



Step-By-Step User Guide

Netformx Discovery™ Step-By-Step User Guide for v21.x

Table of Contents

Revision History	5
Netformx Discovery Overview	6
Special Note: Motivation for CLI-Inspection	6
Special Note: Discovering Meraki Equipment	6
Additional Online Resources	7
Getting Started	8
Setting Your Customer’s Expectation.....	8
Customer Site Prerequisites.....	9
Start a Discovery	9
Discovery Scope	12
Step 1: Define the Discovery Scope.....	13
Add Seed	13
Add Range	14
Add Excluded Range	17
Import Ranges.....	17
Step 2: Define SNMP Variables	18
Add SNMP Credentials	18
Step 3: Telnet/SSH Credentials	20
Add Telnet/SSH Credentials	20
Number of Concurrent CLI Sessions.....	20
CLI Inspection	21
Setup CLI Commands.....	22
Save CLI Output to.....	24
Step 4: Collect Cisco Smart Advisor Data	25
Step 5: Device Discovery Profile	26
Ping.....	26
Cisco IP Phones.....	27
Configuring Meraki Discovery	27
Understanding the Meraki.com Data Sources.....	27
Meraki Cloud Discovery Settings	28
Generating or Accessing the Meraki REST API Key.....	29
Meraki SNMP Cloud Settings – Optional.....	32
Run Network Discovery.....	33
Updated Discovery Results Window	35
IP Discovered Networks	35
Cloud Managed Devices	36
Log Messages.....	37
Details on the Matching Method for Meraki Environment.....	37
Post Network Walk Actions	37
Exporting Raw Results	37
Next Steps.....	38
Network Analysis Using Cisco Smart Advisor (CSA).....	38
Submit Network Assessment Request (Cisco equipment)	39
CSA Customer Search.....	40
Enable CSA Services	40

CSA Service Type	41
CSA – User Contact Details	41
Network Assessment Request Status	42
Downloading a Completed Transaction Analysis	43
CSA Network Assessment Upload Help.....	44
DesignXpert CSA-Based Network Assessment Reports.....	45
Post-Discovery Operations & Other Helpful Options	47
Quick View Reports.....	47
Device Details from the Drawing Page (Right-Click Options).....	48
Netformx Discovery Files and Databases	50
Additional Discovery Related Tips.....	50
Steps for a Successful Cisco Network Assessment Engagement.....	51
Netformx Customer Support.....	51

Table of Figures

Figure 1: Creating Discovery Project.....	9
Figure 2: Selecting Blank Discovery Project.....	10
Figure 3: Discovery User Interface.....	11
Figure 4: Discovery Scope Reference Diagram.....	12
Figure 5: Discovery Scope User Interface.....	13
Figure 6: Setting the Seed Router.....	13
Figure 7: Defining the IP Range.....	14
Figure 8: Defining a From-To IP Range.....	15
Figure 9: Defining a CIDR-based IP Range.....	15
Figure 10: Defining a Subnet Mask IP Range.....	15
Figure 11: Advanced IP Range Definitions.....	16
Figure 12: Controlling IP Ranges via Exclusions.....	17
Figure 13: Importing IP Ranges.....	17
Figure 14: Import IP Range Examples.....	18
Figure 15: Defining SNMPv1/v2c Settings.....	18
Figure 16: Defining SNMPv3 Settings.....	19
Figure 17: Defining Telnet/SSH Settings.....	20
Figure 18: Concurrent CLI Sessions & CLI Inspection.....	21
Figure 19: CLI Inspection Logic.....	22
Figure 20: Defining Custom CLI Commands.....	22
Figure 21: Setup CLI Commands UI.....	23
Figure 22: Custom CLI Command Example.....	24
Figure 23: Saving CLI Command Output.....	24
Figure 24: Default Cisco Smart Advisor CSA Setting.....	25
Figure 25: Device Discovery Profile Settings.....	26
Figure 26: Collecting Cisco IP Phone Details.....	27
Figure 27: Meraki.com API Application Key Control.....	28
Figure 28: Add Application Key.....	28
Figure 29: Meraki Dashboard Organizations.....	29
Figure 30: Exposing Meraki My Profile.....	29
Figure 31: Generating REST API Access Key.....	30
Figure 32: Paste & Verify the Application Key.....	30
Figure 33: Post Verification.....	31
Figure 34: Meraki Cloud SNMP Settings.....	32
Figure 35: Add Meraki SNMP Credentials.....	32
Figure 36: Run a Network Discovery.....	33
Figure 37: Discovery Run in Progress.....	34
Figure 38: Completed Discovery Run.....	34
Figure 39: Discovery Results – IP Discovered Devices.....	35
Figure 40: Discovery Results - Cloud Managed Devices.....	36
Figure 41: Discovery Results - Log Messages.....	37
Figure 42: Submit CSA Trigger.....	38
Figure 43: CSA Upload Scope.....	38
Figure 44: Submit Network Assessment Settings.....	39
Figure 45: Cisco CSA Customer Search Menu.....	40
Figure 46: Service Type Menu Selection.....	41

Figure 47: Network Assessment Status Request 42
 Figure 48: Network Assessment Request Status Menu 42
 Figure 49: Network Assessment Ready for Download Pop-Up 43
 Figure 50: Selecting a Finished Network Transaction for Download 43
 Figure 51: Network Transaction Download Bar 44
 Figure 52: Accessing Cisco Reports 45
 Figure 53: Accessing Quick View Reports 47
 Figure 54: Right-click to Expose Discovery Information 48
 Figure 55: SNMP Interface Table 49
 Figure 56: SNMP Power Supply Table 49
 Figure 57: SNMP Phone Table 49
 Figure 58: Running Config File 49

Revision History

Date	Document Version	Modified By	Changes
12/20/2020	1.00	Evgeni Koifman	Initial version
03/18/2021	1.01	Marshall Eisenberg	Added Meraki Discovery
03/25/2021	1.02	Guy Laks	Review comments
08/11/2021	1.03	Marshall Eisenberg	V21.x Updates

Netformx Discovery Overview

Netformx Discovery is the SNMP/SSH/Telnet-based audit and multi-vendor network discovery solution that is also included in Netformx DesignXpert®. Netformx enables presales, systems, and design engineers to quickly and accurately identify and audit networking assets. Netformx Discovery exposes the network topology using Simple Network Management Protocol (SNMP), SSH & Telnet, Cisco Discovery Protocol (CDP), and Link Layer Discovery Protocol (LLDP), along with Command Line Interface (CLI) based equipment and configuration data to interrogate and expose node details. It can capture a baseline of existing equipment with detailed specs for each device. Used in conjunction with the Cisco Smart Advisor (CSA) formerly known as the Cisco Discovery Service (CDS), DesignXpert - Discovery Reports can assist during the analysis phase by identifying device EoX milestone events (End of Life, End of Support, etc.), IOS versions, Cisco Product Security Incident Response Team (PSIRTs), Field Notices, and resources and gaps in the discovered network.

The v21.x enhanced Discovery engine also uses CLI-Inspection to improve results.

Special Note: Motivation for CLI-Inspection

Previously, the legacy Discovery engine collected and analyzed a networking walk based primarily on SNMP data. An SNMP-only approach encountered the following limitations

- SNMP disabled or not deployed due to security concerns
- SNMP data does not expose all the required details for complete analysis (inventory, ARP neighbors, physical connectivity, etc.)
- Not all vendors program their SNMP public MIB variables adequately

Due to the demand for more comprehensive network walks and analysis and to overcome environmental restrictions, Netformx enhanced the Discovery collection engine (v21.x) with an alternative approach. It is now possible to invoke CLI commands via Telnet or SSH and for the application to parse the data for a limited set of manufacturers.

The V21.x release adds predefined CLI device-level calls to the engine's network walk phase. Combined with the existing SNMP call functionality, this enhancement allows the engine to recognize and expose more vendors and their device-level details during the collection and analysis phases. V21.x currently supports CLI-calls and analysis to the following vendors: Cisco, Juniper Networks, Palo Alto Networks, Dell, Fortinet, VMWare, and 3COM/H3C.

Special Note: Discovering Meraki Equipment

Traditionally, the typical Netformx SNMP Discovery walk did not uncover Meraki assets for a few key reasons

- Not all Meraki products support or respond to CLI commands
- Not all Meraki SKUs support or respond to typical SNMP calls
- SNMP calls to Meraki products must leverage the Meraki Cloud *enhanced* SNMP methodology

However, by leveraging the Meraki Cloud data sources and defining an additional set of credentials and settings, the v21.x Discovery walk can find, process, and present the Meraki assets for the customer's environment.

Please see the Configuring Discovering Meraki Products and Getting Started sections in this Guide if your customer environment includes Meraki products.

Additional Online Resources

We encourage you to take advantage of the additional online resources listed on the [Get Support](#) page. There you will find information, including

- Hot Topics
- Product Updates
- FAQs
- Newsletters
- How to reach support
- Where to submit feature requests

Getting Started

Before conducting a discovery of a customer's network, we recommend users follow these essential steps. Users who followed these steps reported a significant increase in their comfort level using Netformx Discovery. They also improved their success rate when conducting their first customer discovery.

1. Review the UI & this documentation.
2. Conduct a test discovery before contacting the customer.
3. Ask your customer if they have SNMP enabled throughout their network.
4. Ask your customer to supply you with their list of read-only community strings.
5. Ask if they have ICMP enabled throughout their network.
6. Ask your customer to provide you with their list of Telnet/SSH credentials.
7. **Meraki Note:** You must have the Meraki.com API application Key for your Meraki-defined customer organization(s).
 - a. Please consult with your end-customer IT manager and ask them to
 - i. Generate and share their organization API Application Key.
 - ii. Grant access to their organization.
 - b. If you have access to the Meraki Dashboard and customer organization, you can generate the end-customer API Application Key and have their Meraki.com Organization settings in hand.

Setting Your Customer's Expectation

1. Depending on the customer's network's size, it may take as little as 30 minutes to complete the network walk or as long as overnight.
 - a. The average time for 1000 – 2000 network devices is approximately two to three hours.
 - b. Even though the network walk creates a negligible impact on the network's overall performance, Netformx recommends conducting the assessment during non-peak business hours.
2. *SNMP* must be enabled throughout the customer's entire networking environment and running on each device (when applicable) before starting the Discovery.
3. To collect the device information, you must define all relevant SNMP v1/v2c/v3 read-only community strings into the SNMP section. *Please Note: Conducting a discovery does not expose the customer's network or create any security risks.*
4. Please check on the customer's IT policy concerning ICMP. Netformx Discovery leverages Ping to speed the identification of active elements.
5. Telnet/SSH credentials are required to collect the CSA characteristics used by Cisco to perform the necessary backend analysis for the CSA report output. Note that collecting device information with Telnet/SSH increases the amount of detail collected (see below in the appropriate section) and improves accuracy as there are situations when SNMP data is missing.
6. If you want the Netformx Discovery walk to uncover the Meraki assets, you need access to all the associated Meraki.com Cloud Settings.
7. Schedule an appointment with the customer to conduct a network assessment. Inform the customer that this evaluation is an essential first step in the design process as it provides an up-to-date baseline for the design discussions.
8. If you are a non-incumbent Partner, make sure you get the customer to sign a Letter of Authorization (LoA), which grants you access to SmartNet contract characteristics.
9. If you use the Netformx Collection Engine, make sure you define your Netformx Project Repository credentials (username & password) inside DesignXpert options – refer to the [Collection Engine documentation](#) for further details. *Please Note: A lack of a valid Project Repository username & password will cause DesignXpert to error when you attempt to import the discovered network NDF file created by the Collection Engine.*

Customer Site Prerequisites

Before initiating a discovery, please make sure to take the following steps:

1. Ensure SNMP is enabled and running on all the customer's devices.
2. Document all relevant SNMP read community string(s) used in the customer environment
3. Determine the status of ICMP & LLDP for all the devices in the customer environment.
4. Have ready all related Telnet/SSH credentials.
5. Make sure you have the Meraki REST API key (if desired).
6. Have your list of custom CLI commands ready (if desired).

Tips:

- **Start with a limited discovery of routers and subnets only.** Then analyze the Project to decide the limits and requirements of the desired outcome. (Note: a router/subnets only Discovery should complete in just a few minutes.)
- **Start with low limits** (e.g., hops, retries, and timeouts). Gradually expand the Discovery by changing one parameter at a time.

Start a Discovery

1. Open Netformx DesignXpert.
2. From the **Create New Project** menu, select **Discover Network** from the left-pane.

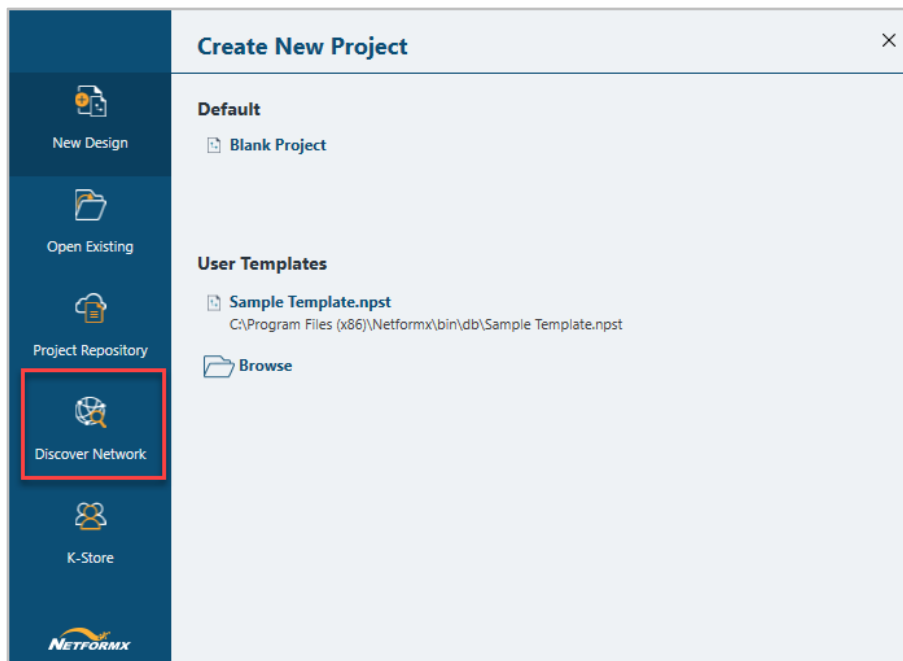


Figure 1: Creating Discovery Project

- From the **Create New Project from Network Discovery** menu, select **“Blank Project.”**

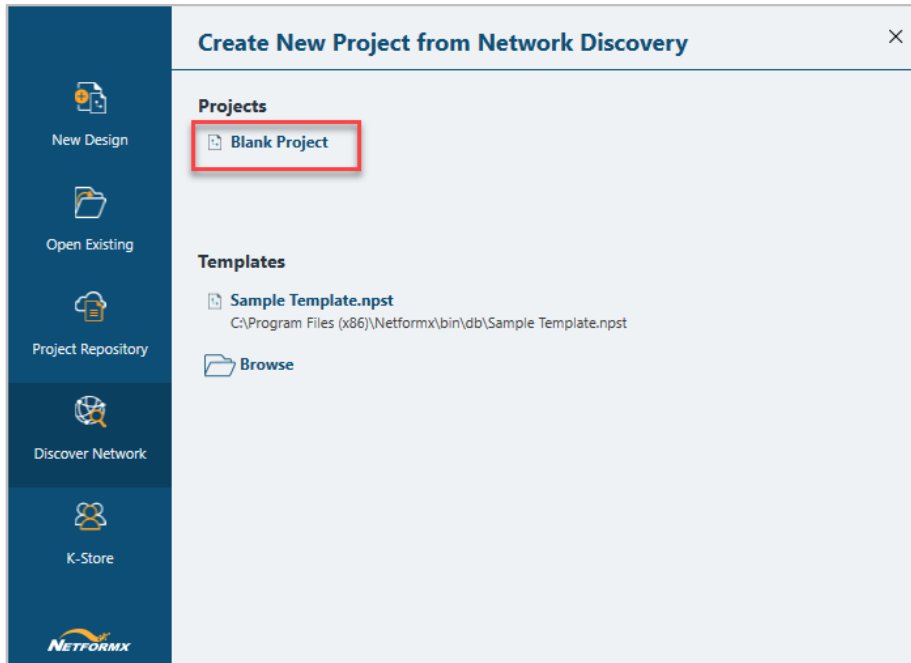


Figure 2: Selecting Blank Discovery Project

- The **Save As** menu opens.
- Name the **Discovery Project**, select the **Folder/Path**, and click **Save**.

