificates in PEM format. Also, certain authentication and authorization services, such as LDAP, allow the use of certificates between the requesting client (NetMRI) and the server to protect connections from passing user login information and client-server exchanges in the clear.

Four tabs appear in the Security page:

| **NetMRI HTTPS Settings** | In the "NetMRI HTTPS Settings" tab, you upload an HTTPS certificate and enable or disable HTTP and HTTPS protocols. Infoblox automatically enables only the HTTPS protocol for web browser access to the system. When HTTPS is enabled, you can select one or more **CipherSuites** to be supported. A Cipher Suite is a combination of a transport protocol (e.g., TLS), an encryption algorithm (e.g., AES128) and an authentication algorithm (e.g., SHA). Most web browsers support a wide range of Cipher Suites; the list of default combinations provided by NetMRI are generally sufficient for most environments. High assurance environments should select only the Cipher Suites that are defined in their specific network security policy. You may also enable or disable use of either HTTP or HTTPS protocols from this page. For information, see [Running the NetMRI GUI in HTTP Mode](#).
| **SSH Settings** | Use the **SSH Settings** tab to configure the SSH protocols and ciphers used by NetMRI when connecting to network devices for configuration file collection and Configuration Command Script execution (i.e., Client mode); and the SSH protocols and ciphers supported by NetMRI when accepting connections to the Administrative Shell (i.e., Server mode). In both cases, you can selectively enable or disable the SSH v1 and SSH v2 protocols, and specify the ciphers to be supported by each protocol. For information, see [Configuring Global SSH Settings](#). SSH v1 does not support cipher selection in Server mode because the NetMRI SSH server automatically negotiates the cipher based on the request from the SSH v1 client.
| **SNMP Settings** | Use the **SNMP Settings** tab to specify the version and community/password for accessing the NetMRI SNMP agent. By default, SNMP v1 and SNMP v2c are enabled with a default community string. High assurance environments may disable those protocols and enable SNMP v3, providing an appropriate passphrase. The NetMRI SNMP Agent is automatically configured and restarted when the settings are updated. For information, see [Configuring Global SNMP Settings](#).

The **SNMP Settings** form applies only to the SNMP agent, not the SNMP protocols used by NetMRI to access network devices. When accessing network devices, NetMRI attempts SNMP v2c first, then tries SNMP v1.
To install a CA certificate, do the following:

1. Go to the Settings icon -> General Settings -> Security page and click the CA Certificates tab.
2. Click Import.
3. In the pop-up window, enter a logical name for the new certificate.
4. Click Browse to locate the certificate file.
5. Click Import to import the CA certificate to NetMRI. The certificate is added to the appliance. The newly imported CA Certificate will appear in the table in the CA Certificates tab after import is complete.

To install an HTTPS certificate, do the following:

This process involves two tasks: generating the CSR and sending it to the CA, and importing the new certificate from the CA.

1. Using SSH or SCP, connect to the NetMRI Administrative Shell and enter the following command:

   ```
   configure certificates
   ```

2. When prompted to select the certificate type, select `https`.
3. When prompted for an action, choose 1. Generate CSR.
4. When prompted to enter information for the CSR, the only required field is Common Name. You must enter the IP address or hostname of the NetMRI appliance. All other fields are optional.
5. When the appliance generates the CSR, copy the text, as shown in the example, and paste it into the Certificate Request page of the site from which you are requesting a certificate.

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIIC5zCCAc8CAQAwZDELMAkGA1UEBhMCR0IxEjAQBgNVBAgTCUJlcmtzaGlyZTEQ
   MA4GA1UEBxMHTmV3YnVyeTEXMBUAGA1UEChMOTXkgQ29tcGFueSBMdGQxFjAUBgNV
   BAMTDTE3Mi4yMj4yNy4xOTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEoAwIB
   AjAAtwAwggEoAgE Baltimore CA 3302-----END CERTIFICATE REQUEST-----
   ```

When you receive the CA-signed certificate, upload it to the appliance and activate it. Note that the certificate must be in PEM format and the file must have a `.crt` extension.

6. In the Settings icon -> General Settings -> Security page, click the NetMRI HTTPS Settings tab.
7. In the HTTP Certificate section, click `Upload`. A message dialog appears:

   ```
The NetMRI HTTP and HTTPS server settings are about to be updated and the web server restarted. If the NetMRI web server becomes inaccessible as a result of these changes, login to the NetMRI admin shell using SSH and run the command configure http to update the web server settings. Do you wish to proceed?
```

8. Click Yes to proceed.
9. In the Upload dialog box, click Browse... for the .PEM-format certificate file, select the file, and click Upload. The HTTPS Certificate section updates with the new information.

Configuring Global SNMP Settings

You can define the default SNMP protocol settings that are used by NetMRI. To configure SNMP settings for the appliance, do the following:

1. Go to the Settings icon -> General Settings -> Security page and click the SNMP Settings tab.
2. Enable or disable Version 1/2c. If enabled, enter a Community String.
3. Enable or disable Version 3. If enabled, enter an SNMPv3 Passphrase.
4. Click Update.
You can define the default SSH protocol settings that are used by NetMRI. To configure SSH settings for the appliance, do the following:

1. Go to the Settings icon -> General Settings -> Security page and click the SSH Settings tab.
2. Configure settings to be used when NetMRI connects to network devices for configuration collection or Configuration Command Script execution (you must enable at least one protocol).
   - Enable or disable SSH v1 Client Status. If enabled, select an SSH v1 Client Cipher.
   - Enable or disable SSHv2ClientStatus. If enabled, click, CTRL+click or SHIFT+click to select SSHv2ClientCiphers.
3. Configure settings to be used by NetMRI when accepting connections to the Admin Shell (you must enable at least one protocol).
   - Enable or disable SSH v1 Server Status.
   - Enable or disable SSHv2ServerStatus. If enabled, click, CTRL+click or SHIFT+click to select SSHv2ServerCiphers.
4. Click Update.

Subsequent attempts to access the NetMRI Admin Shell must comply with the new settings.

Running the NetMRI GUI in HTTP Mode

Note: Infoblox recommends exclusively using HTTPS as the means for accessing the UI through a Web browser, as in https://10.1.1.1. HTTPS is the default. NetMRI provides a setting for quickly enabling HTTP protocol usage.

NetMRI allows operation in both Hypertext Transfer Protocol Secure (HTTPS) mode and in HTTP. By default, NetMRI runs only HTTPS. To run NetMRI in the production network in HTTP mode, do the following:

2. Click the NetMRI HTTPS Settings tab.
3. To allow access to NetMRI in HTTP mode, check the Enable HTTP for the NetMRI Interface check box. This option is disabled by default. You can enable both Enable HTTP for the NetMRI Interface and Enable HTTPS for the NetMRI Interface options to support both protocols.

Note: Use caution when saving your settings for UI browser operation. Settings on this page affect the operation of the Web server that is built into NetMRI, requiring a restart of the NetMRI web service. In case of a mistake (accidentally disabling both HTTP and HTTPS, for example), you may not be able to access the web interface after committing settings. To address this, use a terminal program, using the admin account, to connect to the NetMRI admin shell and run the configure http command, which is the command-line version of the feature set presented in the NetMRI HTTPS Settings tab.

4. Close the Settings window.

Configuring a NetMRI Appliance for IPv6

Users can manage NetMRI on an IPv6 network. The NetMRI Management port has its own factory default link-local IPv6 address that is unique on its connected subnet. The default IPv6 address derives from the Ethernet MAC address of the NetMRI Management port.

NetMRI operates equally well in IPv4 and IPv6 networks, and reports and manages all devices running dual-stack IPv4 and IPv6 protocols. You must use a Windows 7 system or better to configure NetMRI to run on an IPv6 network, because Windows 7 natively supports IPv6.

To configure a new NetMRI appliance to be managed through IPv6, do the following:

1. Reboot Windows 7, ensure that it is enabled for IPv6 networking, and connect it to the management (MGMT) port of the NetMRI appliance, using a standard Ethernet cable.
2. On the Windows 7 system, open a command line window and run ipconfig. Check the listing in the Local Area Connection section of the ipconfig listing, and make a note of the interface number associated with the PC's IPv6 Link Local address. The value will have an fe80: prefix and end with a %n designator, such as fe80:505:ac03:49b7:dc38%15. The value 15 in this example is the interface number.
3. In a Windows command line, run the following command:
   netsh interface ipv6 show neighbor
4. Find the Interface *: Local Area Connection section (the * corresponds to the interface number for your PC system's IPv6 address). No entry should be present in this category for any address starting with the fe80: prefix.
5. In the Windows PC's command line, run a multicast IPv6 ping to all nodes on the subnet where the Management port is running. This executes a multicast IPv6 ping to the NetMRI management port connected to the PC.
6. In the Windows command prompt, run the following command:
   ping -n 5 ff02::1
   Allow the command to complete whether or not responses occur.
7. In the Windows PC's command line, run the following command a second time:
   netsh interface ipv6 show neighbor
   The NetMRI Management port IPv6 link-local address should now appear in the neighbor table under the Interface xx: Local Area Connection section, similar to the following:
   fe80::230:48ff:febc:97da     00-30-48-bc-97-da    Reachable
   This is the link-local address of the NetMRI appliance's management port.
8. Open an SSH client session to the NetMRI CLI at the IPv6 address shown in Step 6 along with the interface number. Log in with the factory default username/password admin/admin.
9. Next, you assign a globally routable static IPv6 address on the management port.
10. In the NetMRI CLI, enter the command:
    configure server
9. Step through the command sequence, and enter a new IPv6 address for the management interface in the IPv6 Address (optional) field when it is requested. The address should begin with the 2001: prefix and conform to the IPv6 prefix for the network. Also enter the Primary DNS Server Address, the default gateway and the Primary DNS Domain. An example appears below:

IPv4 Address (optional): [172.23.27.40]:
IPv4 Subnet Mask (optional): [255.255.255.0]:
IPv6 Address (optional): 2001:db8:a2:2c0:ee22::40
IPv6 Prefix (optional): 64
IPv4 Default Gateway (optional): []:
IPv6 Default Gateway (optional): [2001:db8:a2:2c0:ee22::1]
IPv4 Default Gateway (optional): []:
IPv6 Default Gateway (optional): []:
Primary DNS Server [172.23.27.236]: 2001:db8:a2:2c0::236
Primary DNS Domain [qanet.com]: customer.com

10. Save the new settings.

11. Shut down the NetMRI unit and physically install it in the global network. The unit is now reachable on its global static IPv6 address for further CLI configuration and UI access.

Running the Setup Wizard

**Note:** Infoblox recommends reading the topics in About Network Discovery before running the Setup Wizard for the first time.

The Setup Wizard (Settings icon → Setup → Setup Wizard) provides a multistep process for installing and configuring NetMRI. As shown in the table below, steps in the Wizard depend on whether it is run during installation or from Settings, and whether you choose to use Auto Discovery.

**Setup Wizard: Admin Setup**

**Note:** This step is present during initial NetMRI setup. It does not appear after NetMRI is successfully configured and the wizard subsequently accessed via Settings icon → Setup → Setup Wizard.

The primary administrative account is used by the NetMRI administrator to create user accounts and configure NetMRI. This account's user name and password are also required to access the administrative shell (a command line interface). Other NetMRI users do not have the special privileges available to the administrator. The administrator account is the “superuser” account in the NetMRI appliance. The primary administrative account's user name is “admin” and cannot be changed. Because this user name is easy to guess, it is essential to assign a strong password to prevent unauthorized users from impersonating the administrator.

1. Enter and confirm the password for the NetMRI administrative account. Requirements for the password are listed at the bottom of the screen.
2. Click Next.

**Setup Wizard: License Install**

**Note:** This step is present during initial NetMRI setup. It does not appear after successfully configuring NetMRI and running the setup wizard via Settings icon → Setup → Setup Wizard, or installing the license using the Admin Shell. Subsequent license installations can be carried out by going to Settings icon → Setup → Settings Summary and clicking the Install link above License Configuration.

A license is required to use NetMRI for production or evaluation purposes. Each license is keyed to a specific NetMRI serial number and specifies the maximum number of devices and interfaces that NetMRI can monitor, as well as which software modules are enabled. If you have not received a license file, or you have misplaced it, you can obtain a license file at http://support.infoblox.com. When you receive the file, save it in a location you can access from the Setup Wizard.

1. Browse to the location of the NetMRI license file, then select the license file. The license file ends with the extension .gpg.
2. Click Next.

**Setup Wizard: Welcome**

**Note:** Infoblox recommends enabling automatic discovery during the Setup Wizard.

With automatic discovery, NetMRI attempts to discover devices on the network using SNMP and terminal command-line discovery methods. Less configuration is required by using automatic discovery, but it may take longer to completely discover all the devices you expect to be detected and managed. Disabling discovery means that NetMRI will manage devices that are manually entered during configuration. Devices known to exist, but not explicitly configured, are not included in any reports or topology data. Configuring NetMRI with discovery disabled may take longer depending on the number of devices in the network.

After this step, you specify Discovery Ranges, where you specify the devices, networks and subnetworks that NetMRI communicates with when executing Discovery.

1. Enable or disable auto discovery.
2. Click Next.

**Setup Wizard: Discovery Ranges**

**Note:** You can add new IP address ranges and seed routers at any time after initial NetMRI setup. IPv4 and IPv6 are supported. For more in-depth information, see the Configuring Discovery Ranges topic.

Discovery ranges define the scope of the network that NetMRI explores by defining CIDR address blocks, IP address ranges and IP address wildcards. NetMRI limits its network exploration to the set of ranges defined in this tab. You can also exclude values and ranges from the Discovery process and hence from monitoring by NetMRI.

- A CIDR address block is defined by a network address and bit mask (for example 192.168.1.0/24).
- An IP address range defines a start and ending IP address. For instance, you could define 192.168.1.0 as the start of the IP range and 192.168.1.255 as the end of the IP range.
- An IP address wildcard pattern defines a single IP address range using a wildcard character or range for a specific set of octets. For example, you could define either 192.168.1.* or 192.168.1.0-255 as the IP address wildcard pattern. An IP address wildcard pattern can substitute an asterisk or range for any single octet in the definition.
- A desired set of values can also be imported from a .csv file.
- Every discovery range must be associated with a network view. For more information, see Configuring Network Views.

Ranges included in discovery indicate that any device found matching that range is discovered and managed by NetMRI. Ranges excluded for discovery indicate that any device found matching that range is excluded from discovery. Ranges marked Exclude from Management indicate that any device found matching that range is discovered, but NetMRI will not manage/collect data from the device.

1. Specify IP address ranges to include or exclude during discovery.
   a. Click New, select CIDR, IP Range or IP Pattern and enter the new values according to your selection. Use the CIDR selection to enter an IP prefix with its CIDR mask value; or an IP range with a beginning and ending range of IP addresses. IP Pattern lets you enter a value with a wildcard ("*" or ":-") character. Many users will prefer to use the CIDR option.
   b. To use a ping sweep for the discovery range, check the Enable Discovery Ping Sweep check box.
   c. Ensure that the Network 1 network view is selected from the Network View drop-down list. This network view is automatically created when you run configure server to perform initial setup on the appliance. (You can rename this network view at a later time on the Settings icon → Setup → Network Views page.)

