



## Discovery Use Case

Use Case | December, 2013

### Overview

Network discovery is the foundation for the Network Automation product. Network Automation will discover all known devices on a network and may even find some devices that were unknown to you.

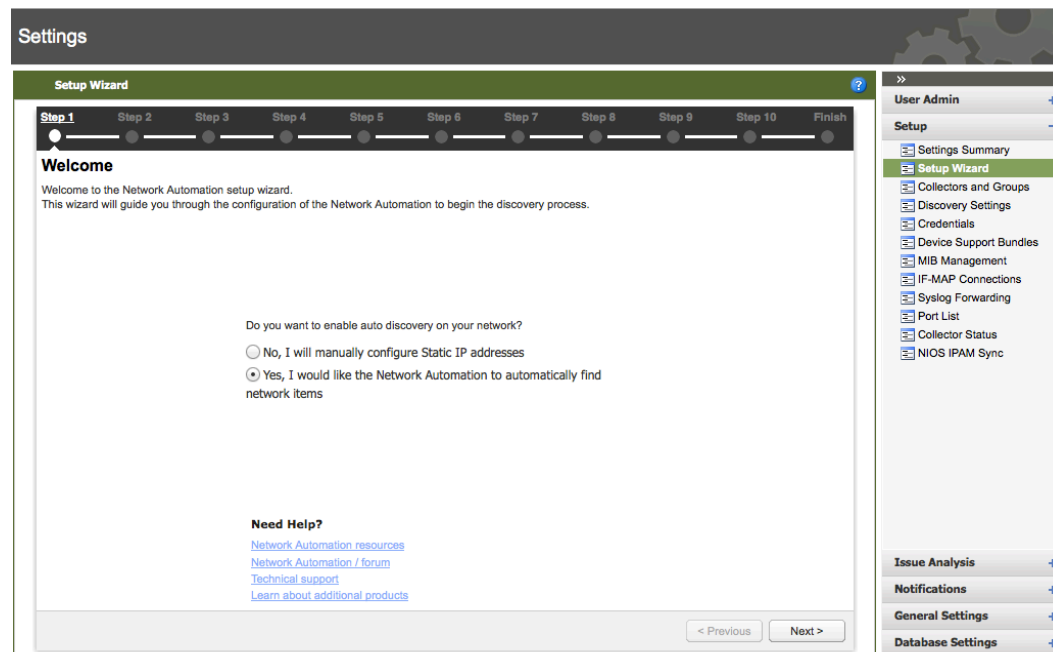
### Current Situation

Most customers use spreadsheets to keep an inventory of their network devices. When a network device is added, the spreadsheet needs to be updated. When a network device is taken out of the network, the spreadsheet needs to be updated. When IP address(es) and SNMP community strings for network devices are changed, the spreadsheet needs to be updated. The accuracy of the spreadsheet depends upon the owner of the spreadsheet to update it accurately and in a timely manner.

### Our Value

Network Automation will discover your network in an unobtrusive manner and constant manner. All you have to supply is an IP address range, SNMP community string(s), username, and passwords. Network Automation will then place the devices into device groups. Device groups are a Network Automation organizational unit that gathers devices in related group-routers in a Routers group, Ethernet switches in a Switches group, and so on. Network Automation stores all of the discovered devices. No need for creating and updating spreadsheets.

### Use Case



© 2013 Infoblox Inc. All rights reserved.

1. Click on the Settings wheel.
2. Click on the Setup tab -> Setup Wizard.
3. Ensure enable auto discovery is set to yes.
4. Click on the Next button.



# Discovery Use Case

Use Case | December, 2013

**Settings**

**Setup Wizard**

Step 1 **Step 2** Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Finish

**Discovery Ranges**

Specify devices to include or exclude by Network Automation in the list below. Devices can be defined as CIDR blocks, IP ranges, or IP address patterns.

New | Edit | Delete | Import

IP Address	Type	Discovery Mode	Ping Sweep
10.60.0.0/16	CIDR	Include in discovery	Enabled
10.102.255.0/29	CIDR	Include in discovery	Disabled
10.120.2.1 - 10.120.2.10	Range	Include in discovery	Disabled

Page 1 of 1 | Displaying 1 - 3 of 3

< Previous Next >

© 2013 Infoblox, Inc. All rights reserved.

- Click on the New button to add an IP range or Import a .CSV file with the IP ranges. See the Network Administrator guide for import file formats.

