Configuring Discovery Properties

To ensure successful discovery, complete the following configurations for the Grid and Grid members that are acting as the Consolidator and Probes before you start a discovery:

- Define the basic polling methods, such as SNMP collection, CLI collection, and others for the Grid. For more information, see Defining Basic Polling Settings for the Grid.
- Define advanced polling settings for TCP scanning and Ping sweeps if you have selected these polling methods. You can also select to use DHCP routers as seed routers or log discovery events to the syslog while configuring advanced polling settings. For more information, see Defining Advanced Polling Settings for the Grid.
- Configure SNMP and CLI credentials if you have selected SNMP Collection and CLI Collection as the polling methods. For more information, see Configuring SNMP v1/v2 Credentials for Polling.
- Enable discovery or port configuration blackout periods, as described in Defining Blackout Periods and Defining Port Configuration Blackout Periods.
- Configure automatic network view mapping for unassigned VRFs that have been discovered, as described in Configuring Automatic VRF Mapping.

**Note:** You must be a superuser to configure discovery properties for the Grid. Some settings, such as seed router definition, take place only on Probes.

Defining Basic Polling Settings for the Grid

Grid polling settings apply to all Probe members and all discovery networks that are assigned to a Probe. You can override the Grid settings at the Probe member and network levels. Only superusers can modify Grid-wide discovery settings.

To define basic polling settings or to override Grid settings on Probe members and networks, complete the following:

1. For Grid: From the Grid tab -> GridManager tab -> Discovery service, select Edit -> Grid Discovery Properties from the Toolbar.
   - For members: From the Grid tab -> GridManager tab -> Discovery service, select Edit -> Member Discovery Properties from the Toolbar.
   - For networks: From the IPAM tab, select the network check box and click the Edit icon.

2. In the Grid Discovery Properties, Member Discovery Properties, or (IPv4 or IPv6) Network editor, click the Polling tab, and then complete the following in the Basic tab:
   - For Probe members and networks, click Override to override the Grid settings.
     - **SNMP Collection:** Select this to execute SNMP protocols to discover and collect information such as traceroute/path collection, vendor and model, SNMP credential collection, routing and ARP tables, switch port data, and VLAN configuration data. If you disable SNMP collection, previously discovered data remains available for viewing; no new data is added and no existing data is removed. Note that some devices may not support SNMP, and some devices may also not be able to execute SNMP, and some may also not be as able to execute SNMP.
     - **CLI Collection:** Select this if you want to use Network Insight to discover devices that support CLI connectivity through Telnet or SSH and that you possess admin account information. NIOS can use device admin account logsins to query network devices for discovery data collection, including IP configuration, port configuration, routing and forwarding tables, and much more. You must also provide the command-line credentials information as the credentials in the Grid Discovery Properties editor.

   **Note:** CLI Collection is the default polling method if SNMP is enabled on the member.

   - **Port Scanning:** Select this to probe the TCP ports. Ensure that you go to the Advanced tab to configure more settings for this option. Should you disable Port Scanning, NIOS attempts to poll all ports other than SNMP on any device.
     - **Profile Device:** If enabled, NIOS attempts to identify the network device based on the response characteristics of its TCP stack, and uses this information to determine the device type. In the absence of SNMP access, the Profile Device function is usually the only way to identify non-network devices. If disabled, devices accessible via SNMP are identified correctly; all other devices are assigned a device type of Unknown. Profile Device is disabled by default for network polling.
     - **Smart IPv4 Subnet Ping Sweep:** Select this to execute Pings sweeps only on subnetworks that are known to exist but no IPs can be found within the subnet, such as through ARP or other means.
     - **Complete Ping Sweep:** Select this to enable brute-force subnet Ping sweeps on IPv4 networks. An ICMP ping is broadcast to all addresses in a subnet. Subnet ping sweeps are used as a last resort in the discovery process. Perform a subnet ping sweep if NIOS cannot identify any network devices in a given subnet.

   **Note:** Note: NIOS will not perform Smart Subnet ping sweeps on subnets larger than /22. NIOS also will not perform Ping sweeps on IPv6 networks because of the dramatically greater scale of network addresses in the IPv6 realm. The Complete ping sweep differs from the Smart subnet ping sweep in the following ways: the Complete ping sweep will run only against the specified range; the sweep will run regardless of the range size, and the size of the sweep will run regardless of the number of discovered devices within the specified range.

