NETFORMX®

Step – By – Step User Guide

Netformx Discovery™ Step-By-Step User Guide Version v20.x (Beta)

Table of Contents

Netformx Discovery Overview

Netformx Discovery is the SNMP/SSH/Telnet-based audit and multi-vendor network discovery feature of Netformx DesignXpert®. Netformx enables pre-sales, 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 equipment and configuration data down to specific nodes. It can capture a baseline of existing equipment with detailed specs for each device. Used in conjunction with the Cisco Smart Advisor (CSA) formally known as the Cisco Discovery Service (CDS), Netformx 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 Discovery engine now uses updated built-in collection mechanisms to improve results.

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 prospect if they have SNMP enabled throughout their network
4. Ask your contact to supply you with their list of read-only community strings
5. Ask if they have ICMP enabled throughout their network
6. Ask your contact to supply you with their list of Telnet/SSH credentials

Setting Your Customer's Expectation

1. Depending on the customer's network's size, it may take anywhere from 30 minutes to overnight to complete the network walk.
   a. The average time for 1000 – 2000 network devices is approximately two to three hours.
   b. Even though the Discovery only creates a negligible impact on the network's 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. You need to set all relevant *SNMP v1/v2c/v3 read-only community strings* into the SNMP section to collect the device information. *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 the collection of 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. 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.
7. If you are the non-incumbent Partner, make sure you get the customer to sign a Letter of Authorization (LoA), which grants you access to SmartNet contract characteristics.
8. 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 out 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 that SNMP is enabled and running on all the customer's devices.
2. Have all relevant SNMP read community string(s) in your possession.
3. Determine the status of ICMP for all the devices in the customer environment.
4. Have ready all related Telnet/SSH credentials.
5. Have your list of custom CLI commands ready (if desired).

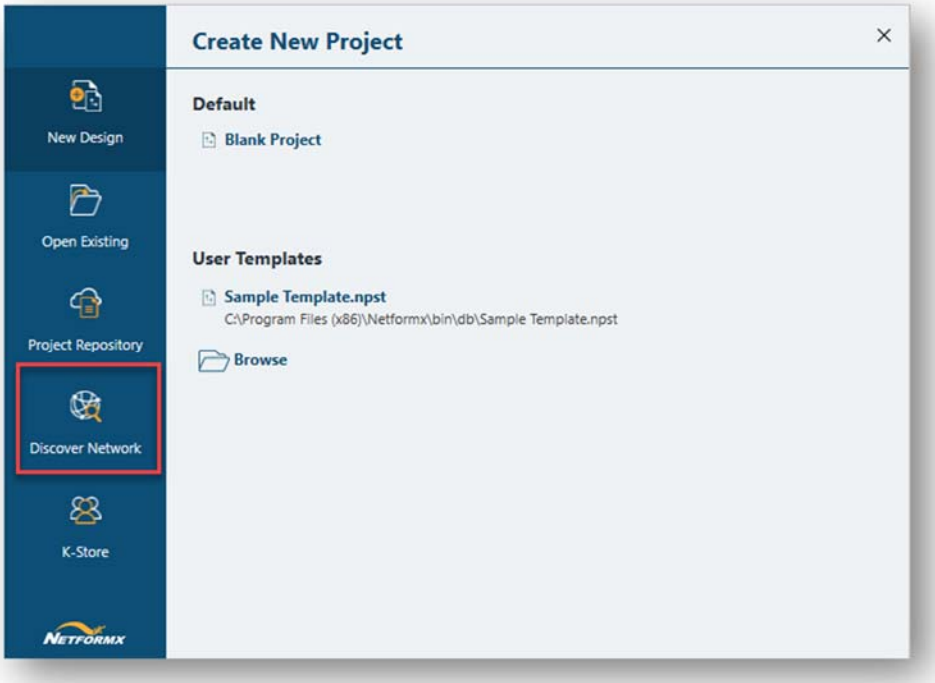
Tips:

- ***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.


Create New Project

Default

Blank Project

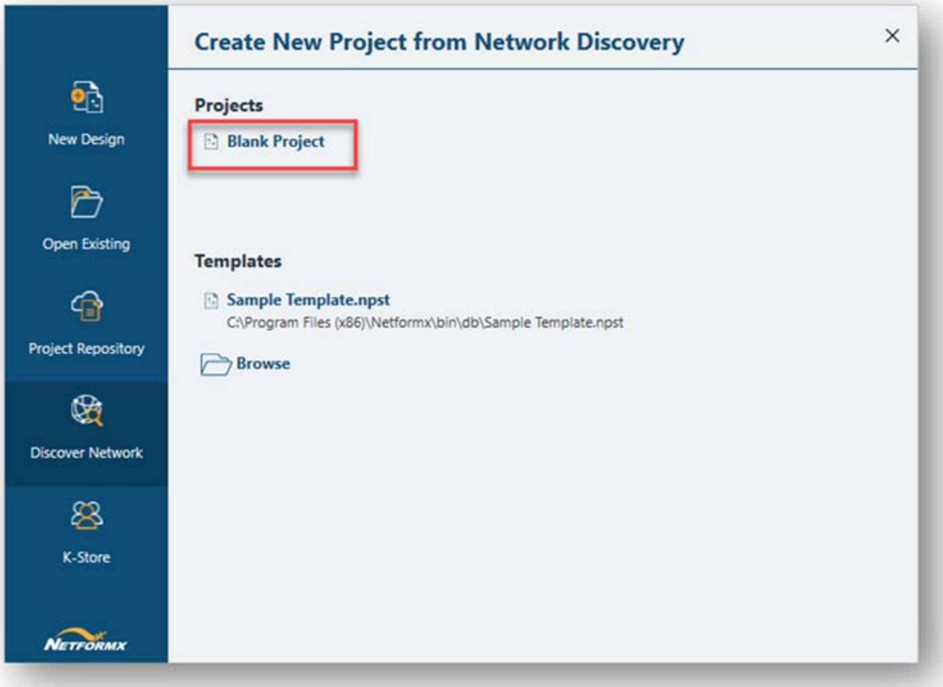
User Templates

Sample Template.npst
C:\Program Files (x86)\Netformx\bin\db\Sample Template.npst

Browse

Figure 1: Creating Discovery Project

3. From the **Create New Project from Network Discovery** menu, select **"Blank Project."**


Create New Project from Network Discovery

Projects

Blank Project

Templates

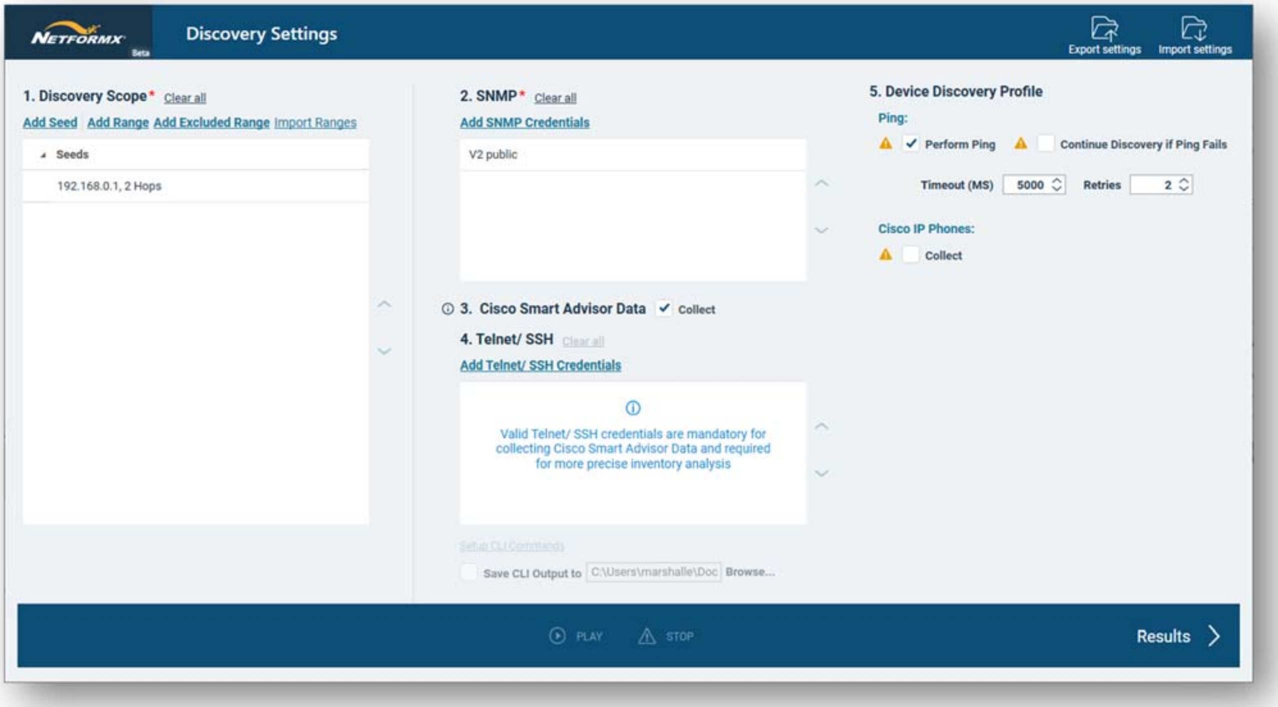
Sample Template.npst
C:\Program Files (x86)\Netformx\bin\db\Sample Template.npst

Browse

Figure 2: Selecting Blank Discovery Project

4. The **Save As** menu opens.
5. 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.



1. Discovery Scope*

Seeds: 192.168.0.1, 2 Hops

2. SNMP*

V2 public

3. Cisco Smart Advisor Data ☑ Collect

4. Telnet/ SSH

Valid Telnet/ SSH credentials are mandatory for collecting Cisco Smart Advisor Data and required for more precise inventory analysis

□ Save CLI Output to C:\Users\marshalle\Doc Browse...

5. Device Discovery Profile

Ping: ☑ Perform Ping □ Continue Discovery if Ping Fails

Timeout (MS) 5000 Retries 2

Cisco IP Phones: □ Collect

Figure 3: Discovery User Interface

The Play button (at the bottom of the UI) activates once you finish defining 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.