**Settings**

**Setup Wizard**

Step 1 **Step 2** Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Finish

**Discovery Ranges**

Specify devices to include or exclude by Network Automation in the list below. Devices can be defined as CIDR blocks, IP ranges, or IP address patterns.

New | Edit | Delete | Import

Network:  /32 (255.255.255.255)  
 IP Range:  through   
 IP Pattern:  Use \* to match any single IPv4 address octet or IPv6 hexadecimal grouping.

Discovery Mode:  Include in discovery

Enable Discovery Ping Sweep

Note: Ping Sweep / Subnet Scan is not supported for IPv6 collection

Cancel Add

IP Address	Type	Discovery Mode	Ping Sweep
10.60.0.0/16	CIDR	Include in discovery	Enabled
10.60.*.0	Pattern	Include in discovery	Disabled
10.102.255.0/29	CIDR	Include in discovery	Disabled
10.120.2.1 - 10.120.2.10	Range	Include in discovery	Disabled

Page 1 of 1 | Displaying 1 - 4 of 4

< Previous Next >

© 2013 Infoblox, Inc. All rights reserved.

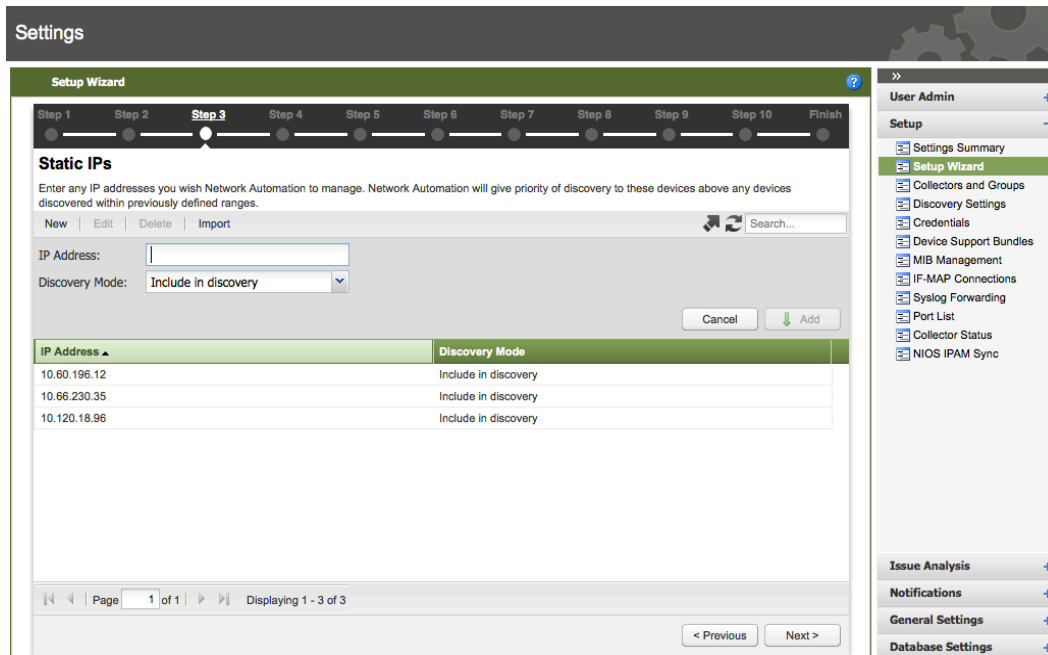
- On this screen, you have a choice of inputting a network, IP range, or IP pattern.
- Select the discovery mode. The choices are:
  - Include in discovery-devices are discovered and managed by Network Automation.
  - Exclude from discovery-devices are not discovered.



## Discovery Use Case

Use Case | December, 2013

- Exclude from management-devices are discovered, but are not managed. This setting allows you to know about the devices for inventory purposes.
8. You can enable ping sweep if you wish. Ping sweep can be used if Network Automation is unable to identify any network devices in a given subnet.
  9. Once you have filled out the form, click on the Add button to add the discovery range. Network Automation will start the discovery process.
  10. Click on the Next button.



IP Address	Discovery Mode
10.60.196.12	Include in discovery
10.66.230.35	Include in discovery
10.120.18.96	Include in discovery

© 2013 Infoblox, Inc. All rights reserved.