   - **NetBIOS Scanning:** Select this to enable NIOS to collect the NetBIOS name for endpoint devices in the network. This feature can be enabled only by users with SysAdmin privileges. This feature is globally disabled by default (and also for device groups) to prevent unexpected scanning of the network by a new collector.
   - **Automatic ARP Refresh Before Switch Port Polling:** Select this to enable refreshing of ARP caches on switches and switch-routers in the managed network before NIOS performs polling of switch ports. Enabling this feature applies only to switched Ethernet devices. This feature enables more accurate detection of all endpoint devices on L2 switches. Without ARP refresh, some endpoint devices may not be detected. This feature is globally disabled by default. Individual ANPs can also be set to enable or disable this feature.
   - **Switch Port Data Collection:** Select this to enable the Probe member to poll L2 enterprise switches. You can completely disable switch port polling by deselecting this check box. You can also separately schedule polling for switch port data collection as follows:
     - **Periodic Polling:** Define regular polling time periods. Choose a polling interval of 30 or more Minutes or in between 1 and 24 Hours.
     - **Scheduled Polling:** Schedule recurrent polling based on hourly, daily, weekly or monthly time periods. Choosing this option, click the Calendar icon and a Polling Schedule editor appears; click the Edit icon to make scheduling changes. Choose a recurrence pattern of Once, Hourly, Daily, Weekly or Monthly; in all cases, you must choose an Execution Time.
Defining Advanced Polling Settings for the Grid

If you have selected any basic polling settings that involve the TCP scanning and Ping sweeps, you must configure additional settings to ensure that these polling methods function properly in a discovery. Advanced SNMP polling settings consist of choosing the TCP Scan Technique, along with a number of specialized settings for Ping Sweeps and other operations.

To defining advanced Grid-wide polling settings for TCP scanning and Ping sweeps, complete the following:

1. For Grid: From the Grid tab -> Grid Manager tab -> Discovery service, select Edit -> Grid Discovery Properties from the Toolbar.
2. In the Grid Discovery Properties, Member Discovery Properties, or (IPv4 or IPv6) Network editor, click the Polling tab, and then complete the following in the Advanced tab:
   - TCP Scan Technique: Select the TCP technique you want to use for the discovery. The default is SYN. For more information, see TCP.
   - SYN: Select this to quickly perform scans on thousands of TCP ports per system, never completing connections across any well-known port. SYN packets are sent and the poller waits for a response while continuing to scan other ports. A SYN/ACK response indicates the protocol port is listening while a RST indicates it is not listening. The SYN option presents less impact on the network.
   - CONNECT: Select this to scan IPv6 networks. Unlike the SYN option, complete connections are attempted on the scanned system and each successive TCP protocol port being scanned.
   - Port: Enter the port number you want to add to the list. You must enter a number between 1 and 65535.
   - Service: Enter the name of the service.
3. You can also delete a specific TCP port in the list, or select multiple ports for deletion.
   - Purge expired assets data after: Removes records of discovered assets that are no longer reachable after a specified period of time. The default is set to one day.
   - Purge expired device data after: Removes records of discovered network infrastructure devices that are no longer reachable after a specified period of time. The default is set to seven days, a more forgiving value given that devices sometimes require maintenance, upgrades or repairs, or in cases where hosts leave the network on long trips.
   - ARP Aggregate Limit: Determines the largest ARP table collectible by discovery. The default is set to 30 ARP table entries (MAC Addresses).
   - Route Limit: Limits the size of the routing table that discovery is required to collect from any given device. Some routers can have tables in the hundreds of thousands of entries, and collecting such a large body of data can impose performance problems in the network and in discovery data collection. This setting defaults to 3000, and automatically excludes BGP routes from collection. Consult Infoblox Technical Support before making changes to this value.
   - Ping Sweep Timeout (ms): Period of time allowed, in milliseconds, beforeea Ping times out to any given device. Default is 1000 ms.
   - Ping Sweep Frequency: Defaults to 1, because ping sweep should not be executed more than once a day when the feature is enabled at the grid level or for a given discovery range. This setting affects the Smart Ping Sweep and Complete Ping Sweep features under Grid Discovery Properties.
   - ARP Cache Refresh: Defines the time period between ARP refreshes by Network Insight across all switch ports. Before any otherswitchport polling and discovery operations take place (including any global discovery polling operations initiated by the administrator), another ARP refresh is carried out by the Probe appliaza, regardless of the time interval. The default is five minutes, because switch forwarding tables are frequently purged from LAN switching devices. (The default on Cisco switches is five minutes/300 seconds.) Network Insight primarily uses ARP Cache refreshes to improve the accuracy of end-device discovery. Without this feature, some endpoints may not be discovered and cataloged.
   - Ignore Conflict Duration: Used when resolving conflicts and when choosing the option to Ignore the conflict when resolving it. The length of time during which conflicts is ignored is defined with this setting. Increments can be defined in Hours or Days.
   - Number of discovered unmanaged IP addresses per notification: The maximum number of unmanaged IP addresses that the appliance discovers before it sends SNMP and email notifications, if enabled. The appliance resets the counter after it hits this number and sends notifications. The default is 20.
   - Interval between notifications for discovered unmanaged IP addresses: This number determines how often the appliance sends SNMP and email notifications, if enabled, when it discovers the maximum number of unmanaged IP addresses (configured for Number of discovered unmanaged IP addresses per notification ). This is the time interval between two notifications for discovered unmanaged objects. Select the time unit from the drop down menu. The default is five minutes.
   - DNS Lookup Option: Specify whether you want to perform a reverse DNS lookup from discovered IP addresses. Select one of the following from the drop-down list:
     - Network Devices: Select this to resolve network device (switches and routers) IP addresses. This option is selected by default.
     - Network Devices and End Hosts: Select this to resolve both network device (switches and routers) and end host IP addresses.
     - Off: Select this to turn off reverse DNS lookups for discovered IP addresses.
   - DNS Lookup Throttle: This is the value in a percentage that throttles the traffic on the DNS servers. Setting a lower value reduces the number of requests to DNS servers. You can specify a value between 1 and 100. The default value is 100.
   - Disable discovery for networks not in IPAM: Enabling this setting disallows Network Insight from executing discovery on any infrastructure networks that are not presented in the Infoblox IPAM system; e.g. present and managed in a network view or network container.
   - Authenticating and poll using SNMPv2c or later only: For credential discovery and device polling exclusively using SNMPv2c and up, prevenuting use of SNMPv1, enable this check box.
   - Use DHCP Routers as Seed Routers: Select this so the Probe members can use the default gateways for associated DHCP ranges and networks as seed routers to more quickly discover and catalogue all devices (such as endpoint hosts, printers and other devices).
All such default gateways are automatically leveraged by discovery, and no further configuration is necessary unless you wish to exclude a device from usage.

**Note:** Check for a list of configured DHCP seed routers for any discovery Probe member in the **Seed** tab → **Advanced** tab of the **Member Discovery Properties** editor.

- **Log IP Discovery events in Syslog:** Sends a message to the configured Syslog service when an IP address of an active host is discovered.
- **Log network discovery events in Syslog:** Sends a message to the configured Syslog service when a network discovery process takes place in the Grid.

4. Save the configuration.

### Configuring SNMP1/v2 Credentials for Polling

**Note:** You can test SNMPv1/v2c and SNMPv3 credentials against any device or any IP address, at the Grid level or from any Probe member or network view. For more information, see Configuring SNMPv3 Properties and Testing SNMP and CLI Credentials.

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Discovery**.
2. For the Grid: Click **Edit** → **Grid Discovery Properties** in the Toolbar.
3. For the Probe member: Select the member check box, and then click **Edit** → **Member Discovery Properties** in the Toolbar.
4. Click the **Credentials** tab. To override Grid settings for a Probe member, click **Override**.
5. Optionally, you can test the credentials you added to the list by selecting a **community string** check box and clicking **Test Credentials**.
6. To export the entire list of community strings in a table file readable by a spreadsheet program, click the Export icon and choose Export Data in Infoblox CSV Import Format.