**Note:** If you want to select another network view, ensure the view you select is associated with a scan interface. If the view you pick is not associated with a scan interface, it will show a caution (⚠️) icon by its name. (The Network 1 network view is automatically associated with the SCAN1 port.)

2. Select the Discovery Mode. For the first network you discover, use the Include in Discovery selection.

3. Click Add.

   To edit an item: Select an entry and click Edit. Change the value in the Network field above the table, including the subnet mask if necessary (the mask value is a dropdown menu), then click Save.

   To delete an item: Select an entry, click Delete, then confirm the deletion.

   To import discovery setting data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Discovery Import Formats topic for information on import file syntax.)

4. Click Next.

**Note:** See Running Network Discovery for more information on the NetMRI Discovery process.

**Setup Wizard: Static IPs**

You can specify individual IPs that you explicitly want NetMRI to manage. Adding values to this Wizard step prioritizes the specified addresses over other IPs or subnets specified for Discovery. Static IP entry supports IPv6 and IPv4 values.

1. Specify IP addresses that you want NetMRI to manage.
   a. Click New, enter the new IP address in the IP Address field (subnet is not necessary), and choose the Discovery Mode. For the first network you discover, use the Include in Discovery selection.
   b. Ensure that the network view chosen in the Wizard step Setup Wizard: Discovery Ranges is selected from the Network View drop-down list. For example, you may use the Network 1 network view.

2. Click Add.

   To edit an item: Select an entry and click Edit. Change the value in the IP Address field above the table or change the Discovery Mode (by default it is set to Include in Discovery), then click Save.

   To delete an item: Select an entry, click Delete, then confirm the deletion.

   To import discovery setting data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Discovery Import Formats topic for information on import file syntax.)

3. Click Next.
Setup Wizard: CLI Credentials

Note: For more information about credential definitions, see Adding and Editing Device Credentials and its subsections.

Note: NetMRI needs the ENABLE password to access configuration files on some devices and to run the Configuration Command Scripts and Perl scripts. To ensure easier identification of NetMRI actions, we recommend creation of a username and password on your network equipment specifically for NetMRI.

Note: Discovery of VRF configurations and VRF-aware devices requires CLI credentials.

NetMRI attempts site-specific username/passwords, in priority order, when first logging in to a device via an SSH or telnet CLI connection. When NetMRI determines a password, it saves it as information specific to the device. Lacking a site-specific password, the system will try vendor default credentials in priority order, and use site-specific username/password combinations when trying to determine the new login credentials for a device. They will not be used for vendor default credential checks.

1. Enter the CLI credentials used by the devices specified in the Discovery Ranges and Static IPs steps. NetMRI will automatically determine which credentials are associated with each device.

To add an item: Click New, enter the values for the Priority, Password Type (User or Enable), Username and Password fields, then click Add.
To edit an item: Select the item, click Edit, change the values for the Priority, Password Type, Username and Password fields, then click Save.
To test an item: Select the item, then click Test. In the test dialog, select the Hostname or IP, then click Start. To delete an item: Select the item, click Delete, then confirm the deletion.
To import credential data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Adding and Editing Device Credentials topic for import file syntax.)

2. Click Next.

Setup Wizard: SNMPv1/2 Credentials

Note: For more information about credential definitions and NetMRI, see Adding and Editing Device Credentials and its subsections.

NetMRI uses SNMP read-only community strings to collect data for analysis. The system is pre-configured with several commonly used community strings taken from the list of default community strings configured by the device vendor at delivery time. If the community strings provided during NetMRI installation do not work for a given device, the system tries well-known vendor defaults. If a default community string works for the device, NetMRI begins normal SNMP processing and the "Weak Community String" issue is fired to alert to this condition.

Note: If you are using the optional Compliance Module, the Default Credentials Report shows all vendor default community strings that were able to return SNMP data for a device.

Manually entered community strings are used first, in priority order, then the default community strings are tried in priority order if the Use Vendor Default Community Strings option is enabled in Settings icon –> Setup –> Collection and Groups –> Global tab –> Network Polling panel. Here, you can disable use of the vendor default community strings for determination of which strings NetMRI can use. This is typically done in installations having tight security setups that have removed all vendor defaults from their installation. Note that this option does not prevent the vendor default from running.

1. Enter the SNMP v1/2 credentials used by any devices specified in the Discovery Ranges and Static IPs steps. NetMRI will automatically determine credentials associated with each device.

To add an item: Click New, fill in the Priority and Community fields above the table, then click Add. To edit an item: Select the item, click Edit, change the fields above the table, then click Save.
To test an item: Select the item, then click Test. In the test dialog, select the Hostname or IP, then click Start. To delete an item: Select the item, click Delete, then confirm the deletion.
To import credential data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Discovery Import Formats topic for import file syntax.)

2. Click Next.

Note: For VRF-aware Juniper devices, to ensure device reachability for VRF configurations, prefix a second community string using the "@" character, such as @snmpnet, along with the normal community string (for example, snmpnet) you define for the device. For more information, see Vendor-Specific Requirements for Virtual Device Discovery.

Setup Wizard: SNMPv3 Credentials (Rare)

NetMRI may use SNMPv3 encrypted community strings to collect data for analysis, if SNMPv3 credentials exist for any devices in the network. If SNMPv3 strings are provided for devices, v3 credentials are used before any SNMPv2 credentials.
You can also define SNMPv3 credentials within NetMRI Settings at a later time.
1. Enter the SNMP v3 credentials used by any devices specified in the Discovery Ranges and Static IPs steps. NetMRI will automatically determine which credentials are associated with each device.

To add an item: Click New, fill in the Priority and Community fields above the table along with the required Authentication and Privacy protocols and passwords, then click Add.
To edit an item: Select the item, click Edit, change the fields above the table, then click Save.
To test an item: Select the item, then click Test. In the test dialog, select the Hostname or IP, then click Start. To delete an item: Select the item, click Delete, then confirm the deletion.
To import credential data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Adding and Editing Device Credentials topic for import file syntax.)

2. Click Next.

Setup Wizard: Seed Routers

Note: Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks. For more in-depth information, see the Adding Seed Routers topic.

NetMRI uses seed routers to quickly perform network discovery. Seed routers are also given priority (like static IP definitions) for determining which devices are counted toward NetMRI's license limits. The table lists each defined seed router with its discovery status (as defined in the Network Explorer -> Discovery tab). By reviewing the discovery status for each seed router you can determine whether NetMRI should be able to discover the network successfully, or if there are possible configuration errors preventing network discovery, without having to wait to see what NetMRI finds.

1. Enter IP addresses for seed routers.
   a. Click New, enter the value in the Seed Router IP Address field, then click Add.
   b. Ensure that the network view chosen in the Wizard step Setup Wizard: Discovery Ranges is selected from the Network View drop-down list. For example, you may use the Network 1 network view.
2. Click Add or Add & Discover.
   To edit an item: Select the item, click Edit, change the fields above the table, then click Save. To force immediate discovery: click Add & Discover.
   To delete an item: select the item, click Delete, then confirm the deletion.
   To import discovery setting data: click Import. In the dialog, click Browse... to select the CSV file, then click Import. (See the Discovery Import Formats topic for information on import file syntax.) The imported file data are applied as a set of one or more Seed Routers. Ensure that the values are correct before importing.
3. Click Next.

Setup Wizard: Device Type Hints

Device hints help NetMRI's discovery engine locate specific types of network devices using IP address patterns and DNS name patterns. For instance, if most routers are found at an IP address ending with ".10", specifying "*.*.*.10", and associating the Router device type for an IP address hint, allows NetMRI to prioritize any discovered devices matching that hint, higher in its credential collection queue to help speed discovery. This hint is considered when NetMRI attempts to determine a device's type. You can also specify the device type itself — router, switch, switch-router, firewall, and numerous other choices.
Valid IP address patterns are either the numeric values of the octet, or an asterisk for any number of octets in the IP address. For device name matches, valid DNS characters and the asterisk character are valid definitions. For instance rtr will match any device name with "rtr" in it's definition.
Device hints are optional and used in helping to speed network discovery and to assist with determination of device types absent other discovery data.

1. Enter information for device type hints, if necessary.
   To add an item: Click New, select the type in the Device Type dropdown list, enter the required value in the IP Address field, then click Add.
   To edit an item: Select the item, click Edit, change the fields above the table, then click Save. To delete an item: select the item, click Delete, then confirm the deletion.
2. Click Next.

Setup Wizard: Device Interrogation Techniques

This Wizard step defines the methods by which NetMRI polls network devices for information. Those protocols are based upon three methods: CLI, SNMP and ARP.

1. Select desired interrogation options (descriptions are provided in the Wizard step, and in the Defining Group Data Collection Settings topic).
   Enable any options you consider applicable for your network.
2. Click Next.

Setup Wizard: Configuration Collection

This Wizard step defines the methods by which NetMRI obtains information such as routing tables, ARP tables and device configuration files.

1. Select desired configuration collection options (descriptions are provided in the Wizard step). Under most circumstances, it should not be necessary to modify settings in this step.
2. Click Next.
Setup Wizard: Summary

The final step of the Setup Wizard summarizes the steps you have taken during setup.

1. Study the summary information in this final Wizard page before finishing setup. For any item flagged as a possible configuration problem, click the Edit link to go directly to the corresponding step in the wizard to make changes. After making changes, return to the Summary step.

2. Click Finish.

Setting the Date and Period

In many tabs and pages, you can constrain data and graphs to a specific date and period. This is useful in many contexts that provide a lot of information, such as Network Analysis -> Issues or in Switch Port Management.

After you set the date and/or period, it is applied to all tabs and pages displaying the Select Date/Period icon. To specify a date or a time period for a data set, do the following:

1. Choose a Device Group on the right menu, and choose a menu item from the left side of the page (Explorer). Click the Time Selector in the left end of the title bar. The calendar drop-down menu appears, showing the current calendar month.

2. Click the Time Selector in the left end of the title bar. The calendar drop-down menu appears, showing the current calendar month.

3. In the calendar drop-down menu, choose a Period. Choices include the following:
   - **Daily**: Select a single date in the currently shown calendar month.
   - **Weekly**: Sunday to Saturday seven day period containing the selected date.
   - **Monthly**: Entire calendar month containing the selected date.
   - **7-Day**: Seven days ending with the selected date.
   - **30-Day**: Thirty days ending with the selected date.

4. In the grey title bar of the calendar, click the left or right selector to choose the calendar month that contains the date or time period you need.

5. Calendar dates shown in Green represent an immediately available data set to display in a NetMRI table. The most current data in any table (such as the most recent 7 days for the Daily selection) is always available by default and appears highlighted in green. Older data appears in white on the calendar but is selectable by the user. Dates in white require the user to wait while NetMRI generates the requested data as a background task. After generation, the requested date appears in green, indicating the data is instantly available by reloading the page. Any date in the past or in the future that appears in grey and cannot be selected, represents information that is unavailable to the current NetMRI system.

6. In the calendar, click a desired date. The table will automatically refresh to display the new date.

**Note:** The currently select device group, date and period appear to the right of the Time Selector icon.

Dates that appear in white in the calendar reflect locally stored data, that is available but not cached for immediate viewing on the NetMRI appliance. In such cases, you will see the following message:

**Data for the requested date is currently offline. Do you want to generate the data now?**

Clicking Yes directs NetMRI to retrieve and display the data from the internal database. During data retrieval, the toolbar displays a progress bar indicating that a background task is taking place. Other tasks can be carried out in NetMRI while fetching data from the database.

Some data tables, such as Network insight -> Inventory, display only in Daily increments.

**Note:** The Interface Viewer (see Using the Interface Viewer) uses a different Time Selector menu that provides separate **Date** and **Period** menus. Users can check the status for an individual device over time.

Using the IP Address Context Menu

Right-clicking any IP address in a NetMRI list or table, such as in the Discovery page or a Devices list, pops up a context menu for quick access to more functions. The menu contains the following commands:

- **Device Viewer**: opens the Device Viewer to the default Network Analysis -> Issues tab, which lists issues for the device.
- **Config Explorer**: opens the Device Viewer to the Device Viewer -> Config Management -> Config Archive tab, which lists configuration files collected from the device.
- **View Running Config**: opens a window to display the configuration currently running on the device.
- **Changes**: opens the Device Viewer to the Device Viewer -> Network Analysis -> Changes tab, which lists detected changes to the device's configuration file.
- **Issue List**: opens the Device Viewer to the Device Viewer -> Network Analysis -> Issues tab, which lists issues for the device.
- **Policy Compliance**: opens the Device Viewer to the Device Viewer -> Network Analysis -> Policy Compliance (see the Introducing Policy Compliance topic), which lists policies run against the device, and the outcomes of those policies.
- **Topology Viewer**: submenu allows viewing of devices in the context of various topologies: L2 n Hop, L3 n Hop, L3 Path Viewer (most likely path) and L2/L3 Path Viewer (most likely path).
- **Schedule Job**: opens the Edit Job dialog, for specifying a job to run on the current device (you can also include other devices and groups).
- **Execute Command**: opens the Run Configuration Command Script dialog, where you can specify and submit a command to run on the device.
- **Open Telnet/SSH Session**: open a new terminal session for the selected device through NetMRI using either SSH or Telnet.

Quick Start
The quick start guide (below) lists common NetMRI tasks. Check the items below for quick introductions to many of NetMRI’s key features.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| View the Network Scorecard and general information about network health | **Network Analysis** → **Issues** tab.  
To change the scope: Choose a group name in the **Select Device Groups** panel. To view a description of an issue: Hover over a hyperlink in the Title column in the table.  
To view issue details: Click a hyperlink in the Title column in the table.  
To view devices having issues: Choose the **Issues by Device** tab below the table. |
| Set interfaces to administratively Up or administratively Down       | **Interface Viewer** → **Settings** → **Port Control Settings**. Click **Edit** for each setting.  
The interface viewer can be found in several different ways; examples include **Network Explorer** → **Inventory** → **Interface Config** or **Network Explorer** → **Inventory** → **Unused Down Ports** and clicking an interface link. |
| Set VLAN assignment for a switch interface                           | **Network Analysis** → **Performance** → **History** section (left panel).                                           |
| View network performance data                                       | **Settings** → **Setup** → **Scan Interfaces**.                                                                      |
| View network events                                                 | **Network Analysis** → **Events** tab.                                                                               |
| List all devices in the network                                      | **Network Explorer** → **Inventory** → **Devices** section (left panel) → **Devices**.                               |
| View all Ethernet switchports managed in the network                | **Network Explorer** → **Switch Port Management** → choose **Interfaces** → **Interfaces Present**.                  |
| View a variety of information about NetMRI appliance setup          | The **Settings Summary** (Settings icon → **Setup** → **Settings Summary**) provides a variety of information about the NetMRI appliance.  
The **NetMRI Configuration** panel displays the current NetMRI version, model, serial number and license limit settings, and information about Platform, Licensed and Effective limits for the current appliance.  
The **Network Configuration** panel displays the NetMRI settings as configured during installation.  