11. Optionally, you can add an IP address for Network Automation to discover or not.
12. Select the discovery mode. The choices are:
  - Include in discovery-devices are discovered and managed by Network Automation.
  - Exclude from discovery-devices are not discovered.
  - Exclude from management-devices are discovered, but are not managed. This setting allows you to know about the devices for inventory purposes.
13. Click on the Add button.
14. Click on the Next button.



15. Add all of the possible credentials for the network devices. The password types are user and enable. The priority number allows you to place the most popular credential at the top. This will make the discovery process more efficient.
16. Click on the New button to add a credential.
17. When finished, click on the Add button.
18. When finished, click on the Next button.



**Settings**

**Setup Wizard**

Step 1 Step 2 Step 3 Step 4 **Step 5** Step 6 Step 7 Step 8 Step 9 Step 10 Finish

**SNMP v1/2 Credentials**

New Edit Test Delete Import Search...

Priority:  Community:

Cancel Add

Priority ▲	Community	Origination	Successful	Invalid
1	infoblox	User	20	0
2	publican	User	4	0
3	Infoblox	User	1	0
4	public	Default	17	0
5	Public	Default	0	0
6	private	Default	0	0
7	Private	Default	0	0
8	Secret	Default	0	0
9	root	Default	0	0
10	Root	Default	0	0
11	admin	Default	0	0
12	Administrators	Default	0	0
13	cable-docsis	Default	0	0
14	ANYCOM	Default	0	0

< Previous Next >

**User Admin** +

**Setup** -

- Settings Summary
- Setup Wizard**
- Collectors and Groups
- Discovery Settings
- Credentials
- Device Support Bundles
- MIB Management
- IF-MAP Connections
- Syslog Forwarding
- Port List
- Collector Status
- NIOS IPAM Sync

**Issue Analysis** +

**Notifications** +

**General Settings** +

**Database Settings** +

© 2013 Infoblox, Inc. All rights reserved.

19. Click on the New button to add SNMP v1/2 community string(s).
20. The priority number allows you to place the most popular credential at the top. This will make the discovery process more efficient.
21. Click on the Add button when done.
22. When finished, click on the Next button.



The screenshot shows the 'Settings' page with the 'Setup Wizard' at Step 6, 'SNMP v3 Credentials (Rare)'. The wizard progress bar shows steps 1 through 10, with Step 6 highlighted. The main content area has a toolbar with 'New', 'Edit', 'Test', 'Delete', 'Import', and 'Show Passwords'. Below this are input fields for 'Priority' (set to 1), 'Username', 'Authentication Password', 'Authentication Protocol', 'Privacy Password', and 'Privacy Protocol'. There are 'Cancel' and 'Add' buttons. Below the form is a table with columns: Priority, Username, Auth Protocol, Privacy Protocol, Successful, and Invalid. The table is currently empty. At the bottom are '< Previous' and 'Next >' buttons. A sidebar on the right contains navigation links for 'User Admin', 'Setup', 'Settings Summary', 'Setup Wizard', 'Collectors and Groups', 'Discovery Settings', 'Credentials', 'Device Support Bundles', 'MIB Management', 'IF-MAP Connections', 'Syslog Forwarding', 'Port List', 'Collector Status', and 'NIOS IPAM Sync'. Below these are 'Issue Analysis', 'Notifications', 'General Settings', and 'Database Settings'.

© 2013 Infoblox, Inc. All rights reserved.

23. Click on the New button to add SNMP v3 credentials.
24. Click on the Add button when done.
25. Click on the Next button when done.

