COMODO
Creating Trust Online®

COMODO
one

Comodo One

Software Version 3.26

Network Assessment Tool Administrator Guide

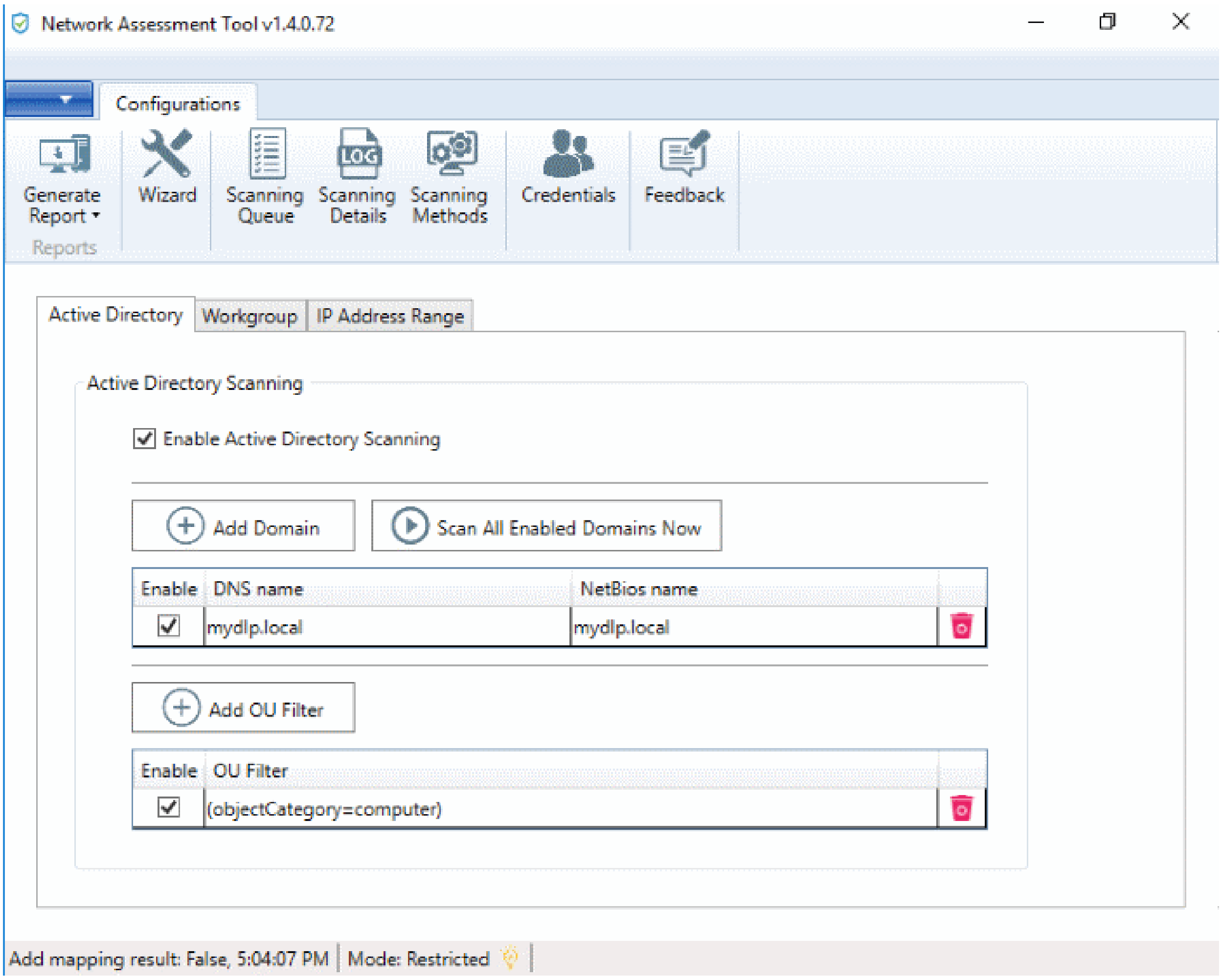
Guide Version 1.3.010820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Network Assessment Tool

- The network assessment tool lets you perform in-depth scans on client networks to identify a wide range of server, endpoint and network vulnerabilities.
- The tool also prepares detailed reports which contain a risk mitigation plan to address each issue.
- Setup is easy with a simple wizard that allows you to import networks via Active Directory, workgroup or IP range.
- This guide takes you through the initial installation and configuration processes before moving onto more detailed descriptions of settings and program usage.



☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted

Guide Structure

- **Introduction to Network Assessment Tool**
  - **Quick Start Guide**
  - **System Requirements**
  - **Installing Network Assessment Tool**
  - **Configuration Wizard**
  - **The NAT Administrative Console**

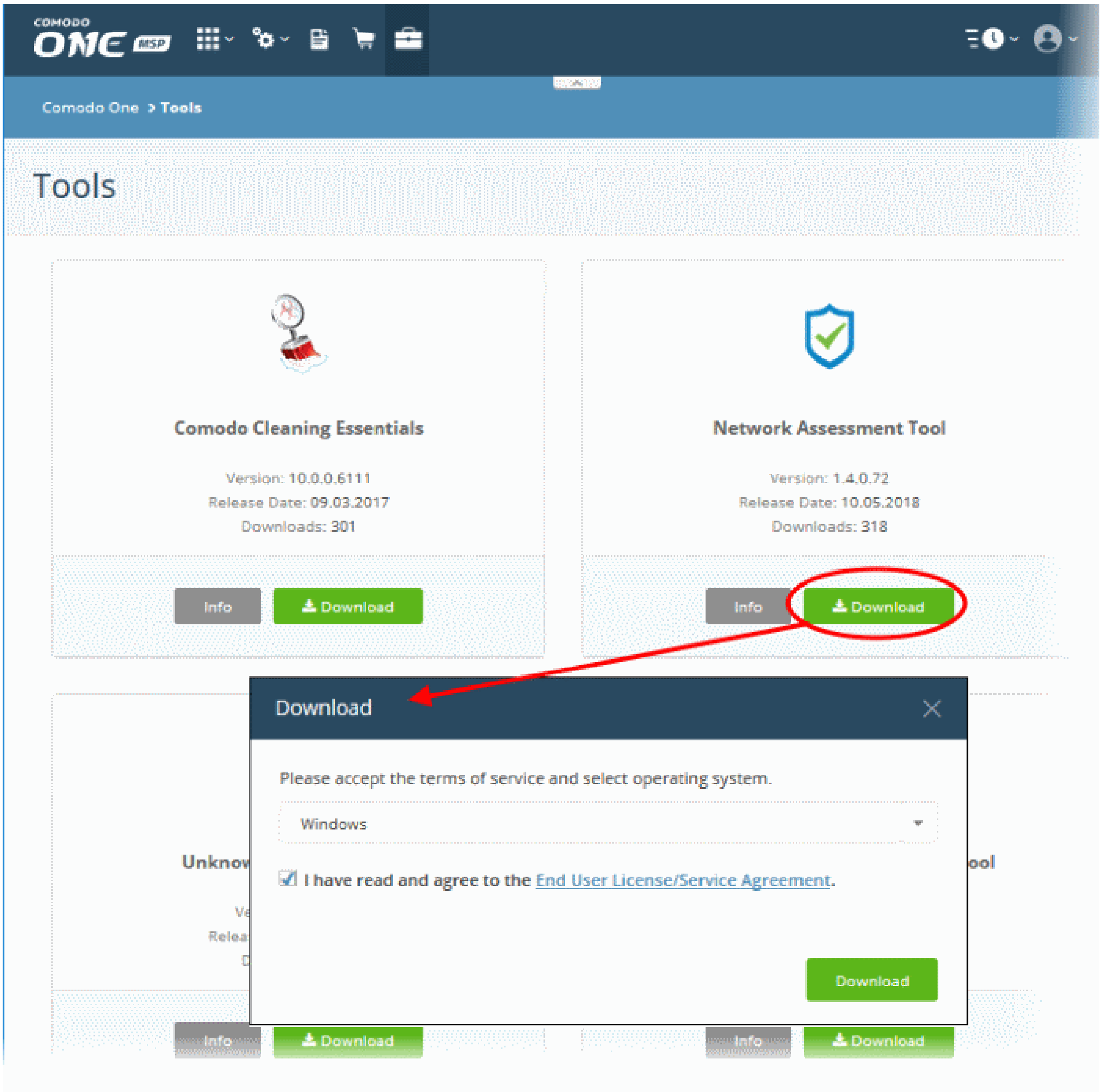
1.1 Quick Start Guide

This tutorial explains how to setup the Network Assessment Tool (NAT) tool and run a scan on a target network.

- **Step 1 - Login to Comodo One and download the NAT Tool**
- **Step 2 - Install NAT Tool**
- **Step 3 - Run Initial Configuration Wizard**
- **Step 4 - Add Networks**
- **Step 5 - Add Credentials and Map to Respective Networks**
- **Step 6 - Run a Scan**
- **Step 7 - Generate Reports**

Step 1 - Login to Comodo One and download the NAT Tool

- Login to your Comodo One account at **https://one.comodo.com/app/login**.
- Click 'Tools' on the top-menu.
- Click 'Download' in the 'Network Assessment Tool' tile:



Please accept the terms of service and select operating system.