The **MGMT Interface Configuration** panel displays the configuration settings for NetMRI’s management interface.  
The **SCAN Interface Configuration** panel displays the configuration settings for NetMRI’s data collection interface.  
The **Collector Settings** panel displays the status of each collector. Some collectors may be disabled if the required license is not installed. (Enable collectors at Settings icon → **Setup** → **Collection and Groups**.)  
The **Module Settings** panel displays the status of the available NetMRI modules. Enabling any disabled module requires an updated NetMRI license.  
The **License Configuration** panel identifies the current license information and provides a hyperlink to a page for updating your NetMRI license. |
| View low-level details about a specific device                       | Click any IP address hyperlink to open the Device Viewer.                                                           |
| List all interfaces in the network                                   | **Network Explorer** → **Inventory** → **Interfaces** section (left panel) → **Interface Config**.                  |
| View information about routes, subnets, VLANs, HSRPs/VRRPs and ports in the network | **Network Explorer** → **Summaries** tab, then select a category in the left panel. To change the scope: Click a group name in the Select Device Groups panel. To see details: Click a hyperlink in the left panel.  
To dig even deeper: Click a hyperlink in the center panel. |
| View Imported and Exported Route Targets                            | **The Route Targets** accordion in the left panel in **Network Explorer** → **Summaries**.                         |
| Check Network Views and their members                               | **Settings** → **Setup** → **Network Views**, and click the network view name.                                       |
| Check the list of VRFs and view their information                   | **The VRFs accordion in the left panel in **Network Explorer** → **Summaries**. For VRFs in a specific network, **Settings** → **Setup** → **Network Views**, and click the network view name. |
| View a graphical map of the network                                  | **Network Explorer** → **Topology** tab, then select a category in the left panel.                                  |
| Compare configuration files between devices on the network          | **Config Management** → **Config Archive** tab, select a device in the left panel, select two configuration files in the right panel, then click **Compare**.  
To compare configuration files for two devices: Click **Compare Second Device**, select one configuration file for each device, then click **Compare**. |
| Write scripts and run jobs                                          | **Config Management**→ **Job Management** tab.                                                                       |
| Quickly find data                                                   | Type an IP address, MAC address, device name, vendor, model, software version or interface identification in the FindIT field (in the upper right corner of the main NetMRI page), then press ENTER.  
To view more information about a found item: In the results page, hover over the plus sign. |
| Perform diagnostic tests                                           | Click **Tools** at the right end of the main navigation area to open the NetMRI Tools window. Select a diagnostic tool in the right panel.  
or  
Click **Tools** at the top of the Device Viewer or Interface Viewer. |
Perform administrative functions, such as manage user accounts, change program settings

Click Settings at the right end of the main navigation area to open the General Settings window. Select an operation in the right panel.

Get help

Click the Help icon at the right end of the navigation page to launch the help system. or

Click Page Help in the title bar of any page to directly access help for that page.

Viewing NetMRI Setup Information

At any time, you can check the overall system settings for the current NetMRI appliance. Click the Settings icon and choose the Settings Summary page (Settings -> Setup -> Settings Summary) to get a quick look at many basic aspects of the system—license limits and configuration, basic network configuration, settings for configuration data collection and other functional areas through which NetMRI does its work.

- The NetMRI Configuration panel shows the NetMRI version, model, serial number and license limit settings.
- The Network Configuration panel displays the NetMRI network domain settings as configured during step one of the installation process.
- The MGMT Interface Configuration panel displays the configuration settings for the NetMRI management interface.
- The Device and Interface Counts panel displays the current number of network devices and interfaces that NetMRI discovers up to the current time through its data collection across the network. Note the Total Interfaces and Up Interfaces counters, along with Frequently Polled interfaces and any possible difference between Network Devices Seen and Managed Network Devices.
- The Collector Settings panel displays the status of each collector used for gathering information about the networks that NetMRI analyzes and monitors. Some collectors may be disabled if the required license is not installed. (Enable collectors at Settings -> Setup -> Collection and Groups.)
- The Module Settings panel displays the currently NetMRI software version. The possible versions are the following: Switch Port Manager, Automation Change Manager, and full NetMRI.
- The License Configuration panel identifies the current license information and provides a hyperlink to a page for updating your NetMRI license.

Many of these settings are defined through the Setup Wizard.

About Automatic Failover

You can create a NetMRI failover pair using two NetMRI appliances, in which one acts as the primary appliance and the other as the secondary appliance. A failover pair provides a backup or redundant operational mode between the primary and secondary appliances so you can greatly reduce service downtime when one of them is out of service. You can configure two Operation Center (OC) appliances, collector appliances, or standalone appliances to form a failover pair.

In a failover pair, the primary appliance actively discovers and manages network devices and serves the Web UI and the CLI over the shared VIP address while the secondary appliance constantly keeps its database synchronized with the primary. Although you can access a failover pair using either the VIP address of the failover pair or the management IP address of the primary appliance, using the management IP is not recommended because during a failover, the roles of the primary and secondary appliances reverse and the management IP becomes unreachable. Accessing the failover pair using the VIP address ensures that you are contacting the active primary appliance. Note that during a failover, all active connections between the NetMRI appliances and the network devices are disrupted and all ongoing processes fail. Also, all active Web UI and CLI sessions are disrupted during a failover and all users with active sessions must reconnect and log in again after the secondary appliance assumes the role of the primary appliance.

Note the following about the automatic failover feature:

- Failover pair is supported only on NetMRI NT-1400, NT-2200, and NT-4000 (G8 only) appliances. It is not supported on NetMRI virtual appliances.
- Failover is supported in NetMRI 7.1.1 and later releases.
- Collector failover is supported in NetMRI 7.1.2 and later releases.
- Both the primary and secondary must be of the same appliance model and same software version number.
- The management IP address of both the primary and secondary must be on the same subnet.
- The VIP address, shared by the primary and secondary must be on the same subnet as the management IP address.

Deploying Automatic Failover for New Appliances

Following are the pre-requisites for deploying automatic failover for new appliances:

- Configure two supported NetMRI appliances with licenses installed.
- Both the appliances must be of the same appliance model and same software version number.
- Provision three IP addresses on the same subnet: a VIP address and two management IP addresses for the appliances.
- If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the systems directly through their HA Ports.
- If you are using the network replication method to connect the appliances, you must connect the systems over a local network and two replication IP addresses must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

Note: Infoblox recommends you to use the direct replication method for best reliability and performance. The network replication method will have higher latency and a greater chance of connection breakage, and thus lower reliability and performance.

You can deploy two new Operation Center (OC), collector appliances, or standalone appliances to form a failover pair, as follows:

1. Set up and configure two new NetMRI appliances as separate systems. Ensure that the appliances are running NetMRI 7.1.1 or later. For collector failover configuration, make sure that the appliances are running NetMRI 7.1.2 or later.
2. Connect both the systems using one of the following methods:
• **Direct replication**: Connect the systems directly through their HA ports.
• **Network replication**: Connect the HA port of both systems to a network using an Ethernet cable.

Infoblox recommends that you connect the systems using the direct replication method.

3. Run the Setup Wizard on both appliances and set the admin password and install the license. The admin password must be the same on both systems. For information, see *Running the Setup Wizard*.

At this point of time, it is not necessary to complete the entire configuration wizard on both systems. You can complete the configuration only on the primary system.

4. Configure the failover settings on the Operation Center and collectors, as described in *Specifying Automatic Failover Settings*.

---

**Note:** After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model.

5. For an Operation Center and collector failover, complete the following:

   • Log in to the Admin Shell on the Operation Center and run the `configure tunserver` command. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center server.
   • To register collector on the Operation Center set up, log in to the Admin Shell on each Collector and run the `register tunclient` command. Enter the VIP address of the Operation Center when prompted for the IP address of the Operation Center.

---

### Specifying Automatic Failover Settings

To specify automatic failover configuration settings:

1. Go to the Settings -> Setup -> Failover Configuration tab.
   The Failover Configuration page appears, listing all device interfaces that are used by the system.
2. In the Failover Configuration page, complete the following:
   • Virtual IP address: Enter the VIP address.
   • Connection Mode: Select the connection mode from the drop-down list. You can select Direct, if the systems are connected directly through the HA port or select Network, if the HA port of both the systems are connected to a network. Infoblox recommends that you use the Direct connection mode.
   • Virtual Hostname: Enter the hostname for the system.
   • Port: Enter the TCP port for replication traffic, if you are using Network connection mode. You must enter a port number greater than 1024.

In the **Replication Nodes** section, enter the following for both **Primary** and **Secondary**.

   • **Role**: Displays the role of the appliance, either PRIMARY or SECONDARY.
   • **Management IP**: Enter the management IP address of the system.
   • **Hostname**: Enter the hostname of the system.
   • **Replication IP**: Enter the IP address used for replication traffic, if you are using Network connection mode.
   • **Subnet**: Enter the subnet mask of the replication IP, if you are using Network connection mode. Note that the subnet mask must be the same for both primary and secondary appliances.

3. Click **Update** to update the settings and replicate data on both the primary and secondary appliances.
4. Click **Enable** to start connecting the systems.

The secondary system synchronizes data with the primary system. This process might take about one hour, depending on the appliance model.

### Migrating Existing Systems as Failover Pairs

You can migrate two existing Operation Center (OC) or standalone appliances to form a failover pair. Ensure that both appliances are running versions NetMRI 7.1.1 or later. To form a collector failover, migrate the existing collector to NetMRI 7.1.2 or later releases.

Following are the pre-requisites for migrating existing systems as a failover pair:

   • Two supported NetMRI appliances with licenses installed. You can choose an existing appliance and a second appliance of the same model.
   • Provision two additional IP addresses on the same subnet: a management IP address assigned to each system and a VIP address shared between the failover pair.
   • If you are using direct replication method to connect both appliances, you need an Ethernet cable to connect the appliances directly through their HA ports.
   • If you are using network replication method to connect the appliances, you must connect the systems over a local network and two replication IPs must be acquired on the same subnet. You must also select a TCP port for the replication traffic.

To migrate two existing systems to form a failover pair:

**Note:** In the below steps, the system that is referred to as the second system takes the primary role and the system that is referred to as the existing system takes the secondary role in the failover pair.

1. Choose an existing NetMRI system and configure a second NetMRI system of the same model.
2. If you are using scan ports, connect the scan ports of the second system to the network in the same way as the existing system. For information, see Failover and Scan Interfaces.

3. Connect both systems using one of the following methods:
   - Direct replication: Connect the systems directly through their HA ports.
   - Network replication: Connect the HA port of both systems to a network using an Ethernet cable.

4. Run the Setup Wizard on the second system and set the admin password and install the license. For information, see Running the Setup Wizard.

5. Exit the Setup Wizard after setting the password and installing the license on the second system.

6. Upgrade the systems to NetMRI 7.1.1, if necessary.

7. After upgrading both systems to NetMRI 7.1.1 or later, repartition the systems to prepare them for automatic failover, as follows:

   a. Log in to the Admin Shell on the second system, and enter the repartition command. Note that if the system is already partitioned for failover, an error message appears when you run the repartition command. Re-enable SNMP collection after restoring the archive on the second system. To enable SNMP collection, go to Settings -> Setup -> Collection and Groups -> Global tab -> Network Polling side tab, and then select the SNMP Collection check box.

   b. If the data restore is successful, do not proceed to the next step. If the restore failed due to disk space exhaustion, you may try reducing data retention settings on your existing NetMRI system to reduce the archive size. For more information, see Data Retention or contact Infoblox Support for further assistance. Note that it might take up to 24 hours for reduced data retention settings to take effect.

   c. Log in to the Admin Shell on the existing system, enter the reset system command, and then enter the repartition command. Note that if the system is already partitioned for failover, an error message appears when you run the repartition command. After repartitioning is complete, run the configure server command, install the license, and then reset the admin password in GUI to match the other system.

8. If you want to use the management IP address of your existing system as the VIP of the failover pair, then you must change the management IP address of the existing system.

9. Configure the second system to take the role of the primary system, as follows:
   - Log into the second system.
   - Go to Settings -> Setup -> Failover Configuration.
   - Specify the configuration settings in the Failover Configuration page. For information, see Specifying Automatic Failover Settings.

10. On the Operations Center, go to Settings -> Setup -> Tunnels and Collectors.

   a. Click the Action icon in the row for the collector you want to replace and choose Collector Replacement.

   b. Change the serial number of the existing collector to that of the replacement collector.

11. For an Operation Center and collector failover, complete the following:

   a. Log in to the Admin Shell on the Operation Center and run the reset tunserver and configure tunserver commands.
   b. Log in to the Admin Shell on each Collector and run the reset tunclient and register tunclient commands.

Note: After specifying the failover configuration settings and completing the enable operation, the systems start synchronizing data. This process might take up to one hour, depending on the appliance model.

12. On the Operations Center, go to Settings -> Setup -> Scan Interfaces. Change the scan interface IP of the existing collector to that of the replacement collector.

13. Click Save.

Manually Initiating Failover

If you want to swap roles between the members of a failover pair, you can manually initiate a failover. In about five minutes after initiating a manual failover, the secondary system assumes the primary role and takes ownership of the VIP address. Note that a manually initiated failover causes a temporary service disruption.

To initiate a manual failover using the GUI:

1. Log in to the primary system using your username and password.
2. Go to the Settings -> Setup -> Failover Configuration tab.
3. In the Failover Configuration page, click Become Secondary.

To initiate a manual failover using the NetMRI Admin Shell, do one of the following:

   a. Log in to the Admin Shell on the primary system and enter the failover role secondary command, and then press Enter.
   b. Log in to the Admin Shell on the secondary system and enter the failover role primary command, and then press Enter.

Monitoring Automatic Failover
You can monitor the current status of the failover pair, as follows:

1. Go to the Settings -> Setup -> Failover Configuration tab.
   The Failover Configuration page appears, listing all device interfaces that are used by the system.
2. In the Failover Configuration page, the Status field displays the current status of the failover pair. The current status can be one of the following:
   - **OK** (green): Indicates that the failover pair is connected and synchronized. If the primary fails, the secondary automatically takes over the primary role.
   - **Syncing** (yellow): Indicates that the failover pair is connected and the primary and secondary are synchronizing data. If the primary fails during synchronization, the secondary system cannot automatically take over as the primary system.
   - **Replication Down** (red): Indicates that the failover pair is disconnected on the HA port but reachable on the MGMT port. This may be due to a cable mishap or when the secondary goes offline.
   - **Peer Down** (red): Indicates that the secondary has lost connection with the primary on both HA and MGMT ports.

You can click the status link and view details about the failover status.

**Viewing Failover Settings**

To view configuration details of the Operation Center (OC) and Collector pair:

1. Go to the Settings -> Setup -> Failover Configuration tab.
   The Failover Configuration page appears, listing all device interfaces that are used by the system.

**Note:** For an OC collector set up, the first row of the Failover Configuration page will display the OC pair information and other rows will display the collector pair information.

- **Actions:** You can click Edit or Status using the Action icon.
- **Virtual IP:** Displays the virtual IP address.