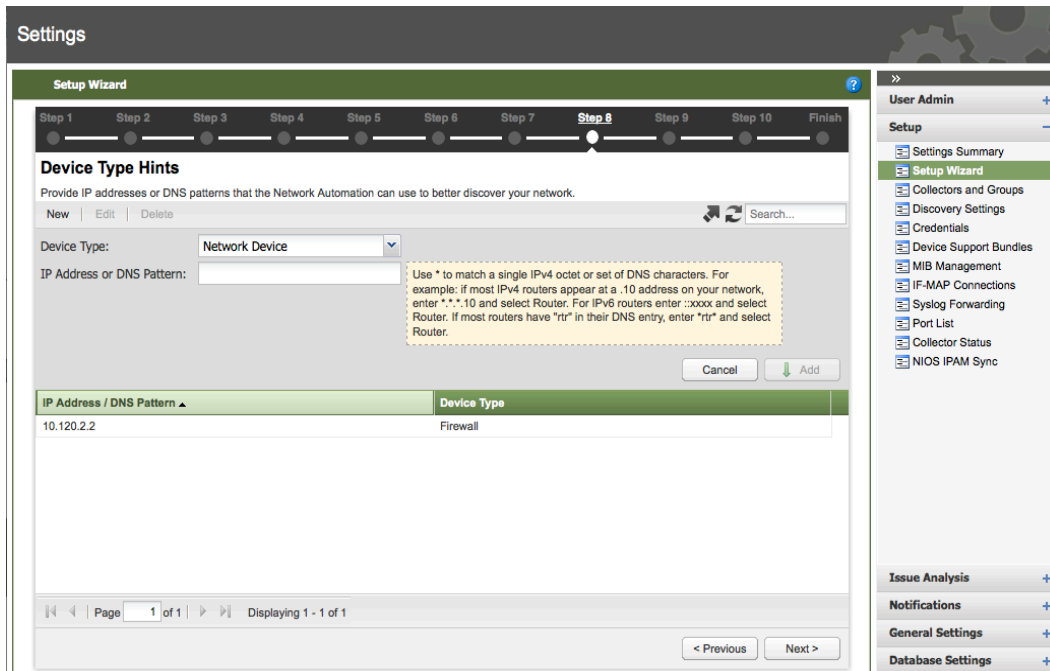
The screenshot shows the 'Settings' page with the 'Setup Wizard' at Step 7, 'Seed Routers'. The wizard progress bar shows steps 1 through 10, with Step 7 highlighted. The main content area has a toolbar with 'New', 'Edit', 'Delete', 'Import', and 'Discover Now'. Below this is a text input field for 'Seed Router IP Address'. There are 'Cancel', 'Add & Discover', and 'Add' buttons. Below the form is a table with columns: IP Address, E, P, R, S, SC, C, CC, Last Timestamp, and Last Action. The table contains one row with IP address 10.60.16.1 and a 'Last Action' of 'Device Groups: Successful...'. At the bottom are '< Previous' and 'Next >' buttons. A sidebar on the right contains navigation links for 'User Admin', 'Setup', 'Settings Summary', 'Setup Wizard', 'Collectors and Groups', 'Discovery Settings', 'Credentials', 'Device Support Bundles', 'MIB Management', 'IF-MAP Connections', 'Syslog Forwarding', 'Port List', 'Collector Status', and 'NIOS IPAM Sync'. Below these are 'Issue Analysis', 'Notifications', 'General Settings', and 'Database Settings'.

© 2013 Infoblox, Inc. All rights reserved.

26. Add an IP address for the seed router. A seed router is used to discover other networks. Network Automation will log into the seed router and download the routing table.



27. Once the IP address of the seed router is added, click on Add & Discover or Add button. The Add & Discover button will tell Network Automation to immediately begin the discovery process. The Add button adds the IP address of the seed router for later discovery.
28. Click on the Next button when done.



29. Input an IP address or DNS Pattern. The Device Hints provides hints to Network Automation’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 “.10”, specifying “\*.\*.\*.10” and associating the Router device type for an IP address hint will allow the appliance to prioritize any discovered devices matching that hint higher in its credential collection queue to help speed discovery. This hint is considered when Network Automation attempts to determine a device type for a discovered device.





# Discovery Use Case

Use Case | December, 2013

**Settings**

**Setup Wizard**

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 **Step 9** Step 10 Finish

**Device Interrogation Techniques**

Provide additional options to improve discovery and interrogation of devices for identification.

- Enable Port Scanning
  - Fingerprint Devices
- Enable SNMP Collection
  - Collect Performance Data
  - Use Vendor Default Community Strings
- Enable Subnet Ping Sweep (IPv4 only)

< Previous    Next >

© 2013 Infoblox, Inc. All rights reserved.

30. Leave these settings at these defaults unless you want to discover and manage devices that do not support SNMP.

31. Click on the Next button.

**Settings**

**Setup Wizard**

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 **Step 10** Finish

**Configuration Collection (Rare)**

Provide changes to Network Automation's use of CLI collection. (Rarely changed)

- Enable Configuration File Collection
  - Use Telnet
  - Use SSH
  - Use HTTP
  - Try Vendor Default Credentials

ARP Collection Priority:  SNMP  CLI

Route Collection Priority:  SNMP  CLI

< Previous    Next >

© 2013 Infoblox, Inc. All rights reserved.