You should now see the Netformx Discovery Settings screen. Be aware the UI includes an example setting for a Discovery Scope and sample SNMP variable – be sure to clear them before proceeding with your customer inputs.

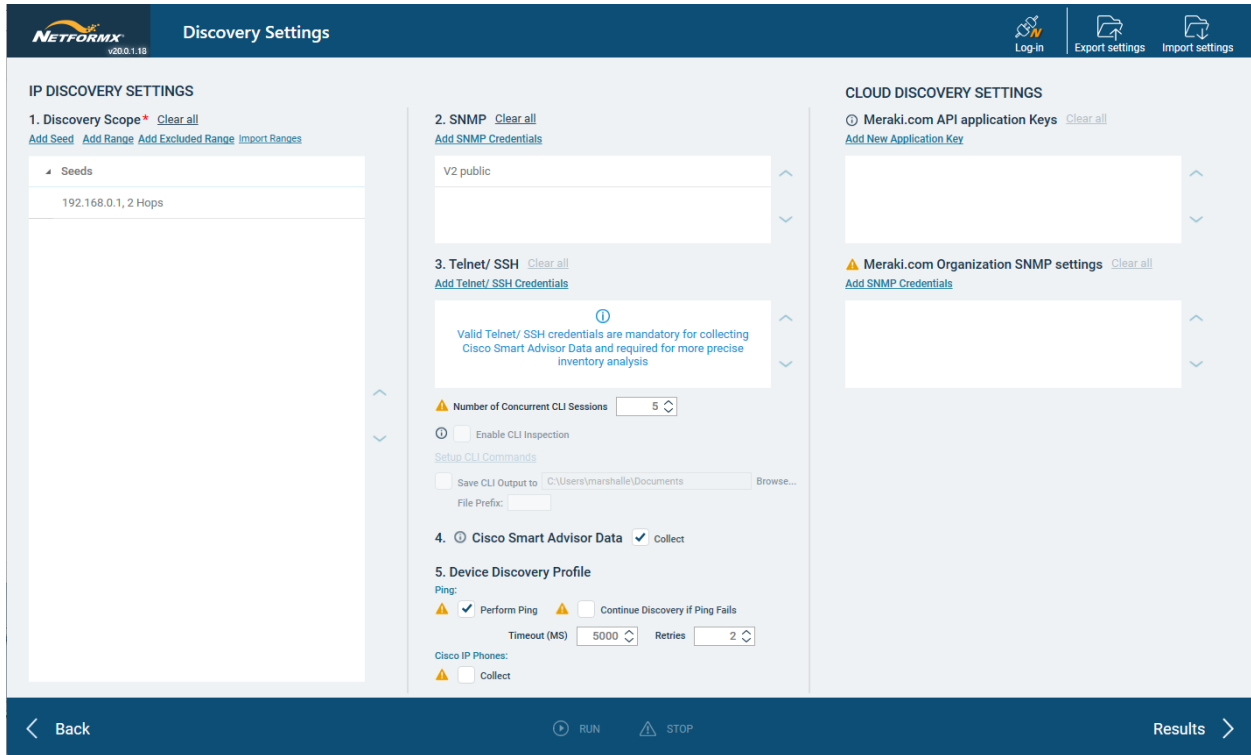


Figure 3: Discovery User Interface

The Discovery Setting screen contains three columns of information: a left, middle, & right division.

- Left: IP Discovery Scope
- Middle: SNMP, Cisco SmartAdvisor, Telnet/ SSH, Device Discovery Profile, & Cisco IP Phone
- Right: Cloud Discovery Setting, Meraki.com API Application Keys, & Meraki.com Organization SNMP Settings

The Run button (at the bottom middle of the UI) activates once you define all required Discovery configuration parameters.

Discovery Scope

The first step is configuring the scope of your customer's network. The Discovery Scope interface includes multiple options you can combine to help define and control your network walk span.

We will use the below diagram to describe how to configure your Discovery Scope.

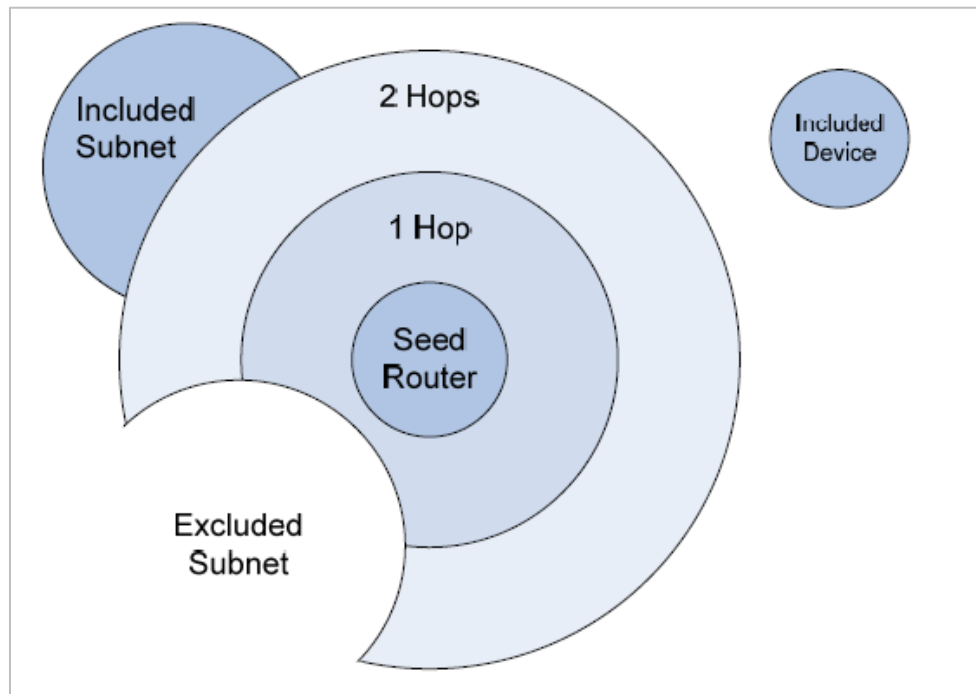


Figure 4: Discovery Scope Reference Diagram

Step 1: Define the Discovery Scope

The Discovery Scope is your definition starting point and includes:

1. Add Seed
2. Add Range
3. Add Excluded Range
4. Import Ranges

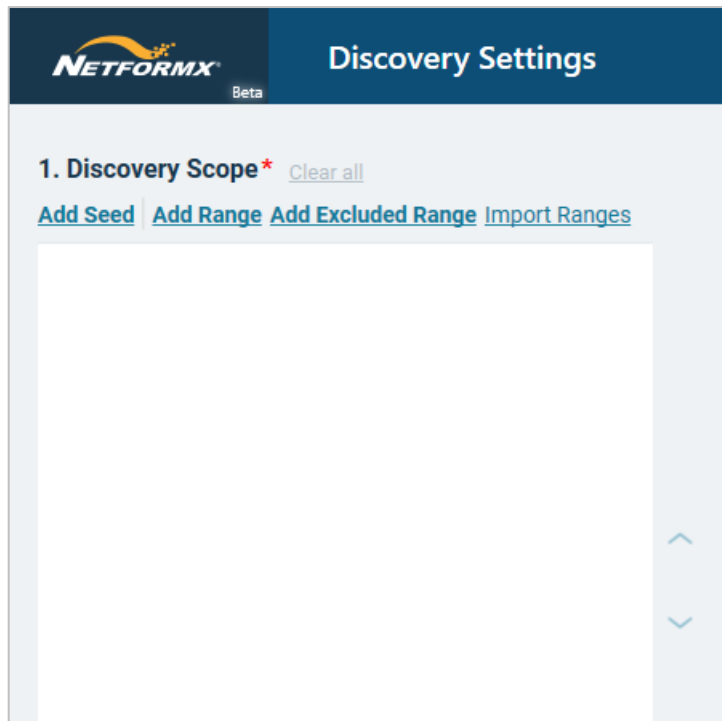


Figure 5: Discovery Scope User Interface

Add Seed

Select **Add Seed** to define the Discovery launch point for the customer environment.

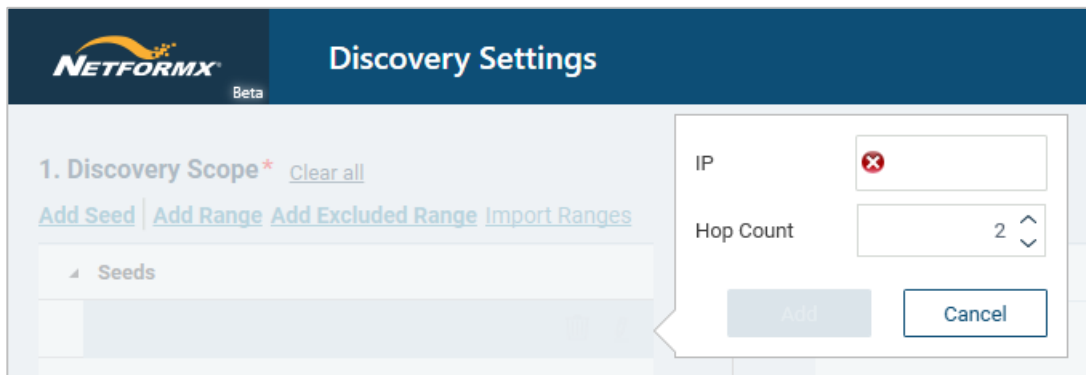






Figure 6: Setting the Seed Router

1. **IP:** This is the seed router IP address starting point for the SNMP network walk.
2. **Hop Count:** Enter the maximum number of hops you want to extend from the seed router to include in the network walk. For example:
 - a. A **0** Hop count discovers the seed router and all devices immediately adjacent to the seed router.
 - b. A **2** Hop count discovers everything up to two routers away from the seed router.
3. Press the **Add** button to save the defined seed router.
4. If required, you can add multiple Discovery seed routers– Please note: Each seed router should belong to an isolated network. Overlapping between seed routers and hop counts may produce incorrect discovery results.
5. To **remove any seed** from the list, **select the listed item** and **click the remove button.** 
6. To **edit any seed** from the list, **select the listed item** and **click the edit button.** 
7. To **change the order of any seed**, use the  and  buttons.

Add Range

You can configure a complete Discovery to include additional IP elements, ranges, addresses, and subnets outside the originating seed router hop count. The previous diagram labels these as an included subnet and included devices.

To define and configure other elements, select **Add Range**:

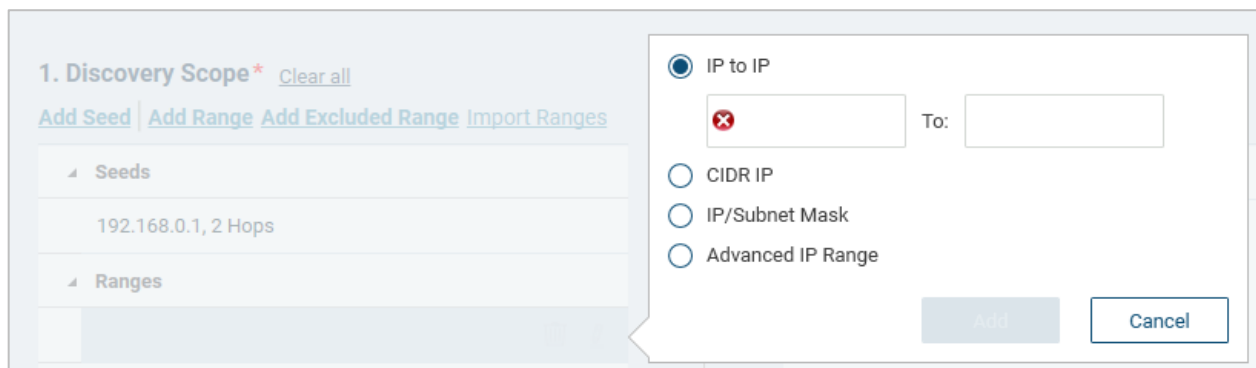
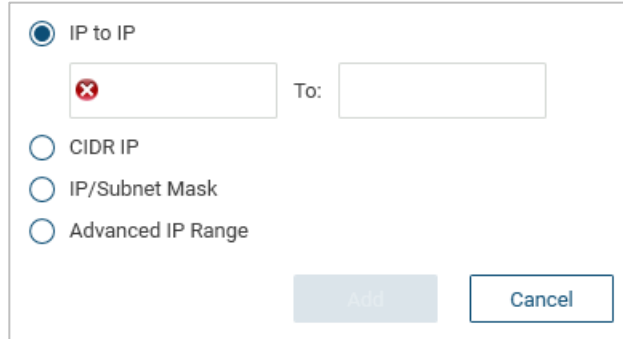


Figure 7: Defining the IP Range

The **Add Range** includes four options.

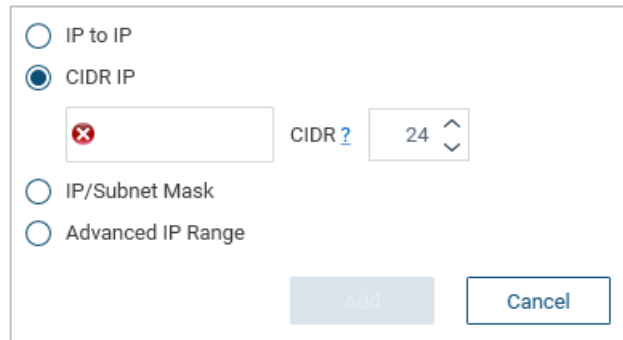
FIRST: IP to IP: Define a contiguous IP range.



The screenshot shows a dialog box with four radio button options: 'IP to IP' (selected), 'CIDR IP', 'IP/Subnet Mask', and 'Advanced IP Range'. Below the options are two input fields: the first contains a red 'X' and is followed by the text 'To:', and the second is empty. At the bottom right are 'Add' and 'Cancel' buttons.

Figure 8: Defining a From-To IP Range

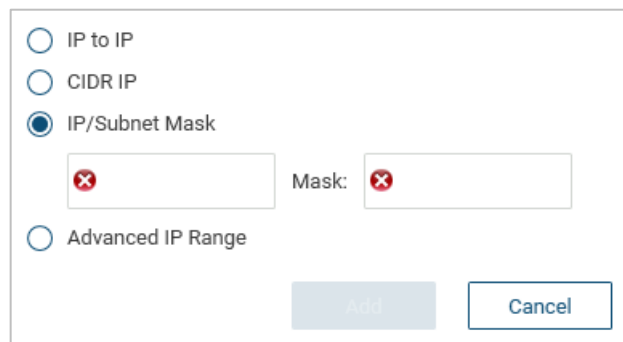
SECOND: CIDR IP: Define a range using the IP address and Network Prefix.



The screenshot shows the same dialog box, but 'CIDR IP' is selected. The first input field contains a red 'X', followed by the text 'CIDR ?'. To its right is a spinner control showing the value '24'. The 'Add' and 'Cancel' buttons are at the bottom right.

Figure 9: Defining a CIDR-based IP Range

THIRD: IP/Subnet Mask: Define a range using the IP Address and Network Mask.



The screenshot shows the same dialog box, but 'IP/Subnet Mask' is selected. The first input field contains a red 'X', followed by the text 'Mask:'. To its right is another input field containing a red 'X'. The 'Add' and 'Cancel' buttons are at the bottom right.

Figure 10: Defining a Subnet Mask IP Range

FOURTH: Advanced IP Range: Define the IP range using short-cut notation.

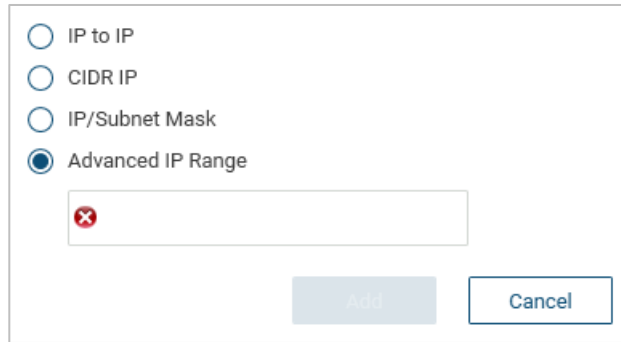






Figure 11: Advanced IP Range Definitions

For example, you would use this exact terminology **10.10.[1-5].[20-22]** inside the **Advanced IP Range** to define this detailed list of consecutive IP devices to include in the network walk:

10.10.10.20
10.10.10.21
10.10.10.22
10.10.11.20
10.10.11.21
10.10.11.22
...
10.10.15.20
10.10.15.21
10.10.15.22

1. To **remove a range** from the list, **select the listed item**, and **click the remove button**. 
2. To **edit a range** from the list, **select the listed item** and **click the edit button**. 
3. To **change the range order** from the list, use the  and  buttons.