- **Virtual Host Name:** Displays the virtual hostname.
- **Connection:** Displays the connection mode.
- **First MGMT IP:** Displays the management IP address of the primary.
- **Second MGMT IP:** Displays the management IP address of the secondary.
- **First MGMT Hostname:** Displays the management hostname of the primary
- **Second MGMT Hostname:** Displays the management hostname of the secondary.
- **First Replication IP:** Displays the IP address of the replication traffic of the primary.
- **Second Replication IP:** Displays the IP address of the replication traffic of the secondary.
- **Port:** Displays the port number for replication traffic.
- **Status:** Displays the connection status. For information, see Monitoring Automatic Failover.

**Failover and Scan Interfaces**

In a failover pair, although the scan interfaces are enabled only on the primary system, the scan interface configurations are replicated on both the systems. When the primary fails, the secondary activates its scan interfaces (physical and virtual) using the same IP configurations. Both the primary and the secondary can access the network using the same scan interface configurations. After a failover, the NetMRI appliance continues to interact with the devices using the same scan interfaces.

If no scan interfaces are configured on both failover systems, then the NetMRI appliances interacts with network devices using the management port. The physical management port configuration is not replicated between the systems. After a failover, the NetMRI appliance interacts with the devices using the management port of the local system. Therefore, you have to configure the management IPs and infrastructure ACLs on both systems.

**Software Upgrades**

To upgrade a failover pair, you need to perform software upgrade only on the primary system. The primary system upgrades locally, and then automatically upgrades the secondary. Note that during the upgrade of both systems, the failover capability is suspended. After upgrading the secondary system, both systems automatically connect and synchronize data.

**Resolving Split Brain Issues**

Generally speaking, "Split Brain" is a term used to describe the undesirable state in which both members of a failover pair act as primary at the same time. This is a rare situation which can occur when both the systems are up and running, but the systems completely disconnect from one another on both the MGMT and HA ports at the same time due to a network outage or a cable mishap. Split brain can also occur due to an error in the failover software. In this case, the secondary system assumes that the primary system has failed and takes over the primary role. The primary system, which does not have any contact with the secondary system continues to perform as the primary system. Having two primary systems introduces issues such as VIP contention and duplication of data.

You can resolve a split brain issue by choosing one of the systems to retain data (the survivor) and the other system to discard data (the victim), and then force the victim into the secondary role. While choosing the survivor and the victim, you should look at each system and select the system which has the most complete data as the survivor. If you are unsure, select the original primary as the survivor, and the secondary as the victim. Typically, the data in both the systems are similar, since both systems have access to the same network, and they collect data from the same pool of devices, and both perform the same tasks. The data prior to the split brain state are identical in each system because the data is replicated when the systems were still connected. Only the data collected during the split brain state differs. The longer the systems are in a split brain state, the more the systems will diverge.

To resolve a split brain issue using the GUI:
1. Connect to the management IP address of the victim system and log in to the system using your username and password.
2. Go to the Settings -> Setup -> Failover Configuration tab.
3. In the Failover Configuration page, click Become Secondary.

To resolve a Split Brain issue using the NetMRI Admin Shell:

1. Use a terminal program to connect to the management IP address of the victim system.
2. Log in to the Admin Shell using your username and password.
3. At the Admin Shell prompt, enter the failover role secondary command, and then press Enter.

Running Network Discovery

A primary application for NetMRI is discovering the network and all its infrastructure devices.

NetMRI’s discovery features perform a crucial task: to locate and categorize all devices on a previously unmanaged network. By providing a high-level view of all devices in a network with which NetMRI can communicate, discovery enables managers to begin controlling a complex network topology, and drill down to individual devices to diagnose communication problems encountered during discovery.

You can define basic discovery settings during system setup (discussed in detail in Running the Setup Wizard), or manually perform discovery using a series of straightforward steps. The following section Discovery with a New NetMRI Deployment describes how to manually configure and run discovery.

If you are migrating your NetMRI platform to the current release, see Discovery with an Existing NetMRI Platform.

About Network Discovery

When network discovery starts after the Wizard setup or platform upgrade, it runs continuously as a background task, staying up to date with device and network changes as they happen. You can watch the progress of discovery as NetMRI learns your network, and adjust discovery settings to control what it finds and how it collects data.

**Note:** You can change discovery settings at any time either through the Setup Wizard (Settings icon -> Setup -> Setup Wizard) or through individual Settings pages (such as Settings icon -> Setup -> Discovery Settings).

You can also flexibly define discovery blackouts at the network, discovery range, device group, and device level to prevent discovery protocols and traffic from occupying network bandwidth at inopportune times, such as latency-sensitive trading or video applications operating during daytime hours. For information, see Configuring Network Discovery Settings and Defining Blackout Periods.

To perform network discovery, you use several fundamental tools: Network Views, Scan Interfaces, Discovery Settings and SNMP/CLI credentials.

- **Network Views** – NetMRI uses network views to create separate management domains for your networks and devices, including VRF-based virtual networks. You manage every network, including virtual networks, through a separate network view. For more information, see Configuring Network Views.
- **Scan Interfaces** – You configure scan interfaces to physically or logically connect to multiple networks, enabling discovery and management in different network domains. Every scan interface you create maps to a network view. For more information, see Configuring Scan Interfaces.
- **Discovery Settings** – You specify the IP prefixes, also called discovery ranges, to define the IP address space that is managed on each network. Another key setting is called a seed router, which is a gateway routing device considered to help speed discovery across more network spaces. For more information, see Configuring Network Discovery Settings.
- **SNMP and CLI Credentials** – NetMRI requires SNMP for most discovery tasks. Many discovery and data collection tasks, including VRF discovery, also require the use of CLI and Enable password credentials to access device configurations. You collect and add these values to NetMRI through a Credentials page. For more information, see Adding and Editing Device Credentials.

Discovery with an Existing NetMRI Platform

When existing customers update a NetMRI deployment to the current release, a number of changes appear in the deployment:

- Your currently managed network, with its current discovery settings, is managed through a new network view named after the previously defined network name. No further configuration is necessary for continued network management but changes can be made at any time. For more information, see Configuring Network Views;
- Existing discovery settings, such as CIDR discovery ranges, are automatically assigned to the network view used for the managed network.
- Your SCAN port for your appliance (or appliances, in the case of Operations Center deployments using Collectors) will automatically be assigned to the network view that is used for your present managed network. This port will be named LAN1. For more information, see Configuring Scan Interfaces;
- For more information, see Configuring Scan Interfaces;
- Depending on your appliance, a second LAN2 port is made available for further network connections;
- Your MGMT port will continue to operate as the appliance’s Web management interface;
- All active Ethernet interfaces on your appliance(s), including the MGMT port, support Ethernet 802.1Q encapsulation for virtual scan interfaces. For more information, see Configuring Virtual Scan Interfaces;
- If VRF-aware devices exist on your managed network, System Health banner messages will notify you about unassigned VRFs. To enable full network discovery and control for each virtual network, these networks need to be mapped to virtual scan interfaces. For more information, see Mapping Virtual Networks to Network Views and Configuring Virtual Scan Interfaces.

Existing Operations Center deployments will see the following changes:
For an OC deployment managing a single large network, you will see multiple entries in the pages under Settings icon → Setup → Discovery Settings for selectable network views. The entire network is assigned to a single network view; however, each network view entry is identified through the association of each Collector. This allows you to edit discovery settings for each Collector in the same network view.

Multi-Network Operations Center deployments automatically assign each managed network to a new Network View. Each network view is named based upon the original network name.

Multi-Network Operations Center deployments automatically define a new set of device groups for each managed network, along with the standard set of device groups. These network-specific device groups are named using the original network name as a prefix.

During upgrade, a Multi-Network OC deployment creates a series of new network views, each of which corresponds to the networks managed under the prior software release. Each device listed in Network Explorer tables provides a link under a new Network View column, which opens the Network Viewer window. This window displays all devices that are members of the network view.

In Multi-Network Operations Center deployments, discovery settings for each network, such as CIDR discovery ranges and seed routers, are automatically associated to the network views for each managed network, that use each of the respective discovery settings.

The following section, Discovery with a New NetMRI Deployment, describes the sequence of high-level tasks you perform to configure and run discovery on your network.

### Discovery with a New NetMRI Deployment

Do the following series of procedures to perform your first network discovery.

1. If necessary, install your NetMRI appliance or appliances. (For more information, see the Infoblox Installation Guide for your NetMRI appliances.) Ensure that you have the full feature licensing and device licensing entitlements for your deployment. For more information, see Understanding Platform attic Limits, Licensing Limits and Effective Limits. If you are upgrading your NetMRI installation, check the installation instructions in the Release Notes for your software (and see the section below, Discovery with an Existing NetMRI Platform). Also, read the section Preparing for NetMRI VRF Access for information on checking and configuring VRF-aware devices to which NetMRI will connect for managing virtual networks.

2. Configure your first network views for network management.

   For new installations, NetMRI automatically provides an initial network view, named Network 1, as part of initial setup. For initial discovery of the network, you may only need this first network view. For more information, see Configuring Network Views.

3. You combine network views with scan interfaces to separate and manage networks. For new installations, the Network 1 network view is automatically bound to your appliance’s LAN1 port. This may be the only interface you need for initial network discovery. This interface connects to the router through which NetMRI begins to discover the network. For more information, see Configuring Scan Interfaces.

4. Configure your discovery settings. They include discovery IP address ranges, possible static IP addresses of devices you explicitly want to discover in your networks, a seed router for network discovery and possible device hints to improve odds of finding devices. The seed router might be, for example, the router to which NetMRI first connects for discovery of the network. For more information, see the sections Configuring Discovery Ranges, Specifying Static IPs, Adding Seed Routers and Adding Device Hints.

5. Add the necessary device SNMP credentials, and CLI admin login and Enable password credentials. For more information, see Adding and Editing Device Credentials and its various sections. You can also add and test credentials for individual devices; for more information, see Adding and Testing SNMP Credentials for a Device.

6. Associate discovery settings to network views. Add your discovery settings from Step 4 to the network views and begin to discover the network. Initial discovery of your networks begins automatically after the discovery ranges and other discovery settings, such as a seed router, are added to the network view, which also must have a scan interface connection. For more information, see Discovery Using Network Views.

7. Watch data collection. Network data collection and virtual network detection take place during your initial network discovery, which begins automatically when the network connection is established from NetMRI, to the network to be discovered. Do the following to view discovered information about your network:

   - **View summaries of discovery events**→ Click the All Devices device group in the right panel, and open the Network Explorer → Discovery page to see a table of all devices being discovered by NetMRI. For more information about the features on this page, see Viewing and Managing Discovery Results.
   - **View a list of devices your appliance has recently discovered**→ Click the All Devices device group in the right panel, and open the Network Explorer → Inventory page to see tables of all member devices. For more information about the features on this page, see Viewing Network Inventory.
   - **View summaries of recently discovered network phenomena**→ Includes summary information of routed networks, VLANS, route targets and virtual networks (VRFs). For more information about the features on this page, see Summarizing Network Topologies.

8. Map virtual networks. If your network has virtual networks, NetMRI automatically discovers them on the devices where they are configured, and alerts you through System Health banner messages at the top of the screen to map those VRF-aware devices to the network views where they belong. By mapping each virtual network to network views, you provide more information to the discovery process. For more information, see Mapping Virtual Networks to Network Views.

**Note:** CLI credentials to devices is required to determine if devices are VRF-aware and to collect VRF-related data.

As NetMRI polls devices deeper into the network, it may find more VRF-based virtual networks. These networks need to be mapped to virtual scan interfaces to enable full network discovery and control for each virtual network. For more information, see Mapping Virtual Networks to Network Views, Configuring Virtual Scan Interfaces and Configuring VRF-Aware Device Interfaces.

The following table summarizes both migrated and new installations (steps 6-9 are common to both procedures):

<table>
<thead>
<tr>
<th>Step #</th>
<th>Migration/Upgrade</th>
<th>New Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade your software using normal Admin Shell utility.</td>
<td>Install new appliance(s) and perform system configuration through the Setup Wizard.</td>
</tr>
<tr>
<td>2</td>
<td>Currently managed network(s) are converted to new network views using the same network name.</td>
<td>Configure network views (if required) for multiple network management.</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. As NetMRI polls devices deeper into the network, it may find more VRF-based virtual networks. These networks need to be mapped to virtual scan interfaces to enable full network discovery and control for each virtual network. For more information, see Mapping Virtual Networks to Network Views, Configuring Virtual Scan Interfaces and Configuring VRF-Aware Device Interfaces.
Scan ports are associated with the network views created from the previously defined Networks.

Configure NetMRI scan interfaces (if required) for multiple network management.

| 4 | All existing discovery settings are automatically associated to their network view(s). |
|   | Configure discovery ranges/seed routers/static IPs and associate to network view(s) where needed. |

| 5 | Existing SNMP/CLI credentials configurations remain unchanged. |
|   | Configure SNMP/CLI credentials. |

**Preparing for NetMRI VRF Access**

For effective use of NetMRI to connect to and manage virtual networks, complete all steps listed in this section before configuring NetMRI. This information in this section applies specifically to the non-Infoblox network devices (e.g., Cisco and Juniper) that route virtual networks:

1. Identify the VRFs/virtual networks you want NetMRI to access and manage.
2. Identify the single VRF-aware Switch/Router on the managed network, that is aware of all of the desired VRFs. NetMRI will need to access the VRFs through this device.
   a. A VRF-aware device may not exist on the network that is aware of all of the VRFs. If it’s not possible to consolidate all VRFs into a single trunked port, you can physically connect NetMRI to multiple places on the network. NetMRI has up to 3 physical scan interfaces available, labeled MGMT, LAN1, and LAN2, that may differ slightly per platform. (For more information, see Configuring Scan Interfaces.)
   b. You also must identify a minimal set of VRF-Aware devices that collectively are aware of all the VRFs you wish NetMRI to manage.
3. Reserve a valid routable IP address on each VRF. These IPs will be configured on NetMRI virtual scan interfaces that will connect to each virtual network. Prepare an IP, subnet mask, and gateway for each VRF.
4. You must configure at least one network device to provide access to the virtual networks for NetMRI. NetMRI can connect to multiple VRFs on the same physical interface, using virtual scan interfaces, each associated with an encapsulated 802.1q tag, to access each VRF:
   a. The interface NetMRI connects to, should be configured to transport via a 802.1q encapsulated traffic (trunked port);
   b. Each tag carried by the trunked port should be associated with a single VRF on the device;
   c. If the device NetMRI is connected to is not VRF aware, then the 802.1q configurations will be in the form of VLANs, with one VLAN for each VRF. In this case, the device must trunk the VLANs to another device that is VRF aware, and can be configured to associate each 802.1q tag to a VRF;

In general, connecting NetMRI directly to a VRF-aware device requires less network device configuration.

5. When connecting NetMRI to a trunk port, for each 802.1q tag in the trunk, create a Virtual Scan Interface by right clicking the physical scan interface in Settings –> Scan Interfaces. Specify the tag, IP, gateway, network mask, and other needed settings. You also associate it with an existing Network View (for more information, see Configuring Network Views), or you may create a new Network View for the virtual scan interface.