32. Leave these settings at the default shown above.

33. Click on the Next button.





# Discovery Use Case

Use Case | December, 2013

**Settings**

**Setup Wizard**

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 **Finish**

**Summary**

⚠ Network Automation setup completed with one or more warnings. You may want to remain on this screen to make the recommended changes and return to it until all of the indications are successful.

- ✔ Auto-discovery enabled.
- ⚠ Include ranges/CIDRs are reasonably small. [Edit](#)
- ✔ At least one Seed router has been specified.
- ✔ At least one CLI credential is specified.
- ✔ SNMP Collection enabled.
- ✔ At least one SNMP credential has been specified.
- ✔ At least one device has been found on the network.
- ✔ At least one device has been fully discovered.
- ✔ At least one device had SNMP status collected.
- ✔ At least one device has a configuration collected.

< Previous Finish

© 2013 Infoblox, Inc. All rights reserved.

34. Click on the Finish button.

We have now finished the setup process for discovering the network devices by Network Automation. Let's look at the results.

MyNetwork **INFOBLOX** FindIT User: admin Logout

Dashboard Network Analysis Network Insight Security Control Config Management Reports

Inventory Summaries Topology **Discovery** Switch Port Management

Entire Network

IP Address	Name	E	P	R	S	SC	C	CC	G	Type	Last Timestamp	Last Action	Last Seen
10.60.30.253	test-switch	✔	⊘	⊘	⊘	⊘	⊘	⚠	✔	Switch-Ro...	2013-12-10 14:38:12	Reachable: Failed to reach	2013-12-01
10.60.30.254	SKO13-kc	✔	⊘	⊘	⊘	⊘	⊘	⚠	✔	Switch-Ro...	2013-12-10 14:38:10	Reachable: Failed to reach	2013-12-01
10.60.81.8	sync.acme.com	✔	✔	✔	✔	✔	✔	✔	✔	vNIOs	2013-12-10 14:38:05	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-11
10.60.16.1	core-6506	✔	✔	✔	✔	✔	✔	✔	✔	Switch-Ro...	2013-12-10 14:38:05	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-11
10.60.3.66	tme-labB	✔	✔	✔	✔	✔	✔	✔	✔	Router	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.192.253	caco-p4r1-29	✔	✔	✔	✔	✔	✔	✔	✔	Switch-Ro...	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.120.2.10	qtsflex_t1_router.inca.i...	✔	✔	✔	✔	✔	✔	✔	✔	Router	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.196.156	asa2-tme	✔	✔	✔	✔	✔	✔	✔	✔	Firewall	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.3.2	tme-gw	✔	✔	✔	✔	✔	✔	✔	✔	Router	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.30.67	VRF-Router	✔	✔	✔	✔	✔	⊘	⚠	✔	Router	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.176.1	bd-3750-48-01.m	✔	✔	✔	✔	✔	⊘	⚠	✔	Switch-Ro...	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.196.155	asa1-tme	✔	✔	✔	✔	✔	✔	✔	✔	Firewall	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.16.5	sw2	✔	✔	✔	✔	✔	✔	✔	✔	Switch-Ro...	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.80.2	wan-br	✔	✔	✔	✔	✔	✔	✔	✔	Router	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.1.254	tme-3750-48-p4r1-23.m	✔	✔	✔	✔	✔	✔	✔	✔	Switch	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11
10.60.254.250	core2-3750	✔	✔	✔	✔	✔	✔	✔	✔	Switch-Ro...	2013-12-10 14:38:04	Device Groups: Successfully assigned to device groups	2013-12-11