### Configuring SNMPv3 Properties

SNMPv3 allows the use of two secret keys for every credential—one for authentication, and another for encryption. Network Insight allows flexible application of keys—authentication but no encryption, for example. You define users in one of three ways:

- SNMPv3 user, with no authentication or privacy credentials
- SNMPv3 user, with authentication but no privacy credentials
- SNMPv3 user, with both authentication and privacy credentials

You can import sets of SNMPv3 credentials from an Infoblox CSV Import format data file.

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Discovery**.
2. For the Grid: Click **Edit** → **Grid Discovery Properties** in the Toolbar.
3. For the Probe member: Select the member check box, and then click **Edit** → **Member Discovery Properties** in the Toolbar.
4. Click the **Credentials** tab → **SNMPv3** tab. To override Grid settings for a Probe member, click **Override**.
5. Click the **Add** icon to add a new SNMPv3 authentication entry to the list. Enter the Name for the new credential; followed by the **Auth Protocol,** **Auth Password,** **Privacy Protocol,** **Privacy Password,** and the **Order value,** which is the order used for attempting use of the SNMP credentials.
6. If you have a substantial list of community strings in this list and need to find a specific string, enter the value in the Go To field and click Go. To remove a community string entry, select the check box and click the Delete icon.
7. To export the entire list of community strings in a table file readable by a spreadsheet program, click the Export icon and choose Export Visible Data.

### Configuring CLI Discovery Properties

SNMP protocols provide a powerful means of querying devices for broad arrays of information. The CLI discovery feature is required for port control tasks including port configuration and network provisioning and de-provisioning, but is not used for other discovery operations or to otherwise manage devices. By default, Probe appliances inherit their member discovery properties, including CLI credential sets, from the Grid level. Enable passwords are entered in separate records and kept as a separate list in Grid Manager.

You manage CLI credentials for devices in similar fashion to SNMP credentials, by defining a global set of Admin account/password tuples (and Enable passwords) at the Grid level; and specifying credentials and Enable passwords for individual devices at the member level, when necessary. Should such a credential not work for a given device, or if command-line access is lost for a device, Network Insight re-guesses credentials from the Grid-level credential list, including vendor defaults if available.
Note: You can test username/password credentials or an Enable password credential. You can also combine a username/password credential and an Enable password credential as part of the same test.

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Discovery**.
2. For the Grid: Click **Edit** -> **Grid Discovery Properties** in the Toolbar.
   For the Probe member: Select a **member** check box, and then click **Edit** -> **Member Discovery Properties** in the Toolbar.
3. Click the **Credentials** tab -> **CLI** tab. To override Grid settings for a Probe member, click **Override**.
4. Click the Add icon to add a new CLI username/password entry to the list. Select the **Credential Type**, which can be one of two choices:
   - **Protocol**: Select **SSH** or **Telnet**. Infoblox recommends the use of **SSH**.
     - **SSH** — SSI credentials require both a username and password. The default protocol is **SSH**.
     - **Telnet** — In Network Insight, Telnet credentials must use both a username or password.

   **Note**: Should you choose to use a Telnet-based credential, Network Insight requires both the username and password for the login account. This also applies when you override the CLI credentials on objects such as a fixed address, host or IPv4 reservation. For more information, see the section *Defining CLI Credentials Settings for Objects*.

   - **Name** — Username for the CLI login account.
   - **Password** — Login password for the CLI login account.
   - **Comment** — A text comment describing the CLI login account.
   - **Order** — By default, Network Insight inserts the new credential record at the bottom of the credentials list, which is reflected by its **Order** value, showing the order used for attempting use of CLI credentials. Enter a new value in the **Order** field if you want the new credential to be in a position other than the last in order.

5. In the **Login Credentials** list, click the Add icon to add a new CLI username/password entry:
   - **Order** — By default, Network Insight inserts the new credential record at the bottom of the list, reflected by its **Order** value, showing the order used for attempting use of CLI credentials. Enter a new value in the **Order** field if you want the new credential to be in a position other than the last in order.

6. In the **Enable Credentials** list, click the Add icon to add a new Enable password entry:
   - **Protocol** — **SSH** or **Telnet**. Infoblox recommends the use of **SSH**.
   - **Password** — Enable password for device configuration access.
   - **Comment** — A text description.
   - **Order** — By default, Network Insight inserts the new record at the bottom of the list, reflected by its **Order** value, showing the order used for attempting use of the CLI credentials. Enter a new value in the **Order** field if you want the new credential to be in a position other than the last in order.