Add Excluded Range

Use the **Add Excluded Range** option to avoid addresses/subnets within the defined **Add Seed** hop count or from the **Add Range** list of Addresses/Subnets. The **Add Excluded Range** interface uses the same set of configuration options as the **Add Range** operation.

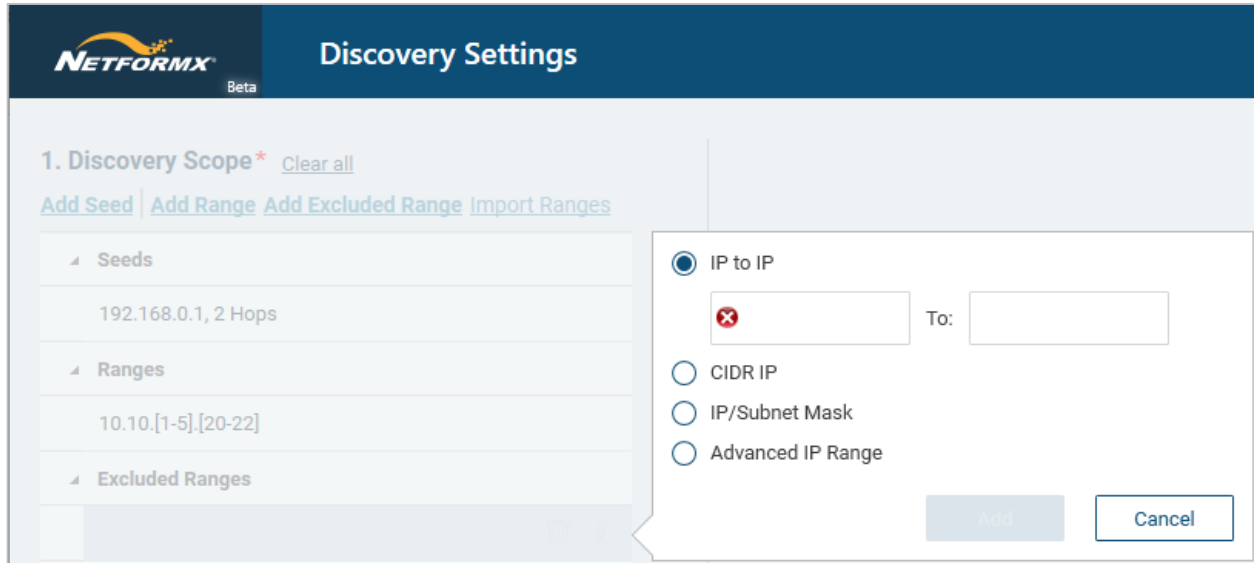


Figure 12: Controlling IP Ranges via Exclusions

Import Ranges

The **Import Ranges** allows you to transfer IP details contained in spreadsheets (XLS) or comma-separated value (CSV) text files into the scope.

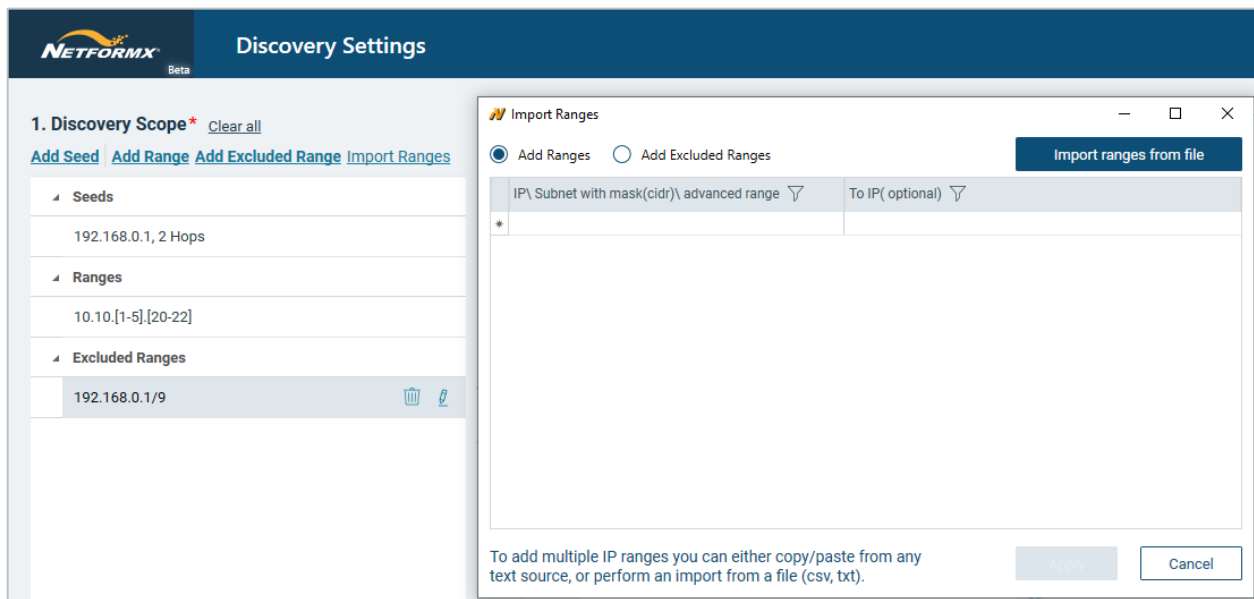


Figure 13: Importing IP Ranges

The UI follows a precise import methodology, as shown below. You can also cut & paste the information into the **Import Range** interface, or you can use the built-in **Add Range** and **Add Excluded Range** to modify your address structures further.

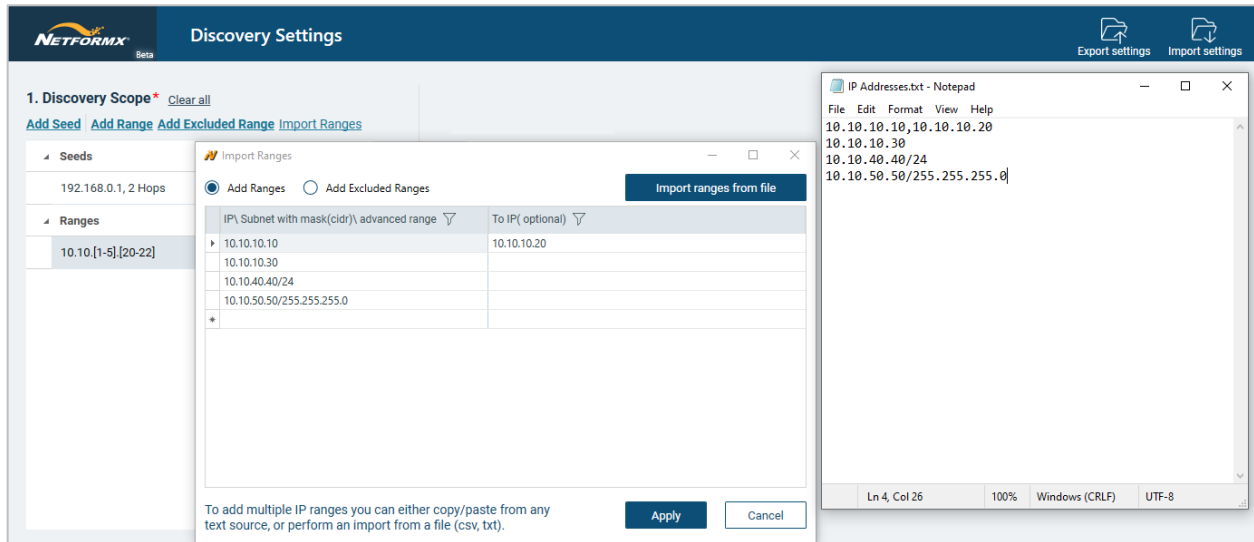


Figure 14: Import IP Range Examples

Step 2: Define SNMP Variables

Add SNMP Credentials

Netformx Discovery uses SNMP to collect device-level details, which requires you to program the SNMP read-only community strings into the Discovery UI to communicate with the installed network elements. Netformx Discovery supports three SNMPv1, SNMPv2c, and SNMPv3 implementation options.

Select **Add SNMP Credentials** to trigger the user interface. SNMPv1 & SNMPv2c present the same configuration options, as shown below. Enter each Community read-only string as deployed throughout the user’s environment.

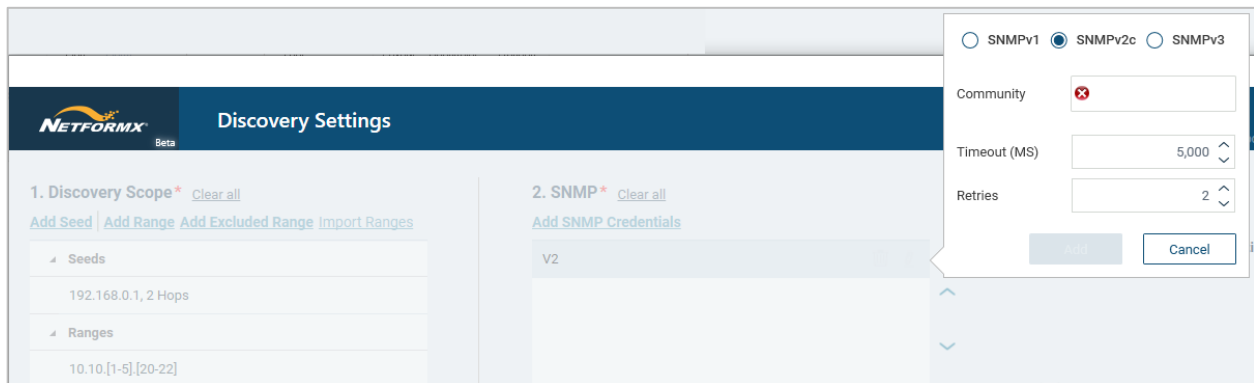


Figure 15: Defining SNMPv1/v2c Settings

Netformx Discovery SNMPv3 interface is slightly different as it needs to support the protocol's v3 security options.

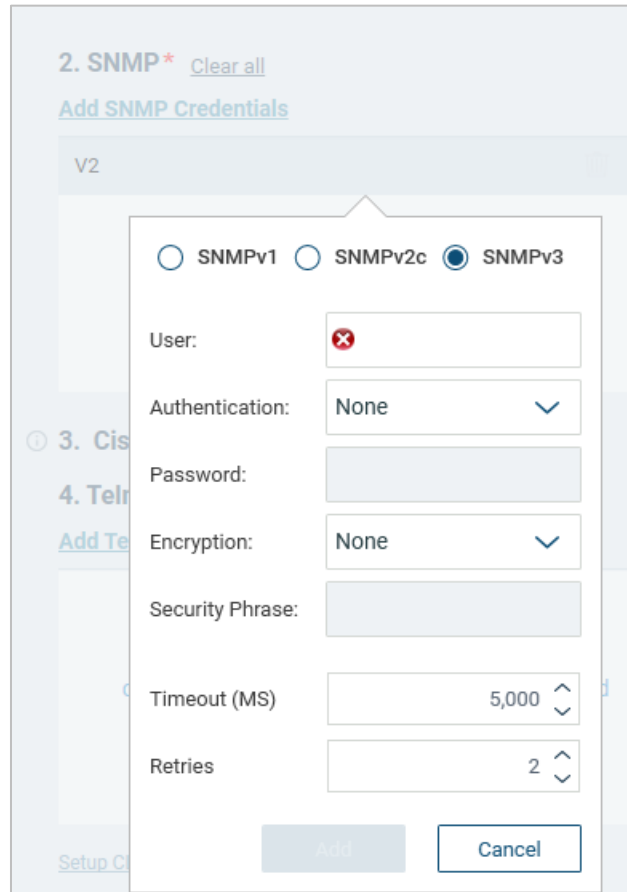






Figure 16: Defining SNMPv3 Settings

- User: Enter the authorized SNMPv3 User ID
- Authentication: Discovery supports SHA or MD5 methodology
- Password: Enter the correlating user password
- Encryption: Discovery supports DES, AES128, AES192, AES256, or 3DES
- Security Phrase: Enter the relevant Security Phrase

Depending on the networking environment, you might need to adjust the Timeout and Retries settings.





- To **remove credentials** from the list, **select the listed item** and **click the remove button.** 
- To **edit credentials** from the list, **select the listed item** and **click the edit button.** 
- To **change the order of credentials** from the list, **use the**  **and**  **buttons.**

Step 3: Telnet/SSH Credentials

Add Telnet/SSH Credentials

Use **Add Telnet/SSH Credentials** to input device login access used throughout the target environment. For each active selection (Telnet or SSH), define the associated Username, Password, and Enable password, as shown in the UI below.

Figure 17: Defining Telnet/SSH Settings

- To **remove credentials** from the list, **select the listed item** and **click the remove button.** 
- To **edit credentials** from the list, **select the listed item** and **click the edit button.** 
- To **change the order of credentials** from the list, **use the**  **and**  **buttons.**

Number of Concurrent CLI Sessions

Take care when adjusting the default value (5). Setting a too large value for here competes with the other 'retry settings' enabled throughout the remainder of the UI and can result in unexpected errors or odd results. Netformx recommends keeping the number of concurrent CLI Sessions balanced (lower) when using larger retry values in the other type of simultaneous (PING, SNMP, HTTP) settings.

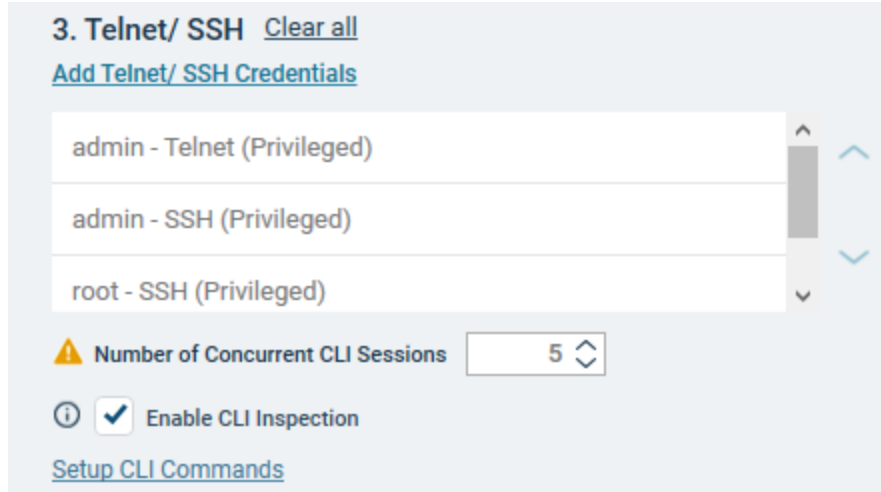


Figure 18: Concurrent CLI Sessions & CLI Inspection

CLI Inspection

Enabling CLI Inspection can improve Discovery accuracy for networking environments containing Cisco, Juniper, Palo Alto Networks, Dell, Fortinet, VMWare, and 3COM/H3C equipment. **Enable CLI Inspection** increases the time it takes to walk and interrogate all the discovered nodes. With Telnet /SSH credentials defined, you can enable the CLI Inspection feature.

The V21.x engine uses predefined vendor templates to extract details. Each template contains a set of matching criteria, including an SNMP System Object ID prefix, a regular expression for SSH Version value, a regular expression for banner value, or a representing CLI-command. Each template contains a list of CLI commands to invoke.

When enabled (checked), the engine

- Attempts to find a matching template based on the SNMP system object ID value for the discovered node to select it
- Otherwise, the engine attempts to connect to the discovered node using user-defined Telnet\ SSH credentials. If it connects, the logic determines the matching template of the discovered node using SSH Version or banner and selects it.
- Otherwise, the engine applies smart '?' logic to leverage the representing command related to the template. Once reached, it invokes. The engine verifies the response and selects it if matched.
- Once the template is selected, the engine invokes all its commands.

See the list of templates with their criteria in the table below.