Page: 1 of 19 | Displaying 1 - 17 of 313

**Entire Network Totals**

Network Devices: 93  
Licensed Devices: 41

IP Addresses: Classified 148 Reached 313 Identified 415

© 2013 Infoblox, Inc. All rights reserved. 2013-12-10 14:46



# Discovery Use Case

Use Case | December, 2013

S	SC	C	CC	G	Type	Last Timestamp	Last Action	Last Seen	First Seen	License Status
✓	✗	○	○	○	vNIOS	2013-12-10 14:53:22	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:50:11	2013-05-23 12:20:50	Licensed
✓	✓	✓	✓	○	Router	2013-12-10 14:53:15	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:51:12	2013-05-17 00:13:38	Licensed, Security Device C...
✓	✗	✗	○	○	Switch-Ro...	2013-12-10 14:53:15	Reachable: Failed to reach	2013-12-09 15:48:33	2013-01-10 13:20:41	Licensed, Switch Port Mana...
✓	✓	○	○	○	vNIOS	2013-12-10 14:53:07	Reachable: Failed to reach	2013-12-06 04:07:25	2013-08-30 16:32:52	Licensed
✓	✓	✓	○	○	Firewall	2013-12-10 14:53:07	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:43:07	2013-06-28 15:44:10	Licensed, Security Device C...
✓	✗	○	○	○	vNIOS	2013-12-10 14:53:06	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:38:05	2013-11-27 13:17:10	Licensed
✓	✗	✗	○	○	Switch-Ro...	2013-12-10 14:53:04	Reachable: Failed to reach	2013-12-09 16:02:51	2013-07-16 14:14:24	Licensed, Security Device C...
✓	✗	○	○	○	vNIOS	2013-12-10 14:52:58	Reachable: Failed to reach	2013-12-06 03:54:39	2013-09-21 17:24:54	Licensed
✓	✓	✓	○	○	Firewall	2013-12-10 14:52:51	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:51:40	2013-05-24 11:46:14	Licensed, Security Device C...
✓	✓	✗	○	○	Router	2013-12-10 14:52:51	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:51:30	2013-11-06 18:51:52	Licensed
✓	✗	○	○	○	Switch-Ro...	2013-12-10 14:52:26	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:50:29	2013-05-22 11:44:21	Licensed, Security Device C...
✓	✗	○	○	○	Switch-Ro...	2013-12-10 14:52:25	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:49:02	2013-05-22 11:44:21	Licensed, Security Device C...
✓	✓	○	○	○	Switch	2013-12-10 14:52:25	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:52:02	2013-05-23 12:15:49	Licensed, Switch Port Mana...
✓	✗	✗	○	○	Switch-Ro...	2013-12-10 14:52:24	Reachable: Failed to reach	2013-12-09 16:15:50	2013-10-17 17:34:56	Licensed, Security Device C...
✓	✗	○	○	○	Switch	2013-12-10 14:52:18	Reachable: Failed to reach	2013-12-10 14:31:05	2013-11-21 11:13:52	Licensed, Switch Port Mana...
✓	✓	✓	○	○	Router	2013-12-10 14:52:09	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2013-12-10 14:51:38	2013-08-15 13:27:34	Licensed

Page: 1 of 19 | Displaying 1 - 17 of 313

Entire Network Totals  
 Network Devices: 93  
 Licensed Devices: 41  
 IP Addresses: Classified 149 Reached 314 Identified 415

In the screens above is the discovery status. A green check mark dot means that part of the discovery process for the device was successful. A gray dot means that part of the discovery process for the device was not applicable. A red x mark dot means that part of the discovery process for the device was not successful. A yellow triangle means that part of the discovery process for the device was skipped. A circling arrows dot means that part discovery process for the device is in progress. The following are descriptions for each column:

- E (Existing Status)-The listed IP address is in the network. All devices will receive this status to indicate where Network Automation first discovered the address.
- P (Fingerprint Status)-If Network Automation is configured to use fingerprinting, device fingerprint status is listed in this column.
- R (Reached Status)-Shows whether Network Automation has sent a packet to the device and received a reply.
- S (SNMP Credentials Status)-Indicates status of the SNMP credential guessing process.
- SC (SNMP Collection Status)-Shows status of the device group generation process. Success indicates that a device has been assigned to at least one group.
- C (CLI Credentials Status)-Displays status of the CLI credential guessing process.
- CC (Config Collection Status)-Indicates status of the configuration file collection process.
- RC (Rule Collection Status)-Show status of firewall/packet filter rule configuration collection. Applies only to devices in the Security Control device group.
- G (Device Group Status)-Shows status of the device group generation process. Success indicates that a device has been assigned to at least one group.
- Type-Lists the device type as determined by Network Automation.
- Last Timestamp-Date and time of last Discovery operation on the device.
- Last Action-The last action performed by Network Automation 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.
- Last Seen-The date and time when the device was last successfully polled by Discovery.
- First Seen-Date where the listed device was first detected by the Network Automation appliance.
- License Status-Licensed devices are listed as such. Unlicensed devices are non-network devices, or devices for which Network Automation license limits have been exceeded. Unmanaged devices are those which Network Automation will discover but not manage.



Over time, the status of each discovery process will change. If a particular status of a device has not change over a period of 24 hours, then troubleshooting the status maybe necessary.