**Configuring Network Views**

You define network views to separately manage network domains that have the following characteristics:

- Physically isolated and completely independent;
- Logically separated networks for convenient management;
- Virtual networks implemented with technologies such as VRF.

You combine network views with scan interfaces to separate and manage networks. This prevents ambiguities that can occur through route leakage and possible overlapping IP address spaces, and provides further information to help in network and device discovery.

Network views provide the useful concept of isolation. Using network views, NetMRI enables you to manage networks that may have overlapping IP prefixes or address ranges, preventing addressing conflicts between separately managed networks. You manage every network in complete isolation from other networks.

When you create discovery ranges, you also directly associate them with a network view. (For more information, see Configuring Discovery Ranges.) When you also associate a virtual scan interface with that network view, the discovery range automatically becomes the range of IP addresses that is scanned and discovered on that scan interface.

For Operations Center deployments, you can create the same network view on different appliances. Each appliance uses its own scan interface to access the same network view.

**Note:** If you delete a network view at a later time, all discovery ranges and static IPs that are associated with the network view will be deleted. For more information, see Discovery Using Network Views.

**Default Network Views**

Most users and deployments will see a single network view, which differs in name based upon whether you are performing a new installation or an upgrade to the current release:
• **New Installation:** Initial setup for a new NetMRI appliance automatically creates a default network view, named **Network 1**, as part of the procedure. This network view is automatically assigned to the appliance’s LAN1 port before you perform discovery of the network. (If the LAN1 port is not active, the MGMT port is associated with the **Network 1** view.)

• **For upgraded installations,** the managed network’s **network name** is automatically used to identify the network view used for managing the network. This value may be changed but changes are not necessary. The network name value is found in Settings icon → Setup → Settings Summary → Network Configuration section, titled **Database Name** in the current release and **Network Name** in the prior release. (For Multi-Net Operations Center deployments, the same principle applies.)

---

**Creating Network Views for the Global Network**

**Note:** If you delete a network view from the Settings icon → Setup → Network Views page, all discovery ranges and static IPs that are associated with the network view will be deleted from their respective pages under Settings icon → Setup → Discovery Settings.

When you perform initial setup of a NetMRI appliance using **configure server**, the appliance automatically uses the default network view, named **Network 1**, for the first discovery. You can also create more ‘unassigned’ network views for use with other physical scan interfaces and other networks. Do the following:

2. Click the Add icon [+ ] to add a new view entry.
3. Enter a **Name** and **Description** for the new view. Press the Tab key to navigate from the **Name** to **Description** fields.
4. Click the Add icon [+] again if you wish to create another view, or close the Network Views settings page.

The new unassigned network view will appear with a caution (⚠️) icon in other dialog boxes, such as discovery ranges configuration. This indicates the network view is not associated with a scan interface. For more information, see Configuring Physical Scan Interfaces and Configuring Virtual Scan Interfaces.

**Note:** If you create unassigned network views, and the view is not assigned to a scan interface, any discovery settings for the view will not be processed and discovery will not take place for the network view.

For information on creating network views for virtual networks, see Mapping Virtual Networks to Network Views.

---

**Mapping Virtual Networks to Network Views**

User action is required to clearly associate each discovered virtual network with its correct network view in the Network View Editor. This provides additional context to collected data and enables NetMRI to fully discover and model the network topology. If you define any new network views in this step, you will also need to configure scan interfaces based on the steps in Configuring Scan Interfaces. If a network view does not have an assigned scan interface, discovery will not take place on that network.

If you do not wish to perform extensive management of VRF-based virtual networks in your deployment and receive a System Health banner alert reporting unassigned VRFs, do not ignore the alert. Simply map all the discovered VRF-based virtual networks to your existing network view (VRF examples include **(Default) IOS** (for Cisco IOS), **default** (for Cisco Nexus) or **master** (for JunOS), which are the global VRFs that may be present in some networks). Doing so automatically instructs NetMRI to use collected VRF data for further discovery.

**Note:** In NetMRI, the SysAdmin Role has access to the Network View editor.

To add a discovered VRF to a network view, do the following:

1. Go to Settings icon → Setup → Network Views.
   The Network Views settings page appears, listing all currently defined views.
2. Hover the mouse over the Action icon for the chosen network view and select Assign.
   The Define and Configure Networks editor appears in a popup window.
3. To see all currently discovered VRFs, click Search VRF Names.
   All discovered VRF instances in all devices are listed alphabetically. Unassigned VRFs appear in white in the left panel, and assigned VRFs are highlighted in gray. If you see more VRF entries than you can easily navigate, check the Show unassigned VRF Only check box.

**Note:** Each network view must have a discovery range associated with it. For more information, see Configuring Discovery Ranges.

4. To see all VRFs listed as discovered on each device, click Display VRFs per Device.
   All VRFs are listed under their respective device names.
5. To see all VRF instances that are associated with any Network View, click Display VRFs per Virtual Network.
   All VRFs are listed under their respective virtual networks. The same network view can manage all VRFs in a single virtual network.
6. To set an entire virtual network to the selected network view, check the check box for all discovered VRF routers in the list that are identified by a specific VRF Name (such as red or blue). In this case, each instance of the same VRF in the list shows its own unique Device Name.
   a. For each discovered virtual network, you will see one or more devices that are running VRF instances in that virtual network.
Discovery Using Network Views

When the network views are configured with their associated discovery settings and scan interface, NetMRI automatically starts discovery across the connected network. After a few moments, newly discovered devices will begin to appear in the main Discovery pages under Network Explorer → Discovery. Click device group names on the right panel to see categories of devices discovered by NetMRI. If NetMRI identifies a device inside any network view as using Cisco IOS, NXOS or Juniper JunOS, it attempts to collect possible VRF configuration data on the device by using the device's CLI. If the CLI is not accessible, (or the device does not have VRF configurations), NetMRI treats the device as not configured for VRF. Full detection of VRF configurations on VRF-aware devices requires CLI credentials, including Enable password access. After discovery, you map VRFs to network views associated with virtual scan interfaces and discovery settings, to allow ARP and routing data collected inside the network view to be leveraged for further discovery. After NetMRI discovers VRF-based virtual networks in your deployment, a System Health banner alert appears at the top of the screen. Click its link to view details about the alert, which appears in the Settings icon → Notifications → System Health page. (For more information, see Managing and Tracking System Health.)

Using the Network Viewer Window

Anywhere you can view device information, such as under Network Explorer → Inventory, the devices table shows a column titled Network View. Each managed device belongs to a network view, and the Network View column shows the device's membership. Each entry under the Network View column links to the Network Viewer window. It shows the complete list of devices that are members of the network view, broken into two categories:

- The complete list labeled as Associated VRFs, which are all of the VRF instances that route traffic for the current network, including the selected device's local VRF.
- The list of Imported VRFs, which are all VRF instances imported based on routing policy from other VRF-aware devices that route traffic in the virtual network. The Route Distinguisher values identify the VRF instance to help specify how routes will be shared between different VRF networks.

Some device types do not use Route Distinguisher values (also known as Route Targets) for VRF configuration and the value will be blank as a result. You can assign other VRF instances to the current network by clicking the Assign button over the Associated VRFs list, which opens the network editor. For more information, see Mapping Virtual Networks to Network Views.

Deleting Network Views

Note: Exercise caution when deleting network views. After the network view is deleted, devices formerly within a deleted network view will not be immediately reachable by NetMRI. NetMRI will attempt to find an alternate IP address for such devices, perhaps from other virtual networks; if other reachable IP addresses for those devices are found, they will continue to be polled from the new location. If they are not located, their records will expire from the managed or discovered device databases.

If you delete a network view from the Settings icon → Setup → Network Views page, all discovery ranges and static IPs that are associated with the network view will also be deleted from their respective pages under Settings icon → Setup → Discovery Settings. When you delete a network view from NetMRI, all VRFs (virtual networks) that are part of the Network View will become Unassigned. When this occurs, a System Health warning message banner appears at the top of the screen. You can then reassign the unassigned VRF to another network view. The scan interface that is associated with a deleted network view also becomes an unassigned interface. To delete a network view, do the following:

1. Go to Settings icon → Setup → Network Views. The Network Views settings page appears, listing all currently defined views.
2. Hover the mouse over the Action icon for the chosen view and select Delete. A confirmation message appears.
3. Click Yes to delete the network view. Its previously assigned network becomes unassigned.

At least one network view will always be active in the system. Attempts to delete the last remaining network view, regardless of name, will be prevented by NetMRI.

Configuring Scan Interfaces
For each network view, NetMRI requires connections to each network that you discover, manage and control. Scan Interfaces are the ports on NetMRI appliances and virtual appliances that perform this function. Physical scan interfaces are actual Ethernet ports.

There are two types of scan interfaces: physical scan ports, where an entire Ethernet interface in the appliance discovers and manages a network; and virtual scan interfaces, that use 802.1Q VLAN tagging between NetMRI and the connecting device, to exchange traffic for multiple networks across a single physical interface. To use virtual scan interfaces, you connect one of NetMRI's physical scan interfaces to a device interface configured to route the desired networks with 802.1Q VLAN tags.

For more information on configuring virtual scan interfaces, see Configuring Virtual Scan Interfaces.

Configuring Physical Scan Interfaces

Your NetMRI appliance's physical scan interface configuration varies depending on your appliance's physical configuration, and even whether the appliance is a VM.

To configure a physical scan interface, do the following:

1. Go to Settings icon -> Setup -> Scan Interfaces.
   The Scan Interfaces page appears, listing all device interfaces that may be used by the appliance. Depending on the hardware and system type, you will see one or more interfaces named MGMT and/or LAN\(n\) (where \(n\) is the physical port number). If your system is an Operations Center, the Collector Name is shown alongside the interfaces. If any virtual scan interfaces are defined, they will have names like LAN2.111. See Configuring Virtual Scan Interfaces below for more information.

2. Hover over the Action icon for any of the physical ports and select Edit from the menu.

3. Choose from the Network View configuration section:
   a. Select Existing: Choose a network view from the list of existing ones that are defined on the system;
      - Select the view from the dropdown list;
      - Selecting Unassigned as the Network View leaves the interface in a disabled state.
   --or--

   b. Create New: Creates a new network view.
      - Enter the name for the new network view;
      - Enter a comment describing the view. These values can be edited at a later time.

4. Enter the IPv4 Address, IPv4 Subnet Mask and the IPv4 Default Gateway; or, enter the IPv6 Address, IPv6 Subnet Mask and the IPv6 Default Gateway values if the connection supports IPv6 in addition to, or instead of, IPv4.

5. Click Save to save the new physical scan interface configuration. On physical ports, you may Edit or Add Virtual Scan Interfaces.

Note: Though the MGMT port provides allows for the same scanning discovery and device control capabilities as other appliance physical port types, Infoblox recommends limiting managing enterprise networks through the MGMT port, using it only for management access to the appliance's web, cli and tunnel interfaces, so those functions cannot be compromised by end-user traffic.

You cannot assign scan interfaces from MGMT ports on appliances in an Operations Center.

Configuring Virtual Scan Interfaces

To define virtual scan interfaces, do the following:

1. Go to Settings icon -> Setup -> Scan Interfaces.
   The Scan Interfaces page appears, listing all device interfaces that may be used by the appliance. Depending on the hardware and system type, you will see one or more interfaces named MGMT and/or LAN\(n\) (where \(n\) is the physical port number). If virtual scan interfaces are defined, they bear names such as LAN2.111.

2. Hover over the Action icon for any of the physical ports and select Add Virtual Scan Interface from the menu.

3. Choose from the Network View configuration section:
   a. Select Existing: Choose a network view from the list of existing ones that are defined on the system;
      - Select the view from the dropdown list;
      - Selecting Unassigned as the Network View leaves the interface in a disabled state.
   --or--

   b. Create New: Creates a new network view.
      - Enter the name for the new network view;
      - Enter a comment describing the view. These values can be edited at a later time.

4. In the Tag field, enter the 802.1Q tag value defined on the facing device that transits the trunk port or router port.

5. Enter the IPv4 Address, IPv4 Subnet Mask and the IPv4 Default Gateway; or, enter the IPv6 Address, IPv6 Subnet Mask and the IPv6 Default Gateway values if the connection supports IPv6 in addition to, or instead of, IPv4.

6. Click Save to save the new virtual scan interface configuration.

You may also Edit or Delete virtual scan interfaces.

Remember the following points about scan interface configuration:
• You can assign a network view to a physical port on your appliance, such as LAN1. Doing so does not prevent the same port from supporting virtual scan interfaces, each of which supports their own network view;
• You can define virtual scan interfaces and assign network views to them, and choose not to apply a network view to the physical LAN port hosting those virtual scan interfaces (LAN1, for example);
• You can create a virtual scan interface with a tagging value, but not immediately assign it to a network view. The virtual scan interface is effectively disabled and you can assign its network view at a later time; you can assign it to an existing network view or create a new one.

Configuring VRF-Aware Device Interfaces

To give NetMRI access to the routed domain for a mapped VRF, the user must connect NetMRI to one of the interfaces, on the VRF-aware device, that belongs to that virtual network. (The user needs to provide visibility on their virtual network to the scan interface that is discovering it.

• If the VRF-aware device is directly connected to NetMRI:

  If the mapped NetMRI scan interface is a physical SCAN interface, the user must use or configure a physical interface on the target VRF-aware device to communicate with NetMRI without using 802.1Q encapsulation.
  If the mapped scan-interface is a logical sub-interface using 802.1Q encapsulation, the user configures the directly connected physical interface of the VRF-aware device, and subdivides it using a logical sub-interface with the same 802.1Q encapsulation. The user may otherwise use a VLAN interface with the same 802.1Q encapsulation and allow its traffic through the physical SCAN interface.

• If the VRF-aware device is not directly connected to NetMRI:

  No additional configuration is required for these devices. NetMRI can reach different VRFs from the moment these resources are routed by a VRF mapped into a Network View which is accessible from a scan interface mapped on that same Network View. You may apply different techniques, such as using VLANs all the way down to the desired VRF to discover, or using intermediate devices that are members of the routed domain of that VRF.

Special Considerations for Managing VRF Virtual Networks

When you define discovery settings and perform management of virtual routing and forwarding networks, some considerations exist that you should be aware of:

• If you limit the context of the SNMP community string in an individual VRF to the context of only that VRF, NetMRI will not be able to determine that the device it has discovered inside that VRF is the same device it has found inside other virtual networks. This will result in extra, uncorrelated devices in the network.
• NetMRI will become aware of some devices inside of virtual networks from the route and ARP tables of routers that it manages; without network connectivity into those virtual networks through a virtual scan interface, NetMRI cannot discover all the devices or manage them. To create the necessary connectivity, you need to configure a NetMRI scan interface to be part of the VRF.
• NetMRI will collect and parse the ARP and routing information from within a VRF context, but this data will not be used for further discovery unless the VRF virtual network is associated to a network view mapped on a scan interface.
• Global VRFs are labeled as: default(IOS) for IOS, default for Nexus and master for JunOS.