☑ I have read and agree to the End User License/Service Agreement.

- Agree to the EULA then click the 'Download' button

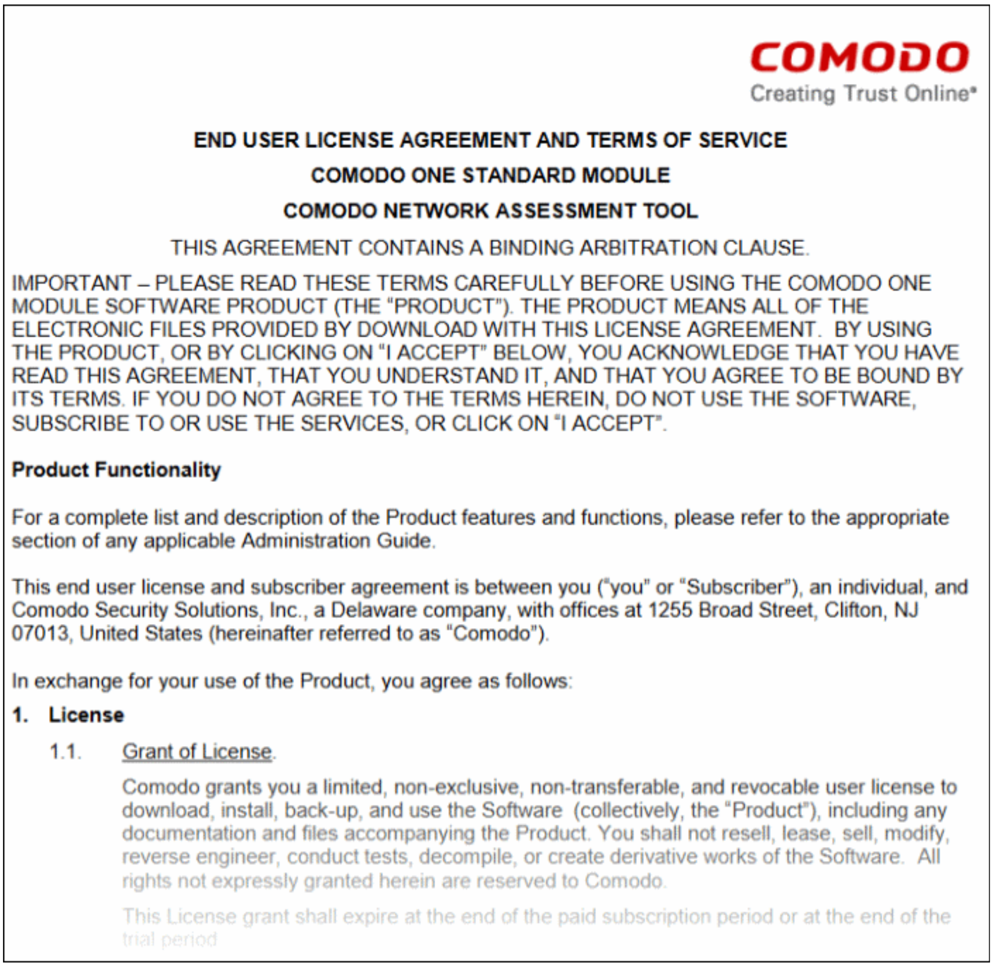
Step 2 - Install NAT Tool

Prerequisite - To work correctly, NAT requires that Network Mapper (NMAP) and Microsoft Baseline Security Analyzer (MBSA) are also installed . The installation wizard allows you to download both both applications if you do not have them already.

- Double click on the setup file to start the NAT installation wizard
- Follow the wizard and continue the installation.

On completion of installation, the wizard will check whether the prerequisite software MBSA and NMAP are installed.

- If available, the installation will complete and will move to the **initial configuration wizard**.



END USER LICENSE AGREEMENT AND TERMS OF SERVICE

COMODO ONE STANDARD MODULE

COMODO NETWORK ASSESSMENT TOOL

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONE MODULE SOFTWARE PRODUCT (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

Product Functionality

For a complete list and description of the Product features and functions, please refer to the appropriate section of any applicable Administration Guide.

This end user license and subscriber agreement is between you ("you" or "Subscriber"), an individual, and Comodo Security Solutions, Inc., a Delaware company, with offices at 1255 Broad Street, Clifton, NJ 07013, United States (hereinafter referred to as "Comodo").

In exchange for your use of the Product, you agree as follows:

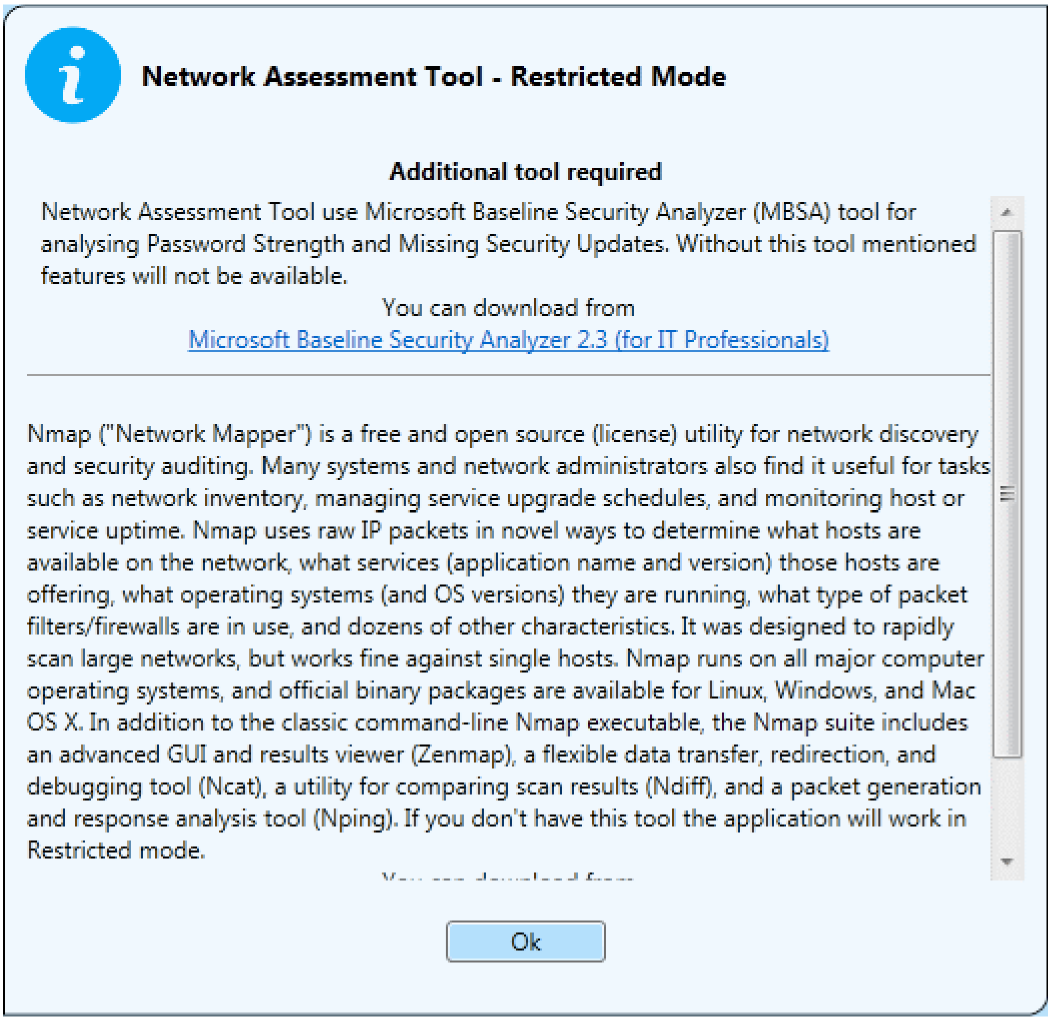
1. License

1.1. Grant of License.

Comodo grants you a limited, non-exclusive, non-transferable, and revocable user license to download, install, back-up, and use the Software (collectively, the "Product"), including any documentation and files accompanying the Product. You shall not resell, lease, sell, modify, reverse engineer, conduct tests, decompile, or create derivative works of the Software. All rights not expressly granted herein are reserved to Comodo.

This License grant shall expire at the end of the paid subscription period or at the end of the trial period

- Agree to the terms and conditions and follow the steps in the installation wizard.
- The wizard will check whether the required NMAP and MBSA software are installed.
  - If they are installed, NAT installation will complete and you'll move to the **initial configuration wizard**.
  - If they are not installed, you will see a dialog with download links for the tools. Follow the instructions and install the two tools:



Network Assessment Tool - Restricted Mode

Additional tool required

Network Assessment Tool use Microsoft Baseline Security Analyzer (MBSA) tool for analysing Password Strength and Missing Security Updates. Without this tool mentioned features will not be available.