Vendor	Family	System Object IDs	SSH Version Criteria	First response (banner Criteria)	Representing CLI command	Match Criteria for response
Cisco		1.3.6.1.4.1.9.	Has Cisco sub word		show version	Starts with Cisco Regex: "Cisco(\s)+"
Juniper		1.3.6.1.4.1.2636.		Contains JUNOS Regex: "(\\s)+JUNOS(\\s)+"		
Palo Alto		1.3.6.1.4.1.25461.			show system info	Contains MAC address with mac-address key and check if it is Palo Alto
Fortinet		1.3.6.1.4.1.12356.			get system status	Contains Version: Forti Regex "Version:(\\s)+Forti"
VMWare	ESXi	1.3.6.1.4.1.6876.		Regex: \\s+ESXi shell\\s+(. \\n \\r)+www\\.vmware\\.com\\Vgo\\sysadmintools		
3com/H3C		1.3.6.1.4.1.43./ 1.3.6.1.4.1.25506.			display device manuinfo	Identify MAC Address and check if it is 3COM EUROPE LTD Regex: MAC_ADDRESS(\\s)*:(\\s)*(?<mac>[A-Z0-9-]+)
Dell	Switch	1.3.6.1.4.1.674.10895.			show version	Identify MAC Address and check if it is Dell Regex: "Burned In MAC Address.(\\s)*(\\s)*(?<mac>[A-Z0-9-]+)
Dell	PowerEdge	1.3.6.1.4.1.674.10892.			getsysinfo	Identify Mac Address and check if it is Dell

Figure 19: CLI Inspection Logic

Setup CLI Commands

Figure 20: Defining Custom CLI Commands

V21x introduces changes to the ability to customize CLI calls. Trigger the **Setup CLI Commands** to open the updated user interface.

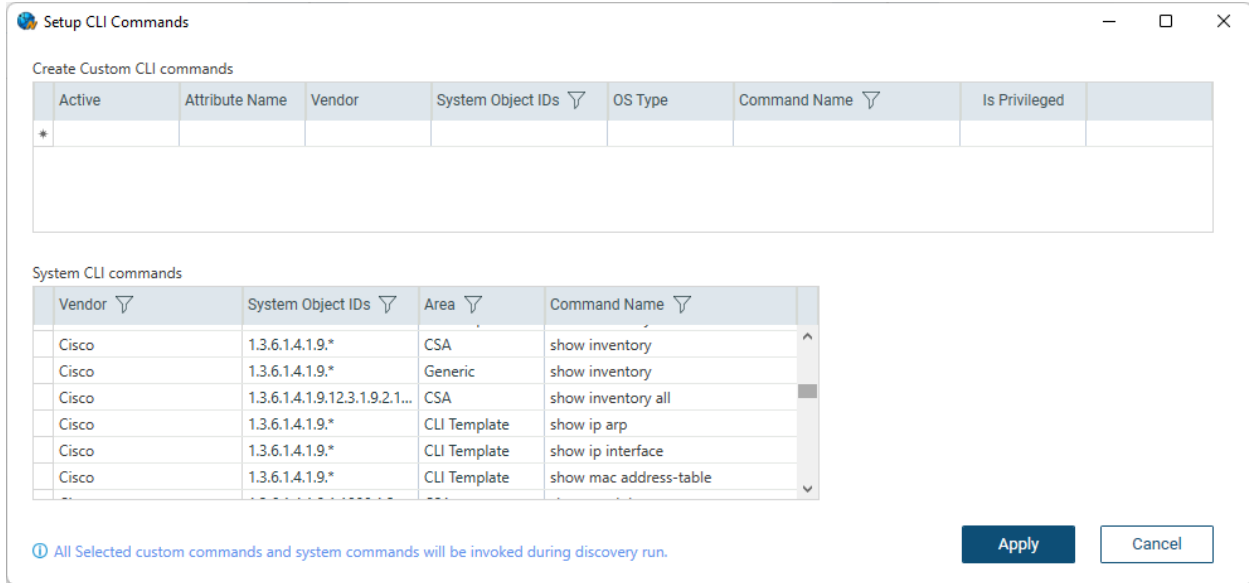


Figure 21: Setup CLI Commands UI

'Vendor,' System Object IDs, Area, and Command Name columns are added to the System CLI Command grid, as shown in Figure 21.

The possible values for the Area field are

- **CSA** (command output tied to CSA)
- **NTT** (command output for NTT)
- **CLI Template** (if the command is a part of CLI template)
- **General** (show inventory, show version, and show diag commands defined in CLICOMMANDS.XML invoked for Cisco equipment)

With the Discovery default set to interact with CSA via the Collect option, the following CLI commands execute for every device uncovered during the network walk:

- show c7200
- show chassis eeprom
- show config
- show diag
- show diag chassis
- show gsr chassis-info
- show hardware
- show IDPROM all
- show inventory
- show inventory all
- show module
- show rsp chassis-info
- show running-config
- show version

If you disable the CSA **Collect** option, the following CLI commands execute:

- Show diag
- Show inventory
- Show version

Using **Setup CLI Commands** allows you to define and execute **Cisco-only CLI calls** and capture the output. After the run and following importing the results into your DesignXpert Project, you can view the captured data for each element from its Device Properties page under the AutoDisc group.

Take care in defining custom CLI commands. It would be best to understand CLI implementation, SNMP OID structures, or knowledge with various OS Types and Vendor-specific calls.

In the example shown below, we turned off CSA Collection and added the SNMP show config command. The matching OID appears (1.3.6.1.4.1.) labeled 'Running Config' and will execute any device responding to SNMP. You can further limit the devices responding by adding Vendor or OS Type characteristics to the SNMP call.

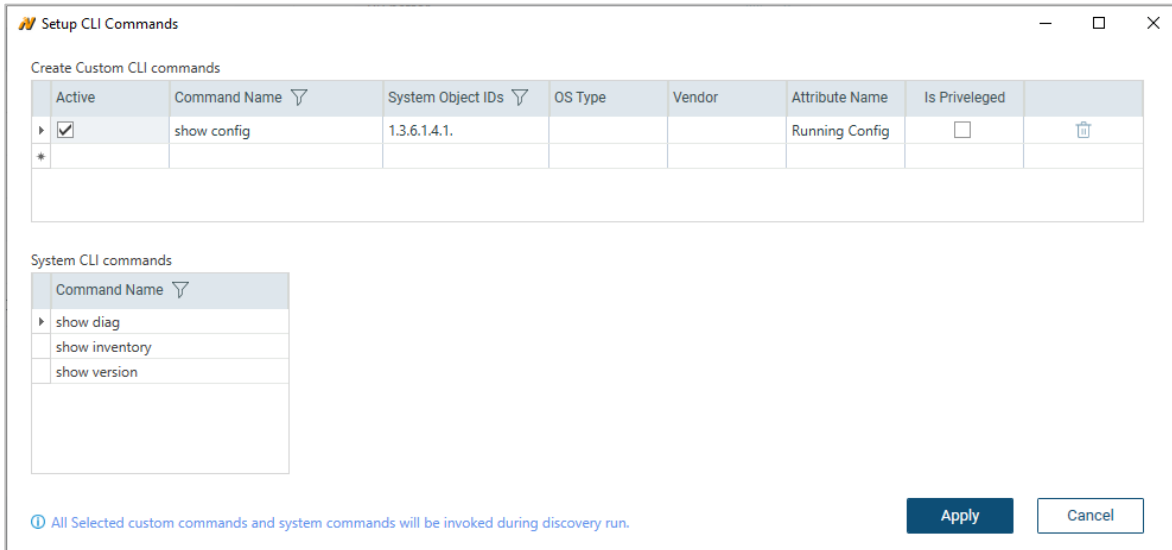


Figure 22: Custom CLI Command Example

Save CLI Output to

Enable the **Save CLI Output to** option to indicate your desire to store the captured CLI data in a folder location of your choice.

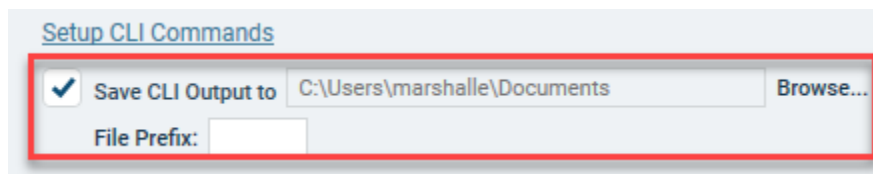


Figure 23: Saving CLI Command Output

Click the **Browse** option to expose your desired folder storage path and location. Each CLI call creates a subfolder according to its command name and contains every responding IP device's results.

Step 4: Collect Cisco Smart Advisor Data

The Discovery engine assumes your desire to interact with the Cisco Smart Advisor (CSA) portal to report on meaningful details associated with the discovered Cisco devices by enabling the Collect option by default, as shown below.

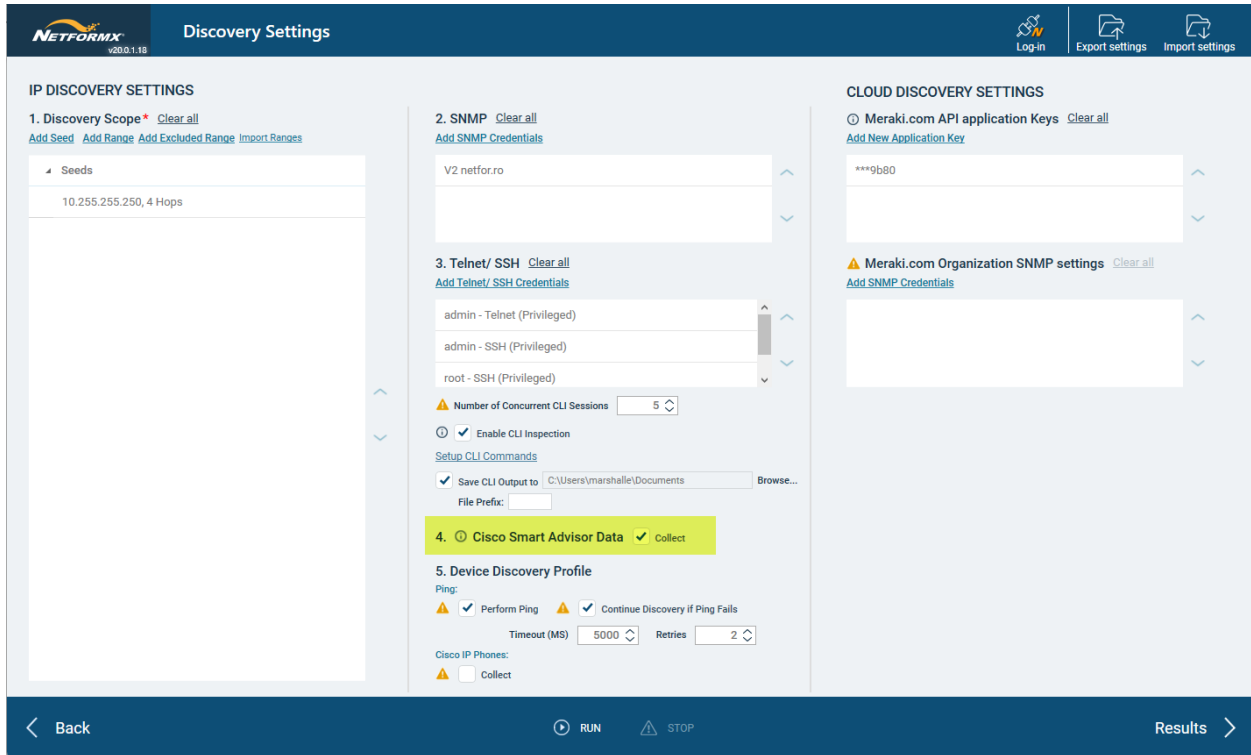
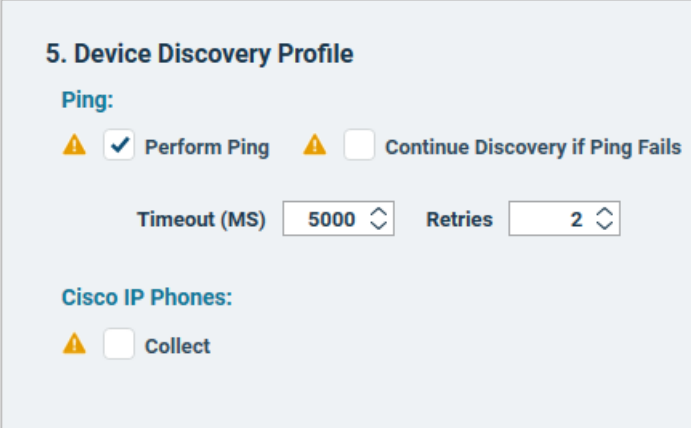


Figure 24: Default Cisco Smart Advisor CSA Setting

The Discovery engine combines SNMP and Telnet/SSH calls to collect all the required raw data for CSA analysis. Enabling CSA necessitates you to define all the Telnet/SSH credentials used throughout the customer's network.

Step 5: Device Discovery Profile

Ping



5. Device Discovery Profile

Ping:

Perform Ping Continue Discovery if Ping Fails

Timeout (MS) Retries

Cisco IP Phones:

Collect

Figure 25: Device Discovery Profile Settings

You must understand how the security policy used throughout the customer's networking environment impacts Netformx Discovery and its ability to uncover device attributes. The Device Discovery Profile allows you to adjust Netformx Discovery to accommodate when the IT department disables ICMP (Ping).

- **Perform Ping (Enabled by Default):** To reduce Discovery runtimes, Perform Ping checks every device throughout the defined IP range(s). When a device responds, Netformx Discovery marks the IP address as active, making it easier to know which addresses to query using the additional calls (SNMP, Telnet/SSH, & HTTP if Collecting Cisco IP Phone) required to gather details. However, when an IP address fails to respond to Ping, Discovery marks the IP address inactive and makes no further calls to the Address.
- **Continue Discovery if Ping Fails:** When enabled, Netformx Discovery continues to query *IP addresses marked inactive from above* in the defined range(s) using SNMP, Telnet/SSH, and HTTP (for Cisco IP Phones) in an attempt to collect device details. It is vital to understand that selecting this option increases the network walk running time due to the additional calls caused by the number of defined SNMP community strings and Telnet/SSH credentials used throughout the environment. If you have many devices, community strings, and Telnet/SSH credentials, you might need to increase the Timeout control and Retries value accordingly.

Cisco IP Phones

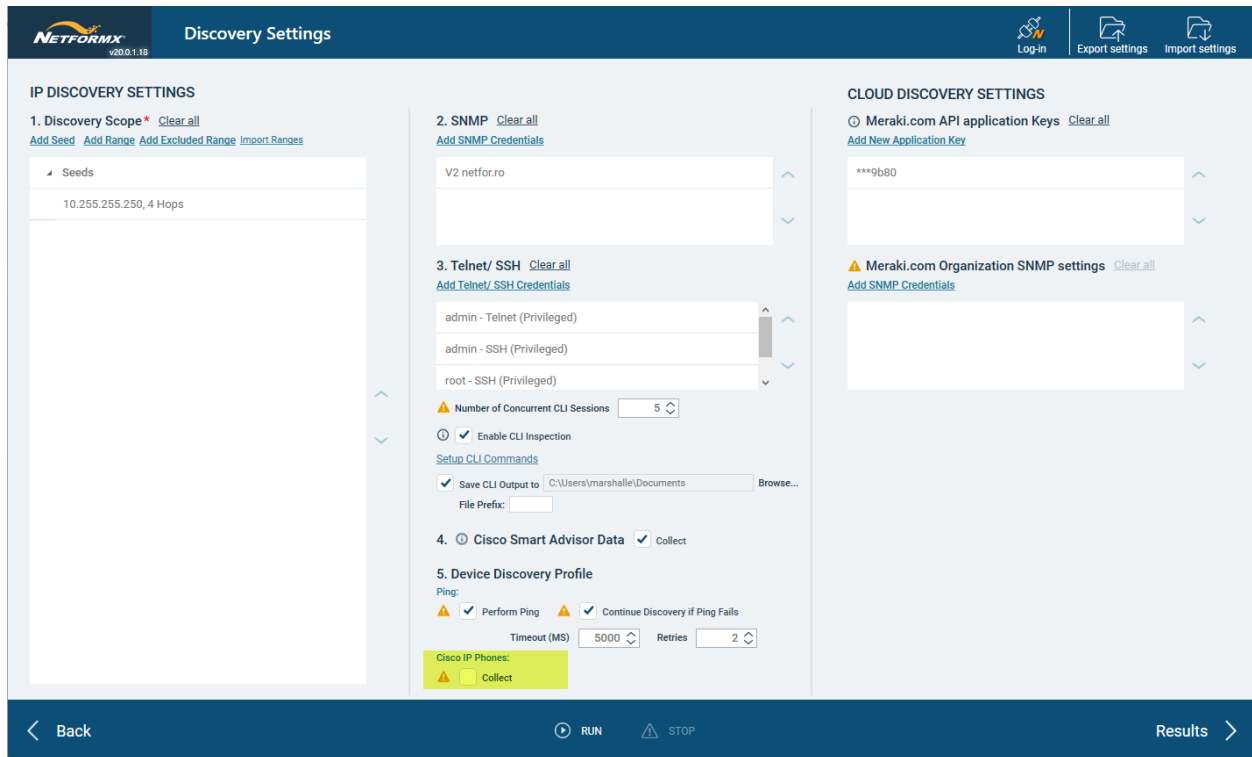


Figure 26: Collecting Cisco IP Phone Details

Enabling **Cisco IP Phones Collect** tells the application to find Cisco IP Phones and to retrieve their configuration. This option allows for HTTP to retrieve the Cisco IP Phone configuration file for each identified Cisco phone. The phone analysis includes the Cisco Model Number, MAC Address, Serial Number, Host Name, SysDesc, IP Address, and Subnet Mask. When disabled, any Cisco IP Phone found during the network walk appears with a generic IP phone icon on the canvas with no additional details supplied. Please note – enabling the collection of Cisco IP Phone details will increase the Discovery runtime due to the extra calls made to collect the relevant information.