• For discovery and periodic polling on Juniper devices through an interface that is not in the Juniper default VRF (master), the query must use a special “default@credential” format. This setting assumes that users do not have management interfaces in a VRF. Your defined SNMP credentials for VRF-aware Juniper devices must use syntax similar to; “@vrfsnmp.” Enter these values for SNMP credentials under Settings icon – > Setup – > Credentials – > SNMP v1/v2c tab. (Note that when querying VRF-aware Juniper devices via an interface that is in the default VRF, a plain community string can be used without the “@” character.)
• When configuring NetMRI to discover networks where route-leaking is employed (the practice of sharing routes between two or more networks, such as VRFs), discovery ranges for each network views should only be defined to include IPs known as belonging to that network view. In other words, any given Device IP should only fall within the discovery ranges of one network view. If discovery ranges are defined such that a Device can be discovered by two different network views, the device may also be discovered via an unexpected network view.

Configuring Network Discovery Settings

Effective discovery of IP networks requires several elements:

• At least one well-connected seed router, which can be the router to which NetMRI first connects (see Adding Seed Routers);
• Valid CIDR discovery IP address ranges (see Configuring Discovery Ranged);
• SNMP credentials for network devices (for more information, see Adding and Editing Device Credentials);
• CLI credentials and Enable credentials for further discovery of device configuration settings (for more information, see Adding and Editing Device Credentials);
• Blackout settings to ensure that discovery traffic takes place during policy mandated time periods (for more information, see Defining Blackout Periods).

The Discovery Settings page (Settings icon – > Setup section – > Discovery Settings) defines the scope of the networks that NetMRI explores using CIDR (Classless Inter-Domain Routing) address blocks, IP address ranges, IP address wildcards, static IP addresses, and seed router definitions. NetMRI applies discovery settings equally to IPv4 and IPv6 networks, with the polling protocols specified in Settings icon – > Setup – > Collection and Groups – > Network Polling.

Use caution when entering address ranges, particularly if you are using IPv6 values. If you have a default route to the Internet and you enter an address range incorrectly, you may receive a call from your ISP asking about a network scanner running from your network.

To perform your first network discovery, go to Settings icon – > Setup – > Setup Wizard. When you use the Setup Wizard, the Wizard guides you through the process of performing discovery on the network. When specifying your first discovery ranges, you also select the network view to use for the discovered network. This step is required, and is further explained in the topic Configuring Network Views.
Configuring Discovery Ranges

Note: For IPv6 network discovery, use of discovery range definitions for all networks is required to ensure that you discover all the required hosts and network infrastructure. Also consider using RFC 4193 local IPv6 network addresses (also called unique local IPv6 unicast). These values are globally routable within the enterprise but are independent of the ISP and allow for filtering at network boundaries. They are not globally routable prefixes. Their local IPv6 unicode address begins with FC00::/7. Examples of this type are used in this section. Globally routable prefixes begin with the 2001/64 or 2001/24 and are not used as examples in this document.

The Ranges tab defines the scope of the networks that NetMRI explores by defining CIDR address blocks, IP address ranges and IP address wildcards, and discovery blackout settings. The appliance limits its network exploration to the set of ranges defined in this tab.

- A CIDR address block is defined by a network address and bit mask (for example 192.168.1.0/24). An IPv6 example: FC00:56:aa12:ea23:a5:ac10:100/119. Any IPv6 CIDR values must include the IP address ranges that you want to discover.
- An IP address range defines a starting and ending IP address. For instance, in IPv4 you could define 192.168.1.0 as the start of the IP range and 192.168.1.255 as the end of the IP range. You cannot configure IP address range values for IPv6 networks.
- An IP address wildcard pattern defines IP address range using a wildcard character or range for a specific set of octets. A single wildcard can be a octet range specified by dash (e.g., 10-254) or an asterisk (*) when the whole range for an octet is specified (0-255 for IPv4 and 0000-ffff for IPv6). For example, you can define either 192.168.1.* or 192.168.1-255.5 as the IP address wildcard pattern. An IP wildcard pattern will be rejected if it contains more than 65536 CIDs. It is recommended to keep the total number of CIDs under 1000, specifying more may affect performance.

Full discovery of an IPv6 network requires use of Discovery ranges.

The Ranges table displays each defined range, its type (CIDR, RANGE, or WILDCARD), and its use in the discovery process. Ranges excluded for discovery indicate that any network device found matching that range is excluded from discovery by the appliance. (See the Ranges Examples section for more information.)

Creating Discovery Ranges

Note: For discovery ranges, configuring Discovery Blackouts requires use of the Admin account.

Every discovery range you create must be associated with a network view. If no network views are specifically defined in your deployment (for details, see Configuring Network Views), your discovery ranges will automatically be assigned to the Network 1 network view.

Note: Setting ranges for Exclude from Management is useful for devices you may not want to manage, but want to know about for inventory purposes. End Host network segments are a good example.

To create a range to perform discovery, do the following:

1. Obtain or calculate the network range values. You can define a Network address (expressed as CIDR: in effect, a subnet prefix), an IP range, or an IP pattern.
2. Choose Settings icon → Setup → Discovery Settings → Ranges.
3. Click New to add a new discovery range.
   - To enter an IP prefix as the Range value, choose CIDR and enter the IP Prefix value and its CIDR subnet value in the dropdown. The prefix supports up to /128 values.
   - To input an IP range using a beginning and ending value, choose IP Range and enter the beginning and ending IP address values of the new discovery range.
   - To specify an IP address pattern, choose IP Pattern and input an IPv4 address pattern.
4. Choose the desired Discovery Mode.
   - Include in Discovery — any device found matching that range is discovered and managed by NetMRI.
   - Discovery gives highest precedence to devices found in an Include in Discovery range, ensuring they will be the first to appear in information tables in the appliance.
   - Exclude from Discovery — instructs NetMRI to ignore the specified values and do not discover them through any of the specified protocols. Ranges set to an Exclude Discovery setting are simply excluded, given the lowest precedence, and will not be discovered.
   - Exclude from Management — NetMRI discovers any device found matching that range, but NetMRI will not manage or collect data from the device. Network devices found in an Exclude from Management range are given moderate precedence and will, over time, appear in information tables applicable to unmanaged devices. (End host network segments are an example.)

Note: If you are Discovering end host subnetworks for Switch Port Management, choose the Exclude From Management option for the end host discovery ranges.

Note: An advanced setting, Discovery Status Precedence (Settings icon → NetMRI Settings → Advanced Settings → Discovery group → Discovery Status Precedence), governs the global setting for exclusion ranges. Changing this Advanced setting to Longest Prefix Match enables an exclusion range to contain smaller IP ranges that can be matched against to allow discovery — for example, you can Exclude a /26 network, but Include a /24 prefix within the EXCLUDE range, because the /24 is a longer prefix.
5. To use a discovery ping sweep (a probe that uses a range of packet types to detect the presence of a system on each IP in the specified range, with ICMP Echo, ICMP Timestamp, TCP SYN to port 80, and TCP SYN to port 443) for discovery on IPv4 networks, check the **Enable Discovery Ping Sweep** check box. Ping sweep is not available for IPv6 network values. (For more information on ping sweeps, see Defining Group Data Collectors on Settings.)

**Note:** The discovery ping sweep feature differs from the Smart Subnet ping sweep in the following ways: the discovery ping sweep will run only against the specified range; the sweep will run regardless of the range size; and the sweep will run regardless of the number of discovered devices within the specified range.

6. Check the **Enable Discovery Blackout** check box and click its Scheduling icon. The Discovery Blackout Scheduling dialog opens.

**Note:** For more information about discovery blackouts and change blackouts, see Defining Blackout Periods.

a. In the **Recurrence Pattern** dropdown, choose how often you want to execute the blackout period. You can select **Once, Daily, Weekly, or Monthly.**

b. If you choose **Once:**
   - Choose an **Execution Time** from the drop-down list.
   - Enter the date of the blackout, in the **Day of** field.
   - Specify the **Duration:** 10 or more Minutes, Hours or Days.

c. If you choose **Daily,** click either **Every Day** or **Every Weekday.**
   - Choose an **Execution Time** from the drop-down list.
   - Specify the **Duration:** 10 or more Minutes, Hours or Days.

d. If you choose **Weekly,** complete the following:
   - Choose an **Execution Time** from the drop-down list.
   - Check the check boxes for one or more days from **Sunday** through **Saturday.**
   - Specify the **Duration:** 10 or more Minutes, Hours or Days.

e. If you choose **Monthly,** complete the following:

   - Choose an **Execution Time** from the drop-down list.
   - **Schedule the day of the month:** A discovery blackout can be executed monthly on a specific day, or blackout instances can be executed more than one month apart on a specific day, in the **Day of every month(s)** field.
   - Specify the **Duration:** 10 or more Minutes, Hours or Days.

7. If more than one network view exists, you can choose the **network view** with which the discovery range will be associated, by clicking the **Network View** drop-down menu. (If only one network exists in NetMRI, this setting does not appear.)

For the first discovery of the network, the network view automatically created by NetMRI (Network 1) is automatically assigned to the SCAN1 port when you set up the appliance using **configure server.** The chosen network view, if more than one exists, must also be associated with a scan interface or discovery will not take place. Network views can contain multiple discovery ranges, so when you create other ranges, you can assign the same network view to each. However, you can assign each discovery range to only one network view. Also, ensure that the ranges you assign to each network view make sense. Selecting the network view in an Operations Center environment also involves other details. For more information, see Defining Discovery Ranges or Operations Center Collectors.

Unassigned network views that do not have an assigned scan interface or virtual scan interface will appear with a caution (⚠️) icon in discovery ranges configuration.

8. Click **Add** to place the new discovery range into the Range table.

### Creating Blackouts for Individual Devices

To support discovery blackouts for individual devices, obtain the Management IP address for the device in question, and assign that IP address to a /32 or /128 discovery range. Define the discovery blackouts settings as you would for any other discovery range. This practice may be handy, for example, for strategic routers and switches that cannot incur excessive latency for transaction traffic. However, this approach means that you cannot create change blackouts for individual devices.

### Defining Discovery Ranges on Operations Center Collectors

If you have an Operations Center with at least two Collector instances, you can assign different discovery ranges to different Collectors, or assign a range to all collectors in an OC for the same purpose. The **Filter by Collector** drop-down menu provides a listing of all Collectors and their respective device limits, which are associated with the licensing limits for each Collector appliance. You also choose the **Network View,** which lists all network views with their collector appliance names in brackets.
For an OC deployment managing a single large network, you choose the network view entry from the Network View list. You will see multiple entries in the pages under Settings icon → Setup → Discovery Settings for the Network View list. The entire network is assigned to a single network view; however, each network view entry is identified through the association of each Collector. This allows you to edit discovery settings for each Collector in the same network view. Examples:

Network 1 (NM35)
Network 1 (NM36)
Here each Collector, NM35 and NM36, is associated to the same network view.

For an OC deployment managing multiple networks, choose the desired Collector from the Filter by Collector list. Then, select the network view under the Network View list.

The licensing limits correspond to those described in the topic Understanding Platform Limits, Licensing Limits and Effective Limits. Each Collector entry listed in the Filter by Collector drop-down menu in the lists the following information:

| Device Limit | Shows the maximum device license count for the Collector—the maximum number of devices the Collector is licensed to manage. (This value does not apply to discovered device counts, which can be higher.) The value in this column corresponds to an Effective Device Limit for the Collector. |
| Devices Licensed | The number of currently used device licenses for the listed Collector. The difference between this value and the Device Limit, if any, represents the number of unused device licenses remaining available to the Collector. |

Note: Discovery ranges associated to network views unassigned to a scan interface will not be used for discovery.

To assign a discovery range to an Operations Center Collector, do the following:

1. Obtain or calculate the network range values. You can define a Network address (in effect, a subnet prefix), an IP range, or an IP pattern.
2. Choose Settings icon → Setup → Discovery Settings → Ranges.
3. Click New to add a new value.
4. To enter an IP prefix as the Range value, choose Network and enter the IP Prefix value and its CIDR subnet value in the drop-down.
5. To input an IP range using a beginning and ending value, choose IP Range and enter the beginning and ending values of the range.
6. To specify an IP address pattern, choose IP Pattern.
7. Select the desired Discovery Mode. Specify the Discovery Mode as:
   - Include in Discovery (any device found matching that range is discovered and managed by NetMRI);
   - Exclude from Discovery (ignore the specified values and do not discover them through any of the specified protocols);
   - Exclude from Management (indicates that NetMRI discovers any device found matching that range, but NetMRI will not manage or collect data from the device).

Note: Discovery processes can occupy significant resources within the network when discovery is taking place. You can avoid possible interference with latency-sensitive network applications by creating time periods when NetMRI will not communicate with devices or networks for discovery. These time periods are called discovery blackout periods. You can create discovery blackout periods for each discovery range you define in NetMRI. Discovery blackout periods are optional and can be enabled and configured, or disabled, at any time. All communications are stopped with a given device, including but not limited to the following:

- SNMP
- SSH
- Telnet
- Ping
Traceroute

A second blackout type, change blackout, allows NetMRI to enforce blackouts for CLI interaction, scheduled or run-now job executions, Telnet/SSH proxy and port control UI features. Change blackouts do not apply to Discovery ranges and cannot be configured for them. Change blackouts will allow read-only discovery, device changes detection and device analysis for issues without permitting any CLI communication or configuration changes. Change blackouts typically disable operations such as enabling or disabling interfaces on devices.

Discovery blackouts and change blackouts can be applied to the following:

- Globally across the entire NetMRI deployment;
- Discovery IP ranges (for information, see Configuring Discovery Ranges);
- Strategic individual devices (for information, see Creating Blackouts for Individual Devices);
- Device Groups (for information, see Creating Device Groups).

Discovery tasks may already be running when a blackout period takes effect. Current tasks will not be interrupted and will complete within their time. NetMRI will not activate new discovery tasks on the chosen network, device group or individual device during the blackout period.

Note: A common use case for discovery blackout windows and/or change blackout windows is to enforce them during normal working hours, such as 8AM to 5PM.

Configuring a Global Discovery Blackout or Change Blackout

You separately configure discovery blackouts and change blackouts. No dependencies exist between blackout types; you may configure either type without defining new settings for the other type. At the Global level, discovery blackouts and change blackouts apply across all network views, discovery ranges, device groups and devices unless otherwise disabled at the range or device group level. Do the following:

1. Choose Settings icon → Setup → Collection and Groups.
2. On the Global page (which appears by default), check the Enable Discovery Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets appear.
   a. In the Recurrence Pattern dropdown, choose how often you want to execute the blackout period. You can select Once, Daily, Weekly, or Monthly.
   b. If you choose Once:
      * Choose an Execution Time from the drop-down list.
      * Enter the date of the blackout, in the Day, field.
      * Specify the Duration: 10 or more Minutes, Hours or Days.
   c. If you choose Daily, click either Every Day or Every Weekday.
      * Choose an Execution Time from the drop-down list.
      * Specify the Duration: 10 or more Minutes, Hours or Days.
   d. If you choose Weekly, complete the following:
      * Choose an Execution Time from the drop-down list.
      * Check the check boxes for one or more days from Sunday through Saturday.
