Viewing Discovered Devices and their Properties

Note: For information about unmanaged devices and managed devices and what their respective status means, see Converting Unmanaged Devices to Managed Devices. You can also use the “Unmanaged devices and networks” filter in global search to locate all the unmanaged devices and networks discovered through discovery. For more information, see Using Global Search.

After discovery begins executing on the network, Grid Manager provides a Devices page under Data Management for a complete list of every device that discovery finds, and lists all unmanaged and managed devices. Starting here, you can explore a substantial body of information about the complete list of discovered and managed devices, and drill down to specific information about every discovered and managed device. Listed devices inhabit one of three states in the Devices page:

- Devices that appear with an empty value in the Managed column are devices that are discovered, but are not recognized by IPAM, are not part of an IPAM network, and hence cannot be changed to managed status in Grid Manager. These discovered devices cannot be changed to managed status, but you can perform actions such as activating and deactivating ports, executing Discover Now on the device, view their list of connected networks, and other actions. Avoid changing the state of ports or taking other actions on a discovered device, unless the action is verified by an administrator.

- Devices shown in yellow table rows are unmanaged devices, but are recognized by IPAM and can be converted to managed status. Yellow rows appear with a value of No in the Managed column. You can convert devices in table rows to managed objects under IPAM (host, fixed address, A record or PTR record);

- Devices shown in light grey table rows are managed devices, with a value of Yes in the Managed column.

Viewing the Complete List of Discovered Devices

The Data Management tab -> Devices tab provides a complete view of all discovered devices discovered by Network Insight. The list includes routers, switches, firewalls and other security devices, wireless APs, end hosts and servers in end-host networks. Use NIOS standard filtering to narrow down the status table to the devices or values you want to examine.

In the viewer, click the Action icon 📊 for any table row to view the following:

- Click ShowIPAddress to open the IPAM status page to view records information for the Router IP address, and information such as any IPAM/DHCP objects associated with the IP address (RelatedObjects) and its recent history in Grid Manager (AuditHistory).

- Click Interfaces to display the complete table of interfaces associated with the network device.

- Click IPAM Networks and choose any network prefix in the list. The IP Map page appears for the chosen network for which the device is a part.

- Click Edit to open the device editor, to change settings for interfaces on the selected device; apply extensible attributes, or apply administrative permissions for Grid Manager admin access to a device.

- Choose DiscoverNow to apply discovery to a listed device to detect configuration changes, status changes and other device information.

- Where applicable, choose Convert to change the status of an unmanaged device to managed status under Grid Manager. (For more information, see Converting Unmanaged Networks under IPAM to Managed Status.)

- Click Device Details to view a short list of key information about the selected device.

- Click Device Support to verify data collection activities in the following tabs:

  - **Data Collection**: You can view the timestamp at which the most recent collection from various data sources was completed. The sources from which device support information is collected are listed under the Data Source column, and it includes the device’s routing table (ipRouteTable), environment monitoring (DeviceEnvMon), and numerous other data sources as applicable to the specific device type. It displays the following information for each discovered device:
    - **Data Source**: The sources from which the device support information was collected.
    - **End Time**: The most recent timestamp of the data collected by the discovery member.

- **Device Support tab**: Lists various types of information support for collection on the current device. You can view the following details for each discovered device:

  - **Function**: Data function that can be collected by Network Insight. The value can be Device Vendor, Device Model, Device Version, VLANs, Forwarding, VRFS, Inventory, and Security Control.

  - **Supported**: Indicates whether this data function is supported for the selected device. The value can be Yes or No. If it is No, Network Insight will not attempt to gather the data. For instance, for a Cisco router, Network Insight does not attempt to gather VLAN information, so a No value will be displayed in the Supported column.

  - **Available**: Reflects whether the data has actually been collected. The value can be Yes or No. A value of Yes for Supported and No for Available indicates a discovery misconfiguration or could possibly require an adjustment to the Device Support Bundle (DSB) for that particular device model.

  - **Value**: Displays the value collected for the Device Vendor, Device Model, and Device Version data functions. Displays Last Collected time for the VLANs, Forwarding, VRFS, Inventory, and Security Control data functions.

- Click ShowActiveUsers to view all the active users on the Active Directory domain for the selected device. For information, see Viewing Active Network Users.

Values listed in the Discovered Devices table include the following:

- **IP Address**: Detected the IP address (IPv4 or IPv6).
- **Name**: Detected name of the device. Each device name provides a link to the complete body of information associated with the device, arranged in five tabs: Interfaces, Networks, IP Addresses, Assets and Components. For more information, see the sections under Accessing Detailed Device Information.

- **Device Type**: The network device type: Router, Switch-Router, Firewall, NIOS (Infoblox appliance), vNIOS, SDN Controller, SDN Element, and others.

- **Model**: The model name as detected by the device during discovery.

- **Serial Number**: The serial number of the discovered device.
Click Discovery Status in the Toolbar to view the same list of network devices showing the discovery data set. You can sort the table by Name or IP address. Use Grid Manager-standard filtering to isolate device names, IP addresses or other values in which you are interested.

For each listed device, the Action icon provides the following options depending on the device type and its status:

- **Active**: Displays the Interfaces page for the chosen device. (For more information, see Viewing Networks Associated with Discovered Devices.)
- **Inactive**: Displays the Devices tab, selecting the Devices tab, and then click VRF Mapping from the Toolbar.
- **Pending**: Displays the Device Editor window; a direct link to the IP Address page; a direct link to the Interface page; a direct link to the Network Details tab.
- **Discovered**: Click the VRF Mapping dialog box. You can view all the active users on the Active Directory domain for the selected device. For more information, see Viewing Active Network Users.

### Viewing VRFs and Mapping Network Views

To view VRF instances (or VRFs) and map corresponding network views, do the following:

1. From the Data Management tab, select the Devices tab, and then click VRF Mapping from the Toolbar.
2. The VRF Mapping dialog appears and displays the following:
   - **VRF Name**: The name of the VRF on the hosting device, which typically contains the interface name and its VRF route distinguisher.
   - **Device Name**: The discovered name of the device that is hosting the VRF.
   - **Device IP Address**: The IP address of the managed VRF hosting device.
   - **Network View**: The network view that is associated with the VRF. You can click this field and select a different network view from the drop-down list.

You can do the following in this tab:

- To assign the same network view to multiple VRFs, select the check boxes of the VRFs, and then click the Edit icon. The VRF Mapping dialog displays the Edit VRF Network View panel. From the Network View drop-down list, select the network view you want to assign to all the selected VRFs, and then click Save. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
- You can use filters to narrow down the list. You can filter the list based on the VRF name, Device name, Device IP address, and network view. For more information, see Using Filters.
- You can sort the data in ascending or descending order by column.

**Note**: The appliance displays a warning message when there are discovered VRFs that are not mapped to network views. To ensure that discovered VRFs are mapped to network views, you can configure automatic VRF mapping, as described in Configuring Automatic VRF Mapping.