Configuring Meraki Discovery

Understanding the Meraki.com Data Sources

The Meraki REST API provides the best access for the v21.x Discovery engine to collect Meraki equipment attributes like Product SKU, Serial Number, System Name, Connectivity Links (via CDP & LLDP), Product Licenses, etc., during the network walk.

Netformx recommends configuring the Meraki REST APIs to walk the Meraki equipment to extract and leverage the equipment configuration details stored inside the Meraki Cloud.

Please note: Using the typical Netformx SNMP calls to the Meraki equipment will not work. If you cannot access the REST APIs and need to use SNMP, you must configure the Meraki.com Organization SNMP

setting UI. However, using the Meraki.com domain definition and organizational SNMP settings results in a limited collection of attributes, including Product SKU, Serial Number, and System Name.

Meraki Cloud Discovery Settings

Following the Netformx recommendation with access to the REST API Application Key, use the Add New Application Key to open the configuration interface.

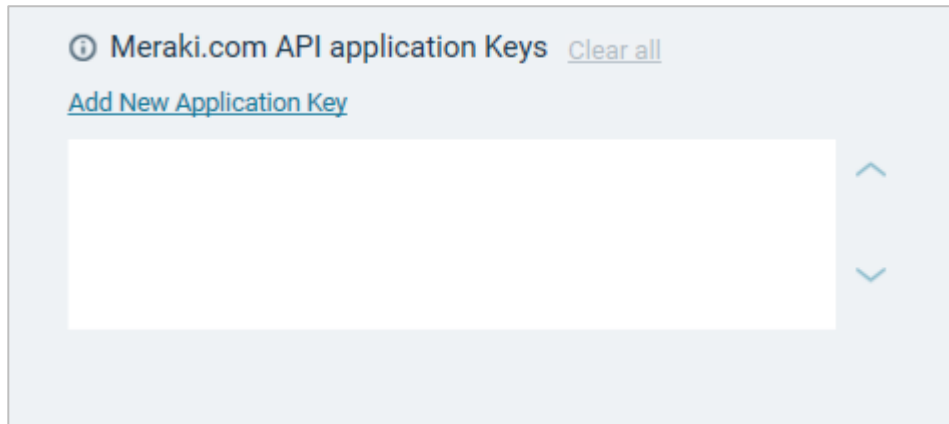


Figure 27: Meraki.com API Application Key Control

Triggering the 'Add New Application Key' opens the UI

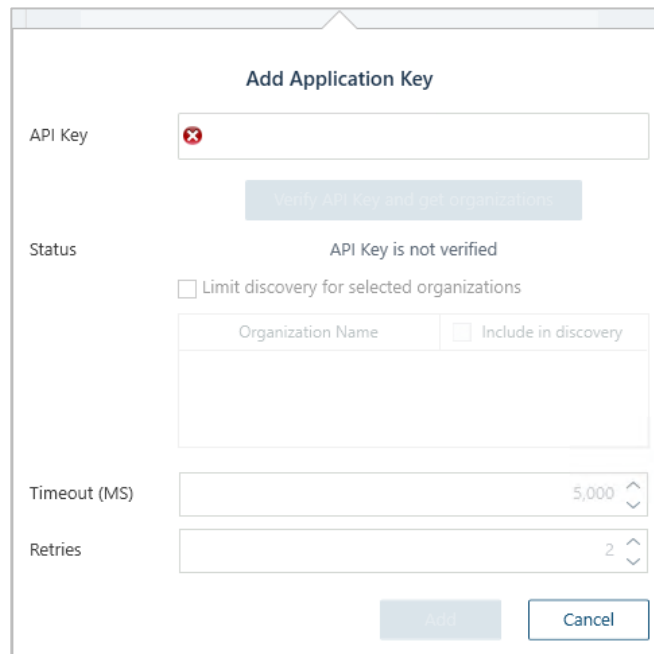


Figure 28: Add Application Key

Generating or Accessing the Meraki REST API Key

The end-customer IT manager or the incumbent Meraki sales Partner should provide you with a copy of their REST API Key. You find the REST API Key inside the Meraki Dashboard. Log in to the Meraki Dashboard (https://account.meraki.com/login/dashboard_login?go=%2F). Depending upon your login access, you might see a choice of Organizations. Be sure to select the organization that aligns with the end-customer environment. The Netformx Meraki Dashboard provides access to three Organizations.

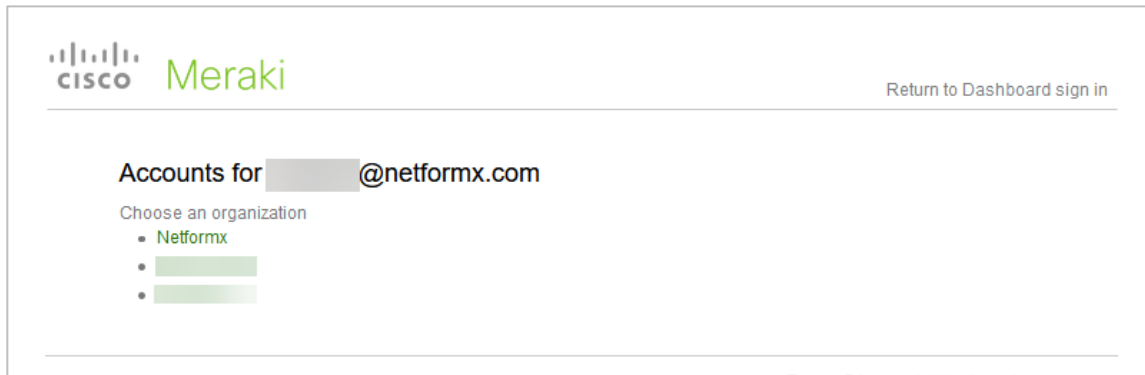


Figure 29: Meraki Dashboard Organizations

We will use the Netformx Organization for this walkthrough. Selecting the organization opens the Meraki Dashboard landing page. Assuming the IT Manager or Incumbent Partner has not provided you with an Application Key, you will need to create it if one does not exist. Application Key details appear inside the “My Profile” sub-menu. Locate your user name along the upper-right and click the dropdown to open the “My Profile” UI.

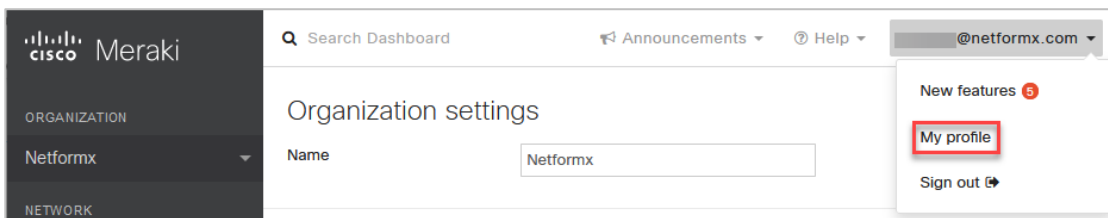


Figure 30: Exposing Meraki My Profile

Scroll down inside the My Profile UI to find the API Access. Click the Generate new API Key and copy the displayed value

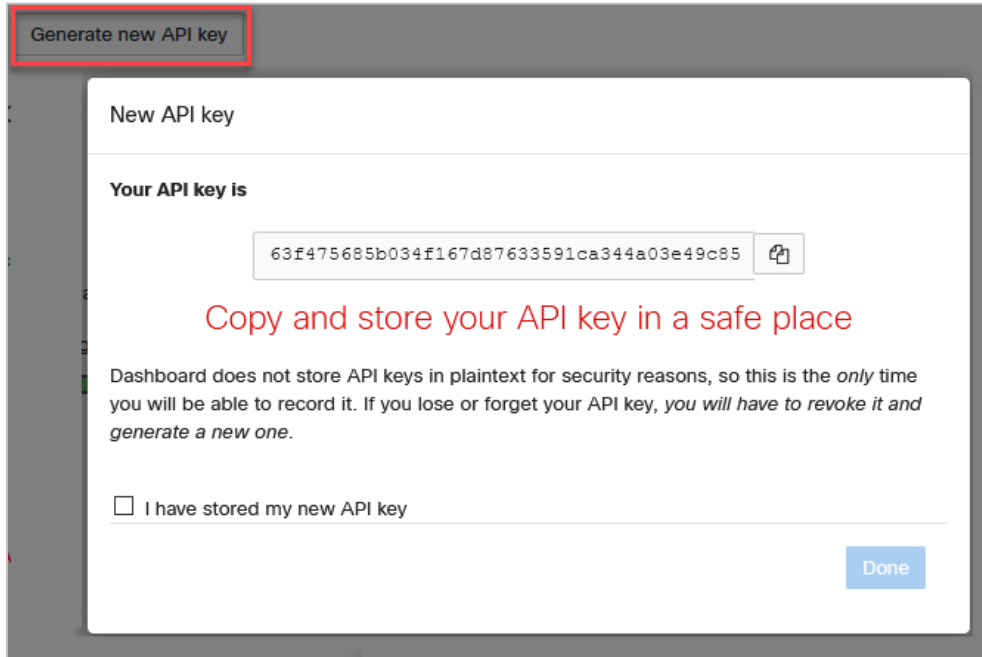


Figure 31: Generating REST API Access Key

Copy, paste, and verify the Application Key into the v20 Add Application Key UI

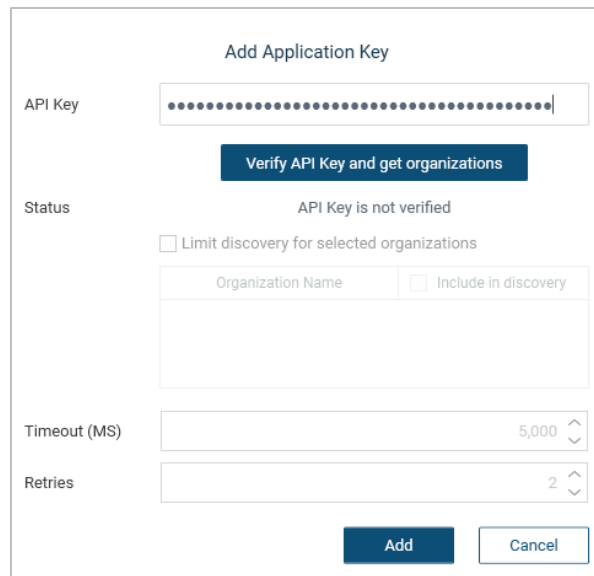


Figure 32: Paste & Verify the Application Key

Verify the API Key and get organizations runs a validation check against the Meraki Dashboard. Depending upon access, it might return a list of other Organizations associated with the user profile.

The screenshot shows a configuration form titled "Add Application Key". It includes an "API Key" field with a masked input, a "Verify API Key and get organizations" button, and a "Status" field showing "Verified". Below this is a checkbox labeled "Limit discovery for selected organizations" which is checked. A table lists organizations with columns for "Organization Name" and "Include in discovery". The "Netformx" organization is highlighted, and its "Include in discovery" checkbox is checked. A green arrow points to this checkbox. At the bottom, there are "Add" and "Cancel" buttons.

Organization Name	Include in discovery
[Redacted]	<input type="checkbox"/>
[Redacted]	<input type="checkbox"/>
Netformx	<input checked="" type="checkbox"/>

Figure 33: Post Verification

If the verification process returns multiple organizations, enable the option '**Limit discovery for selected organizations**' and select the organization(s) that match the scope of the Discovery to the end-customer environment to include in the Discovery walk. Our example set the Netformx Organization.

Meraki SNMP Cloud Settings – Optional

Netformx does not recommend using the Meraki SNMP Cloud Settings given Meraki SNMP responses provide attribute details limited to Product SKU, Serial Number, and Product Name (if configured). However, if you do not have access to the Application Key and still want to include basic details about the Meraki equipment installed in the customer’s environment, you will need the Meraki Cloud SNMP Settings available from the “My Profile” sub-menu.

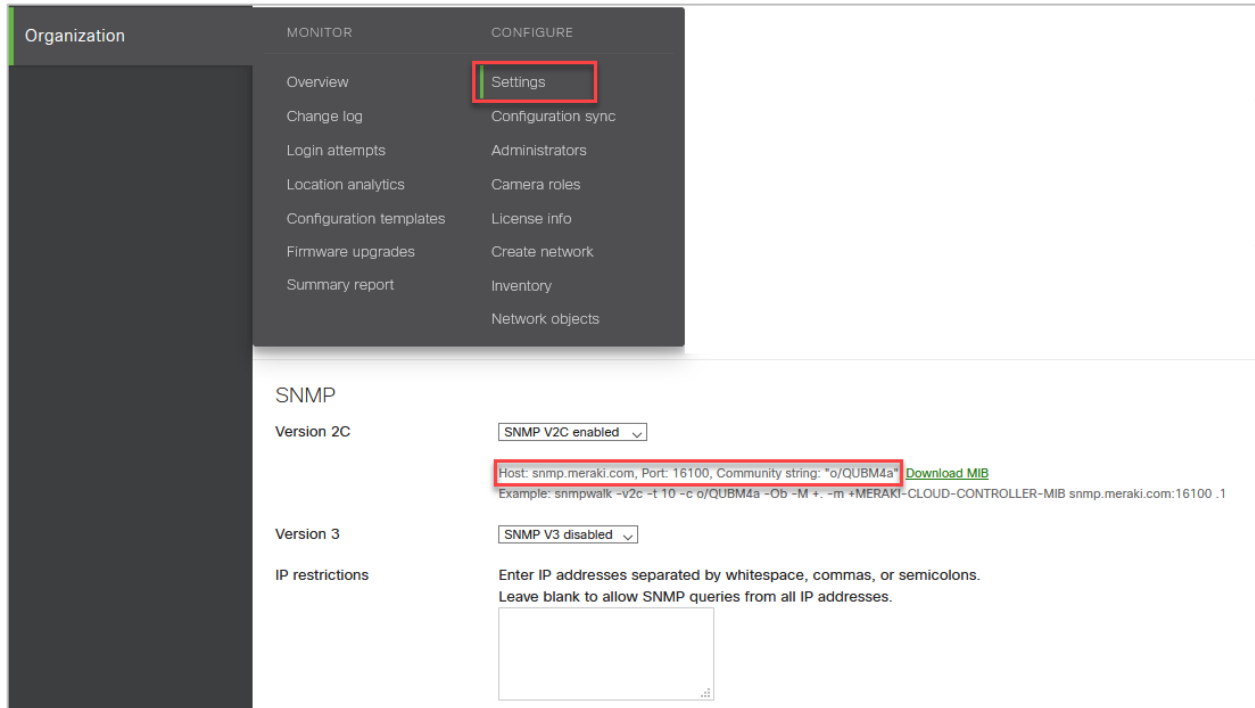


Figure 34: Meraki Cloud SNMP Settings

Click ‘Add SNMP Credentials’ inside the Meraki.com Organization Settings window to input the values described from the Meraki Organization Dashboard noted above and click ‘Add’ to complete the operation. The Meraki Hostname and Port details appear by default.

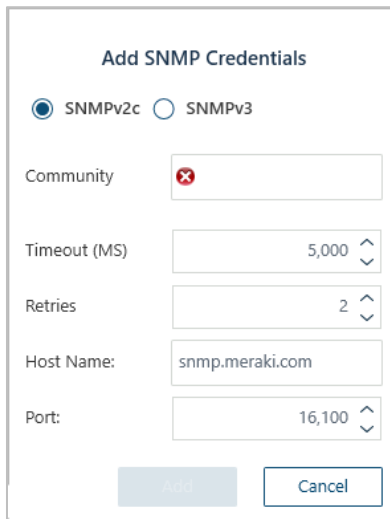


Figure 35: Add Meraki SNMP Credentials

Run Network Discovery

Once you complete all the required and desired Discovery settings for the customer environment, click the 'Run' button to commence the network walk.

