FAQs and Other Information

Consult the following topics to address frequently asked questions about NetMRI operation, using the Cisco Discovery Service utility software, using the NetMRI AutoUpdate feature, viewing hardware status messages from NetMRI appliances, changing the banner logo and other information.

**Note:** For information on NetMRI licensing, including network device licensing, see NetMRI Licensing.

Frequently Asked Questions

User Interface

* Q. How can I do more sophisticated searching and filtering in tables?
  * A. Both the Quick Search field and the Filters dialog enable you to use regular expression syntax to specify search targets. Any characters enclosed between forward slashes (/*/) are treated as a regular expression.

* Q. I returned to a page and data that was there has disappeared. What's going on?
  * A. While you were away from that page, you may have changed the date or period in another page, or you may have constrained the data to a specific device group. Check the device group/date/period at the left end of the green header to see whether that's what you want. To change the device group, or to show data for the entire network, click the corresponding row in the Select Device Groups panel. To change the date or period, see Setting the Date and Period.

* Q. I have an admin account in NetMRI but I can't get my CLI connections to work - my Telnet and SSH connections time out.
  * A. Your admin account does not have CLI credentials enabled. To fix this, open Settings, go to User Admin -> Users, and click the Edit icon for the admin account. Click the CLI Credentials tab. Then, enable the User CLI Credentials Enabled check box, and enter the user name and password, with password confirmation. If you need an Enable password for accessing network devices through the CLI, enter that value and confirm that as well. Click Save and start a new terminal session to the NetMRI appliance.

Device Groups

* Q. I added a new device to my network. Where do I find that device in NetMRI?
  * A. NetMRI checks for new devices every 15 minutes. A new device is assigned to a device group based on the group membership criteria where the group is defined. If NetMRI can't assign a device to a defined group, it places it in the UNKNOWN or NAME-ONLY group.

* Q. Why do device group counts in the Select Device Groups panel appear to be out of sync with the counts at Network Explorer -> Inventory -> Devices?
  * A. Device group membership counts are recalculated every 15 minutes. When the appliance is discovering many new devices, you might see a different count until you refresh your browser following that recalculation. If no new devices are being added to the network, you are unlikely to see a difference.

Discovery

* Q. How can I remove a device from NetMRI?
  * A. A network device is removed if it is in the included CIDR blocks and hasn't been accessed by NetMRI in a 7-day period and it hasn't shown up anywhere on the network based on data collected in the past day. This 7-day period is adjusted with the Device Expiration Days setting in the Settings icon -> General Settings -> Advanced Settings page. Data sources checked to see if the device exists include ARP, routing, CDP and any /32 or /128 CIDR blocks. A discovery diagnostic of a device will show which devices are reporting this device in those tables for help in troubleshooting problems. Any device included in a CIDR block is removed after one day. Any non-network device, such as a PC, is removed from NetMRI if it isn't seen in any collected data in the previous 24 hour period.

* Q. What kinds of IPv6 networks do I need to add to my seed routers or discovery ranges?
  * IPv6 standards define several new types of network prefixes, because the address value is longer and is formatted differently. Unique local IPv6 Unicast network prefixes begin with the designation FC00:/7. (These values are similar to the familiar 10.x.x.x, 172.16.x.x and 192.168.x.x IP prefixes.) Globally routable values begin with the 2000:/ or 2001:/ prefixes but are not used as examples in this document because of the need to use private address spaces in documentation, to avoid possible conflicts with live networks.

NetMRI discovery of IPv6 networks can make use of Hints and CIDR blocks for discovery. Do not use link-local or multicast addresses as a device hint, for a range, or a seed router. Unique local IPv6 unicast values are acceptable. As with the 10.x.x.x and other private IPv4 values, they are not globally routable and are safe for use in the local network. Also see the section Configuring Network Discovery Settings for more information.

* Q. Some devices in my network only support SNMPv2c. Can I use SNMPv2c credentials as the default for discovery?
  * A. Yes. See Choosing SNMP Protocol Preferences for more details.

* Q. Can I define SNMPv3 credentials with both types of secret keys to conform to my organization's security policies?
  * A. Yes. You can define SNMPv3 credentials with separate authentication and privacy key values. See SNMPv3 Credentials for Discovery and Management for more details.