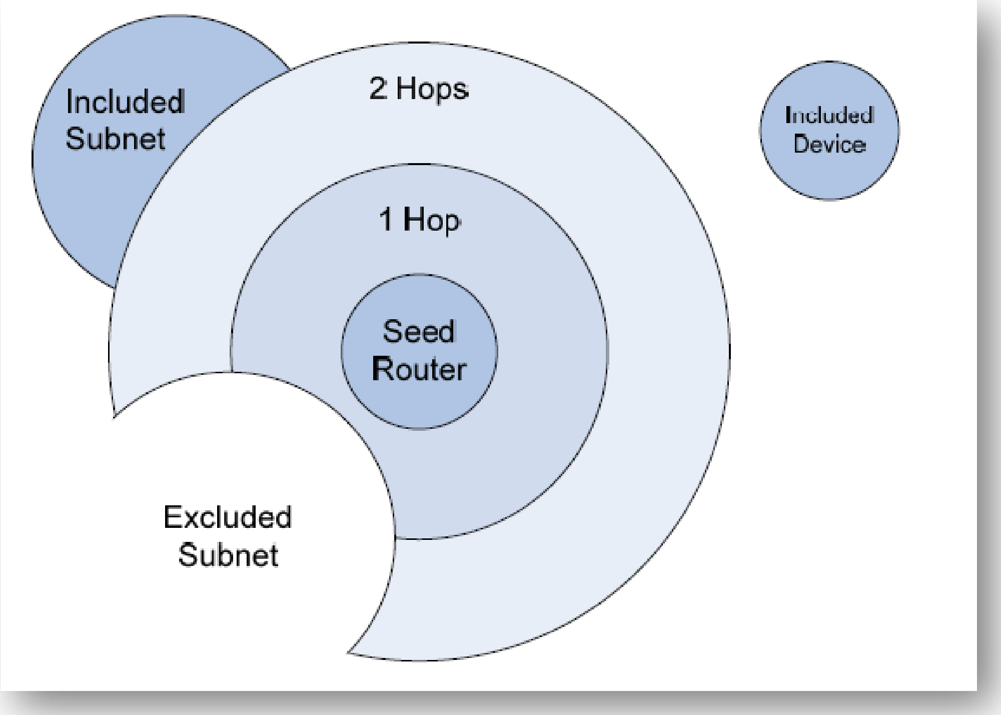


Figure 4: Discovery Scope Reference Diagram

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

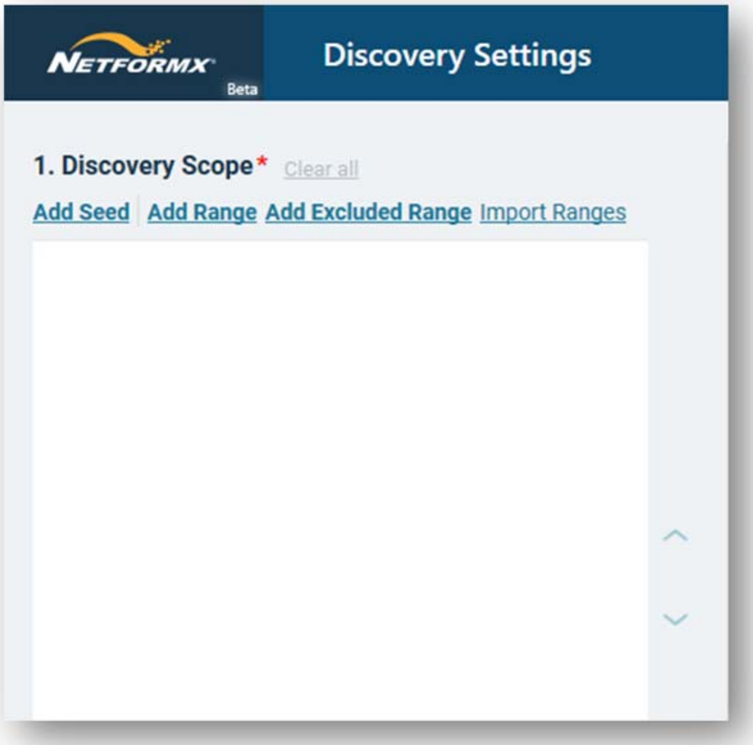


Figure 5: Discovery Scope User Interface

Add Seed

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

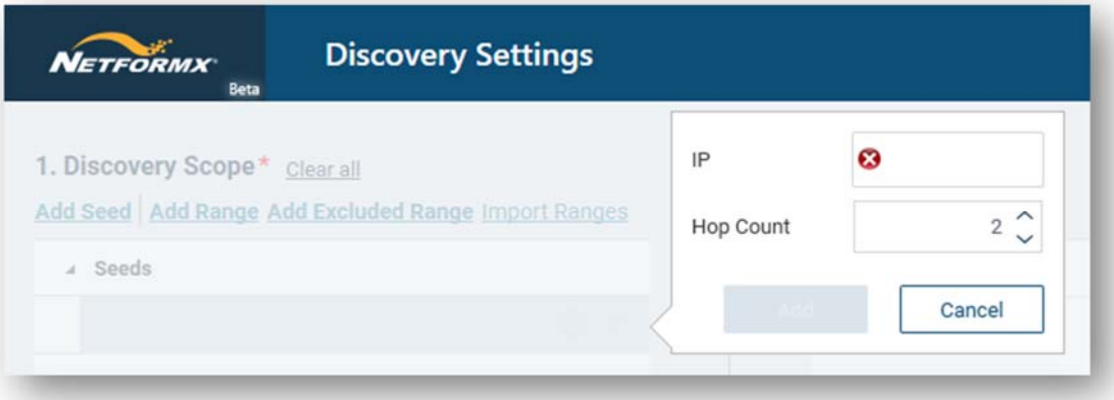


Figure 6: Setting the Seed Router

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 out 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 or inaccurate 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 full Discovery to include additional IP elements, ranges, addresses, and subnets outside of 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**:

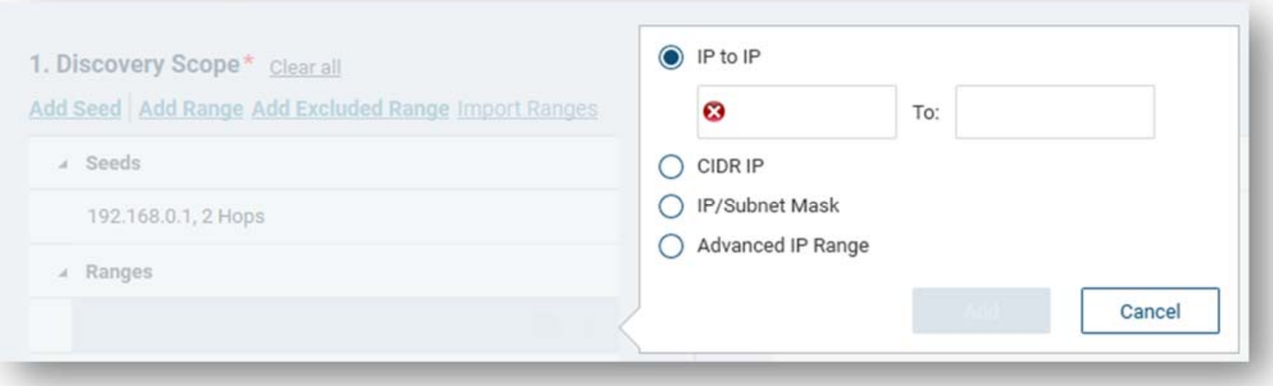
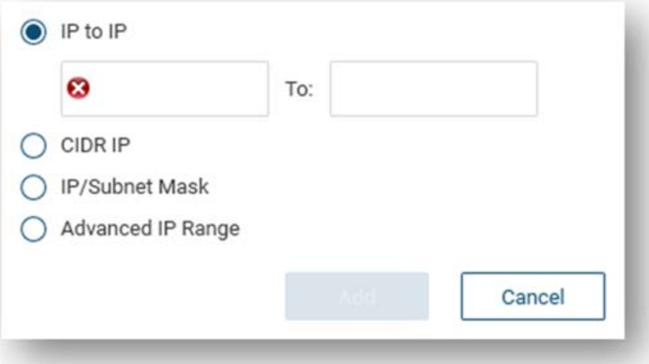


Figure 7: Defining the IP Range

The **Add Range** includes four options.

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



● IP to IP

To:

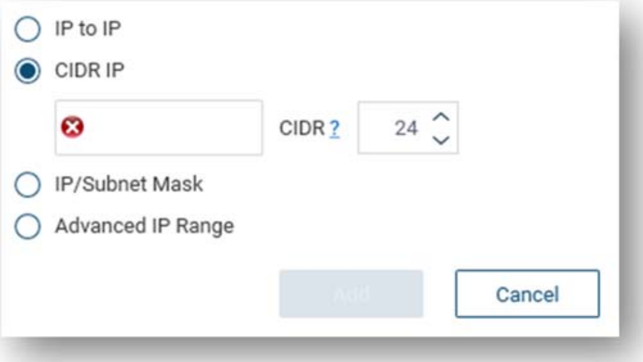
○ CIDR IP

○ IP/Subnet Mask

○ Advanced IP Range

Figure 8: Defining a From-To IP Range

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



○ IP to IP

● CIDR IP

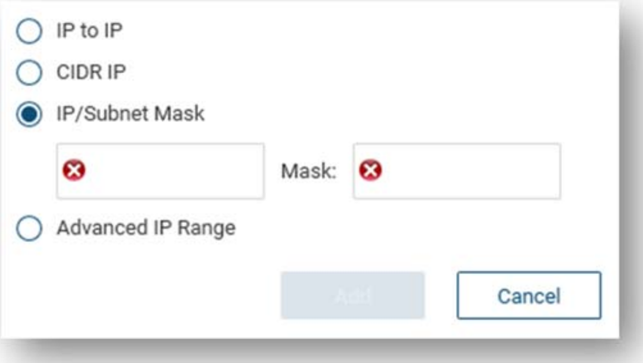
CIDR ? 24

○ IP/Subnet Mask

○ Advanced IP Range

Figure 9: Defining a CIDR-based IP Range

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



○ IP to IP

○ CIDR IP

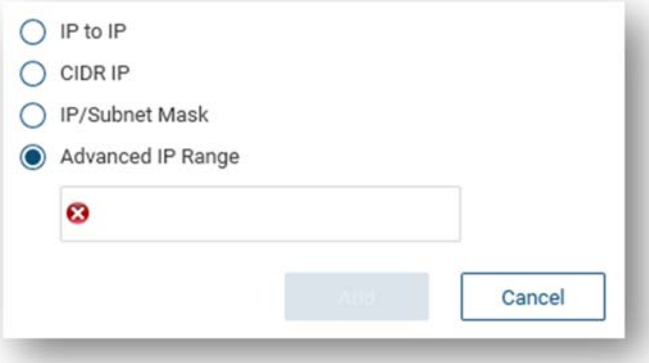
● IP/Subnet Mask

Mask:

○ Advanced IP Range

Figure 10: Defining a Subnet Mask IP Range

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



○ IP to IP
○ CIDR IP
○ IP/Subnet Mask
● Advanced IP Range

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.