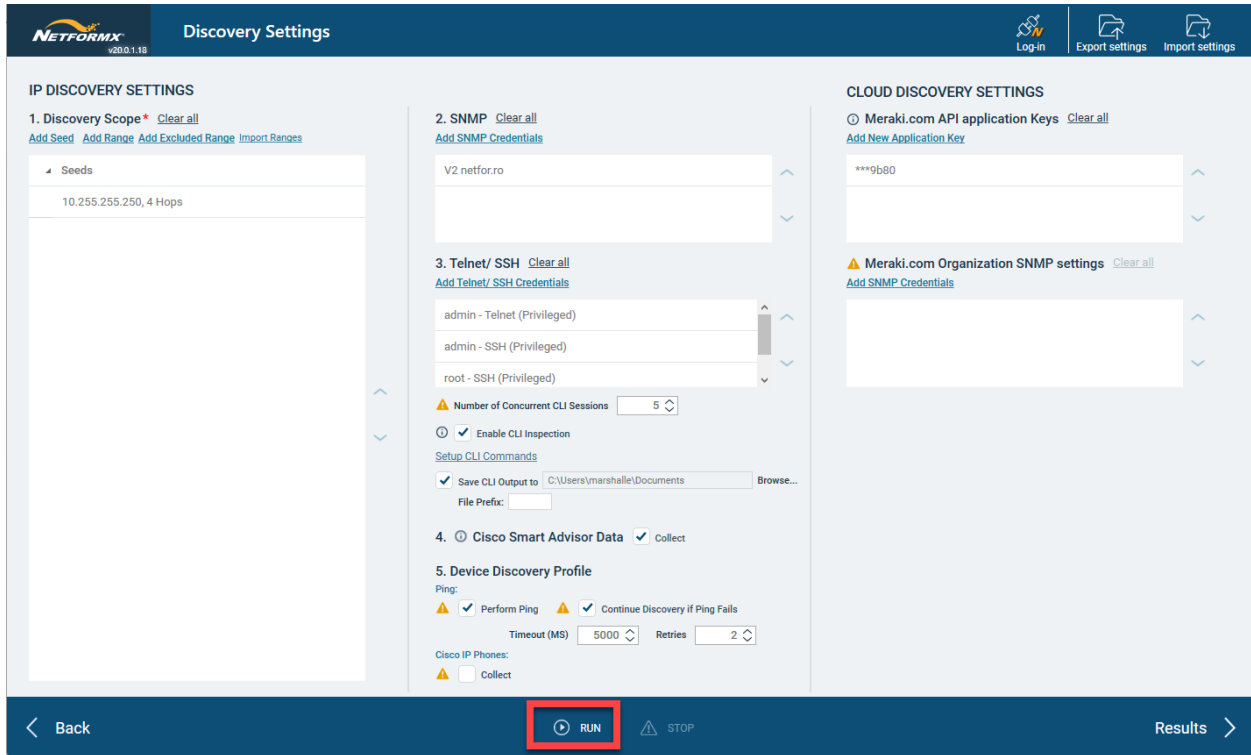


Figure 36: Run a Network Discovery

Upon commencement of the Discovery, your view changes to the **Netformx Discovery Results** interface, and you can track, in real-time, all the calls transacting to devices identified throughout the networking environment.

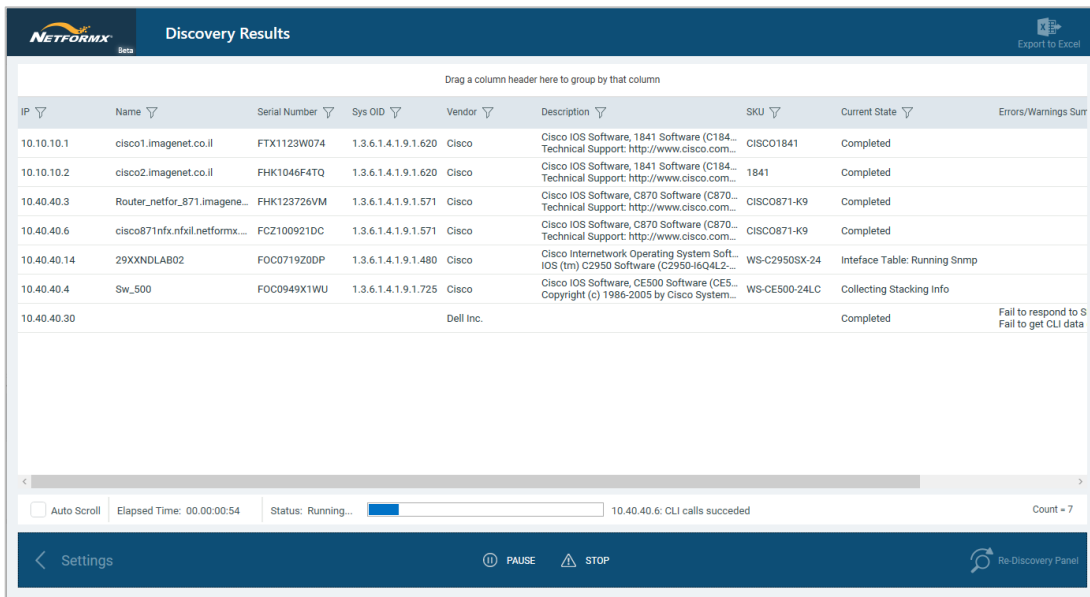


Figure 37: Discovery Run in Progress

As the process walks the customer environment, new devices appear in this display as the application receives their responses. The UI tracks the entire discovery operation, displays the responding IP addresses, maintains a running device total (bottom right corner), tracks elapsed running time (bottom left corner), and provides you with high-level characteristics from responding devices. The UI displays IP, Name, Serial Number, Sys OID, Vendor, SKU, Current State, and any associated error messages.

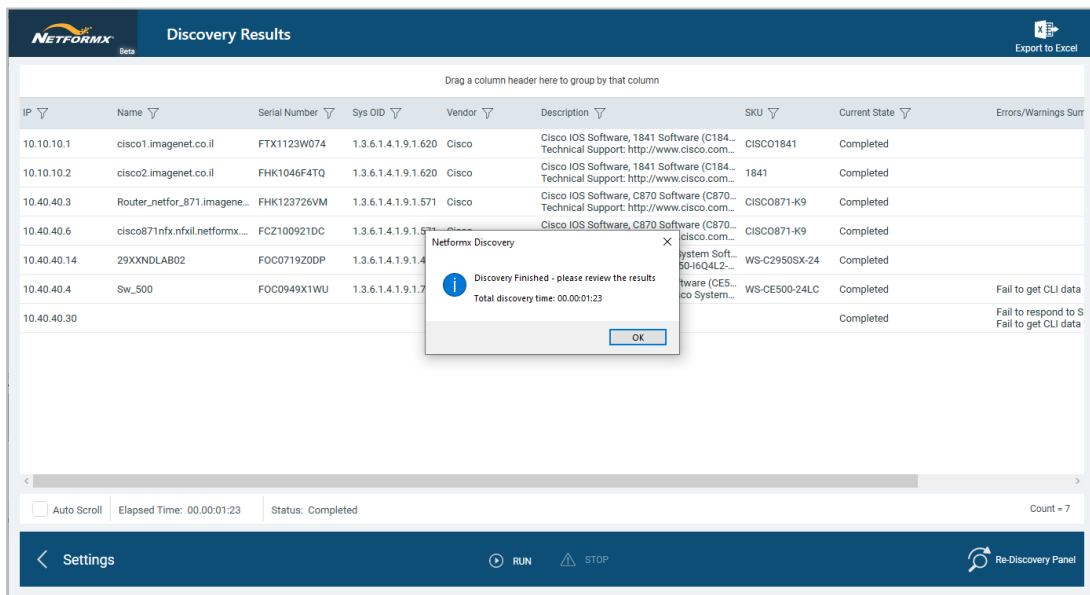


Figure 38: Completed Discovery Run

Updated Discovery Results Window

The inclusion of the Meraki Cloud products required a modification to the Discovery Results interface. The window contains three tabs: IP Discovered Networks, Cloud Managed Devices, and Log Messages.

IP Discovered Networks

The first tab shown in the figure below, IP Discovered Networks, displays all the networking devices uncovered from the basic Discovery settings found during the SNMP walk.

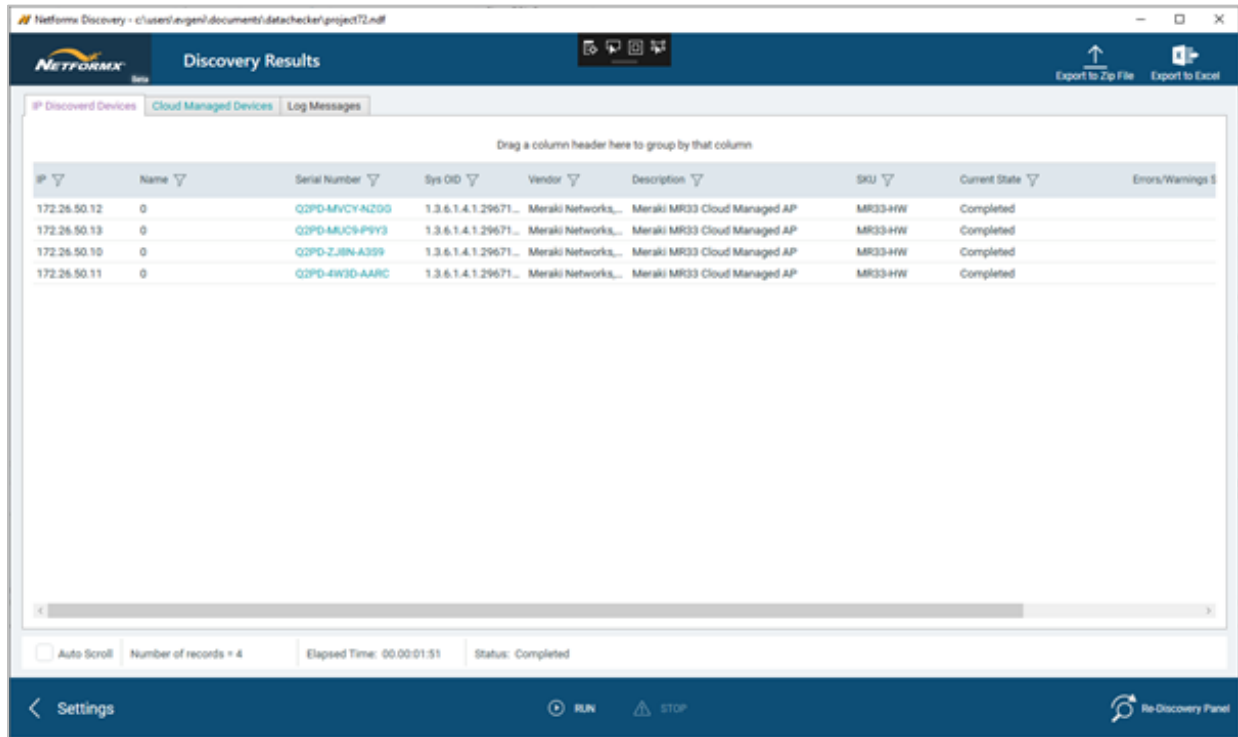


Figure 39: Discovery Results – IP Discovered Devices

Cloud Managed Devices

The second tab, Cloud Managed Devices, displays all nodes discovered using Cloud Discovery settings.

Organization	Network	MAC Address	Name	Serial Number	SKU	LAN IP	Status	Last Update Time	Matching Method	Organization License Stat
orchestra	Orchestra WiFi	e0cb5c4a9812		Q2PD-4W3D-4A8C	MR33-HW	192.168.0.22	online	2021-03-11T12:28:21...	Matched by MAC	OK
orchestra	Orchestra WiFi	e0cb5c494824		Serial number of discovered node at 172.25.50.11 was updated by this value 'Q2PD-4W3D-4A8C' 12742...					Matched by MAC	OK
orchestra	Orchestra WiFi	e0cb5c494842		Q2PD-4W3D-4A8C	MR33-HW	192.168.0.13	online	2021-03-11T12:28:07...	Matched by MAC	OK
orchestra	Orchestra WiFi	e0cb5c4a3f34		Q2PD-2J6N-A359	MR33-HW	192.168.0.21	online	2021-03-11T12:27:59...	Matched by MAC	OK
Rohi Toulouse	London - Home	683a1e2564ae	Lon MX	Q2KY-945L-UXCH	MX68-HW		online	2021-03-11T12:27:59...		OK
Rohi Toulouse	London - Home	9818884101c7	London Home M...	Q2LD-83T5-C8YC	MR52-HW	192.168.128.4	online	2021-03-11T12:28:21...		OK
Rohi Toulouse	IL home	e0553d8b0970		Q2MH-L32V-Z2CB	MX64W-HW		online	2021-03-11T12:28:04...		OK
Rohi Toulouse	IL home	0c8d8bc40506	mr33	Q2PD-5MMT-N298	MR33-HW	192.168.128.2	online	2021-03-11T12:28:35...		OK
Rohi Toulouse	Danny Home	e0cb5c5b7e416	Danny MR20	Q2XD-8YXE-A0LU	MR20-HW	10.100.102.2	online	2021-03-11T12:28:18...		OK

Figure 40: Discovery Results - Cloud Managed Devices

The v21 engine reports the following Cloud Managed attributes

- Organization
- Network
- MAC Address
- Name (if configured by IT Manager)
- Serial Number
- SKU
- LAN IP Address (provided by REST API only)
- Status (online/offline – Provided by REST API only)
 - Online = discovered node turned on when invoking API request
 - Offline = discovered node turned off when invoking the API request
- Last Update Time (provided by REST API only)
- Matching Method (empty/Matched by MAC/Matched by IP)
- Organization License Status (provided by REST API only)
- Device License Type (provided by REST API only)

Log Messages

The third tab, Log Messages, displays all events transpiring during the SNMP walk.

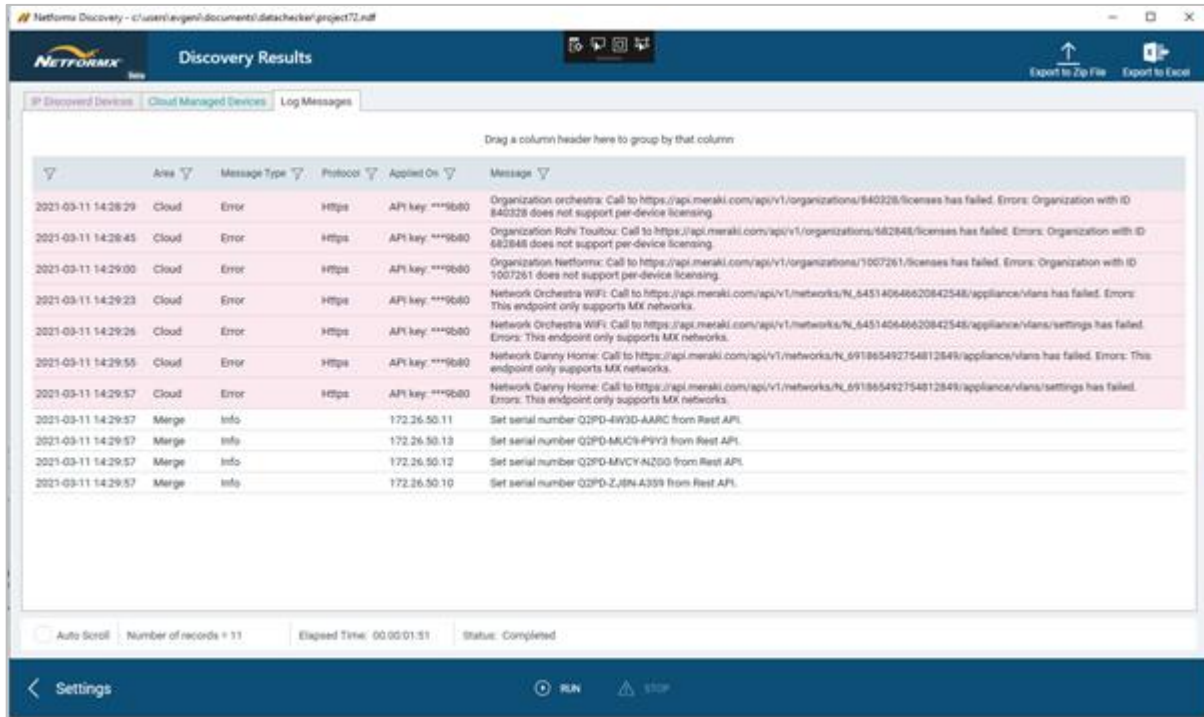


Figure 41: Discovery Results - Log Messages

The Log Message fields and their possible values

- Area: IP, Cloud, Merge
- Message Type: Error, Warning, Info
- Protocol: PING, SNMP, HTTP, HTTPS, Telnet \SSH
- Applied On: IP Address, API Key, SNMP Parameters (used during Cloud Discovery)
- Message: Describing the event and errors provided by the REST API/Meraki.com server

Details on the Matching Method for Meraki Environment

If you configured both the REST API and Meraki Organization SNMP Settings, the v21 Discovery engine attempts to rectify and merge the two data sets after the network walk. It tries to correlate and fix any missing data by examining the Serial Number, SKU, and Name and cross comparing against the data collected by the REST API. Matching starts by comparing MAC addresses and, if unsuccessful, compares IP addresses. The results pane colors all overwritten data and provides hover-over tooltips.