Switch Port Management
Q. I've installed a Switch Port license into NetMRI but none of my Ethernet switches are showing up in the Switch Port Management device tables. The switches appear in my Switch and Switch-Router device groups, but I get a "Polling Started for 0 Devices" message whenever I try to start polling the switches.
A. You must add the switches in the device group(s) to the SPM license, whether it's an evaluation license or a paid-for SPM license. Installing the license does not automatically add the contents of the Switch and Switch-Router device groups to the licensed device count.

Configuration Management

Q. What does the Get Config button in the Config Explorer actually do?
A. The Get Config button schedules back-end processes to retrieve the current configuration files from the selected device. If there is no difference from the currently listed configuration files, then a new instance is not created in the configuration files list. Each listed instance implies a difference, and the timestamp defines when the file was first known to be changed. To determine when the file was last checked, open the "Current" "Running" configuration file. In the resulting window, the Last Update timestamp (in the header) indicates the last time checked.

User Administration

Q. Why can't I specify device groups for the SysAdmin role?
A. The SysAdmin role is not intended as an operator (i.e., restricted to certain network domains), but rather a system administrator with authority throughout the NetMRI appliance. For security and safety, you should only use this role when performing actions that require it.

Security

Q. Can I disable HTTP access to NetMRI?
A. By default, NetMRI disables the HTTP protocol and you must use HTTPS for browser access. Go to Settings icon -> General Settings -> Security – NetMRI HTTPS Settings to check settings.
Q. What well-known ports does NetMRI use?
A. Outbound ports:
- 22/ssh TCP for configuration collection
- 23/telnet TCP for configuration collection
- 25/smtp TCP for notifications
- 161/snmp UDP for SNMP collection
- 162/snmptrap UDP for notifications
- 514/syslog UDP for Syslog notifications
- 1433 TCP TCP for CDR collection (when the IP telephony module is licensed).
- any TCP or UDP port defined by Settings icon -> Setup section -> Port List and port scanning is enabled.
A. Inbound ports:
- 22/ssh TCP for administrative shell access
- 80/http TCP for non-secured GUI access
- 443/https TCP or secured GUI access
- 514/syslog UDP for change detection

System Security

The NetMRI appliance is configured to prevent all non-essential servers and ports, and all user accounts are disabled except for the admin account, which is used for administrative purposes (see below for more information).

Symptom: Unable to connect to Infoblox Technical Support server.

- Use the NetMRI ping/traceroute tool via the browser interface (Tools -> Device -> Ping/Traceroute), or the ping command via the NetMRI Administrative Shell, to verify that NetMRI can reach any server on the Internet.
- Use the NetMRI ping/traceroute tool via the browser interface, or the traceroute command via the Administrative Shell, to verify that NetMRI can reach techdata.infoblox.com on the Internet.
- Verify that your firewall rules allow NetMRI to make an outbound SSH connection (tcp port 22) to techdata.infoblox.com.

Technical Support monitors the CERT advisories for all components used in the appliance and evaluates all appropriate reports with regard to their usage in NetMRI. If a serious vulnerability is discovered, a custom patch is developed and provided to all existing customers via the NetMRI User Mailing list.

Network Connections

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>Administrative Shell</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>Secure Graphical User Interface</td>
</tr>
</tbody>
</table>
The SSH port can be accessed using the administrator password specified by the operator during configuration. All services on the SSH port are provided through the OpenSSH v3.5p1 public domain server. The only commands that can be executed via the SSH port are those provided by the NetMRI Administrative Shell, and the user can access only a restricted directory on the server.

All other ports are supported by a Java-based application server that is inherently resilient to buffer overflow attacks and other common network-based attacks. The HTTP, HTTPS and SNMP ports support standard processing for those protocols. The HTTP and HTTPS ports can be accessed only by authorized users using a valid password, as specified by the administrator.

Access Control Lists

NetMRI supports an Access Control List (ACL) via the NetMRI Administrator Shell that allows the operator to specify one or more CIDR blocks to restrict access to all the non-SNMP ports supported by the appliance. When combined with the existing authentication mechanisms, the ACL effectively safeguards the appliance against unauthorized access.

Protocol Configuration

NetMRI allows system administrators to configure the HTTP, HTTPS, SNMP and SSH protocols used to connect to the appliance via the Console GUI and Admin Shell, and the protocols used by the appliance to connect to network devices when collecting data. Protocol configurations can be defined at the Settings icon → General Settings → Security page, or by executing the configure command in the NetMRI Administrative Shell.