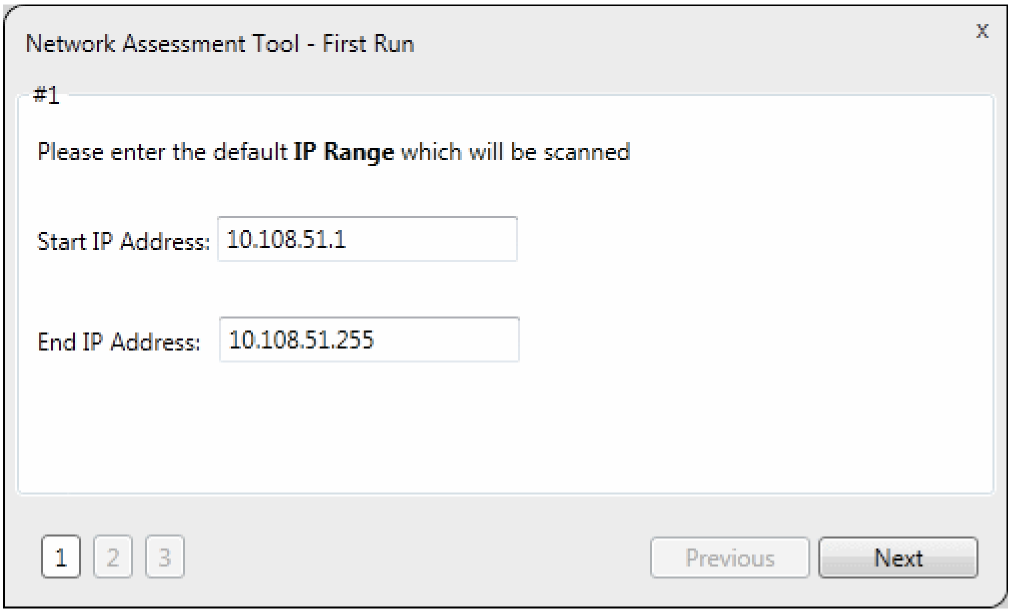
You can download from

Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping). If you don't have this tool the application will work in Restricted mode.

Step 3 - Run Initial Configuration Wizard

The configuration wizard begins once NAT installation is complete:



Network Assessment Tool - First Run

#1

Please enter the default **IP Range** which will be scanned

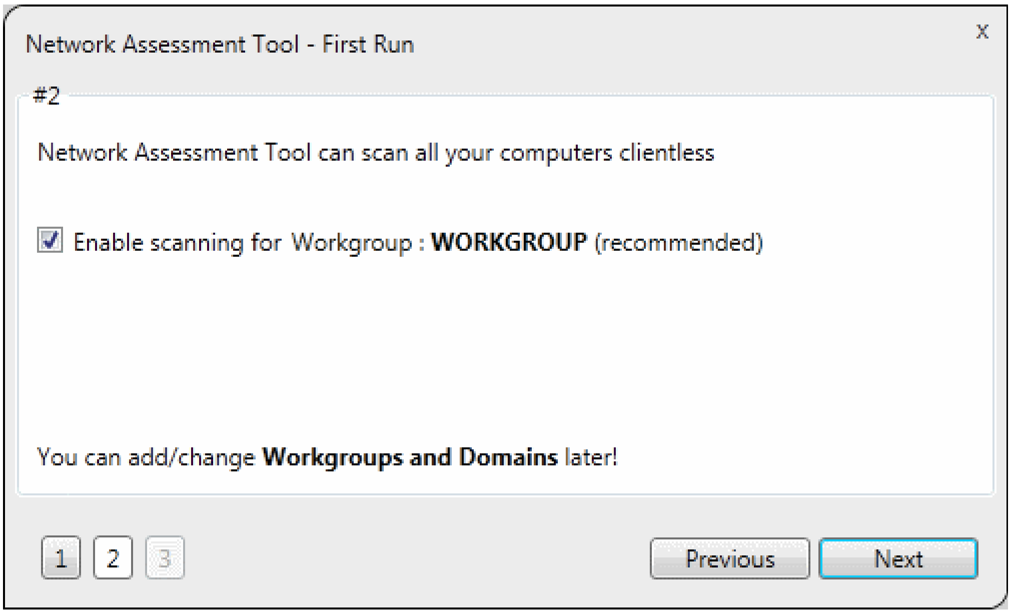
Start IP Address: 10.108.51.1

End IP Address: 10.108.51.255

NAT automatically identifies the workgroup or domain to which your computer is connected.

- Select 'Enable scanning Workgroup/Domain' if you want to automatically add workgroup/domain

- Click 'Next'.



Network Assessment Tool - First Run

#2

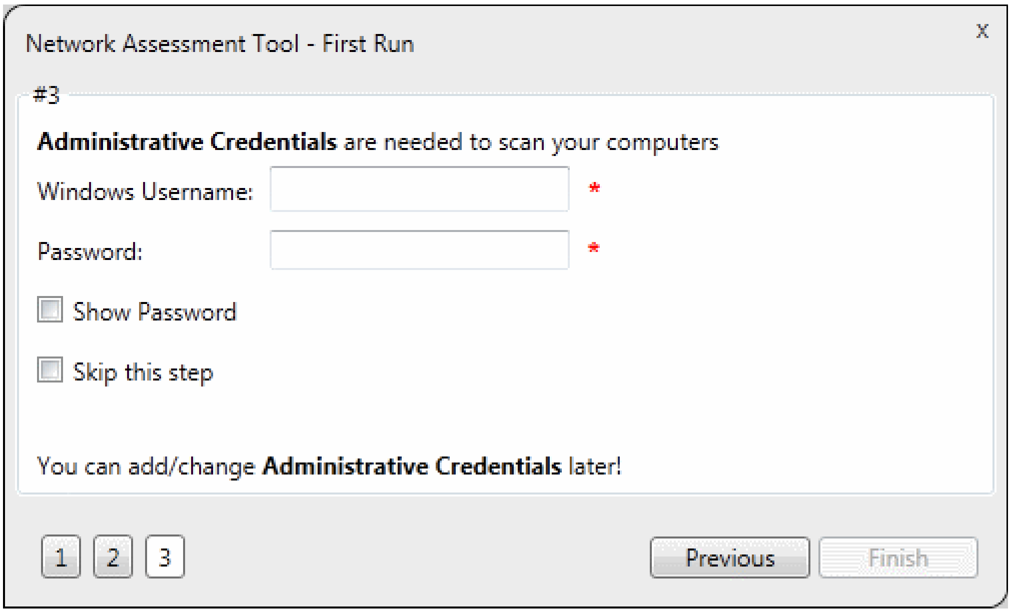
Network Assessment Tool can scan all your computers clientless

☑ Enable scanning for Workgroup : **WORKGROUP** (recommended)

You can add/change **Workgroups and Domains** later!

NAT automatically identifies the workgroup or domain to which your computer is a member of and displays it.

- Select 'Enable scanning Workgroup/Domain' if you want to automatically add workgroup/domain
- Click 'Next'.