Post Network Walk Actions

Exporting Raw Results

All the data collected by the v21 network walk, including details pulled from the Cloud Discovery, can be exported to a Zip file or Excel spreadsheet.

Next Steps

Once you finish reviewing the outcome, close the **Discovery Results** screen, and the application will ask if you want to import your results into your DesignXpert Project. Click OK, and the DesignXpert Project will display the discovered network. The Project might contain one or more sub-drawings based on the subnet distribution.

You are now ready to upload your results to Cisco for CSA analysis and reporting results.

Network Analysis Using Cisco Smart Advisor (CSA)

Once your DesignXpert Project contains a discovered and imported network, you can submit a network assessment request using the Cisco Smart Advisor service.

On the Design tab, click Analysis → Cisco Smart Advisor → Submit Network Assessment Request, as shown in the figure below.

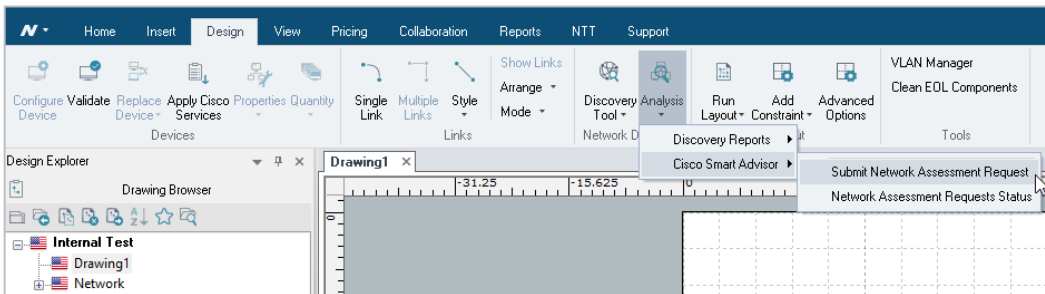


Figure 42: Submit CSA Trigger

Select the discovery Project's scope (Project, Current drawing, or Selection) and click Next.

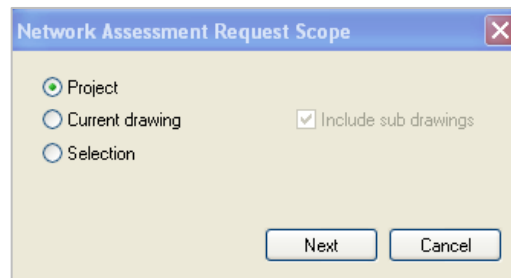


Figure 43: CSA Upload Scope

Submit Network Assessment Request (Cisco equipment)

The CSA registration form appears:

1. **Customer Details – Customer Search:** Identify the end-customer location of the SNMP network discovery.
2. **CSA Transaction Details:** Controlling the details sent to and coming from CSA analysis.
3. **Service Type:** Type of CSA analysis you desire from Cisco.
4. **User Contact Details:** Your contact information.

Submit Network Assessment Request (Cisco equipment)

Request Details
You are about to submit Network Assessment request for project **Internal Testnpz**

Transaction Name:

Service Type:

Enable CSA Services:

- Service Coverage Report
- Include IPv6 Report
- Upload IP Addresses
- Upload 3rd party device
- Field Notices
- Enhanced PSIRT Reporting

Customer Details

* Customer Name:

Vertical Market:

Theater:

Country:

Market Segment:

State/Province:

User Contact Details

* First Name: * Last Name:

* Email: Enable email notification

* User Type: Cisco SE Cisco Partner

Sales Engineer details

Contact type	CCOId	First name	Last name	E-mail
Primary Cisco Sales Engineer	marshallnetformx			
Alternate Cisco Sales Engineer				
Cisco Sales Engineer Manager				
Cisco Sales Engineer Director				

* Mandatory fields

Figure 44: Submit Network Assessment Settings

CSA Customer Search

The Customer Detail menu connects via API to a backend Cisco database. You must identify the end-customer installation address location of the network discovery. Cisco requires this linkage to associate the discovered network devices' characteristics to the information stored in their backend databases. Click the magnifying glass icon (1) to launch the Cisco Customer search menu.

Customer Name	Address Line 1	City	Country	State
NETFORMX	275 SARATOGA AVENUE SUITE...	SANTA...	UNITED STATES	CA
NETFORMX	275 SARATOGA AVE	SANTA...	UNITED STATES	CA
NETFORMX	20454 BLAUER DRIVE SUITE 150	SARATOGA	UNITED STATES	CA
NETFORMX	400 RACE STREET SUITE 201	SAN JOSE	UNITED STATES	CA

Figure 45: Cisco CSA Customer Search Menu

Input the **Customer Name** and **City** location to help narrow the Cisco results and click **Search**. The Cisco interface responds with a list of potential matches. Select the most appropriate address location and click **OK**. Only select **New Customer** if you need to define and use a new customer installation location.

Enable CSA Services

You have control over the amount of information you want to upload to CSA for analysis and details you wish to receive for the customer-facing network assessment report you can produce from DesignXpert. Click the checkbox to enable the following:

- **Service Coverage Report:** SmartNet details for the devices.
- **Include IPv6 Report:** Details if the devices can support IPv6 address structures.
- **Upload IP Addresses:** Share the customer IP addressing convention with Cisco.
- **Upload 3rd party devices:** Includes details about non-Cisco devices.
- **Field Notices:** Receive security updates on the hardware installed in Cisco devices.
- **Enhanced PSIRT Reporting:** Receive security updates on IOS and software loads

CSA Service Type

You have explicit control over the type of CSA analysis you want Cisco to perform and can select from the dropdown menu (3) as shown in the image below:

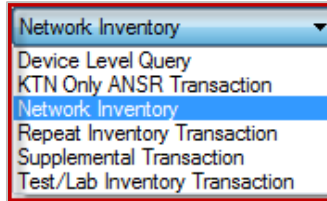


Figure 46: Service Type Menu Selection

- **Device Level Query (DLQ) Definition:** Limitation of up to 5 devices. The process is fast; however, it does not include KTN analysis. The transaction tracks in standard metrics as a device-level query.
- **Network Inventory Transaction:** This is the most common transaction type, including a complete network assessment scan, including site and segment assessment. This service type:
 - Creates a regular Transaction ID (TID)
 - Works with the CSA/CDS databases
 - Tracks in metrics as a standard transaction
- **Repeat Inventory Transaction:** Repeats the profiling of an existing transaction without uploading the Discovery data a second time. 'Repeat' analyzes the discovered network again based on up-to-date data from Cisco.
- **Supplemental Transaction:** This transaction is an add-on to an existing transaction to add additional devices. This transaction does not have a TID and can't be traced separately from the associated transaction. However, it requires an existing TID in the initial registration to process new devices, resulting in additions to the same TID record.
- **Test/Lab Inventory Transaction:** Profiling transaction is not tracked in metrics and does not include CSA/CDS analysis.

CSA – User Contact Details

The User Contact Details define you, the Network Partner, performing the Network Assessment. This information comes from your CCO ID credentials stored in the Options → Vendor Specific → Cisco menu. **Enable email notifications** to receive notifications on the CSA process status and indicate when the report is ready to download from Cisco.

Once you finish filling out the Network Assessment Request form, click Submit to start the Network Assessment upload process to the CSA servers, a non-blocking background process.

Network Assessment Request Status

To check the status of an outstanding CSA analysis from the Design tab, manually click → Analysis → Cisco Smart Advisor → Network Assessment Requests Status, as shown below.

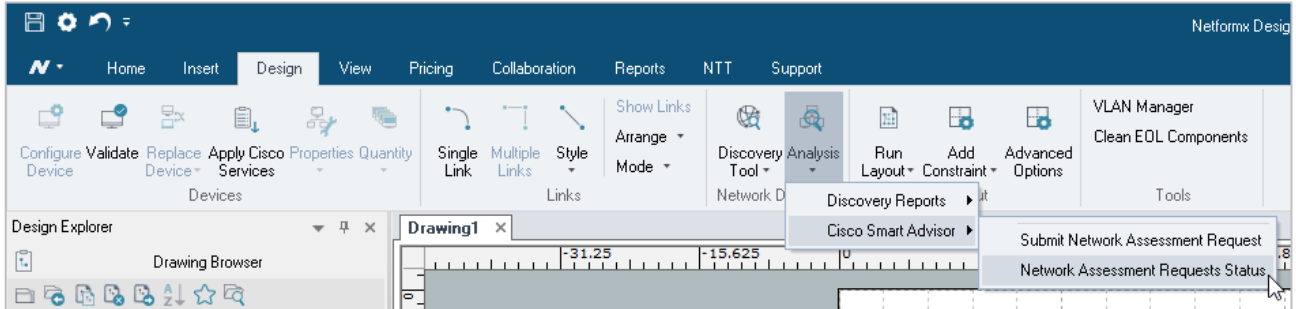


Figure 47: Network Assessment Status Request

The Network Assessment Request Status menu appears.

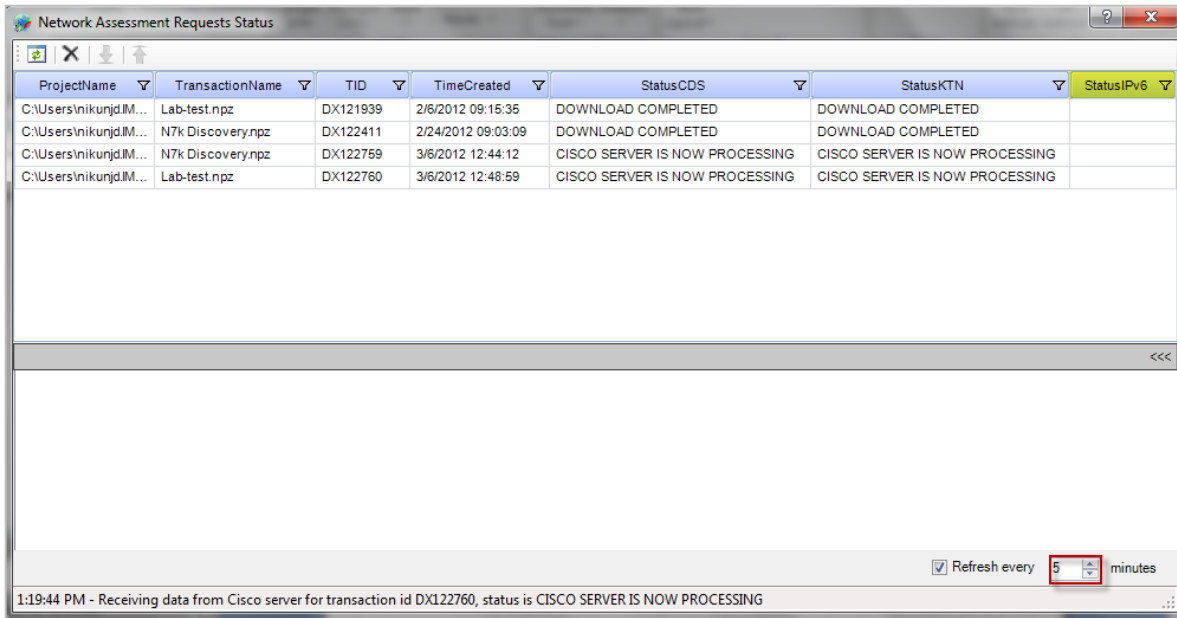


Figure 48: Network Assessment Request Status Menu

This interface provides details about the status of the transaction analysis uploaded by you. Transaction analysis and processing time depend on the overall size of the network discovery (number of devices and cards loaded) and the number of pending transactions ahead in the queue; pending transactions submitted by other users in your organization or other Partner organizations will not appear in this interface.

The interface details the Project Name and storage path from your machine, the Transaction Name, Transaction ID (TID), Upload create time, CDS/CSA analysis status, KTN analysis, and IPv6 status. While possible, we do not recommend changing the **Refresh every time**.

Netformx DesignXpert continues to poll the server in the background (based on your timing selected), checking for a transaction status change. Once a submitted transaction is complete and ready for download, the following informational message appears inside DesignXpert.

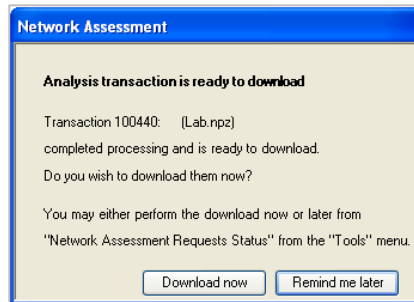


Figure 49: Network Assessment Ready for Download Pop-Up

Selecting **Download now** only changes the transaction status flag in the Network Assessment Request Status menu to Completed; it does not start the download process. You can only initiate the download report sequence from within the Network Assessment Request Status menu, shown in the figure below. Clicking **Remind me later** changes the flag to Waiting for Download.

Downloading a Completed Transaction Analysis

Launch the Network Assessment Request Status menu from the Design tab by clicking → Analysis → Cisco Smart Advisor → Network Assessment Requests Status. Select the desired Transaction ID line and click the Download button as noted below.

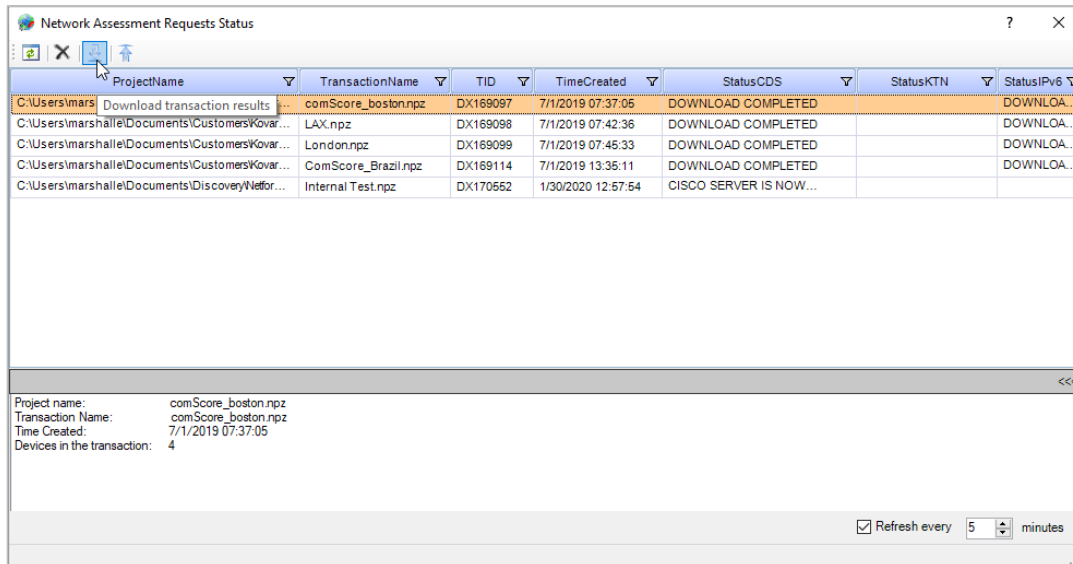


Figure 50: Selecting a Finished Network Transaction for Download

A progress bar pops up, noting the progress of the download status into your Project.

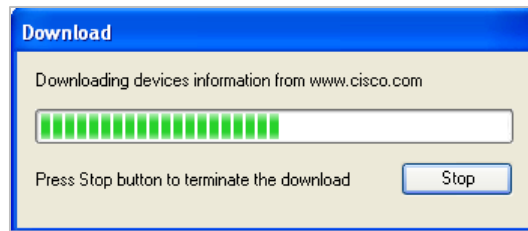


Figure 51: Network Transaction Download Bar

Once the transaction completes downloading, the Network Assessment Request Status line updates to **Download completed**. There is no restriction on downloading your TID report more than once, although it will not add any new information to your Project. Note: you cannot select and download more than one transaction at a time.