      * Specify the Duration: 10 or more Minutes, Hours or Days.
   e. If you choose Monthly, complete the following:
      * Choose an Execution Time from the drop-down list.
      * Schedule the day of the month: A discovery blackout can be executed monthly on a specific day, or blackout instances can be executed more than one month apart on a specific day, in the Day of every month(s) field.
      * Specify the Duration: 10 or more Minutes, Hours or Days.
3. If necessary, select the Enable Change Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets appear.
   a. Follow steps 2a through 2e to define the change blackout schedule.
4. Click Save to commit changes.

Specifying Static IPs

The Static IPs tab can specify IPv4 and/or IPv6 devices that must have a high priority of discovery and data collection by the appliance. Devices matching IP addresses listed in this tab are given priority over other discovered devices, for data collection and for priority in counting toward any device found matching the license limits. The process is similar to a seed router, except that in the latter, we assume the specified device is a router, and specifying it as such accelerates discovery and data collection on that device. A device specified through a static IP can also be excluded from discovery or management. Static IPs and prefixes can also be written in an Excel file for import into the appliance.

Devices in the Static IPs list also will be immediately rediscovered by NetMRI even after you delete the device and its discovered data by other means. If you remove a device from the network that may be in the Static IPs list, ensure that you also delete the device from this page to prevent attempts at rediscovering the device.

- For an OC deployment managing a single large network, you choose the network view entry from the Network View list. You will see multiple entries in the pages under Settings icon → Setup → Discovery Settings for the Network View list. The entire network is assigned to a single network view; however, each network view entry is identified through the association of each Collector. This allows you to edit discovery settings for each Collector in the same network view. Examples:
  
  Network 1 (NM35)
  Network 1 (NM36)

  Here each Collector, NM35 and NM36, is associated to the same network view.

- For an OC deployment managing multiple networks, choose the desired Collector from the Filter by Collector list. Then, select the network view under the Network View list.

It is also possible that a statically defined device in the Static IPs tab is in an Exclude or Ignore range in the Settings icon → Setup → Discovery Settings → Ranges tab. In all such cases, the range is excluded or ignored but a statically defined device found matching an IP address within that range will be
discovered and managed.

To create a new static IP entry, do the following:

1. Choose Settings icon → Setup → Discovery Settings → Static IPs and click New.
2. Enter the IP address for the static device. The value can be IPv4 or IPv6.
3. Select the Discovery Mode. Specify the Discovery Mode as:
   - Include in Discovery – NetMRI will discover and manage any device found matching that range;
   - Exclude from Discovery – Ignore the specified values and do not discover them through any of the specified protocols;
   - Exclude from Management – NetMRI will discover any device found matching that range, but will not manage or collect data from the device.
4. (For Operations Center only) From the Filter by Collector: dropdown menu, choose the Collector from the list.
5. Choose the network view with which the static IP will be associated, by clicking the Network View drop-down menu. This step is required.
   a. If this is part of the first discovery of the network, and no other network views are configured, the Network View selector does not appear, and the default Network 1 network view is automatically assigned. Otherwise, choose the network view from the list.
   - or –
     b. (For Operations Center only) From the Network View dropdown menu, choose the network view to which the static IP for discovery will be assigned. If the network view is divided among two or more Collectors, choose the desired network view based upon the associated Collector name.
6. Click Add to place the new static IP address into the table.

To import discovery setting data: Click Import. In the dialog, click Browse... to select the CSV file, then click Import.

Note: When exporting discovery settings from an Operations Center (using CSV Export), the Collector will not be present in the exported data.

See Credential Import Formats for import file syntax.

Adding Device Hints

Note: Any device hint applies only to Router or Switch-Router device types during discovery. You can apply other hints to any supported device type to ensure detection and management by NetMRI.

The Device Hints tab provides hints to NetMRI’s discovery engine for locating specific types of network devices (for discovery purposes, chiefly routers and switch-routers) by using IP address patterns and DNS name patterns. For instance, if most routers are found at an IP address ending with ".1", specifying "*.*.*.1" and associating the Router device type for an IP address hint allows the appliance to prioritize discovered devices matching that hint higher in its credential collection queue to help speed discovery. NetMRI considers this hint when it attempts to determine a device type for a discovered device.

- Use a single asterisk (*) to wildcard an entire IPv4 octet (192.168.1.*). The "*" wildcard is not applicable for IPv6 hint rules. The double colon ("::") is used for IPv6 hint values.
- Valid IP address patterns are either the numeric values of the octet, or an asterisk for any number of octets in the IP address. For device name matches, valid DNS characters and the asterisk character are valid definitions. For instance, rtr will match any device name with "rtr" in its definition.
- Device hints are optional and are used only to speed network discovery and to assist with determination of device types absent other discovery data.

To create a new router hint, do the following:

1. Choose Settings icon → Setup → Discovery Settings → Device Hints and click New.
2. Select the Device Type from the dropdown list. Typically, this should be Router or Switch-Router.
3. Enter the IP address pattern or DNS pattern needed for device detection.
4. Click Add to place the new hint into the table.

Device Hints apply across the entire system and are not associated with network views.

IPv6 Hint Details

For IPv6, router hints are formatted to start with a double-colon designator ("::") and followed by the host-side identifier for the hint. IPv6 router rules can be up to 48 bits in length, applying only to networks where the rule fits. The shorter the hint, the broader the rule. Such rules apply to Routed Switch-Router devices to be used during discovery. For IPv6 networks, the process entails discovering routes and then sending probes, using those hints, into those networks to discover the intermediate hops leading to them. Discovery performance can be improved if a site uses static IPv6 addresses for routers, such as

<any 64-bit network prefix>::<first 56 bits of host IP>::10

These values can be added as hints. Further examples are below:

<table>
<thead>
<tr>
<th>Discovered/Found Route</th>
<th>Hint</th>
<th>Resulting Discovery Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC00:db8:a2b01::64</td>
<td>::1</td>
<td>FC00:db8:a2b01:1</td>
</tr>
<tr>
<td>FC00:2345:3400:1678::64</td>
<td>::2022:0:1</td>
<td>FC00:2345:3400:1678::2022:0:1</td>
</tr>
</tbody>
</table>
Adding Seed Routers

You define Seed Routers for NetMRI to speed up network discovery. Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks. Seed routers are also given priority (like static IP definitions) for determining which devices are counted toward NetMRI's license limits. For discovery of any IPv6 network, at least one well-connected IPv6 router (preferably with routes to all other networks to be managed by NetMRI) must be placed in the Seed Router list. In some cases, seed routers may not have the full routing tables or be unable to provide full information for some reason. The general rule of thumb is that more seed routers are better, but the connectivity of the seed router(s) also helps determine how many seed routers you need. Avoid having more seed entries than necessary.

Note: For effective use of seed routers, you must also provide admin credentials to NetMRI to allow it to pull the key routing and connectivity information, including the IPv6 routing table and the local Neighbor Discovery Cache, from the device. NetMRI uses the standard IPv6 counterparts to standard communications protocols, including SSH and SNMP.

The Seed Router table lists each defined seed router with its discovery status (as defined in the Network Explorer -> Discovery page). By reviewing the discovery status for each seed router you can determine whether NetMRI should be able to discover the network successfully, or if there are possible configuration errors preventing network discovery, without having to wait to see what NetMRI finds.

The general rule of thumb is that more seed routers are better, but the connectivity of the seed router(s) also helps determine how many seed routers you need. Avoid having more seed entries than necessary.

Note: If you have disabled discovery, or discovery is disabled because the NetMRI license is for evaluation, you can define static IP addresses and only the Static IPs tab is available. If discovery is disabled, NetMRI restricts the number of static IPs to the device limit for which the system is licensed.

- For an OC deployment managing a single large network, seed routers can be assigned to each Collector. Choose the network view-collector entry from the Network View list. You will see multiple entries in the pages under Settings icon -> Setup -> Discovery Settings for the Network View list. The entire network is assigned to a single network view; however, each network view entry is identified through the association of each Collector. This allows you to edit discovery settings for each Collector in the same network view. Examples:

  Network 1 (NM35)
  Network 1 (NM26)

  Here each Collector, NM35 and NM36, is associated to the same network view.

- For an OC deployment managing multiple networks, you choose the desired Collector from the Filter by Collector list. Then, select the network view under the Network View list. Also bear in mind that any single Collector can have multiple network views.

You enter IPv6 seed router values in a different fashion from a conventional IPv4 router address, because the address value is longer and is formatted differently. You use the same data entry field for adding a new seed router whether the entry is an IPv4 or IPv6 address. Seed router values have other considerations when working with IPv6. Collected IPv6 routing information uses link-local unicast (indicated with the FE80: prefix) addresses as the next hops from a current device, but globally advertised routes (or local IPv6 unicast routes that are known throughout the enterprise network) will not automatically be available. Because NetMRI uses routing protocol advertisements and other elements to determine global addresses of next hops for further discovery, the lack of global routing advertisements in IPv6 limits the detection of IPv6 router addresses. As a result, one or more globally accessible IPv6 router addresses must be added as seed routers (whether local unicast or global unicast is dependent on the network). Ideally the seed router would have routes to all other locations in the network; otherwise, you will need more than one seed router value to discover the full network. Don't enter link-local router addresses as seed routers, because link-local addresses have no significance for devices such as NetMRI that are not locally attached to that link.

After NetMRI discovers the routers and collects their routing tables, it uses that information to communicate with and discover adjacent routers, and other devices local to the seed router and otherwise discovered in that part of the topology—including any routers in defined Ranges—to discover the next series of hops in the IPv6 network. The process continues until all IPv6 devices are discovered, including endpoints appears.

To add new router values into the Seed Routers table, do the following:

1. Choose Settings icon -> Setup -> Discovery Settings -> Seed Routers and click New.
2. Enter the new value into the Seed Router IP Address field.
3. (For Operations Center only) From the Filter by Collector: dropdown menu, choose the Collector from the list.
4. Choose the network view with which the seed router will be associated, by clicking the Network View drop-down menu. This step is required.
   a. If this is part of the first discovery of the network, and no other network views are configured, the Network View selector does not appear, and the default Network 1 network view is automatically assigned. Otherwise, choose another network view from the list.
   - or -
   b. (For Operations Center only) From the Network View dropdown menu, choose the network view to which the seed router for discovery will be assigned. If a network view is divided among two or more Collectors, choose the desired network view based upon the associated Collector name.
5. Once the new value is entered into the Seed Routers table, click Add and Discover to immediately begin the discovery process, or click Add to place the router value into the table for later discovery.

Configuring Cisco APIC
You can configure Cisco APIC (Application Policy Infrastructure Controller) on NetMRI and discover Cisco APIC components, such as SDN Controller and Elements, including spine switches, leaf switches, EPG (End Point Groups).

For each configured Cisco APIC, NetMRI discovers the following information:

- **APIC Controller (managed device):** Collects basic information on ACI fabric devices such as device model, vendor name, OS information, IP address, and user name.
- **ACI specific endpoint information such as EPG, Bridge Domain, and Tenant.**
- **General Endpoint (devices) information such as name, IP address, VRFS, and physical connection (fabric port).**

NetMRI categorizes leaf and spine switches, API controller as network devices, and end points as end hosts. After executing the discovery process, you can view the discovered device information in the **Discovery** tab (Network Explorer → Discovery). For more information, see Viewing and Managing Discovery Results.

Complete the following to configure a Cisco APIC:

1. Go to **Settings** → **Setup** → **Discovery Settings** → **APIC** and click **New**.
2. Complete the following:
   - **Protocol:** Select HTTP or HTTPS as the protocol. When you select HTTPS, you must upload the corresponding SSL CA certificate in order for NetMRI to communicate with Cisco APIC and the host name mentioned in the **APIC Controller Address** field must match the host name of the APIC certificate. For information about how to upload CA certificate, see **NetMRI Security Settings**.
   - **Network View:** Select a network view that is associated with the scan interface of the Cisco API controller.
   - **User Name:** Enter the user name of the Cisco APIC.
   - **Password:** Enter the password of the Cisco APIC.
3. Click **Add** to save the Cisco APIC details into the table for later discovery or click **Add and Discover** to immediately begin the discovery process.

You can do the following in the **APIC** tab:

- **Edit:** You can modify information about the Cisco APIC you just added.
- **Delete:** Click this to remove Cisco APIC from the list.
- **Import:** Click this to import a CSV file containing Cisco APIC information. For information about syntax formats, see Discovery Import Formats.
- **Show/Hide Credentials:** Click this to display or hide the user name and password credentials of the Cisco API controller.
- **Discover Now:** Click this to start the discovery process.

### Running Network Discovery on Routed and Switched Networks

After you establish your scan interface's connection to their network, discovery automatically begins polling the IP addresses in the network view (based on discovery settings) and begins to report what it finds to the Discovery tables under **Network Explorer** → **Discovery**.

NetMRI automatically collects discovery data from pure L3 routing devices every 180 minutes. This setting cannot be changed.

Discovery identifies contacted devices by their IP address and hostname, and IP addresses are gathered under a few categories: **Classified, Reached** and **Identified**, which is the complete aggregate of all discovered IPs. **Classified** and **Reached** IPs are subsets of the **Identified** classification. These values appear in a simple bar graph at the bottom of the **Discovery** page.

**Note:** A device is considered an active device for management if NetMRI can poll and monitor the device using the SNMP protocol.

**Note:** Network polling settings can also be defined for managing a more or less continuous discovery process during NetMRI operation. Do this under **Settings** → **Collection and Groups** which provides a second group of important settings for governing automatic discovery behavior.

For all networks, NetMRI discovers and stores the following information:

- **Globally routable interface IP addresses;**
- **VRRP/HSRP virtual IP address (if applicable);**
- **Associated VLANs;**
- **BGP AS and neighbor adjacencies (if applicable);**
- **Cisco VoIP endpoint devices;**
- **GLBP virtual IP (if applicable);**
- **VRF configurations, including their respective private network information. NetMRI notifies the user through a System Health alert when it discovers VRF configurations; the alert advises you to assign the VRFs to a network view.**
- **IPv6 networks and subnet masks;**
- **IPv6 Link-local interface IP addresses.**

### Controlling Switched Network Discovery

You can manually control the frequency of discovery polling of switched Ethernet networks. To fully discover them, you must define these settings. NetMRI's Switch Port Manager feature governs how L2 and L2/L3 Ethernet switching devices are polled for discovery and data collection. To enable automatic polling through ARP for switched devices (network devices that belong to the Switching and Switch-Router device groups), do the following:

1. Go to **Settings** icon → **Setup** → **Collection and Groups** → **Switch Port Management** side tab.
2. Set the **Periodic Polling** time interval. This defines the ARP polling interval for repeated data collection. The default value is 1 Hour.
3. Go to the Advanced Settings page (Settings icon --> General Settings --> Advanced Settings --> Discovery group --> Poll ARP with SPM) and choose the True option. (The setting is set to False by default.)

Note: For more details on switch port management settings, see Global Switch Port Management Polling Settings.