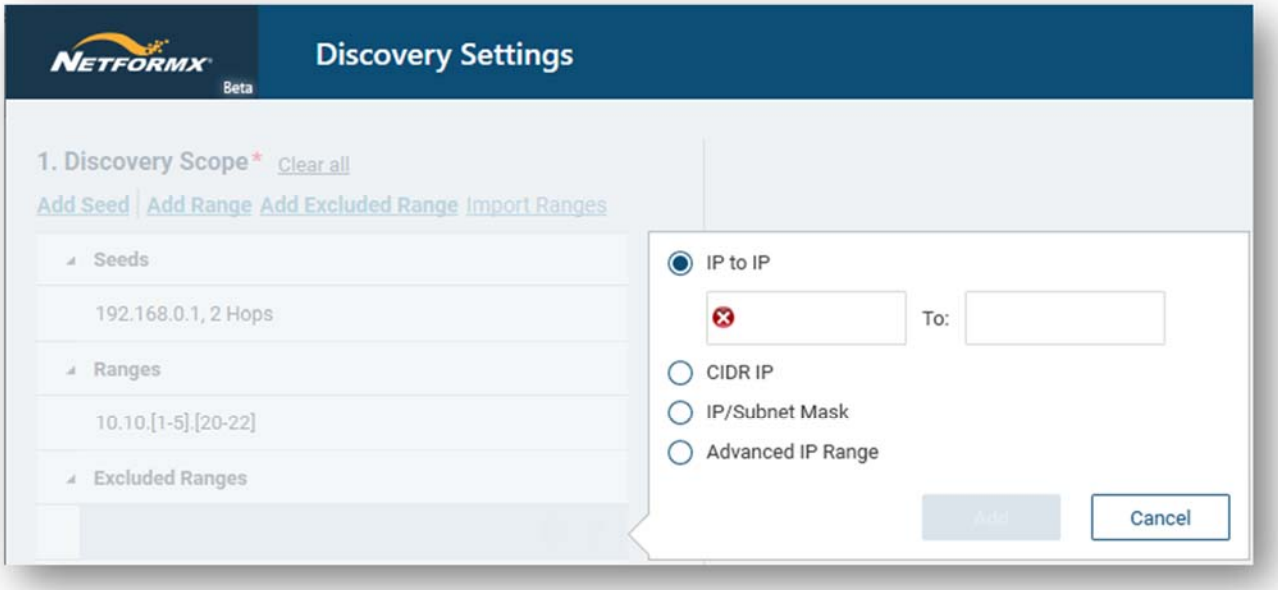
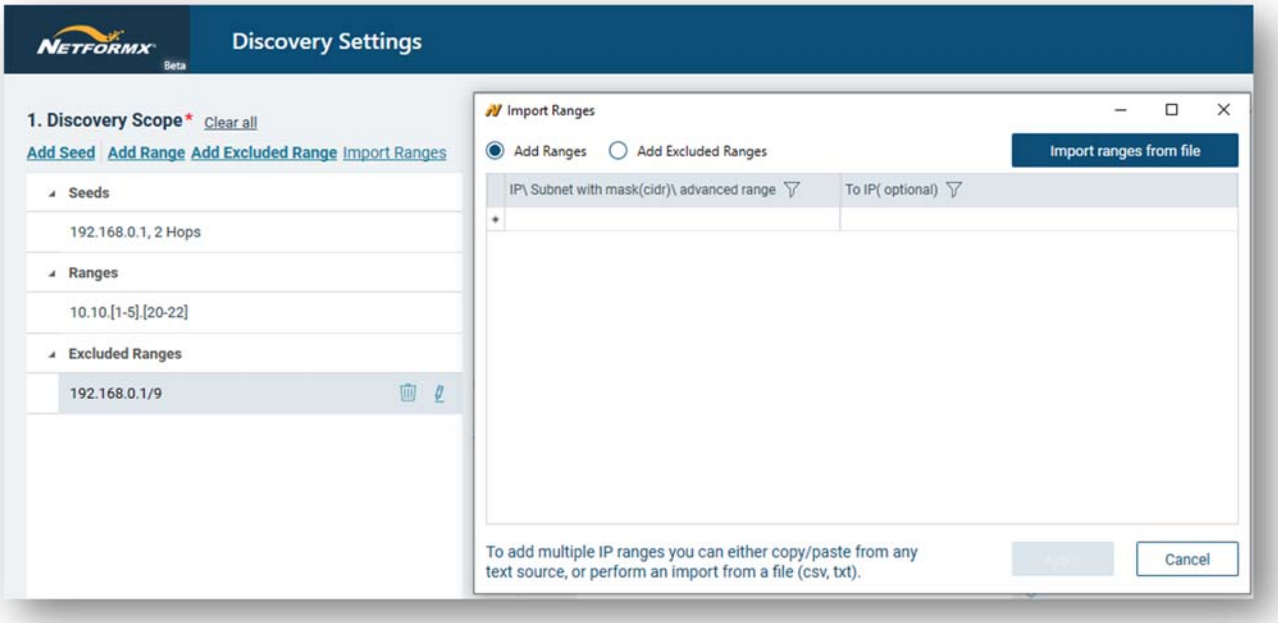


Figure 12: Controlling IP Ranges via Exclusions

Import Ranges

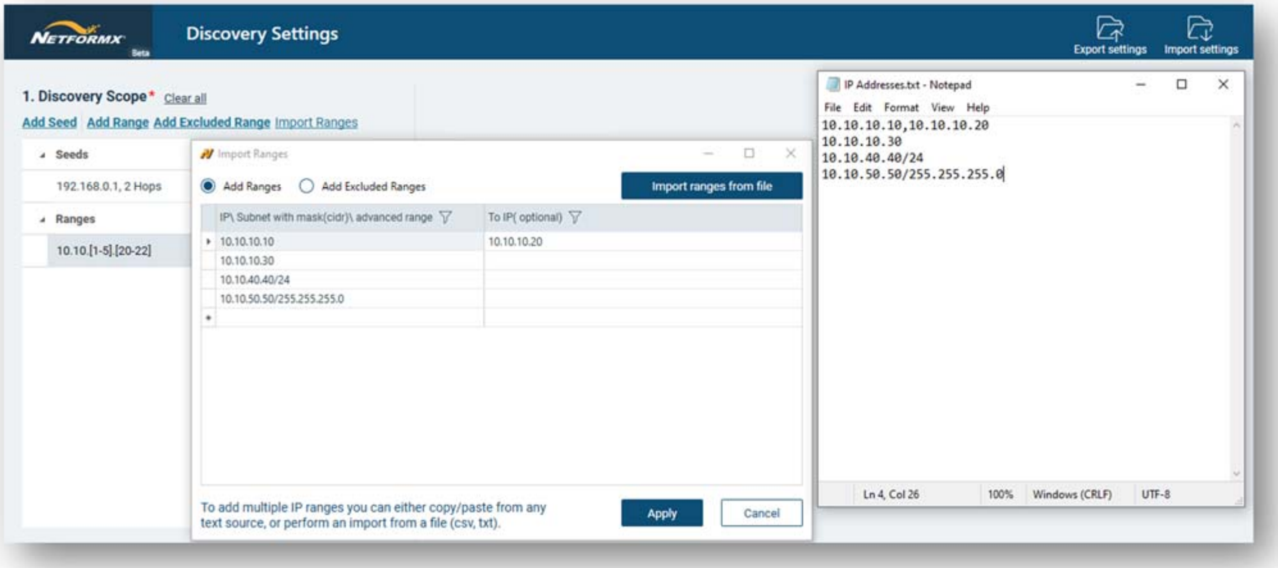
The **Import Ranges** allows you to transfer IP details contained spreadsheets (XLS) or comma-separated value (CSV) text files into the scope.



To add multiple IP ranges you can either copy/paste from any text source, or perform an import from a file (csv, txt).

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.



192.168.0.1, 2 Hops

10.10.[1-5].[20-22]

● Add Ranges ○ Add Excluded Ranges

IP\ Subnet with mask(cidr)\ advanced range	To IP(optional)
10.10.10.10	10.10.10.20
10.10.10.30	
10.10.40.40/24	
10.10.50.50/255.255.255.0	

To add multiple IP ranges you can either copy/paste from any text source, or perform an import from a file (csv, txt).

```
10.10.10.10,10.10.10.20
10.10.10.30
10.10.40.40/24
10.10.50.50/255.255.255.0
```

Ln 4, Col 26   100%   Windows (CRLF)   UTF-8

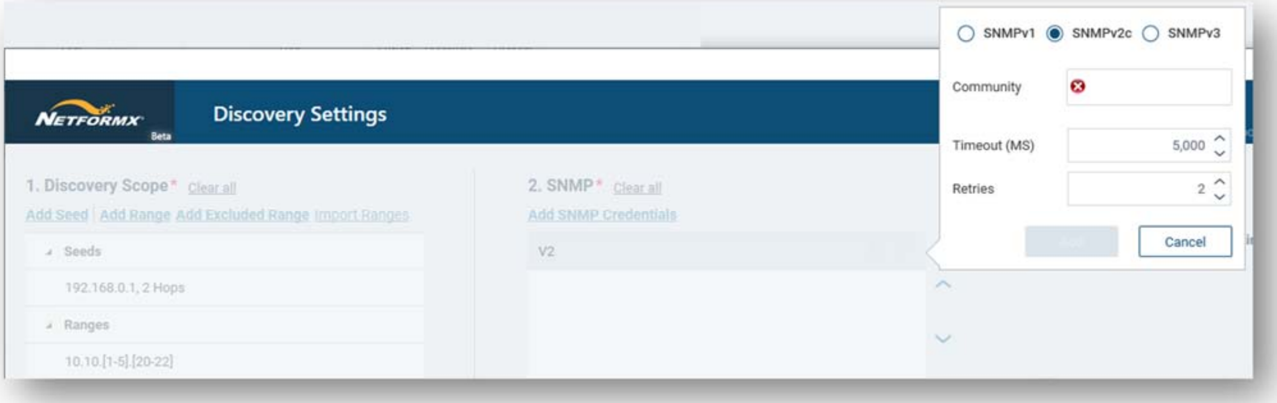
Figure 14: Import IP Range Examples

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 SNMP v1, SNMPv2c, and SNMPv3 implementation options.

Select **Add SNMP Credentials** to trigger the user interface. SNMPv1 & SNMP v2c present the same configuration options, as shown below. Enter each Community read-only string as deployed throughout the user’s environment.



192.168.0.1, 2 Hops

10.10.[1-5].[20-22]

V2

○ SNMPv1 ● SNMPv2c ○ SNMPv3

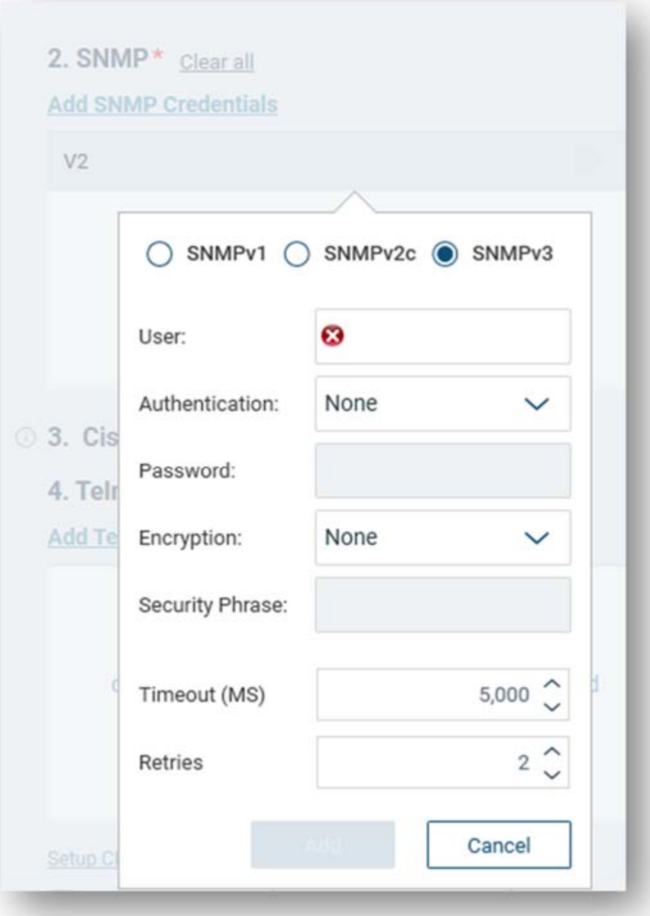
Community:

Timeout (MS): 5,000

Retries: 2

Figure 15: Defining SNMPv1/v2c Settings

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



V2

○ SNMPv1 ○ SNMPv2c ● SNMPv3

User:

Authentication: None

Password:

Encryption: None

Security Phrase:

Timeout (MS): 5,000

Retries: 2

Figure 16: Defining SNMP v3 Settings

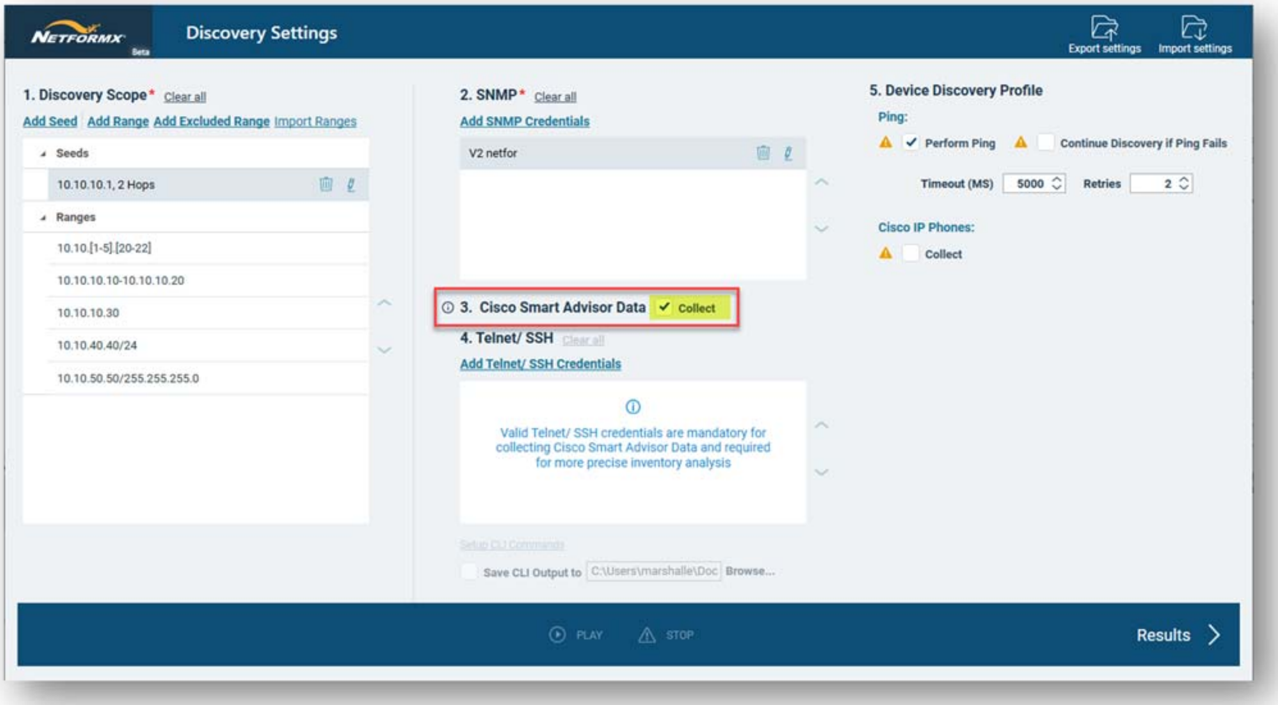
- User: Enter the authorized SNMPv3 User ID
- Authentication: Discovery supports SHA or MD5 methodology
- Password: Enter the correlating user password
- Encryption: Discovery supports DES, AES128, AES192, AES256, or 3DES
- Security Phrase: Enter the relevant Security Phrase

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: 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.



1. Discovery Scope* Clear all

Add Seed | Add Range | Add Excluded Range | Import Ranges

Seeds
- 10.10.10.1, 2 Hops

Ranges
- 10.10.[1-5].[20-22]
- 10.10.10.10-10.10.10.20
- 10.10.10.30
- 10.10.40.40/24
- 10.10.50.50/255.255.255.0

2. SNMP* Clear all

Add SNMP Credentials

V2 netfor

3. Cisco Smart Advisor Data ☑ Collect

4. Telnet/ SSH Clear all

Add Telnet/ SSH Credentials

Valid Telnet/ SSH credentials are mandatory for collecting Cisco Smart Advisor Data and required for more precise inventory analysis

Setup CLI Commands

□ Save CLI Output to C:\Users\marshalle\Doc Browse...

5. Device Discovery Profile

Ping:

☑ Perform Ping □ Continue Discovery if Ping Fails

Timeout (MS) 5000 Retries 2

Cisco IP Phones:

□ Collect

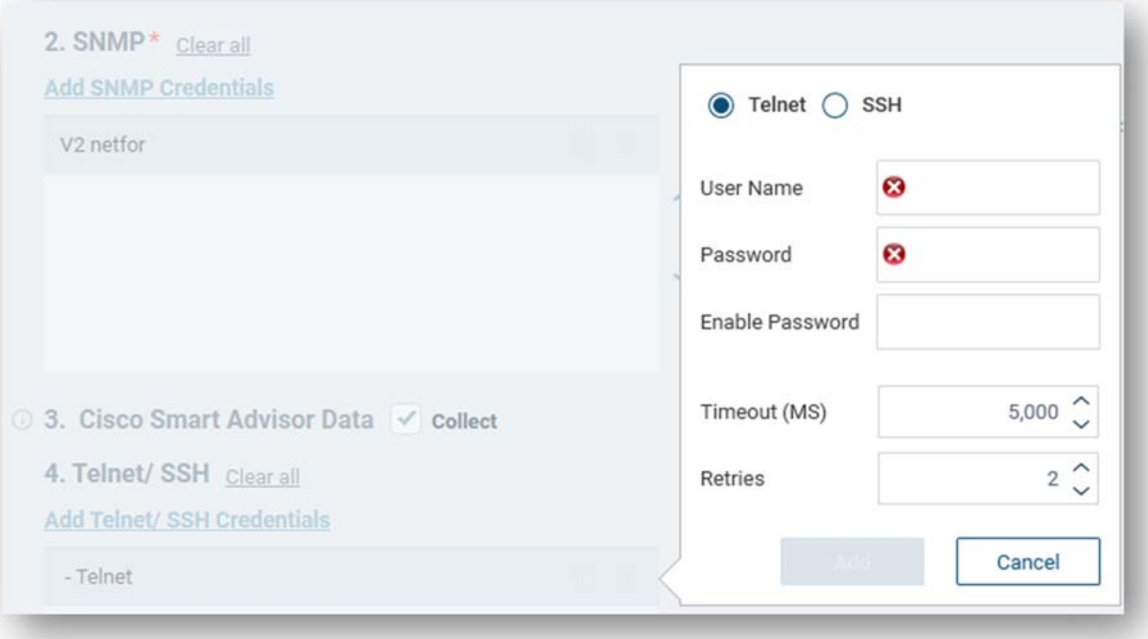
Figure 17: Default Cisco Smart Advisor CSA Setting

The Discovery engine uses both SNMP and Telnet/SSH methods to collect all the required raw data for CSA analysis. Enabling CSA also requires you to define all the Telnet/SSH credentials used throughout the customer's network.

Step 4: 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.



2. SNMP* Clear all

Add SNMP Credentials

V2 netfor

3. Cisco Smart Advisor Data ☑ Collect

4. Telnet/ SSH Clear all

Add Telnet/ SSH Credentials

- Telnet

● Telnet ○ SSH

User Name

Password

Enable Password

Timeout (MS) 5,000

Retries 2

Figure 18: 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.**

Setup CLI Commands

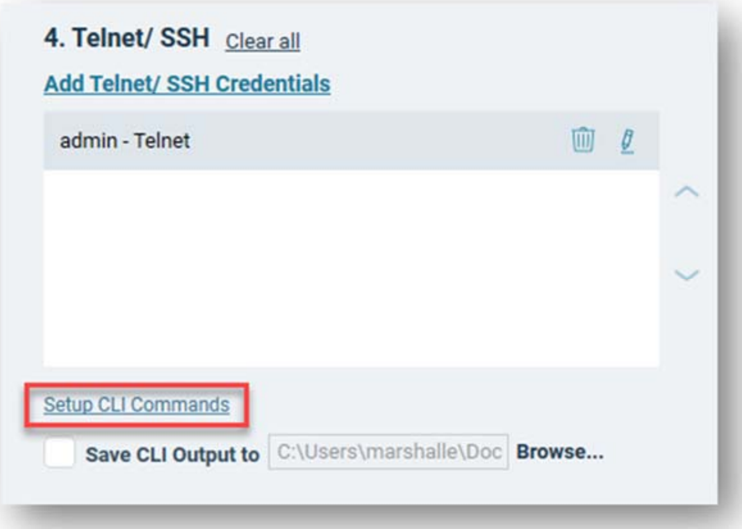


Figure 19: Defining Custom CLI Commands

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

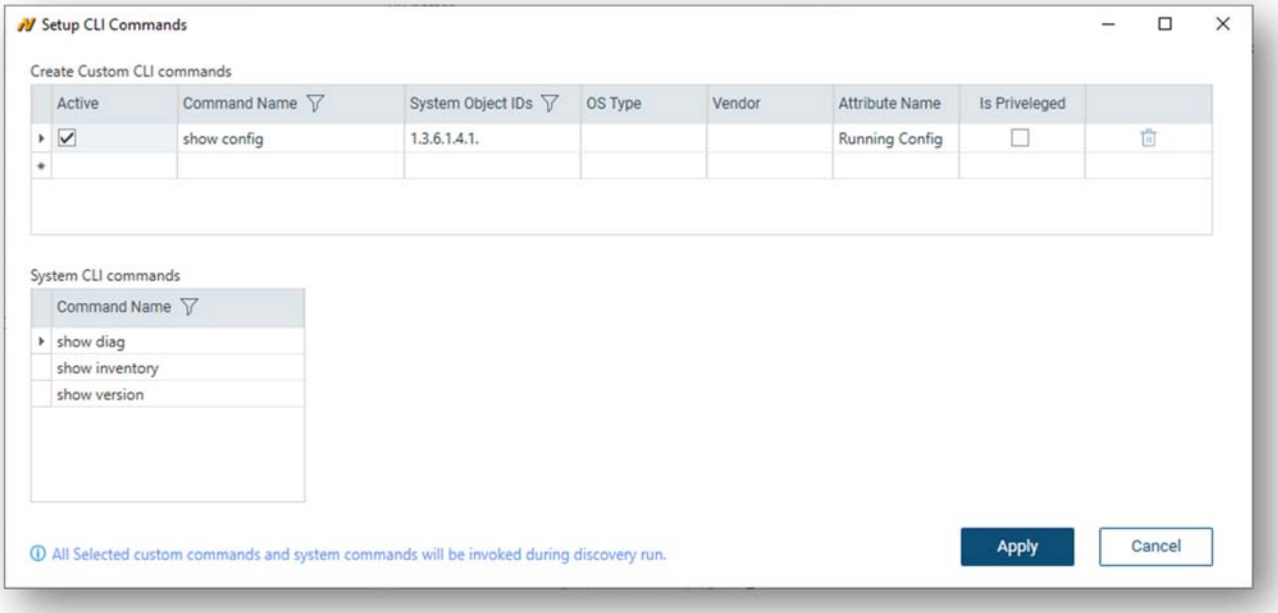
If you disable the CSA **Collect** option, the following CLI commands execute:

- Show diag
- Show inventory
- Show version

Using **Setup CLI Commands** allows you to define and execute CLI calls and capture the output. After the run and after 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 the 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.



Create Custom CLI commands

Active	Command Name	System Object IDs	OS Type	Vendor	Attribute Name	Is Priveleged
☑	show config	1.3.6.1.4.1.			Running Config	□

System CLI commands

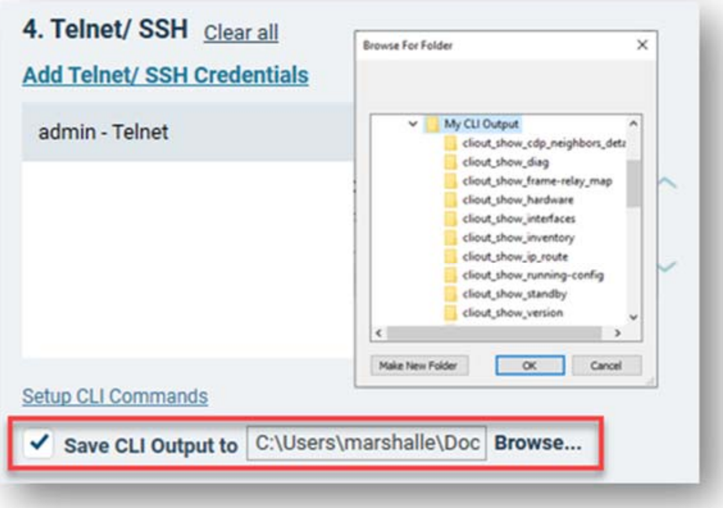
Command Name
show diag
show inventory
show version

ⓘ All Selected custom commands and system commands will be invoked during discovery run.

Figure 20: 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 outside of DesignXpert.