CSA Network Assessment Upload Help

It could take anywhere from 24- to 48-hours for Cisco to complete an analysis and indicate the report is available for download. If you need assistance from Cisco, send an email to cds-support@cisco.com. If it takes longer than expected for the analysis to finish or if it does not include the Field Notice or PSIRT information in the report, contact Cisco and note the applicable Transaction ID in your communication. Cisco should respond to your initial request for within 24-hours.

DesignXpert CSA-Based Network Assessment Reports

Netformx Discovery and Netformx DesignXpert integration with the Cisco Smart Advisor/Cisco Discovery Service systems allows you to produce highly valued customer reports. These reports include detailed analysis about the Cisco devices uncovered during the SNMP discovery, offered as Network Discovery, Network Assessment, and Device History. Access these from the Report Tab by clicking the Discovery Related dropdown in the Cisco Report section, as shown below.

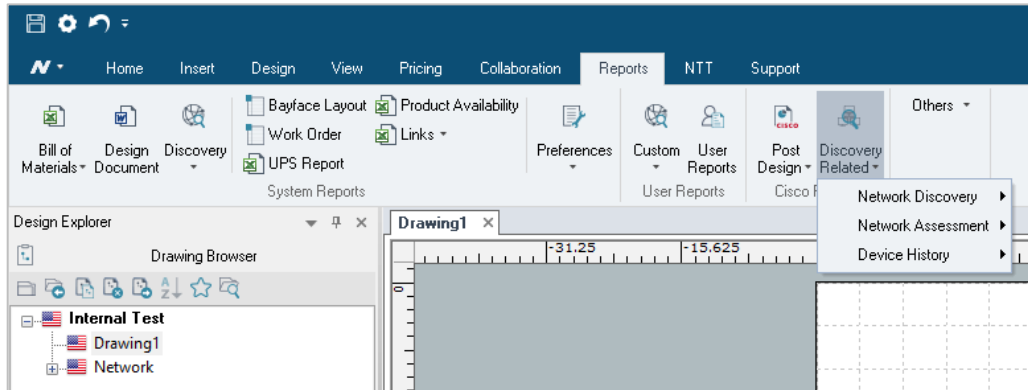


Figure 52: Accessing Cisco Reports

The three main groups provide additional report options.

- **Network Discovery:** Individual Excel-based reports outlining:
 - **Equipment Report Summary** – detailing the Device Name, IP Address (if included), Vendor, Product Category, Serial Number, Part Number (SKU), and System Name.
 - **Equipment Report Full** – includes all the above plus System Description, Used Memory RAM, Free Memory RAM Size, and Flash Memory Free.
 - **Serial Number Report** – highlights the Device Name, Catalog Number (SKU) Description, Serial Number, and Quantity.
 - **Configuration Files** – provides you with the Running Config text files when you triggered the downloading of them in the Cisco Specific tab.
 - **Port Statistics** – highlighting overall port connectivity statistics.
- **Network Assessment** reports include the information from the CSA/DSA analysis from Cisco.
 - **Full Report** – The report provides a detailed analysis of the data, including information down to the level of single device (by IP address) and models (catalog numbers and OS versions), including Detailed Equipment List, Chassis Summary, Component Summary, Contract Validation Summary, Detailed PSIRT Report, Chassis PSIRT Summary.
 - **Executive Report** – The executive report shows aggregated information on the analyzed data at the product line and family levels. This report emphasizes and highlights equipment that has reached or is approaching the Last Day of Support (in other words, the product has reached its End-of-Life (EoL) date. Reports include Summary, Product Series – IOS, Product Series – CatOS, Product Series, Train, Field Notices, and PSIRT details.
 - **Data Review Report** – The report allows you to view the information uploaded to Cisco to trigger the overall analysis.

- **Summary Document** – This summary document is a helpful customer-facing document with a professional look and feel. Customize this report by applying your company’s logo. This report includes valuable Pie charts, Bar charts for IOS, CatOS, Train, Field Notices, PSIRTS, Contracts, etc.
- **Device History** reports provide a running analysis of your overall Project discovery activities.
 - **All** – A complete spreadsheet report details the Device Name, IP Address (if included), Product Category, Serial Number, MAC Address, last discovery run date, and initial discovery run date.
 - **Missing** – An incremental comparison report used when you run multiple discoveries for the same Project, identifying devices that appeared in the previous SNMP walk, not appearing in the latest SNMP walk.
 - **New** – An incremental comparison report used when you run multiple discoveries for the same Project, capturing newly identified devices as compared against those identified in the last SNMP walk.

Post-Discovery Operations & Other Helpful Options

A post-discovery Project contains a wealth of device-level information gleaned from the customer's environment before uploading the CSA analysis results and downloading the analyzed information from Cisco. Netformx DesignXpert and Netformx Discovery provide many ways to access that data.

Quick View Reports

You can access the Quick View Reports from the Design Tab → Analysis → Discovery Reports → Quick View reports, as shown below.

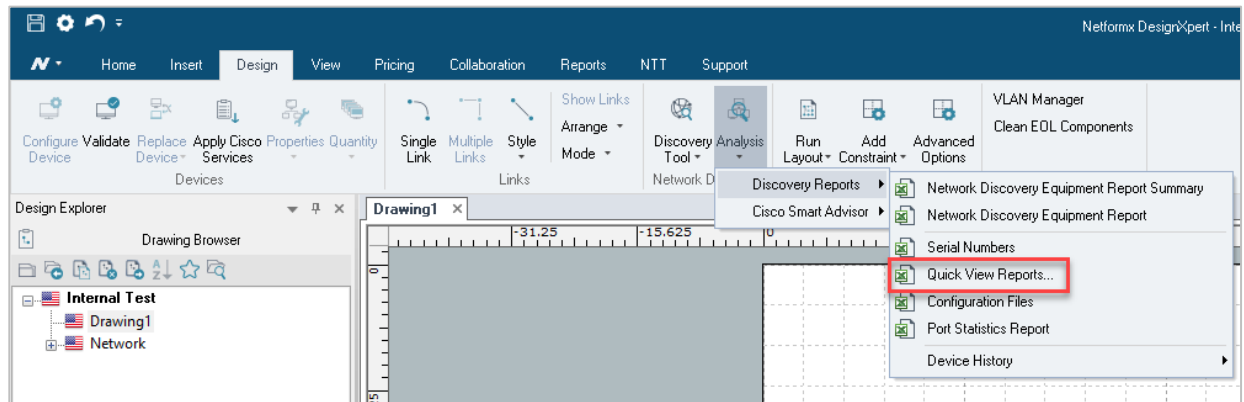


Figure 53: Accessing Quick View Reports

The **Quick View Reports** provides you with fast access to summarized details about the discovered network. You can choose from the following:

- **Serial Number Report** – Displays the Serial Number for chassis-level devices.
- **Physical Connections** – Displays the connectivity between Port X in Device A to Port Y in Device B.
- **VLANs** – Displays the list of VLANs for associated discovered devices, including VLAN numbers and descriptions.
- **Switch Ports to VLANs** – Displays the switch port connections to VLAN numbers.
- **Cisco Online EoX Report** – Uses the Cisco API to check the Product Lifecycle Milestones for the Product SKUs uncovered during the SNMP walk.
- **Stacks-VSS Report** – Provides you with insight for all Virtual Switch Stack (VSS) devices and their membership.

Device Details from the Drawing Page (Right-Click Options)

You can access discovery-related details directly from the drawing page by right-clicking on the device and selecting Discovery from the context menu, as shown in the image below.

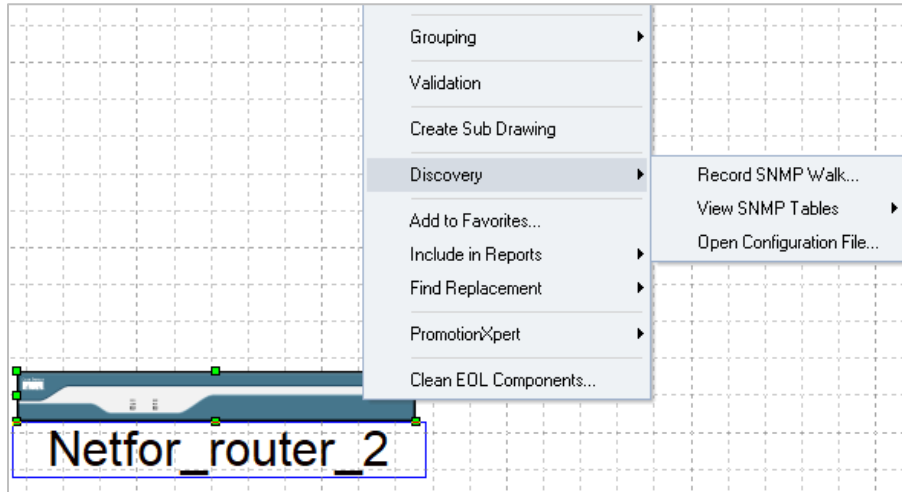


Figure 54: Right-click to Expose Discovery Information

The context menu includes a Discovery option that contains three additional elements:

- **Record SNMP Walk** (covered below)

To create and record **SNMP Walk**:

1. From the Design Tab → Discovery Tools → Record SNMP Walk to display the Record **SNMP Walk** menu.
2. Define your **Output File Name** and Folder location.
3. Enter the IP Address of the device you wish to track (log) in the **IP Address** field.
4. Enter the Root OID. The SNMP will log all entries for this SNMP subtree level.
5. Set the device SNMP **Version** (v1, v2c, or V3).
 - Enter the Community String for SNMP v1/v2c.
 - Enter the username, authentication, and password for SNMPv3.
6. Click **Run** to start the recording.
7. Click **Stop** to complete the recording.

- **View SNMP Tables** – This allows you access to the following SNMP tables
 - **Interfaces**
 - **Power**
 - **IP Phones**

Interface#	IP Address(es)	Subnet Mask	Physical Address	Type	Speed	Description	Vlan ID
1	10.40.40.1	255.255.255.0	001a2fef21dc	ethernet-csmacd(6)	100000000	FastEthernet0/0	
2	10.10.10.2	255.255.255.0	001a2fef21dd	ethernet-csmacd(6)	100000000	FastEthernet0/1	
3				propPointToPointSerial(22)	1544000	Serial0/0/0	
4				other(1)	2147483647	Null0	
6	10.80.80.1	255.255.255.0	001a2fef21dc	lvlan(135)	100000000	FastEthernet0/0.50-80 2.1Q vLAN subif	

Figure 55: SNMP Interface Table

Description	Power Supply State	Power Source
12V System PS	normal(1)	dc(3)
48V System PS	normal(1)	dc(3)

Figure 56: SNMP Power Supply Table

Phone Index	Phone MAC Address	Phone Description	Phone User Name	Phone IP Address
	b8fac8ea0000	SCCP Gateway (AN)		0.0.0.0
	b8fac8ea0001	SCCP Gateway (AN)		0.0.0.0
	b8fac8ea0002	SCCP Gateway (AN)		0.0.0.0
	b8fac8ea0003	SCCP Gateway (AN)		0.0.0.0
	001f9e25551f	7911		10.50.50.2

Figure 57: SNMP Phone Table

- **Open Configuration File** – Provides you access to the Running Config File (if you set the option to collect these – see Cisco Specific Tab in this document).

```

Edit value
Edit
Building configuration...

Current configuration : 1395 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Netfor_router_2
!
boot-start-marker
boot-end-marker
!
    
```

Figure 58: Running Config File

Netformx Discovery Files and Databases

After the Netformx Discovery process completes, the application generates the following files and database:

- **Log Files:** Lists all network elements with their IP address and status. This file is generated automatically during a Netformx Discovery session.
 - Path: %appdata%/Roaming/Netformx/ND/log
- **Interface Table:** Provides detailed information about each device's interface in a customizable table.
- **Netformx Discovery Database:** Netformx DesignXpert creates a database with a file name consisting of the Project's filename with a ".ndf" extension. By default, this file is in the same directory as the project file. The file name can change using the Project Properties dialog box.

Additional Discovery Related Tips

After the Netformx Discovery process completes, the application generates the following files:

- Start with a limited discovery of routers and subnets only before analyzing the Project to decide the desired outcome's limits and requirements (a router/subnets discovery only should complete in just a few minutes).
- Start with low limits (hops, retries, and timeouts) and progress to discover more by changing one parameter at a time. Usually, no retries and a shorter timeout limit on SNMP and Pings will suffice for a response receipt from all nodes.
- When doing a Ping Sweep, raise the rate to 50pps (The traffic generated will be around 25Kbps, considered negligible in today's networks). Note that packets will need to travel back and forth, so the firewall needs to allow SNMP and Telnet in both directions.
- If the Firewall or the Networks do not allow ICMP, check that device configurations do not include Ping as an SNMP filter.
- Pay attention to the Discovery running log, which displays errors and warnings. Messages of this type might indicate misconfigured or incorrect discovery settings.
- For optimum performance, Discovery runs from workstations directly connected to the network and not across a low-speed WAN or wireless connection.
- SNMP must be enabled on a device and configured for RO (read-only) or RW (read-write) to discover the device's internal configuration. Enter the specific community string in Netformx DesignXpert; otherwise, Discovery uses the "public" default.
- Make sure to allow SNMP access from the workstation running the Discovery for the customer environment.
- To read multiple NT domains, enter a single username and password that is a member of all these domains under the NOS Services tab in the Windows Service window.

- On the workstation hosting the discovery process, be sure to disable the firewall, anti-virus, and other third-party protection products. These could hinder the discovery process from running successfully.

If the discovery log file is huge, it may not open properly with WordPad. In this situation, it is best to save the log as a .txt file and open it manually with Microsoft Word.

Steps for a Successful Cisco Network Assessment Engagement

- Information addressing customer security concerns [click here](#).
- Verify your CCO credentials level: Make sure you have Level 3 (Partner Level) access.
- Gather required information from the customer like (SNMP (RO), Telnet (Including Enable Password), SSH, Router Address, Seed File, etc.)
 - Enable SNMP on the customer's devices.
 - Have the *SNMP read-only password(s)* readily available to collect SNMP information.
 - Have Telnet/SSH credentials ready – Telnet Enable Password for CSA transaction (Enhanced PSIRT) as well.
 - Have the *SNMP read-write password(s)* readily available if you wish to collect Cisco Config Files.
 - If using Telnet to capture the Cisco Config Files, be sure to have available all *Telnet Username(s), password(s) & Enable password(s)*.
- Verify service contract status.

The Cisco partner may need to do some work in advance to obtain complete service coverage data for their associated Network Assessment reports. Specifically, a non-incumbent Partner must have in hand or submit to their Cisco Service Contract Manager a Letter of Authority (LoA) signed by the end-customer to confirm permission and authorization to access SmartNet contact data.

- Obtain and Install Netformx Discovery.
- Perform a test network assessment.

The following traffic should be allowed back and forth from the Netformx Discovery station during the network assessment:

- Ping, SNMP versions 1-3, Telnet, SSH, SSL, CDP.

Netformx Customer Support

To request Netformx Customer Support, please email support@netformx.com and attach details and files as appropriate. Doing so enables Customer Support to assess and answer any discovery questions quickly. Customer Support will need the following information:

1. **Software and Library Version of Netformx DesignXpert** (see Help>About Files)
2. Provide the following files:
 - a. **Discovery File** – The file name is *projectname.ndf*. To find this name, follow this path: *Project* → *Properties* → *Discovery* from the open Discovery project.
Note: The default is the directory location of the saved project file.
 - b. **Zip the file** to reduce the size before sending it.
 - c. **Log File** - To find this file, follow this path: %appdata%\Netformx\ND.
3. Provide a list of **IP addresses of the incorrectly discovered chassis** from the discovery file.
4. Please confirm you enabled the following before submitting the request of improperly discovered devices:
 - a. *Right-click* → *Properties* on the device in question and make sure to populate the Discovery tab with the SNMP information captured during the Discovery.
 - b. Attach results of Design Menu → Network Discovery → Discovery Tool → Record SNMP. Watch SNMP log for issues with missing SNMP information in device Netformx Discovery properties for a specific IP device.

To create and record **SNMP Walk**:

1. From the Design Tab → Discovery Tools → Record SNMP Walk to display the **Record SNMP Walk** menu.
2. Define your Output **File Name** and Folder location.
3. Enter the IP Address of the device you wish to track (log) in the IP Address field.
4. Enter the Root OID. The SNMP will log all entries for this SNMP subtree level.
5. Set the device SNMP Version (v1, v2c, or v3).
 - Enter the Community String for SNMPv1/v2c.
 - Enter the username, authentication, and password for SNMPv3.
6. Click **Run** to start the recording.
7. Click **Stop** to complete the recording.

Send all details to support@netformx.com