General Settings Section

The General Settings section (Settings icon → General Settings group) provides access to server statistics and a variety of server settings. Pages in this section enable the following tasks:

- Set and reset any of numerous advanced settings (for information, see NetMRI Advanced Settings);
- Configure authentication service settings (for information, see Defining Authentication Services);
- Configure NetMRI to automatically check for software updates, and optionally install updates (see the Auto Update topic);
- Substitute your own banner logo (for information, see Replacing a Banner Logo);
- Create custom fields for manually recording any device information (for information, see Defining and Using Custom Fields);
- Shut down the server (for information, see Shutting Down the Server);
- Define routing distance settings (for information, see Defining Path Analysis Settings);
- Manage NetMRI server security (for information, see NetMRI Security Settings);
- Review NetMRI patches and updates.

NetMRI Advanced Settings

NetMRI Advanced Settings (located in Settings icon → General Settings → Advanced Settings) provides a multi-page grouping of configuration settings for many NetMRI features. Advanced Settings are designed so NetMRI users can run a fully functioning system without changing any defaults settings in this category.

To modify items in Advanced Settings, click the Action icon for any setting and choose Edit. To reset the Advanced Setting to its defaults, choose Reset.

- **Job Self Approval** setting allows or disables the ability of job authors to approve the jobs they create. **Job Requires User Credentials** defines when job script execution needs command-line credentials for the devices against which the job runs.
- **Concurrent Jobs**, the number of maximum concurrent Config Management jobs, defaults at 20 and is available only on NT-4000 NetMRI platforms.
| **Data Collection** | A significant group of settings to determine how NetMRI reacts to large data sets. **ARP Aggregate Limit** determines the largest ARP table collectible by NetMRI. The **Route Limit** setting defines the threshold for NetMRI to switch to CLI data collection for collection of large routing tables (typically but not exclusively compiled by BGP4 routers with connections to the external Internet). Routing table collection can also be enabled or disabled. **CatOS Configuration Command** allows you to specify `show config` or `show config all` when collecting switch configurations. Two more settings (**Interface Live Viewer Polling Interval** and **Interface Live Viewer Poller Limit**) define the polling interval in seconds, and limit the number of concurrent polling instances triggered by Interface Live Viewer. Another setting, (**Enter Enable Mode**, default On) determines whether the Configuration Management and Job Management systems in NetMRI should enter the Enable mode on managed devices before entering device commands; **Extended Device Discovery** is a Cisco Discovery Service setting that allows some extended levels of SNMP data to be gathered by CDS from Cisco devices. Off by default, this setting potentially improves download times when the CDS user requests the data collection for a report. For virtual device contexts data collection, enable the **Collect Virtual Device Context (VDC) Data** setting. (For more information, see **Understanding Virtual Device Contexts**.) An SNMP-related setting, **SNMPv1 Data Collection Fallback**, enables or disables the use of SNMPv1 if the device does not support SNMPv2c for any reason. |
| **Discovery** | Several Discovery settings that affect how devices are collected in the NetMRI database. **Device Expiration in Days** governs the ‘stickiness’ of device records in the database. **Default Naming Priority** allows setting of DNS or SNMP as the primary protocol for naming devices when added to the database. **Ping Sweep Frequency** determines the elapsed time period, in hours, between ping sweeps within IP address ranges (default value 24). Enabling the **Discovery Ignore Duplicate MACs** setting forces NetMRI to delete pre-existing records for a switch identified by a specific MAC address should the device change its assigned IP. Discovery **Truncate IP History** prevents IPs that aren’t assigned to interfaces from being assigned in NetMRI to particular devices, which preserves the functions of the Cisco `ips alias` command where needed. The **SNMPv1/SNMPv2c Discovery Version** setting allows a choice between three options: Use **SNMPv1 for credential discovery**; Use **SNMPv2c for credential discovery**; or Use both **SNMPv2c and SNMPv1 for credential discovery**. See **Choosing SNMP Protocol Preferences** for related information. |
| **NIOS Administration** | Define the NIOS administrator login password, used primarily for Automation Change Management applications (see **Automation Change Manager (ACM)** and associated topics for more details). |
| **Notification** | Choose the Syslog facility used for tagging Syslog notifications. |
| **Reports** | Define the number of concurrent reports allowed to run on the NetMRI appliance (**Concurrent Running Reports**). The default is 2 and should be retained in most cases. |
| **Security** | Provides a single setting for visually hiding passwords as they are entered on the login screen (**Hide Password Fields**). |
| **Switch Port Management** | Settings to **Convert Free Ports to Available** ports on a switch, following a certain number of days after interfaces are disconnected from an end device; and the **ARP Cache Refresh Period**, which causes NetMRI to issue pings to discovered devices before collecting switch port information. This can have a beneficial effect on the availability of devices in Cisco Catalyst switch forwarding tables when NetMRI does its periodic query of those forwarding tables. The **ARP Cache Refresh Ignore Discovery Ranges** Advanced Setting helps to optimize the discovery of end hosts by disabling pinging of such devices outside of specified discovery ranges. By default, this feature is set to False, which means that devices outside the configured discovery ranges will be pinged by NetMRI. Set this value to True if deemed necessary. Switch Port Management can use the new Advanced Setting **ARP Cache Refresh Device History** to enable pinging of devices from older tables compiled from previous polling days, prior to the most recently compiled End Host data tables. The default value is 14 days and the minimum value is one day. This feature helps rediscover devices that move off the managed network and eventually rejoin, such as laptops returning from travel. |
| **System** | Provides a pair of helpful settings for NIOS IPAM Sync functionality (**IPAM Sync Retries** and **IPAM Sync Retry Interval**) and a pair of JVM server settings that default to zero and should only be modified if the NetMRI appliance is a VM running under VMware. Disabling by default, the **Quick Maintenance Enabled** allows archiving of the NetMRI data set without reboots or restarts. Quick Maintenance disables collection during archiving but allows access to the UI and the API. See **Executing NIOS IPAM Sync** for more information. |
| **User Administration** | User Administration settings, found and 5 of Advanced Settings, to determine the required length of passwords, whether a password should be more complex, the number of permitted login failures before lockout, and more (see **Advanced User Administration Settings** for details). |
Checking Hardware Status Messages