Network Assessment Tool - First Run

#3

Administrative Credentials are needed to scan your computers

Windows Username: *

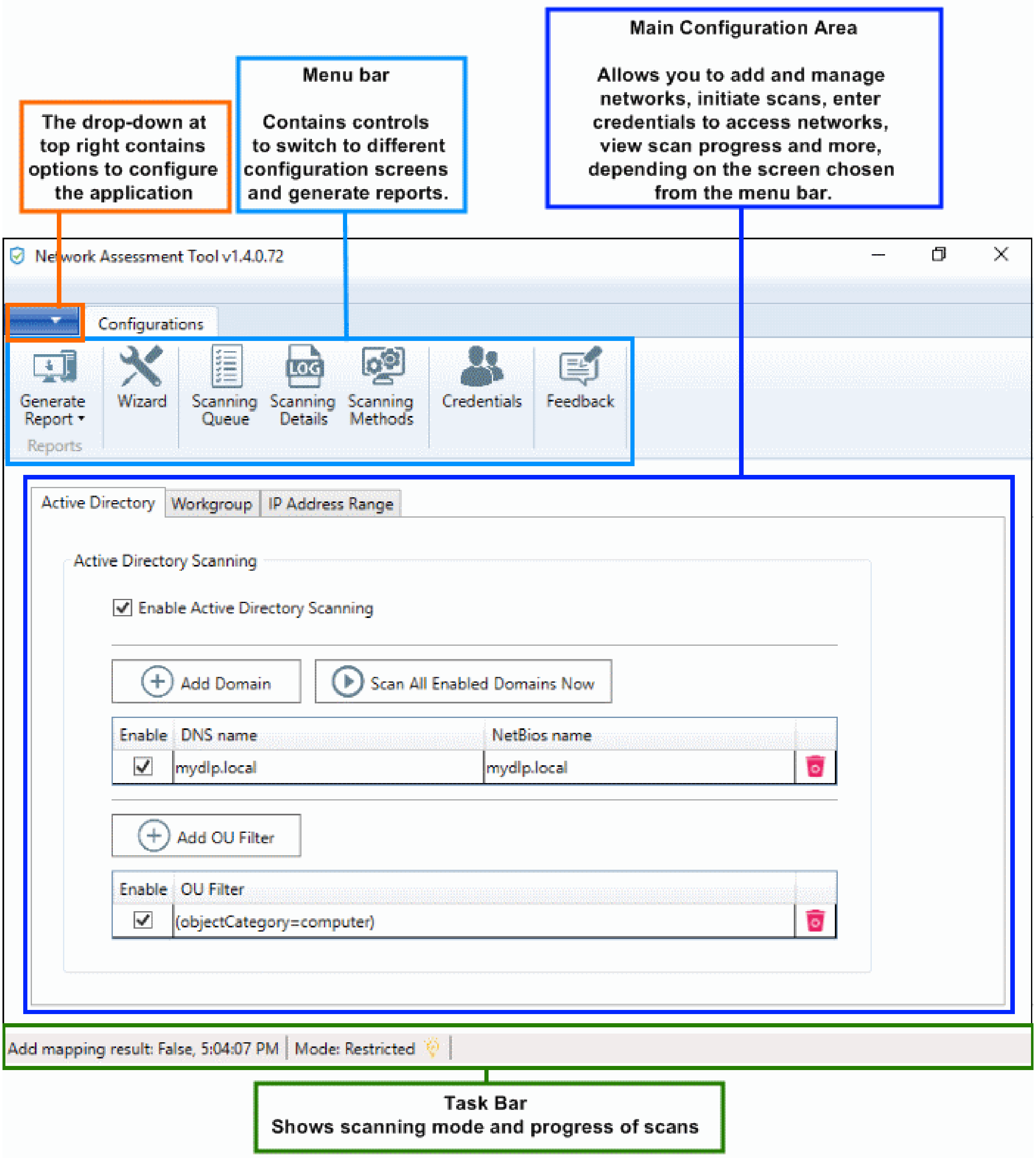
Password: *

□ Show Password

□ Skip this step

You can add/change **Administrative Credentials** later!

- Enter an admin username and password for the target network and click 'Finish'.
- NAT will immediately begin scanning your network. Progress is shown at the bottom of the main interface:



Main Configuration Area

Allows you to add and manage networks, initiate scans, enter credentials to access networks, view scan progress and more, depending on the screen chosen from the menu bar.

Menu bar

Contains controls to switch to different configuration screens and generate reports.

The drop-down at top right contains options to configure the application

☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted

Task Bar
Shows scanning mode and progress of scans

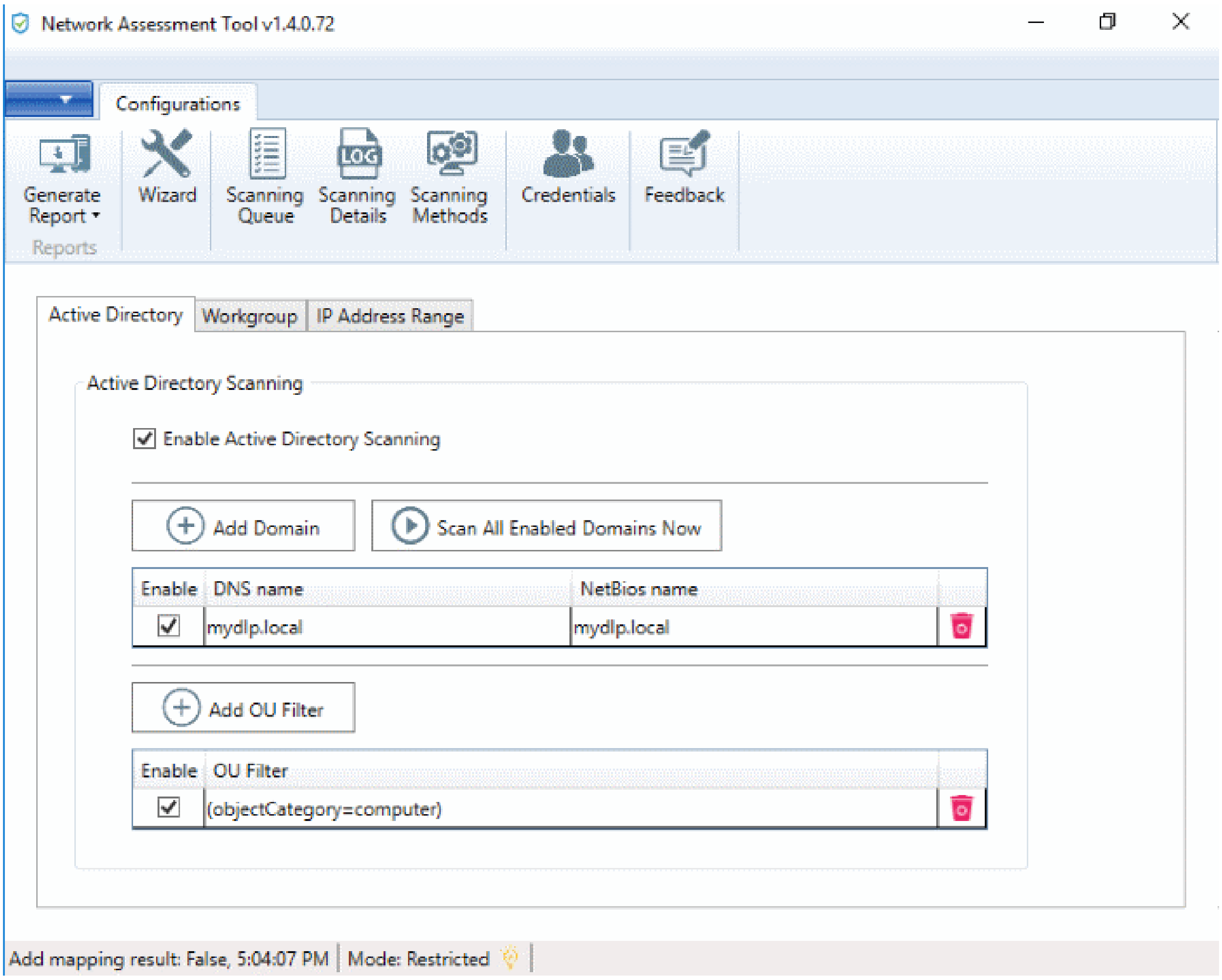
- To view scan progress, click the 'Scanning Queue' button
- To generate reports on completion of scan, click 'Generate Report'.

Step 4 - Add Networks

NAT allows you to add multiple target networks. You can add networks via Active Directory domain, by Workgroup or by IP range.

To add a network:

- Click 'Scanning Methods' on the menu bar:

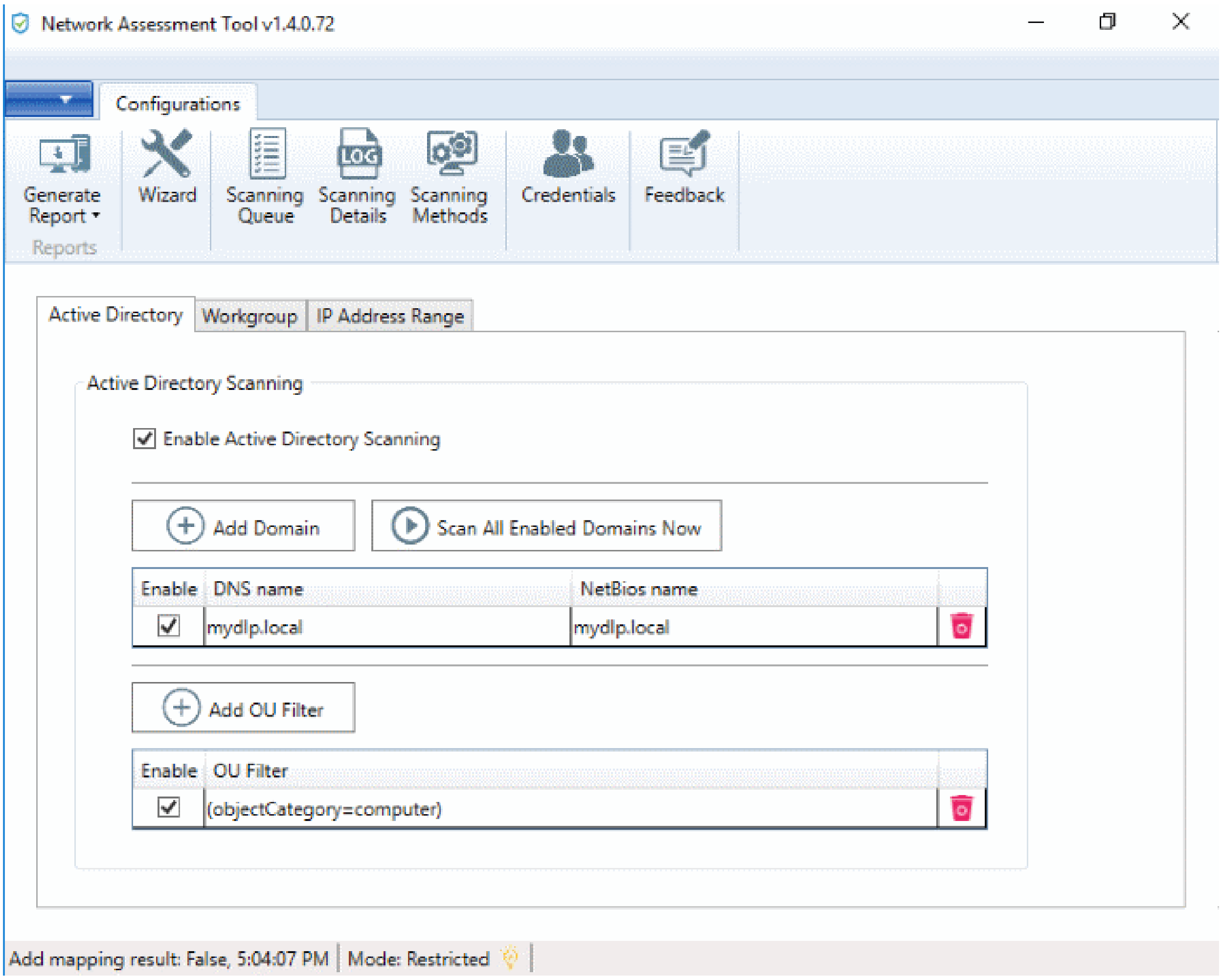


☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted



☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted

- Select 'Active Directory', 'Workgroup' or 'IP Address Range' tab depending on the type you want to add.

Add an Active Directory domain

- Click the 'Active Directory' tab
- Make sure 'Enable Active Directory Scanning' is selected
- Click 'Add Domain'

  A new row will be added to the list
- Enter the DNS and NetBios names in the respective fields.

Add a workgroup

- Click the 'Workgroup' tab
- Make sure 'Enable Workgroup Scanning' is selected
- Click 'Add Workgroup'

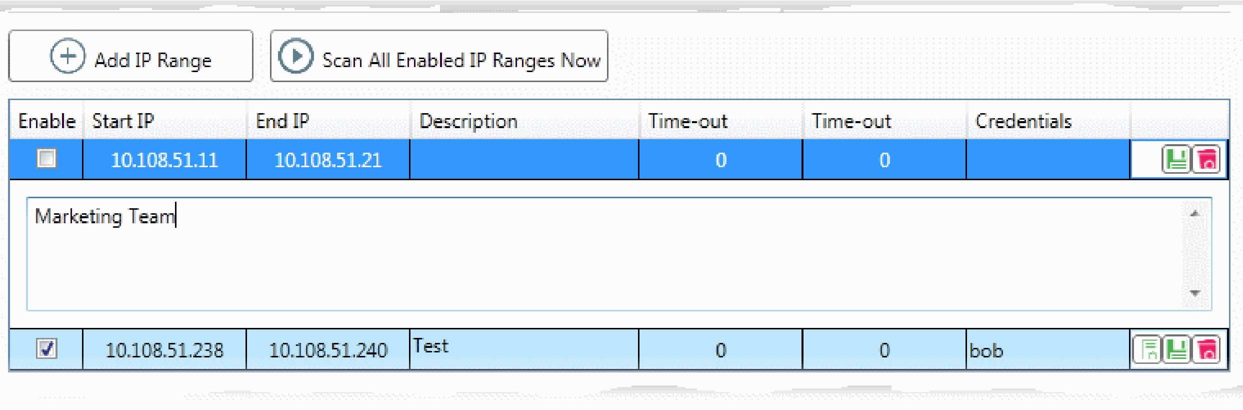
  A new row will be added
- Enter the name of the workgroup you want to scan

Add an IP Address Range

- Click the 'IP Address Range' tab
- Make sure 'Enable IP Address Range Scanning' is selected
- Click 'Add IP Range'

  A new row will be added to the list
- Enter the start and end IP addresses in the respective fields
- Enter a description for the IP range in the text-box

- Time out period - Skip scans on endpoints that do not respond in the set time.



Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials
☐	10.108.51.11	10.108.51.21		0	0	
☑	10.108.51.238	10.108.51.240	Test	0	0	bob

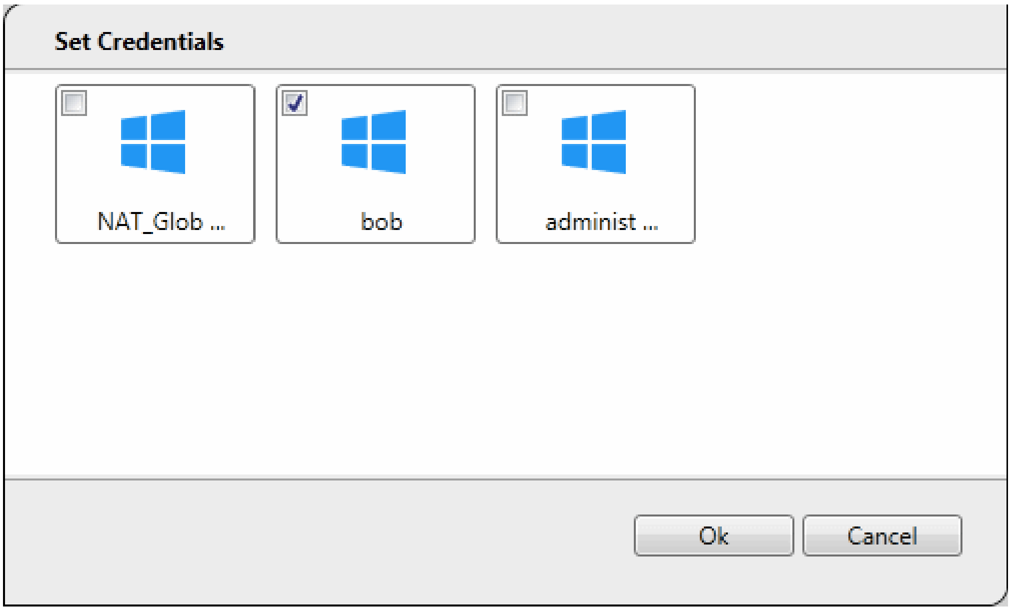
Marketing Team

- Click the 'Save' button to add the IP range.

  The next step is to map login credentials to the IP address range. NAT saves the credentials you entered during initial configuration.

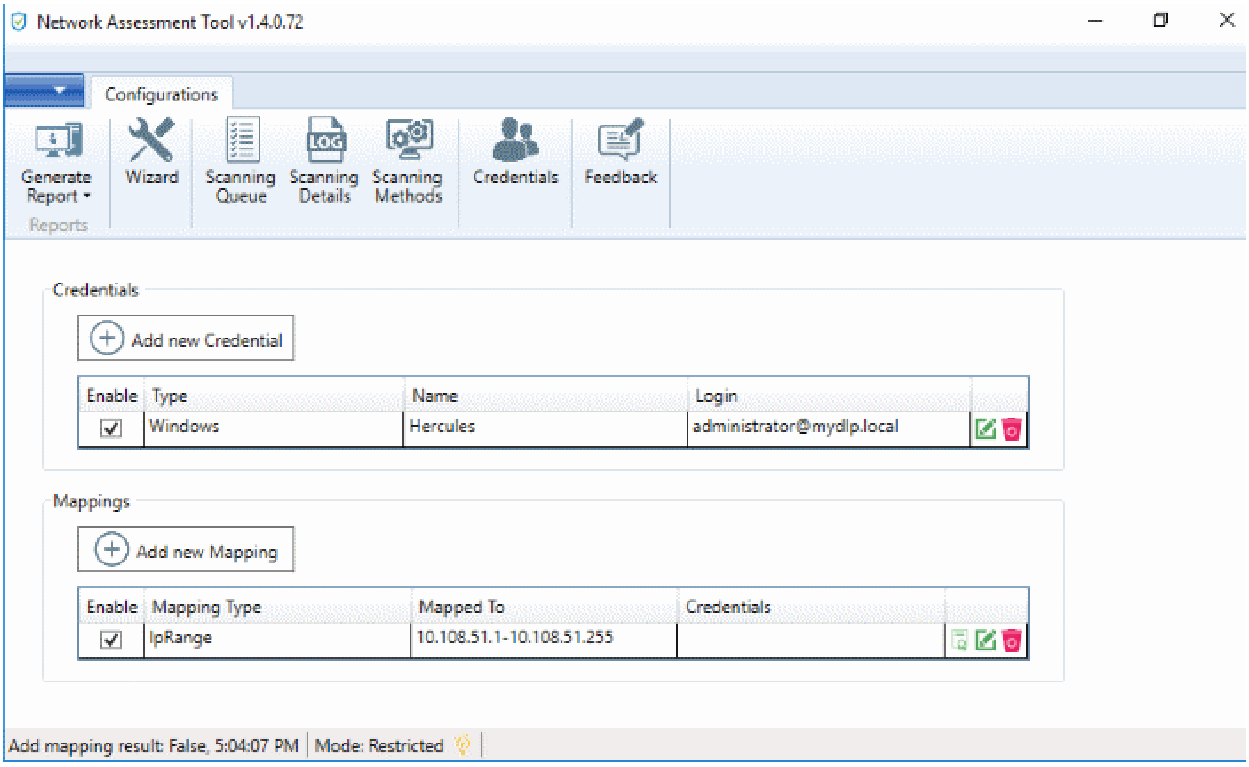
  - Click the 'Credentials' button in the top-menu if you want to add more accounts. The next section, **Step 5 - Add Credentials and Map to Respective Networks**, offers help with this if you need it.