Running Discovery on a Single Device

To refresh discovery for a single device, or force discovery for a single device, do the following:

In the Device Viewer --> Settings & Status --> Management Status, click Discover Now. A pop-up dialog appears, displaying the command-line and SNMP directives that NetMRI immediately sends to the selected device. NetMRI executes the processes required against the device to complete discovery. These include SNMP credential collection, SNMP data collection, device group assignment and CLI credential collection. Scroll through this listing to view specific details on what types of information are being obtained by NetMRI for the selected device. Some time may be required to finish the process.

To force a device to the top of the discovery queue: Click Discover Next (below the table).

To remove a device from NetMRI Management: Click Unmanage and confirm the operation. Unmanaged devices remain discovered, but the appliance will not collect data from them. NetMRI will not obtain details—such as vendor, model and operating system version—because SNMP access is required to complete those processes.

To delete the device from NetMRI's database, do the following:

1. Click Delete (below the table).
2. In the Delete dialog, select Exclude from discovery (this is optional; also see below).
3. Click Yes to confirm deletion.

Note: If the device continues to appear in collected data, NetMRI will re-list it unless you choose to exclude the device from discovery when it is deleted.

Vendor-Specific Requirements for Virtual Device Discovery

NetMRI discovers Cisco-based virtual device contexts through the Cisco command-line interface. Telnet and/or SSH access must be enabled on the Virtual Host, and the credentials for the contexts must be known to NetMRI.

NetMRI discoversJuniper-based virtual device contexts through SNMP. Juniper’s term for virtual routers/switches is Logical System. For uniformity, NetMRI labels all Juniper-based Logical Systems as Virtual Devices. SNMP must be enabled on the Juniper virtual host and access granted for the NetMRI appliance to all virtual devices/Logical Systems.

A Juniper command sequence illustrates how to enable the Juniper device's SNMP access using a community string

```
community @snmppub {
    authorization read-only;
    routing-instance M5VdcTest1/default {
        clients {
            0.0.0.0/0;
        }
    }
    routing-instance-access {
        access-list {
            *
        }
    }
}
```

In all cases, the Juniper Virtual Host (i.e. the device hosting the virtual instances) acts as a proxy to the virtual devices for all SNMP communication. Direct SNMP access to Juniper Virtual Devices is not permitted. This is largely transparent in NetMRI. If connectivity to the Virtual Host is lost, SNMP collection of the Virtual Devices is not possible and the VDCs will appear on the Devices Not Present page.

Both the virtual hosts and their virtual devices must be discovered by NetMRI as independent network devices before it will identify them as Virtual Hosts and Virtual Devices.

Note: All IP addresses of the virtual hosts and virtual devices must be in NetMRI's discovery IP ranges.
NetMRI supports indirect partial discovery of otherwise unreachable virtual device contexts. A minimal subset of information is gathered by NetMRI, consisting of the following:

- Device type
- Uptime
- Vendor
- Model

Cisco devices supporting CLI access through the physical host will also allow collection of the configuration files. This information is entered into the NetMRI database. Full discovery of any virtual device context requires SNMP access. On Cisco virtual devices for Cisco ASA, Pix, ACE load balancers and Nexus switches, SNMP access is available only to each virtual device context. As noted SNMP access to Juniper virtual device contexts is done indirectly through the SNMP activation on the virtual host, acting as a proxy for the VDCs.

Note: If virtual devices on a specific virtual host do not provide direct access through SNMP, you will see a warning message on the virtual device’s Device Viewer, noting that CLI interaction is the only supported communication mode.

Viewing and Managing Discovery Results

The Discovery tab (Network Explorer -> Discovery) provides detailed information about NetMRI’s discovery processes through a special drop-down menu. Use this tab and menu to do the following:

- View discovery and data collection processes in real time. IP addresses are listed as they are discovered from any source;
- View discovery milestones and status, which provide a context for fixing problems;
- Monitor IP address processing to gauge overall progress;
- Correlate device IP addresses with management IP addresses;
- Search all known IP addresses;
- View and control credential guessing queues. You can see where a device falls in the sequence, and prioritize it if desired;
- Tell NetMRI to immediately perform the full discovery process on a device. Results are displayed when received;
- Administer devices: view and change licensed/unlicensed/unmanaged status. “Unmanage” a discovered device, set the licensing status for a device, delete a device from the list, and other operations.

The following views are available via the Discovery drop-down menu:

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recent Activity</td>
<td>Lists all known IP addresses discovered by NetMRI</td>
</tr>
<tr>
<td>License Management</td>
<td>Provides data similar to Recent Activity, sorting the list according to priority in the algorithm for determining where a device fits in the device license scheme. This view helps determine why a given device is or isn't licensed, where it is on the list to change the NetMRI license (if necessary) or to adjust a setting so a given device is given license priority.</td>
</tr>
<tr>
<td>Problems</td>
<td>Provides data similar to Recent Activity, but filtered to devices reporting discovery errors.</td>
</tr>
<tr>
<td>Non-Detected IPs</td>
<td>Provides data similar to Recent Activity, but filtered to devices that NetMRI hasn't been able to communicate with.</td>
</tr>
<tr>
<td>SSH Queue, Telnet Queue and SNMP Queue</td>
<td>Shows whether a given device is in the processing queue for determining credentials. Data about each device in the queue includes time of the prior attempt, time the device is going to be attempted again, and status. SNMP discovery is the key to complete device discovery. Until a device has fully discovered SNMP credentials, data collection and analysis can't continue.</td>
</tr>
</tbody>
</table>

Note: Operations Center only: Data displayed in a view is limited to the Collector selected in the Filter by Collector field in the right side of the header.

Interpreting Discovery Table Data

The Recent Activity, License Management, Problems and Non-Detected IPs tables organize information in the following columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E (Existing Status)</td>
<td>The listed IP address exists in the network. All devices will receive this status to indicate where NetMRI first discovered the address.</td>
</tr>
<tr>
<td>P (Fingerprint Status)</td>
<td>If NetMRI is configured to use fingerprinting, device fingerprint status is listed in this column.</td>
</tr>
<tr>
<td>R (Reached Status)</td>
<td>Shows whether NetMRI has sent a packet to the device and received a reply, establishing that the device is reachable. Devices are typically tested for reachability through SNMP and the CLI, usually with an ICMP Ping operation.</td>
</tr>
<tr>
<td>S (SNMP Credentials Status)</td>
<td>Indicates status of the SNMP credential guessing process.</td>
</tr>
<tr>
<td>SC (SNMP Collection Status)</td>
<td>Shows status of SNMP data collection for the device. Success indicates that a device successfully allows data collection through SNMP. If this is not successful, check the S field to see whether the correct credential is given.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>CLI Credentials Status</td>
<td>Displays status of the CLI credential guessing process.</td>
</tr>
<tr>
<td>CC (Config Collection Status)</td>
<td>Indicates whether a device supports command-line connectivity and whether configuration collection is successful. If this is not successful, check the C field to see whether the correct credential is given.</td>
</tr>
<tr>
<td>G (Device Group Status)</td>
<td>Shows status of the device group generation process. Success indicates that a device has been assigned to at least one group.</td>
</tr>
<tr>
<td>DB (Discovery Blackout Status)</td>
<td>Indicates whether or not the selected device is in a Discovery Blackout period. Two states are possible: In Blackout and Not in Blackout.</td>
</tr>
<tr>
<td>CB (Change Blackout Status)</td>
<td>Indicates whether or not the selected device is in a Change Blackout period. Two states are possible: In Blackout and Not in Blackout.</td>
</tr>
<tr>
<td>Status</td>
<td>Licensed devices are listed as such. Unlicensed devices are non-network devices, or devices for which NetMRI license limits have been exceeded. Unmanaged devices are those which NetMRI will discover but not manage.</td>
</tr>
<tr>
<td>Type</td>
<td>Lists the device type as determined by NetMRI.</td>
</tr>
<tr>
<td>Last Timestamp</td>
<td>Date and time the data in the device records were updated, or verified as unchanged.</td>
</tr>
<tr>
<td>Last Action</td>
<td>The last action performed by NetMRI upon device after discovery takes place. An example: Device Groups: Successfully assigned to device groups indicates that the device was successfully discovered and added to a device group.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time when the device was last seen on the network; for example reading the IP address in the ARP table from a router.</td>
</tr>
<tr>
<td>First Seen</td>
<td>Date and time when the listed device was first detected by the NetMRI appliance.</td>
</tr>
</tbody>
</table>

You can pass the mouse over any E, P, R, S, SC, C, CC, and G icon in the table to display a tooltip explaining the OK, Error or Skipped messages for the icons. Each of the column categories provides a reason or explanation how a discovery phenomenon took place upon each device. Consider the E (Exists) columnn, for example. Possible explanations for why a device was found to exist in the network include the following:

- Exists: Device exists / Source: SNMP
- Exists: Device exists / Source: Net-SNMP
- Exists: Device exists / Source: CIDR Table
- Exists: Device exists / Source: CDP
- Exists: Device exists / Source: Route Table
- Exists: Device exists / Source: ARP Table
- Exists: Device exists / Source: Path
- Exists: Device exists / Source: CDP Table
- Exists: Device exists / Source: LLDP
- Exists: Device exists / Source: HSRP
- Exists: Device exists / Source: VRRP

- Exists: Device exists / Source: NIOS
- Exists: Device exists / Source: NetMRI
- Exists: Device exists / Source: Seed
- Exists: Device exists / Source: Wireless Controller
- Exists: Device exists / Source: IP Phone
- Exists: Device exists / Source: Call Server
- Exists: Device exists / Source: VPN Table
- Exists: Device exists / Source: Wireless AP
- Exists: Device exists / Source: Subnet Scan
- Exists: Device exists / Source: Discover Now

Three status icons appear in the Recent Activity, License Management, Problems and Non-Detected IPs tables:

- **Passed**: The device passed the process.
- **Failed**: The device failed the process.
- **Not Applicable**: The process is not applicable to the device.

Some guidelines for the Recent Activity, License Management, Problems and Non-Detected IPs tables:

- Hover over a status icon to see the action (with timestamp) that generated the status.
- A pink row indicates that there is at least one failed process for the device.
- Click the arrow to the left of the IP address to list other IP addresses on the device, and the corresponding interface to which it is assigned (if known).

The area at the bottom of the Discovery tab provides a progress bar and summary data:

- **Network Devices**: number of devices discovered.
- **Licensed Devices**: number of licensed devices discovered.
- **IPs Classified**: number of IP addresses the appliance has fully discovered with SNMP collection and assigned to a device group.
- **IPs Reached**: number of IP addresses NetMRI has touched.
- **IPs Identified**: number of IP addresses known to exist on the network.
Performing Discovery Operations on Multiple Devices

In the **Network Explorer** -> **Discovery** table, NetMRI displays data on multiple pages when the number of items to be displayed exceeds the maximum number of items that can appear on one page. Use the navigational buttons at the bottom of the table to page through the display.

You can select multiple rows in a table. For example, in a Windows browser, you can do the following to select multiple rows:

- Click check boxes adjacent to each other to select contiguous rows.
- Click check boxes for any row, separated by any number of rows, to select multiple non-contiguous rows.
- Click the check box in the Select column of the table header to select all rows on a page, as shown in the figure.

When you click the check box in the Select column of the table header, in a table that contains multiple pages, only the rows on the current page are selected. All selected rows are greyed out on the table page, denoting their selection. After you select all rows on a page, you can deselect a specific row by clearing the check box for the row; the remaining table rows remain selected.

For Discovery tasks, you can do the following:

- Click **Discover Next** to execute Discovery protocols on the selected devices. A prompt appears: **Are you sure you want to discover the selected 23 device(s) next?**
- Click **License** to change the licensing status of all selected devices (for information, see **NetMRI Licensing**);
- Click **Unmanage** to remove the selected devices from management by NetMRI. A prompt appears: **Are you sure you want to stop managing the selected xx devices?** The chosen devices will be removed from their licensing and NetMRI will add the license allocation to its availability pool.

Viewing Device Discovery Status and Re-Discovering a Device

To view discovery status for any device, open the Device Viewer by navigating to **Network Explorer** -> **Discovery** and clicking a device link, or **Device Viewer** -> **Settings & Status** -> **Management Status**. You will see the Management Status for the device. This is an important block of information that immediately describes the effectiveness of communications to the device by NetMRI.

This page provides a subset of the same information listed on the **Discovery** page, showing the E (Exists) P (Port Scanned), R (Reached), S (SNMP), SC (SNMP Collection), C (Config Credential) CC (Config Collection) and G (Groups) data results for a single device, each with their respective explanation.

The **Exists** field indicates the listed device has been successfully discovered by the network. The **R** field stands for Reached. A device can be discovered by any method but not necessarily be reachable. Devices are typically tested for reachability through SNMP and the CLI, usually with an ICMP Ping operation. **S** and **SC** are the status indicators for SNMP Credentials and SNMP Collection, respectively. Corresponding **C** (CLI Credentials) and **CC** (Config Collection) indicators also show whether a device supports command-line connectivity and whether configuration collection is successful. Finally, **G** indicates whether NetMRI successfully assigns the device to a device group.

At times, a device may need a discovery refresh because of significant configuration changes or because it has just been installed. You can choose to run discovery against any individual device at any time.

- Click **Discover Next** to set the device to be the first one discovered in the device group’s next discover cycle.
- Click **Discover Now** to immediately re-discover the device listed in the Device Viewer.
- Click **License** to change the licensing status of the current device. The default state for device licensing is **Automatic** (NetMRI uses global licensing guidelines to determine whether a device should occupy a license entitlement). For switches and firewall devices, you can choose to explicitly license the device by selecting **Licensed** and checking the check box for either category.
- If the device is licensed and you wish to revoke it, or override the global licensing behavior, select **Unlicensed**.
- To revoke the current device’s Managed status, click **Unmanage**. The device will be removed from managed status under NetMRI and automatically be Excluded from management. The device will continue to be discovered, however.
- To remove the device completely from the NetMRI database, click **Delete**.
- You can export the device management data to an Excel-compatible .CSV spreadsheet. To do so, click **Export**. NetMRI creates the file and places it in your browser’s Downloads directory.

Overriding Device Names and Types in the Device Viewer

During device discovery, NetMRI determines the Management IP address, device name and device type and displays those values in several locations in the UI, including the **Network Explorer** -> **Discovery** page and the Config Explorer (Configuration Management -> **Config Explorer**). Once those values are discovered, should any of those values change at some point in network operation, NetMRI detects those changes and modify the appropriate values in its database.

If the system admin changes the **Name** or **Type** of device in the Device Viewer’s General Settings page (**Device Viewer** -> **Settings & Status** -> **General Settings**), re-discovery of that device’s settings will no longer be active. For more information, see **Viewing and Changing General Settings for a Device**.

To revert to auto-discovery of changes to that device's identifying information in the network, you need to delete the device from the **Discovered Devices** list in the **Network Explorer** -> **Discovery** tab. The device is removed from the table. You will need to wait for NetMRI to re-discover the device on the network, and then refresh or re-open the **Network Explorer** -> **Discovery** tab to view the updated information. Click the device group name in the right pane if you need to locate the updated device in its expected group.

**Note:** For more information about Device Viewer functions, see **Inspecting Devices in the Network** and its subsections.