The Hardware Status page (Settings icon → Notifications section → Hardware Status page) provides status information about hardware components in the NetMRI NT-4000 appliance, including component failures and general messages about the health and operation of elements such as the fan assemblies, LCD screen, removable hard disks, power supplies, events that are reported when the case is open, overall System Health messages and others.

The Hardware Status page does not apply to NetMRI virtual appliances or to NetMRI 1102-A 1U or NT-1400 appliances. Also consult the Infoblox Installati on Guide For The NetMRI NT-4000 Appliance for more information about the NT-4000 system.

Auto Update

NetMRI can be configured to periodically check for minor software updates, and can optionally automatically download and install those updates. Software update notifications appear as the issue "NetMRI Update Available," and users are notified of automatic software installations through a system message, visible in the Settings icon → Notifications → System Messages page, to notify users of Applied or Available updates.

NetMRI must be able to reach the server techdata.infoblox.com using TCP port 22.

To configure automatic updates, do the following:

1. Select the Auto Update Setting option:
   - Disabled: Do not check for updates. If you select this option, go to step 4. Notify Only: Check for updates.
   - Automatic: Check for updates, and if an update is available, download and install it.
2. Select the Frequency for notification or automatic updates.
3. Select the Hour to Start and Minute to Start.
4. Click the Update button.

Replacing a Banner Logo

Use the Banner Logo page (Settings icon → General Settings → Banner Logo) to display your logo in reports generated by NetMRI. Your logo will replace the default logo that is provided with NetMRI.

To replace the default logo with your logo, do the following:

1. Click Browse, then locate and select the logo file.
2. The file can be any common image format, such as JPEG, GIF, PNG, etc. The ideal image size is 220 x 60 pixels (an image that is not this size is automatically resized to those dimensions).
3. Click Update.

To restore use of the default logo: Click Reset.

Defining Path Analysis Settings

Note: The NetMRI appliance uses the Cisco-defined defaults for Routing Distance values.