- Click the 'Add Credential' button and select the logins you want to map to the IP range. All credentials must be able to access endpoints in the range.



Step 5 - Add Credentials and Map to Respective Networks

- You need to provide admin username and password for target networks so NAT can scan their endpoints.
- You can map multiple credentials to a single network. NAT will try all credentials if one set fails on a particular endpoint.
- Click 'Credentials' on the menu bar to get started:



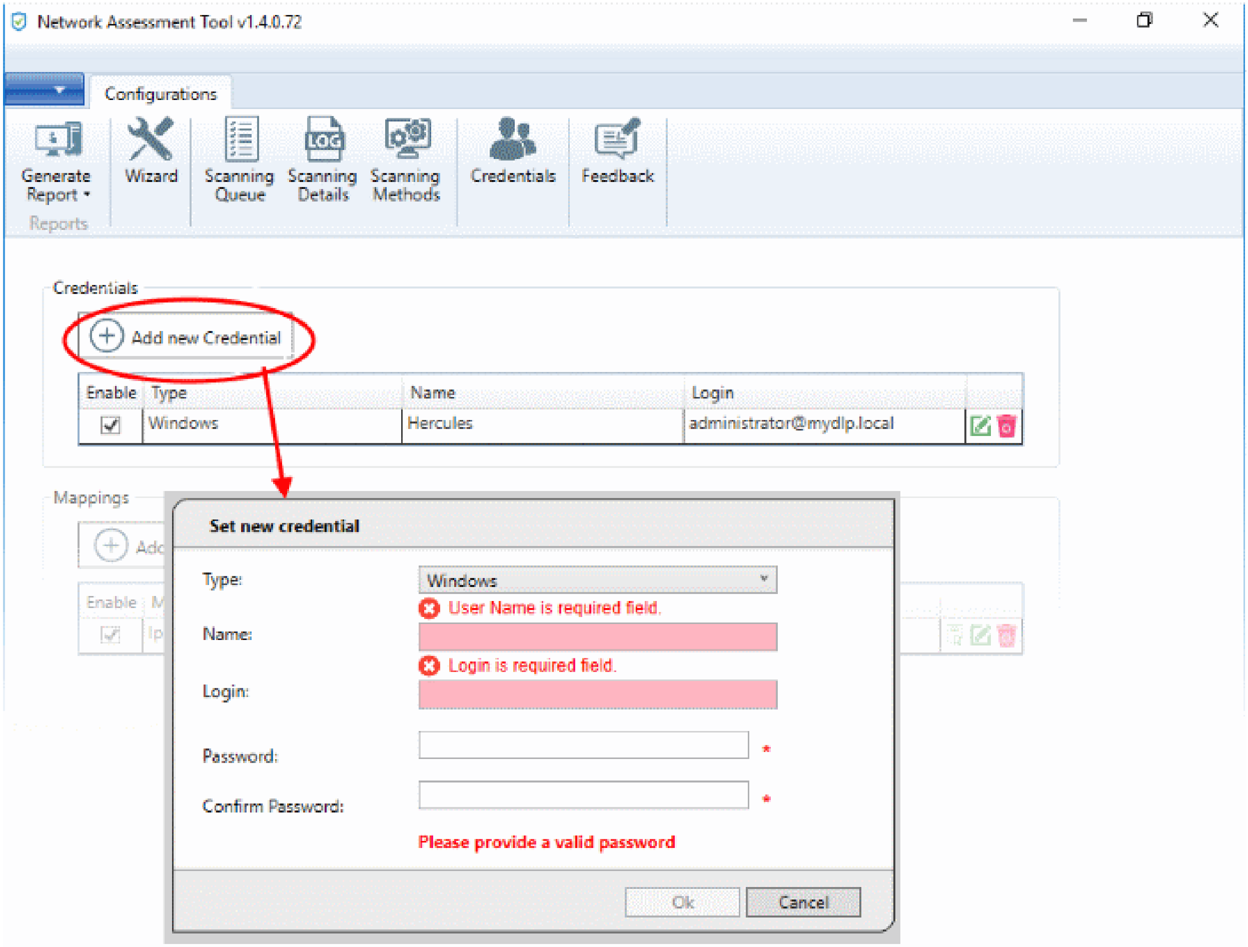
Enable	Type	Name	Login
☑	Windows	Hercules	administrator@mydlp.local

Enable	Mapping Type	Mapped To	Credentials
☑	IpRange	10.108.51.1-10.108.51.255	

Add mapping result: False, 5:04:07 PM | Mode: Restricted

To add a new login credential

- click 'Add new Credential'



Enable	Type	Name	Login
☑	Windows	Hercules	administrator@mydlp.local

Set new credential

Type: Windows

User Name is required field.

Name:

Login is required field.

Login:

Password: *

Confirm Password: *

Please provide a valid password

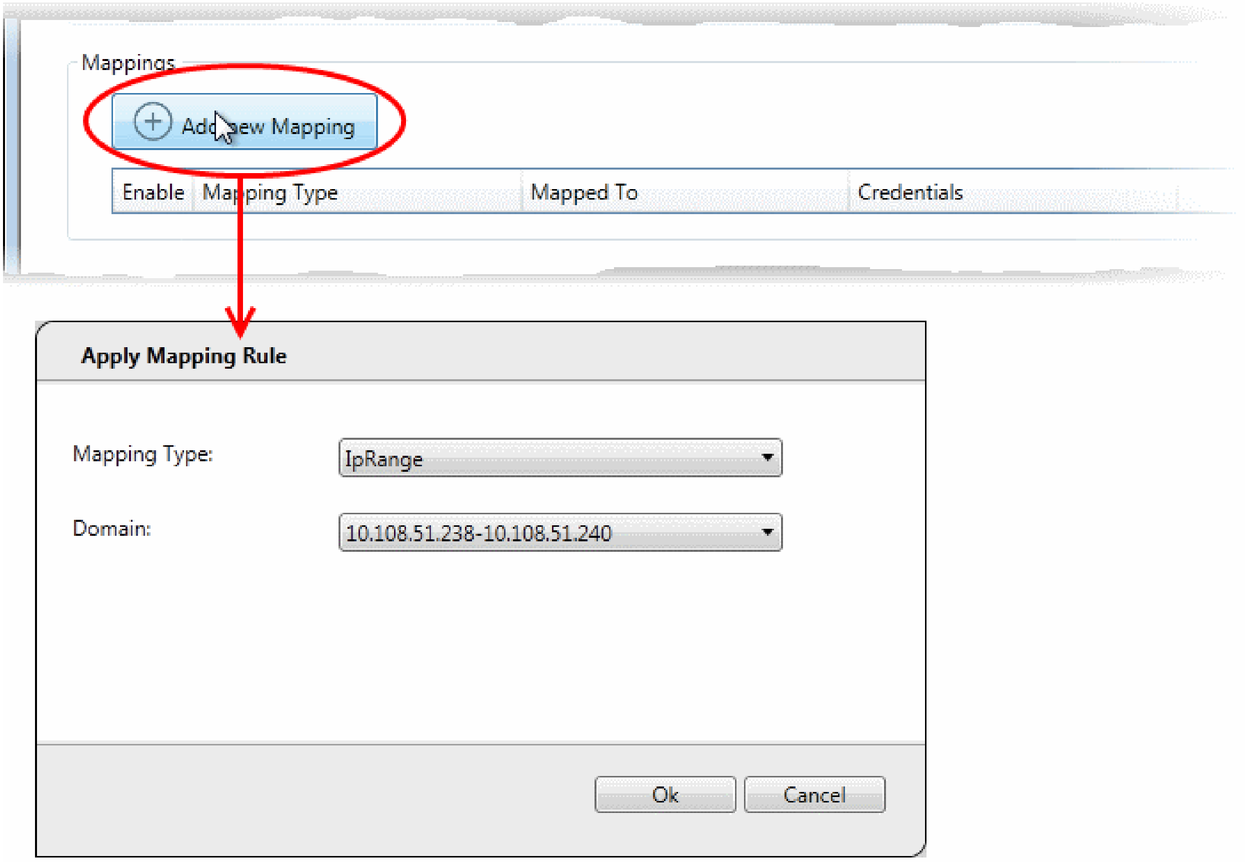
The 'Set new credential' dialog will open.