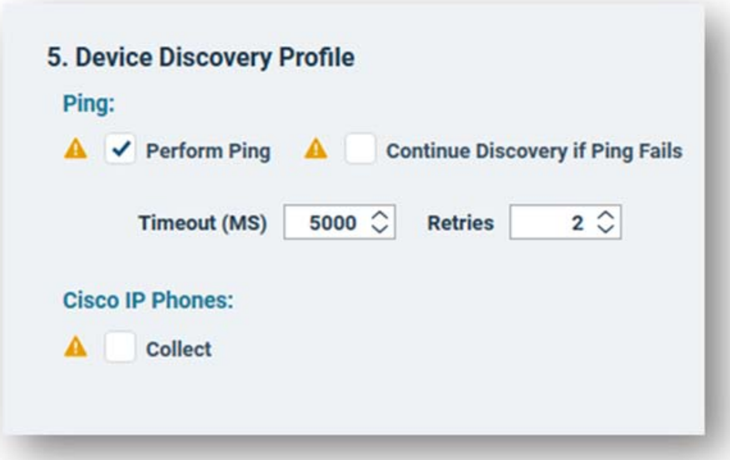
☑ Save CLI Output to C:\Users\marshalle\Doc

Figure 21: Saving CLI Command Output

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

Step 5: Device Discovery Profile

Ping



5. Device Discovery Profile

Ping:

⚠ ☑ Perform Ping ⚠ □ Continue Discovery if Ping Fails

Timeout (MS) 5000 Retries 2

Cisco IP Phones:

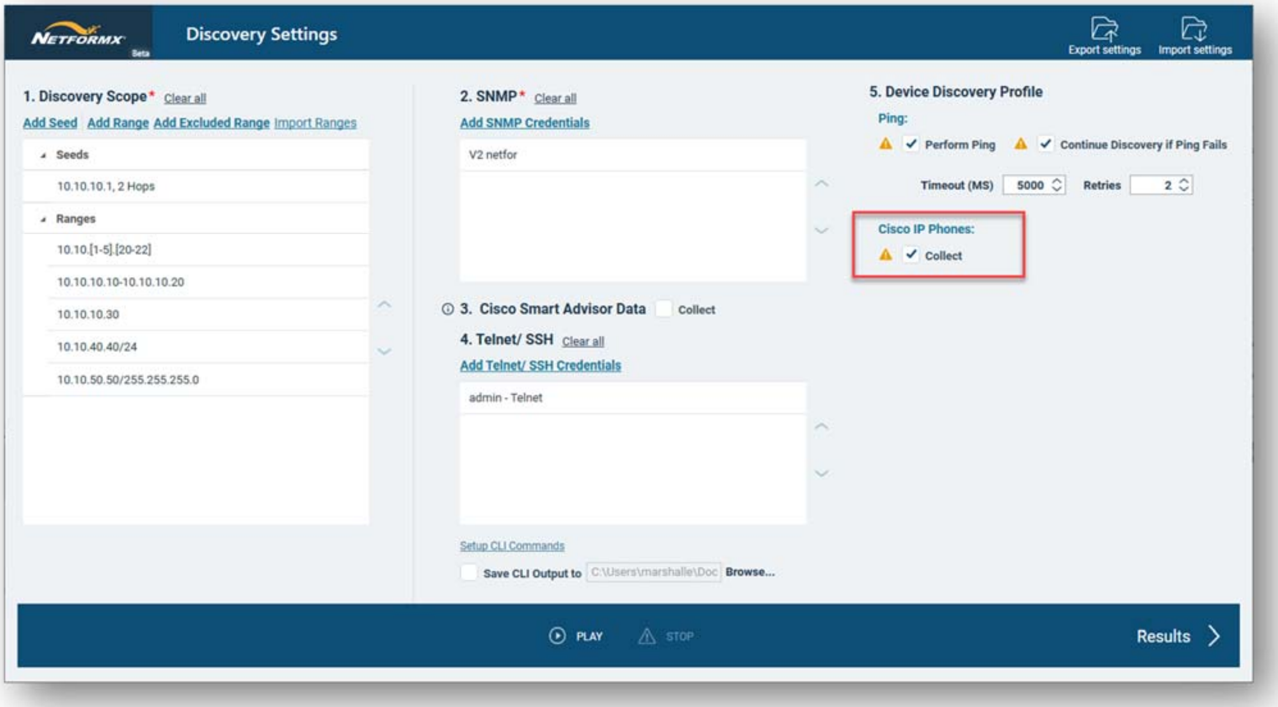
⚠ □ Collect

Figure 22: 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).

- <u>Perform Ping (Enabled by Default)</u>: 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.
- <u>Continue Discovery if Ping Fails</u>: 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 realize selecting this option increases Discovery running time due to the additional calls caused by the factoring of 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



1. Discovery Scope* Clear all

Add Seed Add Range Add Excluded Range Import Ranges

- Seeds
  - 10.10.10.1, 2 Hops
- Ranges
  - 10.10.[1-5].[20-22]
  - 10.10.10.10-10.10.10.20
  - 10.10.10.30
  - 10.10.40.40/24
  - 10.10.50.50/255.255.255.0

2. SNMP* Clear all

Add SNMP Credentials

V2 netfor

3. Cisco Smart Advisor Data □ Collect

4. Telnet/ SSH Clear all

Add Telnet/ SSH Credentials

admin - Telnet

Setup CLI Commands

□ Save CLI Output to C:\Users\marshalle\Doc Browse...

5. Device Discovery Profile

Ping:

☑ Perform Ping ☑ Continue Discovery if Ping Fails

Timeout (MS) 5000 Retries 2

Cisco IP Phones:

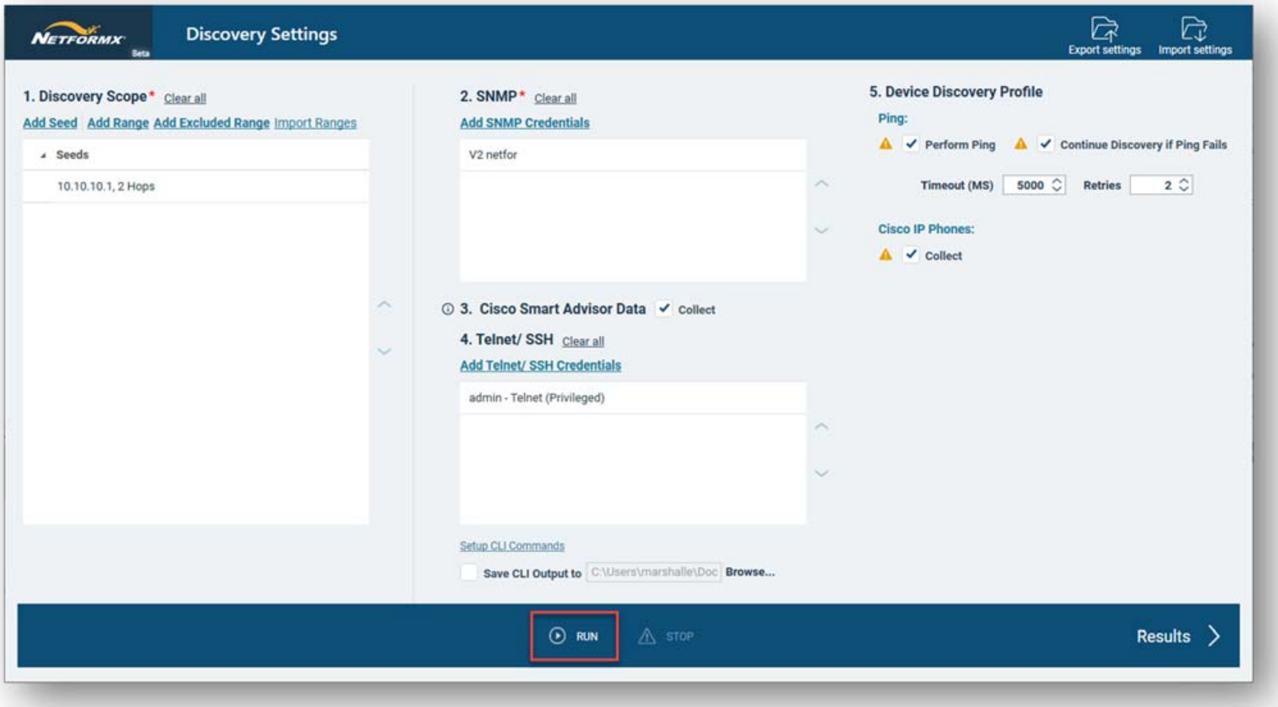
☑ Collect

Figure 23: Collecting Cisco IP Phone Details

Enabling Cisco IP Phones Collect tells Discovery to find Cisco IP Phones and to retrieve their configuration. This option instructs Discovery to use 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.

Run Network Discovery

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



1. Discovery Scope*

Seeds
10.10.10.1, 2 Hops

2. SNMP*

V2 netfor

3. Cisco Smart Advisor Data ✓ Collect

4. Telnet/ SSH

admin - Telnet (Privileged)

□ Save CLI Output to C:\Users\marshalle\Doc

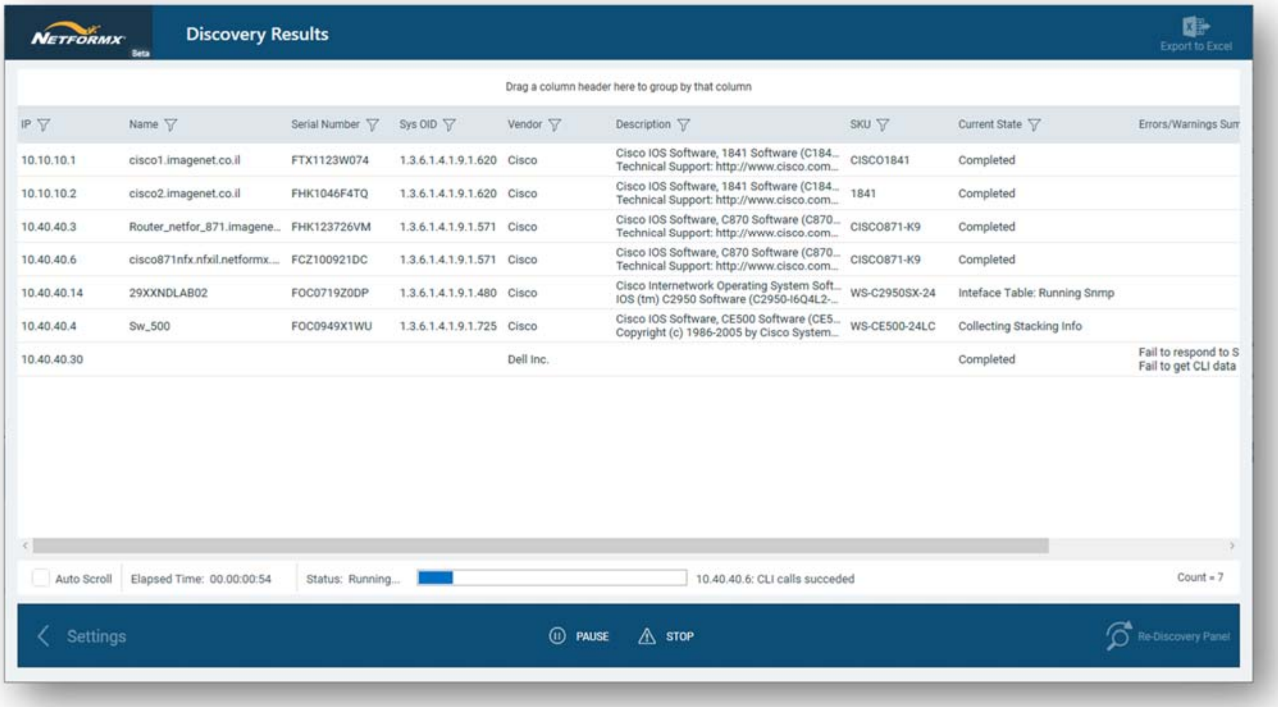
5. Device Discovery Profile

Ping:
✓ Perform Ping ✓ Continue Discovery if Ping Fails
Timeout (MS) 5000 Retries 2