Routing Administrative Distance is a feature originally used by Cisco routing to select the "best" path when two or more paths exist, using two or more protocols that can forward packets to a given destination. Because NetMRI is not a router, Routing Distance provides for two specific use cases:

- Determine the preferred protocol used for the NetMRI appliance for receiving and transmitting packets. For example, an appliance might reside on a network that runs both OSPF and RIP. The Cisco default administrative distance for OSPF is 110, and the administrative distance default for RIP is 120, making OSPF the 'preferred' routing protocol for forwarding network traffic. The lower a Distance value, the more preferred or 'reliable' the system considers the protocol;
- For Topology, Administrative Distance has effects on how Path Analysis conducts calculations between any two points in the network. Under Path Analysis, a path could use two or more dynamic routing protocols (BGP4 and OSPF, for example). The Routing Distance settings determine how NetMRI reports its analyzed paths, indicating the protocol that takes precedence in the analyzed path.

Under Routing Distance, the values used by NetMRI reflect the Cisco-defined default values. You can change these values for the local NetMRI appliance or Operations Center system. Changing these values only has an effect on the local NetMRI appliance's calculations for Path Analysis if the appliance is one of the endpoints, or is an intermediate node in a path being calculated.

1. Go to Settings → General Settings → Path Analysis.
   - The Routing Distance column provides the editable value.
   - Entering a value of 255 as the Admin Distance will cause the protocol to be ignored by the device and not use the protocol.

The Routing Distance feature also may be useful for Operations Centers and their associated Collectors.
Specifying Path Calculations

In a large network, more than one possible path may exist between two devices. You can control the number of path calculations performed for the same Source/Destination pair. The default number of simultaneous path calculations is 2, with a maximum value of 10. Go to Settings icon → General Settings → Path Analysis and edit the Number of Calculated Paths setting. Avoid setting this value to too high a number, as multiple active path calculations can affect performance.

Shutting down the server

Use the Shutdown Server page (Settings icon → General Settings → Shutdown Server) to stop or restart NetMRI. NetMRI includes embedded database and file systems to manage the vast amount of information it gathers from the network. Although the database and file systems are designed to be resilient to failures, it is always best to shut the appliance down gracefully whenever possible to avoid data corruption.

Note: Failure to properly shut down NetMRI may result in corruption of one or more database tables. Although NetMRI automatically attempts to repair tables when restarted, such repairs may not always work, resulting in a loss of data or functionality. In certain cases, you may need to restore the database or reset to factory defaults.

To shutdown the server from the browser interface, do the following:

1. Select a shutdown option:
   -Restart Server. This option will shut down NetMRI and then immediately restart it.
   -Power Down Server. Use this option for a planned power outage or to move NetMRI to another location.
   -Disable Collection, Then Power Down Server. Use this method when removing NetMRI from a network, possibly for further review of analysis information. This option will likely be used most frequently by consulting organizations who use NetMRI on a network for a few days, then take it back to their office to prepare a customer report.
   -Save Network Database and Force Re-Configuration On Server Startup. Use this method when NetMRI is being moved to a new network or to a different section of an existing network. A consultant could also use this mode when moving NetMRI between different sites. A campus or enterprise customer can use this mode when moving NetMRI to different logical sections of a single network. The next time NetMRI is booted, the setup wizard will run, allowing you to configure it for a new network or a previously existing network. If a previously existing network is selected during the startup process, the system loads the archived copy of the database for that network, allowing NetMRI to pick up where it left off or allowing you to analyze the old data.

2. Click OK.

You can also shut down the server from the Administrative Shell. the appliance is configured for separate analysis and management operation, check its rear panel. For separate operation, the SCAN port is connected to the production network for analysis, and the MGMT port is connected to the management network for system administration. If the appliance is connected to only one network, instructions in this section are not necessary.

1. Go to Settings icon → General Settings section → Shutdown Server.
2. Type the CIDR-format Address (using syntax A.B.C.D/NN), type the Gateway IP address, then click Add. To delete a static route: Click the Delete button for any static route listed in the Static Route List on the page.

NetMRI Update History

The Update History page (Settings icon → General Settings → Update History) lists NetMRI patches and upgrades that have been installed. Each action is time-stamped. If an installation failed, it is shown in red, with the failure status code.

File Transfer Operations

Occasionally, software update files or database archive files must be transferred to or from NetMRI. NetMRI supports two methods for transferring files:

- File transfer between NetMRI and an external workstation or server using the SCP protocol.
- File transfer between NetMRI and an external server from the Administrative Shell using the SCP or FTP protocol.

Although NetMRI allows the FTP client to be used for transferring files from within the Administrative Shell, NetMRI instances of any kind do not allow external FTP clients to send or receive files directly into the system. No FTP server is provided on NetMRI appliances or VMs.