Set new credential dialog - Form parameters	
Form Element	**Description**
Type	Choose the operating system of the endpoints to which the credentials apply.
Name	A name to identify the account. For example, the name of the administrator
Login	The admin username
Password	The admin password

- Click 'OK' to add the credential
- Repeat the process to add more credentials

Map credentials to a network

- Click the 'Credentials' button in the top menu
- Click 'Add new Mapping' to open the wizard:



Apply Mapping Rule

Mapping Type: IpRange

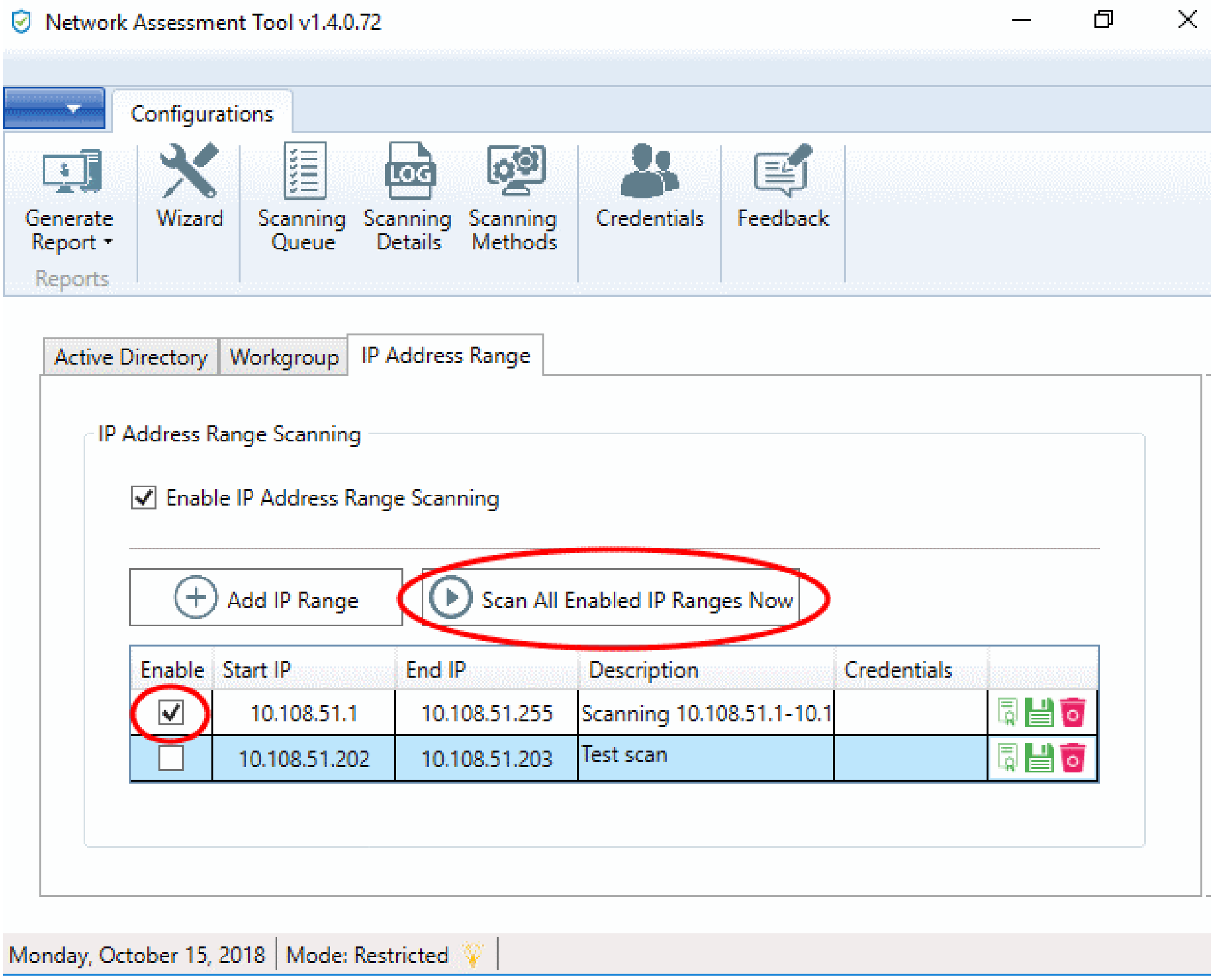
Domain: 10.108.51.238-10.108.51.240

- Mapping Type - Choose the type of network to which the credentials. Choices are 'IP Range', 'Domain' and 'Workgroup'.
- Domain - Choose the network to which the credentials apply. The drop-down shows all networks you have added of the type you chose as the 'Mapping Type'.
- Click 'Ok'
- Repeat the process to map the credentials to different networks as needed

Step 6 - Run a Scan

- Click 'Scanning Methods' on the menu bar

- Click the tab of the type of network you want to scan - 'Active Directory', 'Workgroup', 'IP range'.
- Ensure the networks you want to scan are enabled. Disable those you do not want to scan.
- Click 'Scan All Enabled Domains/Workgroups/IP Ranges Now':

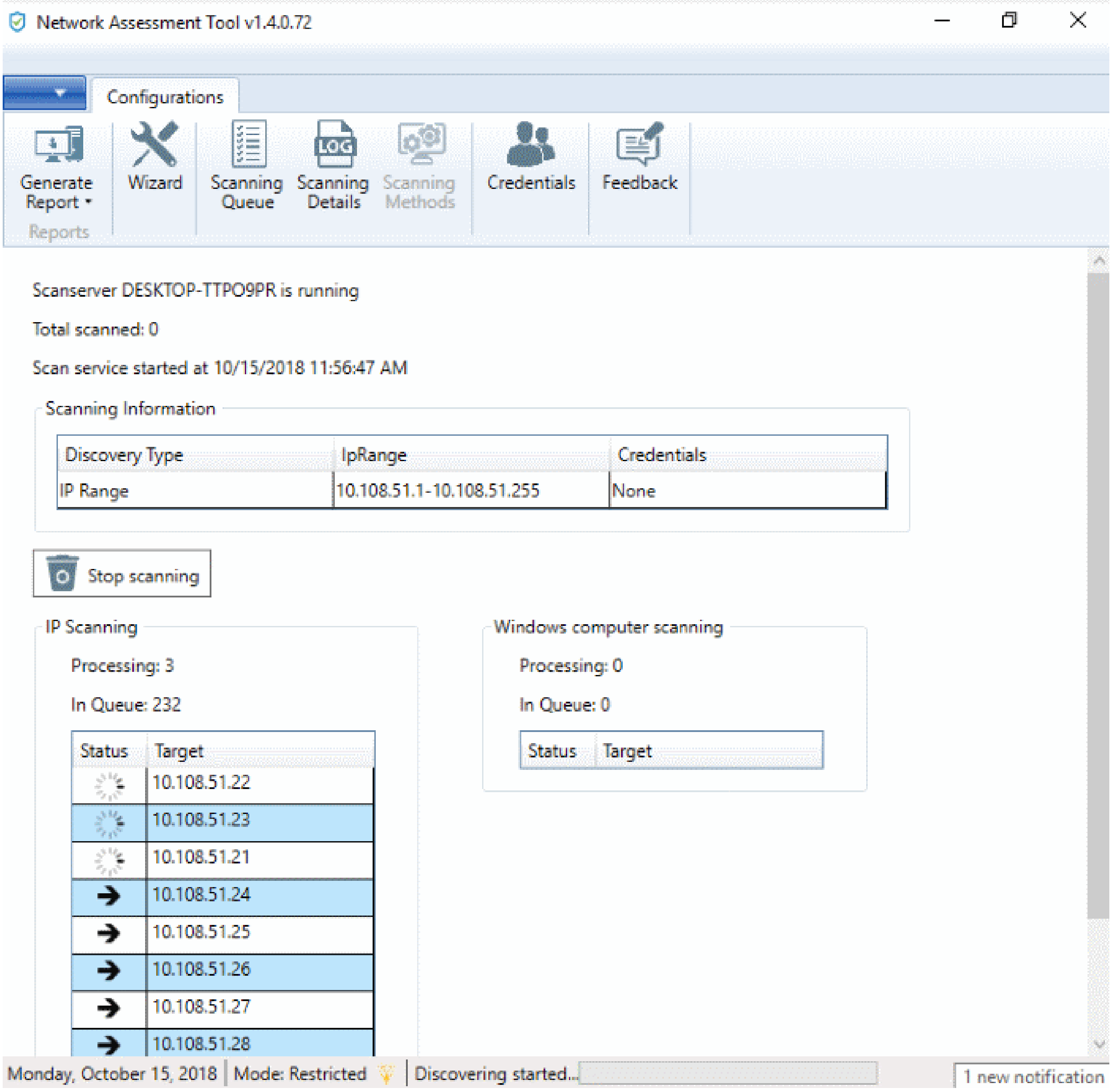


☑ Enable IP Address Range Scanning

Enable	Start IP	End IP	Description	Credentials
☑	10.108.51.1	10.108.51.255	Scanning 10.108.51.1-10.1	
□	10.108.51.202	10.108.51.203	Test scan	

Monday, October 15, 2018 | Mode: Restricted

- The scan will start.
- Click the 'Scanning Queue' button to view scan progress:



Scanserver DESKTOP-TTPO9PR is running

Total scanned: 0

Scan service started at 10/15/2018 11:56:47 AM

Scanning Information

Discovery Type	IpRange	Credentials
IP Range	10.108.51.1-10.108.51.255	None

IP Scanning

Processing: 3

In Queue: 232

Status	Target
	10.108.51.22
	10.108.51.23
	10.108.51.21
→	10.108.51.24
→	10.108.51.25
→	10.108.51.26
→	10.108.51.27
→	10.108.51.28

Windows computer scanning

Processing: 0

In Queue: 0

Status	Target

Monday, October 15, 2018 | Mode: Restricted | Discovering started... | 1 new notification

- **Scanning Information -** Details about current scans on domains, workgroups and IP addresses.
- **IP Scanning -** List of IP addresses discovered by Nmap on the current network.
- **Windows Computer Scanning -** Host-names and IP addresses that are currently being scanned using Windows Management Instrumentation (WMI) and Microsoft Baseline Security Analyzer (MBSA).