Cisco IP Phones:
✓ Collect

Figure 24: Run a Network Discovery

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

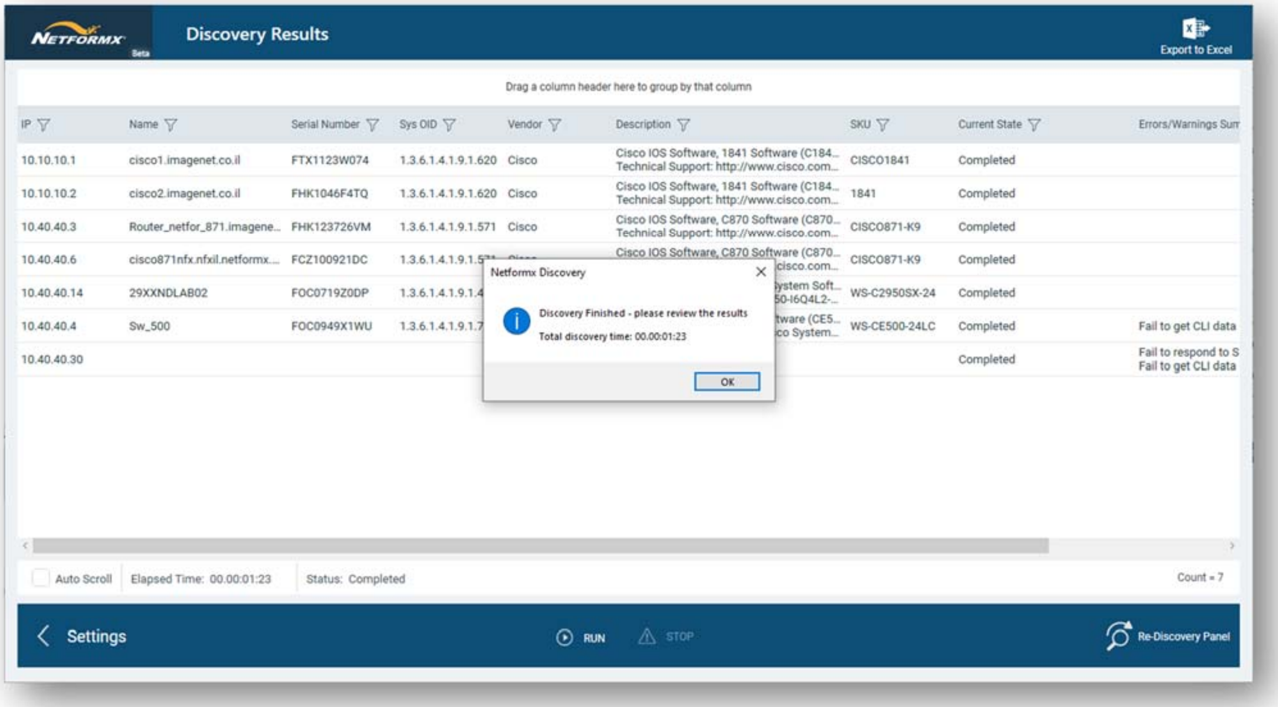


IP	Name	Serial Number	Sys OID	Vendor	Description	SKU	Current State	Errors/Warnings Sum
10.10.10.1	cisco1.imagenet.co.il	FTX1123W074	1.3.6.1.4.1.9.1.620	Cisco	Cisco IOS Software, 1841 Software (C184... Technical Support: http://www.cisco.com...	CISCO1841	Completed	
10.10.10.2	cisco2.imagenet.co.il	FHK1046F4TQ	1.3.6.1.4.1.9.1.620	Cisco	Cisco IOS Software, 1841 Software (C184... Technical Support: http://www.cisco.com...	1841	Completed	
10.40.40.3	Router_netfor_871.imagene...	FHK123726VM	1.3.6.1.4.1.9.1.571	Cisco	Cisco IOS Software, C870 Software (C870... Technical Support: http://www.cisco.com...	CISCO871-K9	Completed	
10.40.40.6	cisco871nfx.nfxil.netformx....	FCZ100921DC	1.3.6.1.4.1.9.1.571	Cisco	Cisco IOS Software, C870 Software (C870... Technical Support: http://www.cisco.com...	CISCO871-K9	Completed	
10.40.40.14	29XXNDLAB02	FOC0719Z0DP	1.3.6.1.4.1.9.1.480	Cisco	Cisco Internetwork Operating System Soft... IOS (tm) C2950 Software (C2950-I6Q4L2-...	WS-C2950SX-24	Inteface Table: Running Snmp	
10.40.40.4	Sw_500	FOC0949X1WU	1.3.6.1.4.1.9.1.725	Cisco	Cisco IOS Software, CE500 Software (CE5... Copyright (c) 1986-2005 by Cisco System...	WS-CE500-24LC	Collecting Stacking Info	
10.40.40.30				Dell Inc.			Completed	Fail to respond to S Fail to get CLI data

□ Auto Scroll   Elapsed Time: 00:00:00:54   Status: Running...   10.40.40.6: CLI calls succeded   Count = 7

Figure 25: 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 shows displays IP, Name, Serial Number, Sys OID, Vendor, SKU, Current State, and any associated error messages.



Discovery Results

Drag a column header here to group by that column

IP	Name	Serial Number	Sys OID	Vendor	Description	SKU	Current State	Errors/Warnings Sum
10.10.10.1	cisco1.imagenet.co.il	FTX1123W074	1.3.6.1.4.1.9.1.620	Cisco	Cisco IOS Software, 1841 Software (C184... Technical Support: http://www.cisco.com...	CISCO1841	Completed	
10.10.10.2	cisco2.imagenet.co.il	FHK1046F4TQ	1.3.6.1.4.1.9.1.620	Cisco	Cisco IOS Software, 1841 Software (C184... Technical Support: http://www.cisco.com...	1841	Completed	
10.40.40.3	Router_netfor_871.imagene...	FHK123726VM	1.3.6.1.4.1.9.1.571	Cisco	Cisco IOS Software, C870 Software (C870... Technical Support: http://www.cisco.com...	CISCO871-K9	Completed	
10.40.40.6	cisco871nfx.nfxil.netformx...	FCZ100921DC	1.3.6.1.4.1.9.1.5		Cisco IOS Software, C870 Software (C870... cisco.com...	CISCO871-K9	Completed	
10.40.40.14	29XXNDLAB02	FOC0719Z0DP	1.3.6.1.4.1.9.1.4		ystem Soft... 50-I6Q4L2-...	WS-C2950SX-24	Completed	
10.40.40.4	Sw_500	FOC0949X1WU	1.3.6.1.4.1.9.1.7		tware (CE5... co System...	WS-CE500-24LC	Completed	Fail to get CLI data
10.40.40.30							Completed	Fail to respond to S Fail to get CLI data

Netformx Discovery

Discovery Finished - please review the results

Total discovery time: 00.00:01:23

OK

☐ Auto Scroll Elapsed Time: 00.00:01:23 Status: Completed Count = 7

Figure 26: Completed Discovery Run

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.

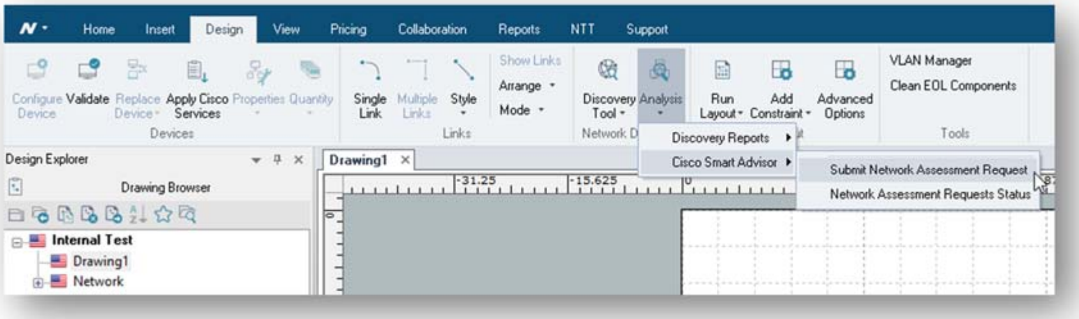
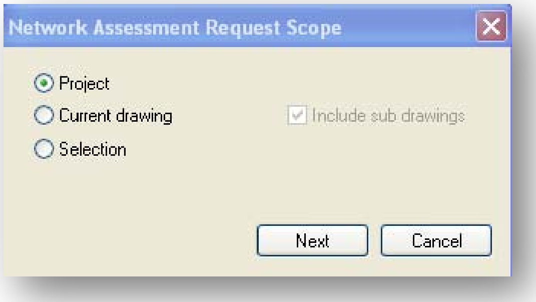


Figure 27: Submit CSA Trigger

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


Network Assessment Request Scope

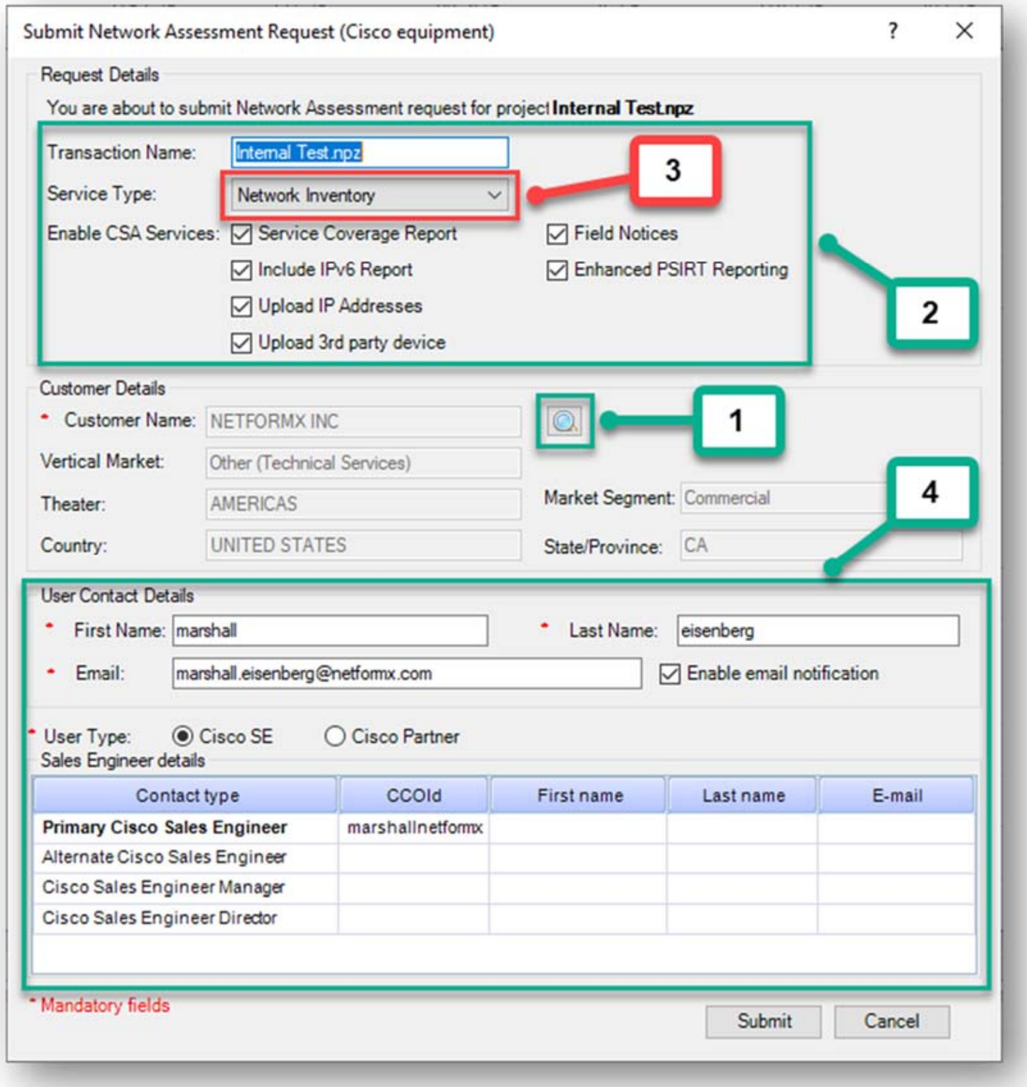
● Project
○ Current drawing
○ Selection
☑ Include sub drawings