Client Workstation File Transfer Using WinSCP

The Windows Secure Copy (WinSCP) utility is a Windows-based tool with a graphical user interface that allows you to copy files to/from NetMRI using a drag-and-drop approach. WinSCP is available from http://winscp.net/eng/index.php and other public domain web sites. Follow the directions that come with the utility to install it on a Windows-based PC. Then

1. Log in to the Administrative Shell by specifying the DNS name (or IP Address), a username of admin and the admin account’s password.
2. WinSCP will display the contents of the Backup directory.
3. Transfer files between the source directory and NetMRI by dragging and dropping.
Client Workstation File Transfer Using FTP and SCP

The method for starting the SCP client will depend on the operating system. Examples below are based on Unix. All command line inputs to the SCP client are case-sensitive.

The Secure Copy (scp) utility is a command line tool that can be used to download or upload files. It runs on most major operating systems and can be obtained from http://www.openssh.org. Only the **scp client** utility is needed on the storage device, not the **scp server** daemon. Follow the directions that come with the utility to install it on the storage device where the files are stored.

Exporting using SCP

1. Log in to the storage device that will receive the exported file, and navigate to the directory where it will be stored.
2. At the prompt, enter this command:
   ```bash
cp "admin@<NetMRI>:Backup/*"
   ```
   including the double-quotes and the trailing space and period, but replacing `<NetMRI>` with the DNS name or IP address of the NetMRI machine that has the file to be downloaded.
3. The first time you access NetMRI from a given storage device, you will be prompted by SCP to verify the authenticity of the instance. Answer `yes` to continue the download. (Once authenticity has been established on the storage device, this question will no longer be asked when accessing NetMRI from the same storage device using the same login.)
4. After the connection authenticity has been established, SCP will prompt for the `admin` password. Enter the same password used to access the NetMRI admin account via the web interface.
5. After accepting the password, SCP will copy the file from NetMRI to the storage device.

Importing using SCP

Use SCP to download files:

1. Log in to the storage device that holds the file to be imported, and navigate to the directory where it is stored.
2. At the prompt, enter this command:
   ```bash
cp <importfile> "admin@<NetMRI>:Backup"
   ```
   including the double-quotes, but replacing `<NetMRI>` with the DNS name or IP address of the NetMRI machine, and replacing `<importfile>` with the name of the file to be imported.
3. After the connection authenticity has been established, SCP will prompt for the `admin` password. Enter the same password used to access the NetMRI admin account via the web interface.
4. After accepting the password, SCP will copy the file from the storage device to NetMRI.

External server import/export using FTP

The NetMRI Administrative Shell supports the use of the FTP client within the shell itself to import/export files from and to an external server. Thus, instead of using your client application to access the NetMRI server, you can use the NetMRI client application to access other servers, such as the Infoblox Support FTP server.

1. Log in to the Administrative Shell using an SSH application.
2. Execute this command:
   ```bash
def <servername>
   ```
   where `<servername>` is the name of the FTP server.

The **Settings** window organizes configuration options in the following sections:

**User Administration section**: create and manage user accounts and roles, and view the audit log.

Sending Technical Support Bundles to Infoblox

To obtain and send technical data from any NetMRI appliance for troubleshooting purposes, do the following:

1. Click the Actions icon and choose **Send Support Bundle**.
   **– Or –**
2. Go to Settings icon -> **Database Settings** -> **Send Support Bundle**.
3. Choose a Transfer Mode: Download to Client Workstation or Send to Infoblox Support Site.
4. Click, CTRL+click or SHIFT+click to select one or more **Data Categories**. Sending technical data requires at least one category selection. Data categories include the following:
   - **Discovery Stats**: Logs documenting events related to device discovery, network path collection, ping sweep results, and discovered device support information;
   - **SNMP/CLI Logs**: Collections of SNMP and CLI data collection event logs;
   - **Config Logs**: Device configurations, downloaded from the devices that NetMRI is managing;
   - **Standard Logs**: Event log data for all server protocols and tasks used by NetMRI;
   - **Visualization Logs**: NetMRI GUI processing events;
   - **System Health Logs**: Event log journals directly related to System Health alerts.
5. Click **Start** and confirm the operation. Depending on the amount of requested data, a few minutes may be required to generate and download the bundle.