7. Click **Save & Close** to save changes. You may also select **Save** to keep the dialog box open for further changes. You can press Tab to navigate across the fields for the credential entry.

To test CLI credentials for the current appliance, see *Testing SNMP and CLI Credentials*.

**Defining CLI Credentials Settings for Objects**

You can override CLI credentials, and enable password credentials, for IPAM objects such as fixed addresses, IP reservations, and host objects. You can also do so for networks under IPAM and DHCP.

When you do so, you define and test the CLI credentials and enable passwords locally to the object.

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. In the IPAM **IP List** page or the IPAM **IP Map** page, navigate to the network and then the IP associated with the object you want to edit.

   **Note**: For each network, the IP list page provides a **Type** data column showing the IPAM object type that is associated with any IP address. Also check the **MAC Address** column in the IP List page for information about associated objects.

   For a quick way to locate all objects of a certain type in the Grid, you can also create 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.

3. Click the IP address. In the IP address page, click the **Related Objects** tab.
4. Select the check box for the object in the Related Objects panel and click **Edit**.
5. In the object editor, click the **Discovery** tab.
6. For the object, click the **Override CLI Credentials** check box to override the inherited set of CLI credentials taken from the Grid level.
   By default, CLI credential definitions use SSH at the object level. Select the **Allow Telnet** check box if you want to allow both SSH and Telnet credential usage; Infoblox recommends SSH because of better security.
7. Enter the **Name** and **Password** values, and the **Enable Password** value.
8. Click **Test CLI Credentials** to test the CLI discovery credential settings applied to the object.
9. When finished, click **Save & Close**.

**Testing SNMP and CLI Credentials**

After configuring SNMP and CLI credentials, you can click **Test Credentials** in the SNMP Credentials or CLI Credentials panel to test the credentials. Credential testing ensures that the configured credentials work for as many devices and networks as possible. The procedure in this section applies to both the Grid and the member levels. You can override the Grid settings at the member level.

For CLI credentials, you can test an admin login name and password tuple as well as a following enable credential, if necessary. You can also override CLI credentials and enable credentials for IPAM objects such as fixed addresses, IP reservations, and host objects. You can test any credential set, an enable credential or both in combination against any device within any network view. Network Insight sets the login sequence to match the command-line standards for the selected device.

To test SNMP credentials or CLI credentials, complete the following:

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Discovery**.
2. For the Grid: Click **Edit** -> **Grid Discovery Properties** in the Toolbar.
   For a Probe member: Select a **member** check box, and then click **Edit** -> **Member Discovery Properties** in the Toolbar.
3. In the Grid Discovery Properties or Member Discovery Properties editor, click the Credentials tab → SNMPv1/v2 tab, SNMPv3 tab, or CLI tab.
4. Select the check box or check boxes for the credentials and/or enable credentials (if applicable) you want to test. For a Probe member, click Override, and then select the credential check boxes.
5. Click Test Credentials.
6. In the Test SNMP Credentials editor, complete the following:
   - IP Address: Select this to test the credential against an IP address of a reachable device in a network (even if it has not been discovered or managed through NIOS), within a specified network view. Enter the IP address in the field. Ensure that you select the respective network view in which this IP address resides.
   - Network View: If you have multiple network views, select the network view in which the IP address resides from the drop-down list. If you have only one network view, which is the default view, the Network View drop-down list is hidden by default. NIOS conducts credential testing for the IP address in the selected network view.
   - Device: Select this to test against a selected device. Click Select Device and the Device Selector appears. If you have multiple network views, you must first select the network view in which the device resides from the Network View drop-down list, located at the upper left-hand corner of the selector. If you have only one network view, which is the default view, the Network View drop-down list is hidden by default. You can check the device categories under All Devices to locate discovered switches and routers or any unmanaged devices previously detected by discovery under NIOS. You can explore categories including Discovered Switches/Routers, Microsoft Windows Devices (this can include items such as Windows Servers of various types), Router and Wireless Access Point Devices. Unmanaged, and others. By default, all devices previously discovered appear in this selector. If you have a long list of devices, you can enter a device name search value or a search expression in the Find field and click Go. You can also click Show Filter to narrow down your selection by selecting available filters. Click OK after you have selected a device and its corresponding network view.
7. Click Start to begin testing the credential against the IP address or selected device. The communication and testing processes appear in the lower pane of the editor.

