Discovering Devices and Networks

To start discovery on connected networks, complete the following:

1. Ensure that your appliances are licensed for discovery.
2. Add the needed seed routers to each Probe appliance, as described in Defining Seed Routers for Probe Members.
3. Add the necessary SNMPv1/v2 and SNMPv3 credentials at the Grid level and/or Member/Probe level. For information, see Configuring SNMPv1/v2 Credentials for Polling, Configuring SNMPv3 Properties, Defining Seed Routers for Probe Members, and Defining Seed Routers for Probe Members.
4. If necessary, add CLI Credentials, including device admin username/password tuples and Enable passwords, at the Grid level and/or Member/Probe level, as described in Configuring CLI Discovery Properties and Testing SNMP and CLI Credentials.
5. If necessary, enable the use of DHCP routers and servers as seeds to increase device discovery, as described in Configuring SNMP1/v2 Credentials for Polling.
6. If you have extensive end host Ethernet segments connected to Ethernet switches, enable switch port discovery, as described in Defining Seed Routers for Probe Members.

With these settings, the Probe appliances automatically begin discovering network infrastructure devices.

You can elect to immediately discover or schedule discovery of new objects that you create and enable under IPAM or DHCP. Objects that allow immediate discovery include the following:

- **IPv4 Fixed Address** (see Configuring IPv4 Fixed Addresses for the complete procedure).
  - You can Enable Immediate Discovery or Exclude from Network Discovery after creating the IPv4 fixed address, and override the SNMP credentials if necessary.
- **IPv6 Fixed Address** (see Configuring IPv6 Fixed Addresses for the complete procedure).
  - You can Enable Immediate Discovery or Exclude from Network Discovery after creating the fixed address, and override the SNMP credentials if necessary.
- **IPv4 Reservation** (see Configuring IPv4 Reservations for the complete procedure).
  - You can Enable Immediate Discovery or Exclude from Network Discovery after creating the IPv4 reservation, and override the SNMP credentials if necessary.
- **Host** (see Adding Host Records for the complete procedure).
  - You can Enable Immediate Discovery or Exclude from Network Discovery after creating the host, and override the SNMP credentials if necessary.
- **IPv4 Network** (see Configuring IPv4 Networks for the complete procedure).
  - You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new network.
- **IPv6 Network** (see Configuring IPv6 Networks for the complete procedure).
  - You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new network.
- **IPv4 DHCP Range** (see Configuring IPv4 Address Ranges for the complete procedure).
  - You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new IPv4 DHCP range.
- **IPv6 DHCP Range** (see Configuring IPv6 Address Ranges for the complete procedure).
  - You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new IPv6 address range.

During configuration, you can choose to Exclude from Network Discovery if you wish to postpone discovery for specific object types.

**Note:** Individual IP addresses within a network, and specific object types (IPv4 reservation, fixed address, and host), may be excluded from discovery. You must explicitly select Enable Discovery for other object types (IPv4 and IPv6 Ranges, IPv4 and IPv6 Networks); you can optionally Enable Immediate Discovery.

If you choose not to perform immediate discovery, but do Enable Discovery, the new network or other object is discovered at a normal time determined by Network Insight.

You can manually perform discovery on any object at any time by selecting the object and choosing

- Discover Now.
- Pending
- Discover Now
- Complete

Discover Now from the Toolbar. For more information, see Object. When you do so, you see a status icon appear in the Discover Now data column for the object under IPAM, in the Data Management → DHCP page and other locations.

By default, Grid discovery settings are the prevailing settings for all newly created objects. You can override basic discovery polling options for networks and DHCP ranges allowing immediate discovery.

In such cases, local settings take priority. Credentials cannot be overridden for networks and DHCP ranges.

Using Discover Now to Discover an Existing Object
Note: If after you select a network, object or IP and the **Discover Now** button is not enabled, make sure the network or other object has a discovery Probe member assigned to it.

After you create any supported IPAM object, you may wish to perform discovery on it at a later time. You can simply select the object and discover it.

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. Select the network or other object over which you want to perform discovery.
   Depending on the object type, navigate from the network level to the individual IP table in the **List** page to locate the object for immediate discovery.
3. Expand the Toolbar and click **Discover Now**.
   You can also click the Action icon
   for the network and choose **Discover Now** from the menu.

The Probe member associated with the network or other object initiates a discovery procedure.

### Smart Folders and Discovered Devices

Grid Manager maintains a Smart Folder titled **Discovered Switches/Routers**, under which appears a list of all routers, switches and switch-routers that thus far have been discovered and catalogued through discovery. Clicking a device name opens the device's main page, with **Interfaces**, **Networks**, **IP Addresses**, **Assets** and **Components** panels. For more information, see [Managing Discovered Data](#).

Open the Smart Folders category under the Finder menu and click on the **Discovered Switches/Routers** folder. Clicking on a device name opens the device page under **Data Management -> Devices** and shows the **Interfaces** page for the chosen device. For related information, go to [Predefined Smart Folders](#).

### Using the Device Selector

You use a dedicated Device Selector window to choose a discovered device for creating a port reservation with various IPAM objects such as IPv4 reservations, fixed addresses, host records, and provisioning of IPv4 and IPv6 networks on device interfaces; testing SNMP or CLI credentials, and other purposes, as shown in [Figure 15.3](#).

![Figure 15.3 Using the Device Selector Window](image)
The chosen device is discovered and listed in the Devices panel in IPAM, or any other device on the network under the All Devices category in the left pane of the device selector. Clicking a managed device's device name selects the device and brings you back to the originating page. Otherwise, select a device and click OK to continue. If you have a long list of devices even after selecting a smart folder, enter a device name search value or a search expression in the Find field and click Go.

**Tips for Quick Navigation**

To locate interface and device information quickly, along with associated IPAM objects that may be associated with elements such as port reservations, you can use Device and Interface terms in Global Search. (For additional information on Global Search, see [Global Search](#)). Smart Folders provide another means of locating items such as IP addresses and IPAM objects of various types. Smart Folders provide additional filters for Device Type, Vendor, Model and Version. In a Smart Folder containing interfaces, you can filter by Admin Status, Operation Status, Trunk Status, VLAN ID or VLAN Name, and Description. Using Smart Folders, you can also isolate all objects of a certain type by creating a smart folder with settings such as: **Type equals IPv4 Fixed Address**. Title the smart folder appropriately, to make clear what data set it is presenting.