Figure 28: 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 Test.npz**

Transaction Name: Internal Test.npz

Service Type: Network Inventory

Enable CSA Services: ☑ Service Coverage Report ☑ Field Notices ☑ Include IPv6 Report ☑ Enhanced PSIRT Reporting ☑ Upload IP Addresses ☑ Upload 3rd party device

Customer Details

* Customer Name: NETFORMX INC

Vertical Market: Other (Technical Services)

Theater: AMERICAS

Market Segment: Commercial

Country: UNITED STATES

State/Province: CA

User Contact Details

* First Name: marshall

* Last Name: eisenberg

* Email: marshall.eisenberg@netformx.com

☑ Enable email notification

* User Type: ● Cisco SE ○ Cisco Partner

Sales Engineer details

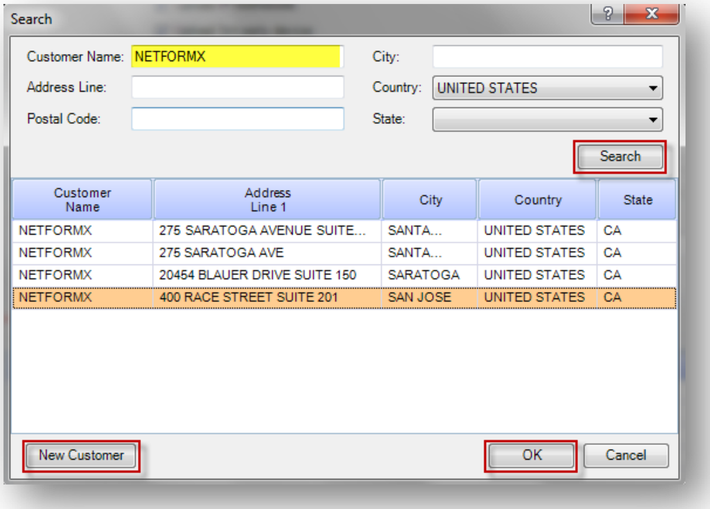
Contact type	CCOId	First name	Last name	E-mail
Primary Cisco Sales Engineer	marshallnetformx			
Alternate Cisco Sales Engineer				
Cisco Sales Engineer Manager				
Cisco Sales Engineer Director				

* Mandatory fields

Figure 29: 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: NETFORMX
City:
Address Line:
Country: UNITED STATES
Postal Code:
State:

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 30: 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:

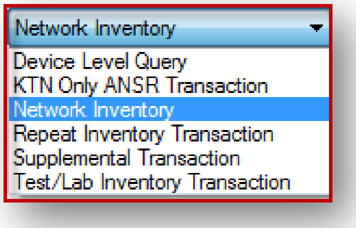

Network Inventory
Device Level Query
KTN Only ANSR Transaction
Network Inventory
Repeat Inventory Transaction
Supplemental Transaction
Test/Lab Inventory Transaction

Figure 31: 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 type of transaction, which includes a full 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 regular 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 that 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 get updates on the status of the CSA process and indication when the report is ready to download from Cisco.

Click **Submit** once you finish filling out the Network Assessment Request form 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.

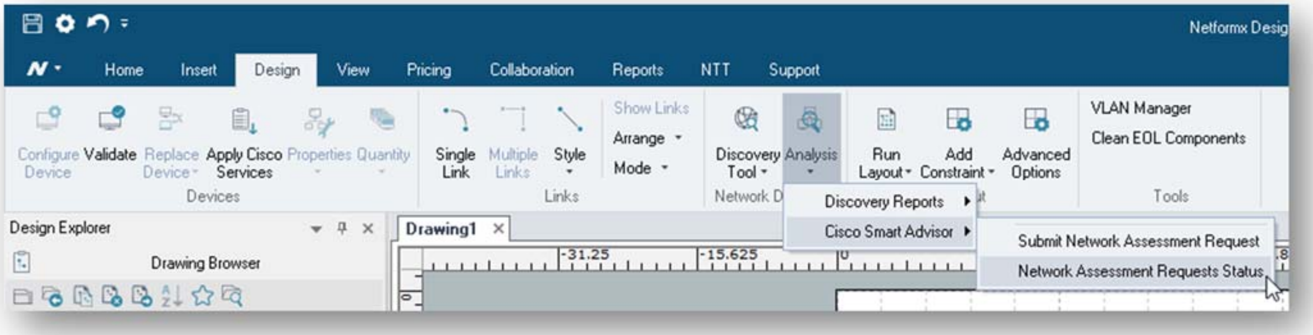
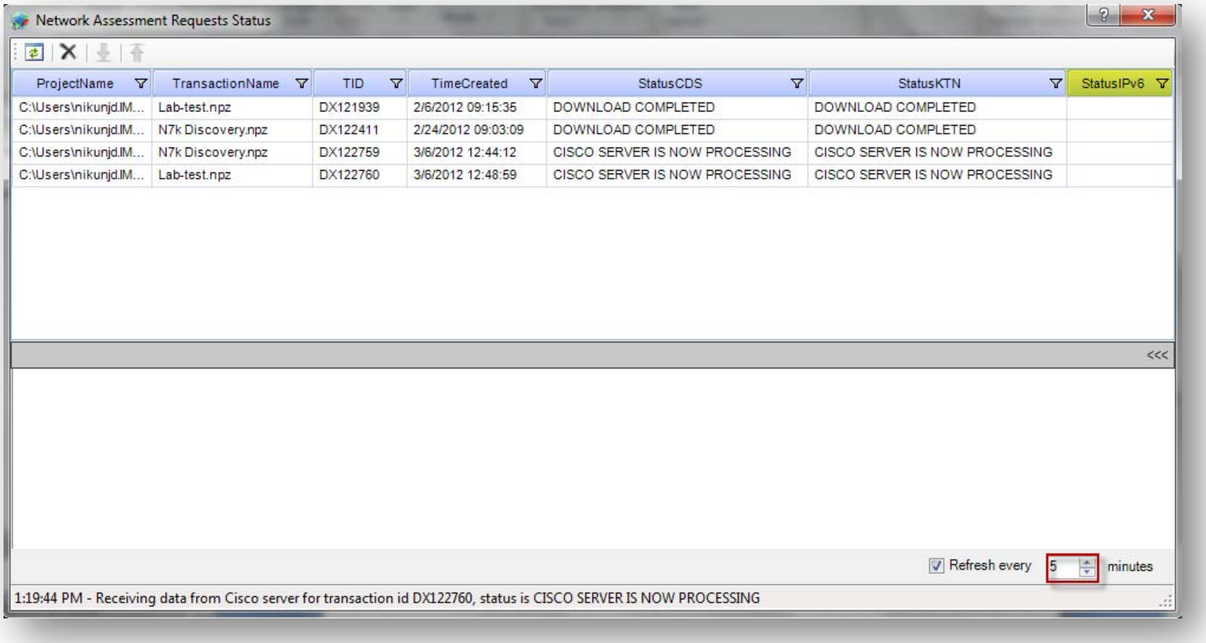


Figure 32: Network Assessment Status Request

The Network Assessment Request Status menu appears.



ProjectName	TransactionName	TID	TimeCreated	StatusCDS	StatusKTN	StatusIPv6
C:\Users\nikunjd.IM...	Lab-test.npz	DX121939	2/6/2012 09:15:35	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED	
C:\Users\nikunjd.IM...	N7k Discovery.npz	DX122411	2/24/2012 09:03:09	DOWNLOAD COMPLETED	DOWNLOAD COMPLETED	
C:\Users\nikunjd.IM...	N7k Discovery.npz	DX122759	3/6/2012 12:44:12	CISCO SERVER IS NOW PROCESSING	CISCO SERVER IS NOW PROCESSING	
C:\Users\nikunjd.IM...	Lab-test.npz	DX122760	3/6/2012 12:48:59	CISCO SERVER IS NOW PROCESSING	CISCO SERVER IS NOW PROCESSING	

☑ Refresh every 5 minutes

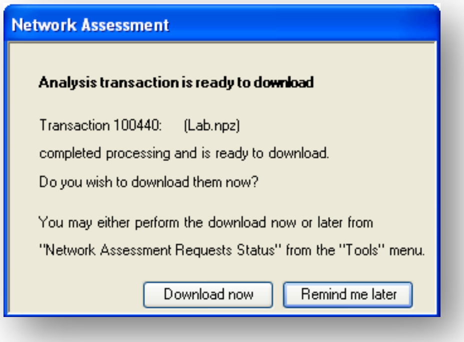
1:19:44 PM - Receiving data from Cisco server for transaction id DX122760, status is CISCO SERVER IS NOW PROCESSING

Figure 33: 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 status, 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.



Analysis transaction is ready to download

Transaction 100440: (Lab.npz)
completed processing and is ready to download.
Do you wish to download them now?

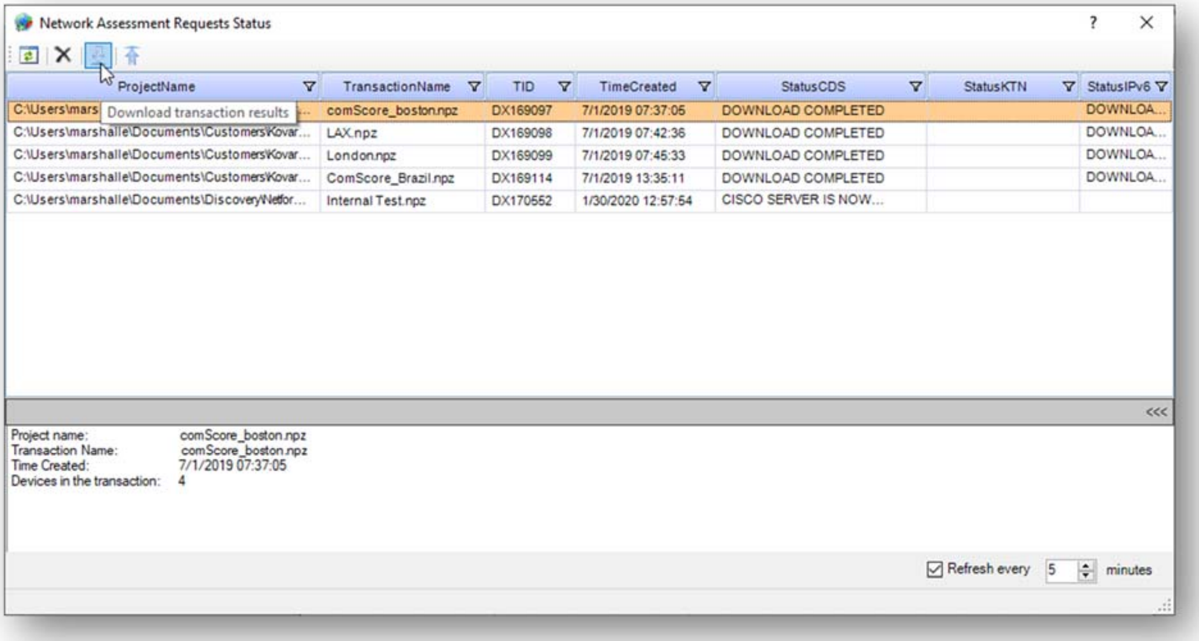
You may either perform the download now or later from
"Network Assessment Requests Status" from the "Tools" menu.

Figure 34: 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.