Note: If the specified IP address is excluded from all discovery ranges or is not part of the selected network view, or the credential is entered with missing information, a message appears at the top of the editor after clicking Start. Otherwise, the test begins and its process and results appear in the lower pane of the editor.

Defining Seed Routers for Probe Members

Seed routers can be defined only on Probe appliances. You can define seed routers that NIOS uses in quickly performing network discovery. Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks. For the discovery of any IPv6 networks, you must use seed router values that comprised of at least one well-connected IPv6 router, preferably with routes to all other networks to be managed. 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 seed router(s) also helps determine how many seed routers you need. You must associate each seed router with a network view so the appliance can properly discover virtual networks when using multiple seed routers.

Note: All NIOS Probe members automatically use their default gateway as a seed router. These gateways are automatically displayed in the table. For effective use of seed routers, you must also provide SNMP credentials to NIOS 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. If you do not define a seed router, it is recommended that you enable discovery for a network or DHCP range.

You can check Discovery Status to see whether a seed router is successfully being reached and whether the seed is providing information. By reviewing discovery status for each seed router, you can determine whether Network Insight 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 Network Insight finds. For seed routers, Reached Status and Overall Status should both read Passed.

To add, view, or delete seed routers for a Probe, complete the following:

1. From the Grid tab, select the Grid Manager tab, and click Discovery.
2. Select the check box for any Probe appliance on the Discovery page and click Edit → Member Discovery Properties from the Toolbar.
3. In the Member Discovery Properties editor, Click the Seed tab. Grid Manager displays the following:
   - Click the Add icon to add a seed router. Grid Manager adds a row to the table. Complete the following in the table:
   - Router: Click this field and enter the IP address for the desired IPv4 or IPv6 seed router. Note that you can assign a seed IP address to different network views if your deployment has overlapping IP addresses.
   - Network View: Displays the current network view with which the interface is associated. A newly added seed IP does not have any associated network view by default. From the drop-down list, select the network view you want to reassign to the interface.
   - Comment: Enter information about the seed router.

You can delete a seed router by selecting it and then click the Delete icon. Note that you cannot delete any seed router that is a default gateway.

IPv6 Seed Router Usage

For the discovery of any IPv6 network, you must use seed router values, comprised of at least one well-connected IPv6 router, preferably with routes to all other networks to be managed. 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 seed router(s) also helps determine how many seed routers you need. Avoid having more seed router entries than necessary.

Note: For effective use of seed routers, provide SNMP credentials to the Probe member 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. For more information, see Defining Seed Routers for Probe Members.
Configuring Cisco Application Policy Infrastructure Controller (APIC)

Integrating Cisco APIC on NIOS provides visibility into your Cisco APIC infrastructure, which allows you to view and manage discovered IP addresses from Cisco ACI cluster. You can discover the SDN Controller and Elements (Spine, Leaf, End Points) using the Network Insight feature. You can view devices discovered by a discovery member in the Devices tab. For information, see Viewing the Complete List of Discovered Devices.

To configure Cisco APIC on NIOS, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then click Discovery.
2. Select the member check box, and then click Edit -- Member Discovery Properties in the Toolbar.
3. Click the Cisco APIC Configuration tab and click the Add icon and complete the following:
   - **Protocol**: Select HTTP or HTTPS as the protocol. When you select HTTPS, you must upload the corresponding SSL CA certificate to the Grid in order for NIOS to communicate with Cisco APIC, as described in Managing Certificates.
   - **Network View**: Select the network view to which the device is associated.
   - **Username**: The login name of Cisco APIC.
   - **Password**: The login password of Cisco APIC.
   - **Address**: Enter the hostname or IP address of Cisco APIC.
   - **Comment**: Enter additional information Cisco APIC.
4. Click Add to add Cisco APIC.
5. When finished, click Save & Close.