Network Assessment Requests Status
?
Download transaction results
<<<

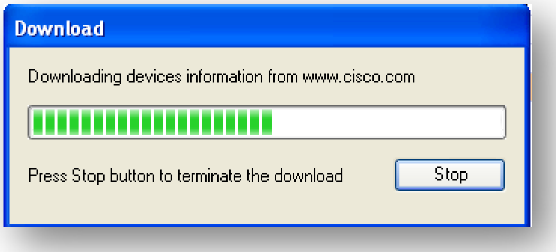
ProjectName	TransactionName	TID	TimeCreated	StatusCDS	StatusKTN	StatusIPv6
C:\Users\mars…	comScore_boston.npz	DX169097	7/1/2019 07:37:05	DOWNLOAD COMPLETED		DOWNLOA…
C:\Users\marshalle\Documents\Customers\Kovar…	LAX.npz	DX169098	7/1/2019 07:42:36	DOWNLOAD COMPLETED		DOWNLOA…
C:\Users\marshalle\Documents\Customers\Kovar…	London.npz	DX169099	7/1/2019 07:45:33	DOWNLOAD COMPLETED		DOWNLOA…
C:\Users\marshalle\Documents\Customers\Kovar…	ComScore_Brazil.npz	DX169114	7/1/2019 13:35:11	DOWNLOAD COMPLETED		DOWNLOA…
C:\Users\marshalle\Documents\DiscoveryNetfor…	Internal Test.npz	DX170552	1/30/2020 12:57:54	CISCO SERVER IS NOW…		

Project name:	comScore_boston.npz
Transaction Name:	comScore_boston.npz
Time Created:	7/1/2019 07:37:05
Devices in the transaction:	4

☑ Refresh every 5 minutes

Figure 35: Selecting a Finished Network Transaction for Download

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



Download

Downloading devices information from www.cisco.com

Press Stop button to terminate the download

Figure 36: 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. In the event 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 does not receive Field Notice or PSIRT information in your report, contact Cisco and note the applicable Transaction ID in your communication. Cisco should respond to your initial request for help 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.

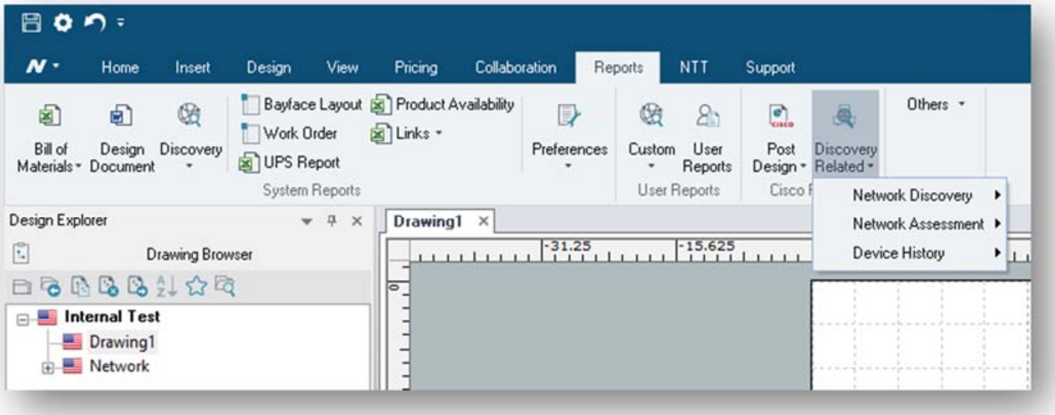


Figure 37: Accessing Cisco Reports

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 places particular emphasis on highlighting equipment that has reached or is approaching the Last Day of Support (also called EOL). 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 useful 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 results for CSA analysis 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.

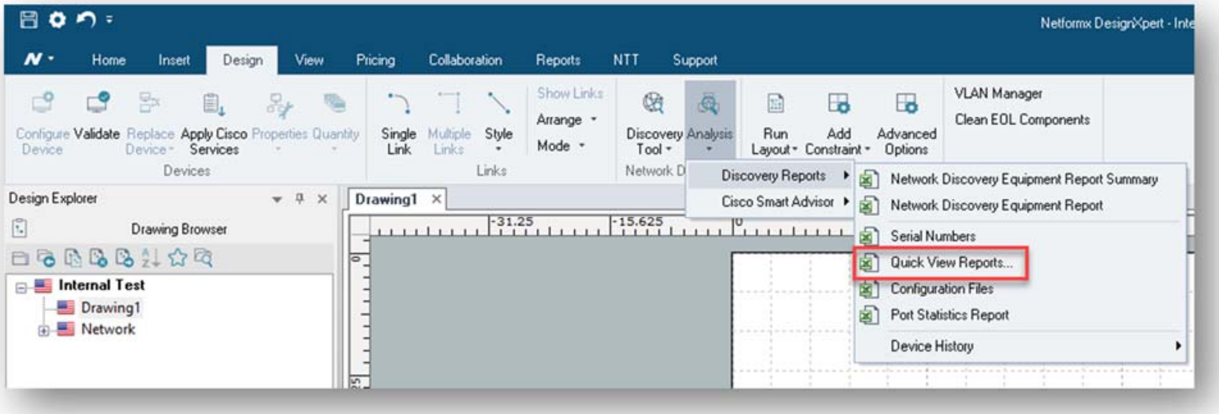


Figure 38: Accessing Quick View Reports

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 description.
- **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.

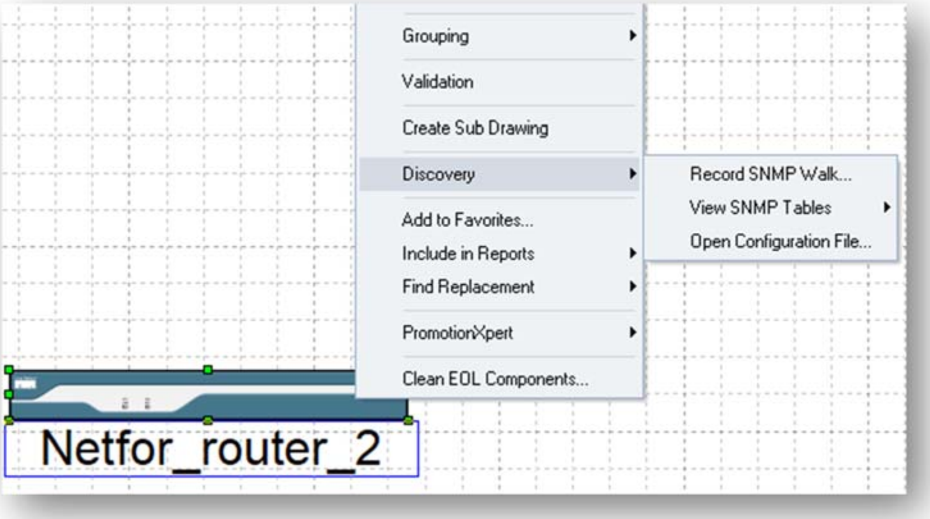


Figure 39: Right-click to Expose Discovery Information

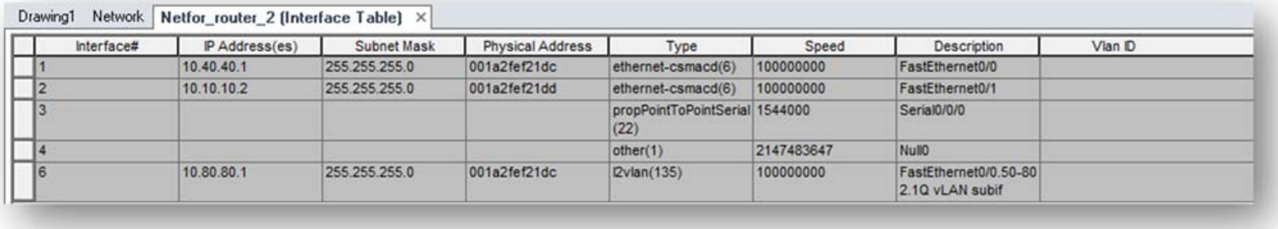
The context menu includes a Discovery option that contains three additional elements:

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

  To create and record **SNMP Walk**:

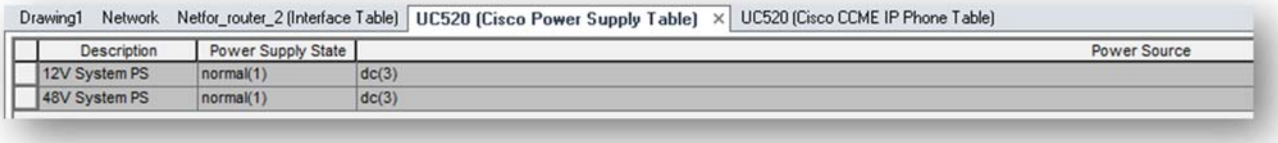
  1. From the Design Tab → Discovery Tools → Record SNMP Walk to display the Record **SNMP Walk** menu.
  2. Define your **Output File Name** and Folder location.
  3. Enter the IP Address of the device you wish to track (log) in the **IP Address** field.
  4. Enter the Root OID. The SNMP will log all entries for this SNMP subtree level.
  5. Set the device SNMP **Version** (v1, v2c, or V3).
     - Enter the Community String for SNMPv1/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** – Allows you access to the following SNMP tables
  - **Interfaces**
  - **Power**
  - **IP Phones**



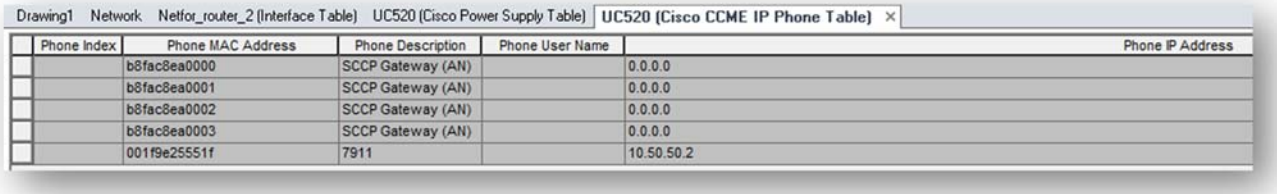
Interface#	IP Address(es)	Subnet Mask	Physical Address	Type	Speed	Description	Vlan ID
1	10.40.40.1	255.255.255.0	001a2fef21dc	ethernet-csmacd(6)	100000000	FastEthernet0/0	
2	10.10.10.2	255.255.255.0	001a2fef21dd	ethernet-csmacd(6)	100000000	FastEthernet0/1	
3				propPointToPointSerial (22)	1544000	Serial0/0/0	
4				other(1)	2147483647	Null0	
6	10.80.80.1	255.255.255.0	001a2fef21dc	l2vlan(135)	100000000	FastEthernet0/0.50-80 2.1Q vLAN subif	

Figure 40: SNMP Interface Table


Drawing1
Network
Netfor_router_2 (Interface Table)
UC520 (Cisco Power Supply Table)
UC520 (Cisco CCME IP Phone Table)

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

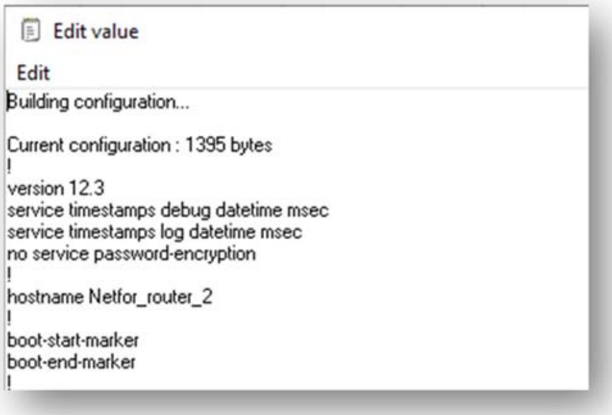
Figure 41: SNMP Power Supply Table


Drawing1
Network
Netfor_router_2 (Interface Table)
UC520 (Cisco Power Supply Table)
UC520 (Cisco CCME IP Phone 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 42: 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).



```
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 43: 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 ".ndr" 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.
- Discovery runs from workstations directly connected to the network and not across a low-speed WAN or wireless connection for optimum performance.
- 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.ndr*. 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.

    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