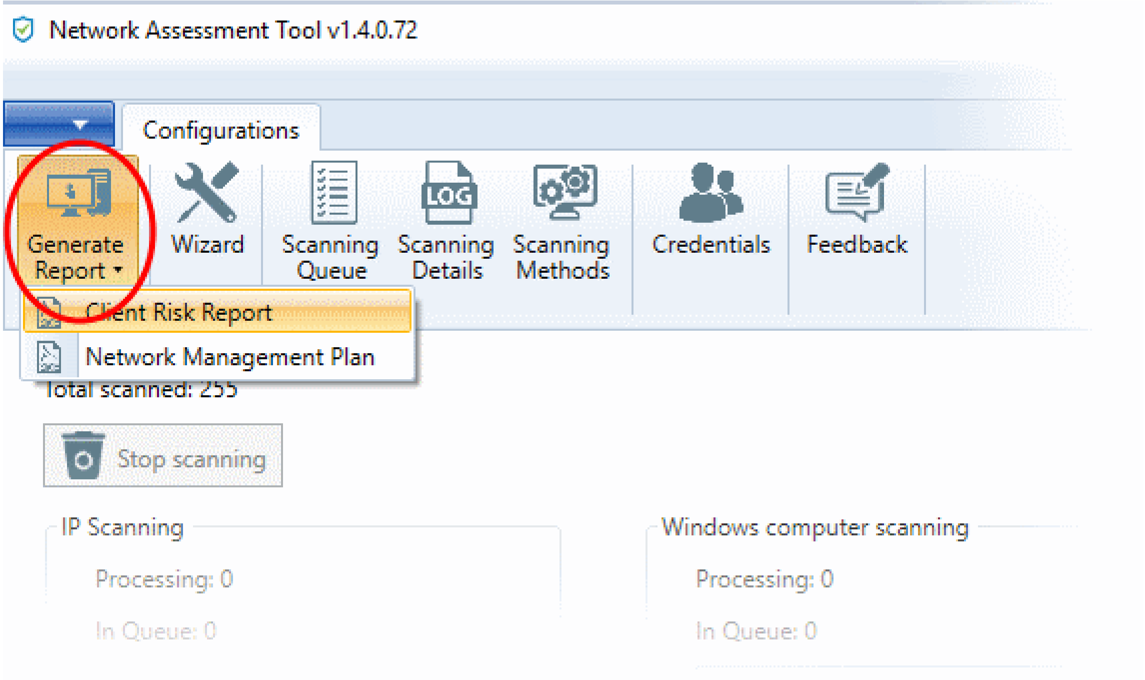
Step 7 - Generate Reports

There are two types of report you can generate after each scan:

- Client Risk Report – A breakdown of security issues on discovered network assets.
- Network Management Plan - Remediation advice for items listed in the risk report.

Download reports from the last scan

- Click 'Generate Report' on the menu bar
- Choose the report type from the drop-down:



NAT will start generating the report and on completion you will be able to download and save the report on your computer.

1.2 System Requirements

The following apply to the computer on which you install NAT:

Supported Operating Systems:

- Microsoft Windows client family
  - Windows Vista with SP2
  - Windows 7 with SP1
  - Windows 8
  - Windows 8.1
  - Windows 10
- Microsoft Windows Server family
  - Windows Server 2008 with SP2
  - Windows Server 2008 R2 with SP1
  - Windows Server 2012 (64-bit edition only)
  - Windows Server 2012 R2

Required Software:

- .NET Framework 4.5,
- Microsoft Baseline Security Analyzer (MBSA)
- Network Mapper (NMAP)

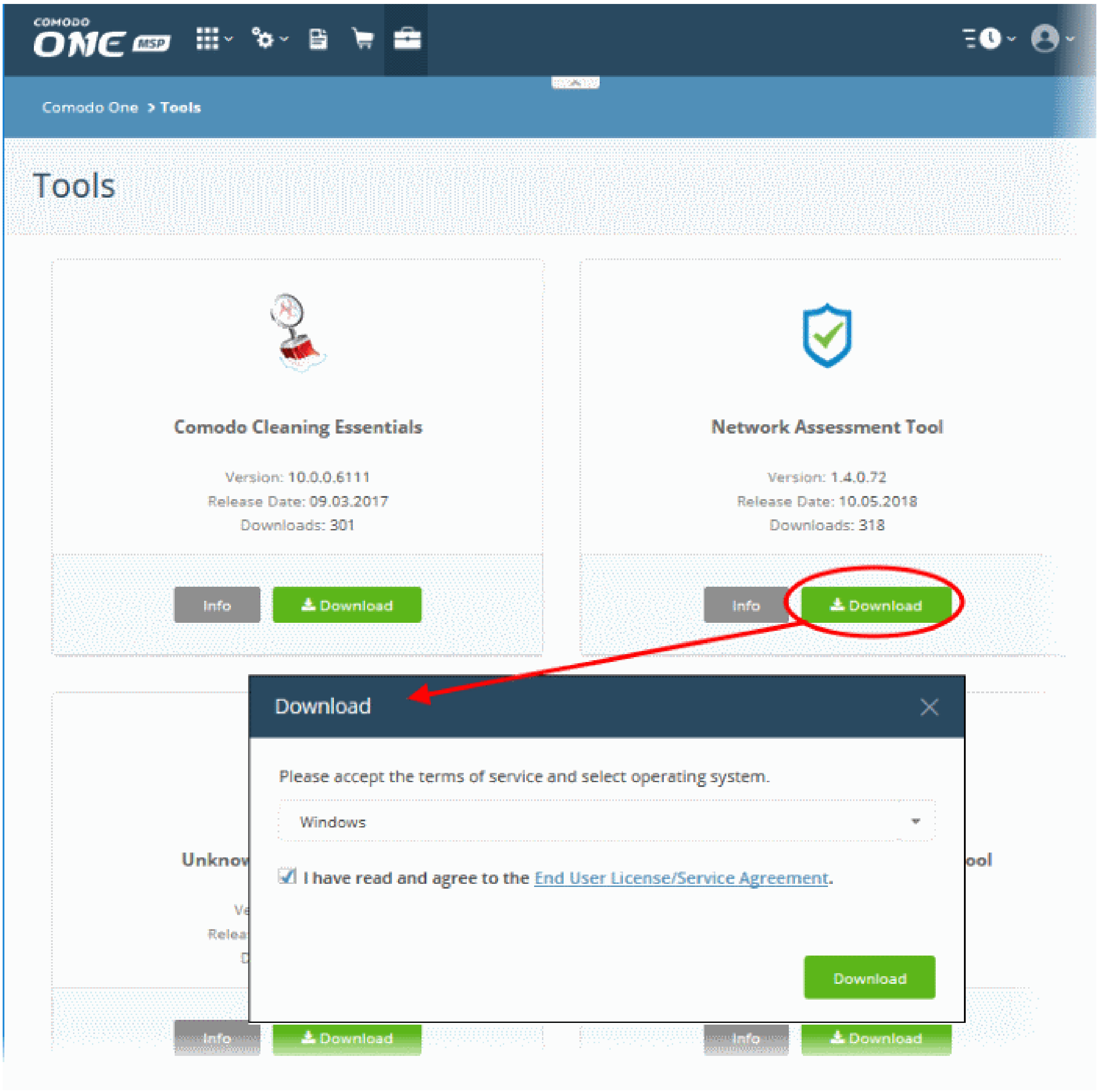
NAT searches for MBSA and NMAP during installation. If not available, it allows you download the software and install them.

Minimum Hardware Requirement

- Disk space - 4.5 GB
- Memory - 512 MB
- Processor - Single core 1 GHz or better

1.3 Download and Install Network Assessment Tool

- Login to your Comodo One account at **https://one.comodo.com/app/login**
- Click 'Tool Set' in the top-menu
- Click 'Download' in the NAT tile:



Tools

Comodo Cleaning Essentials

Version: 10.0.0.6111
Release Date: 09.03.2017
Downloads: 301

Network Assessment Tool

Version: 1.4.0.72
Release Date: 10.05.2018
Downloads: 318

Download

Please accept the terms of service and select operating system.

Windows

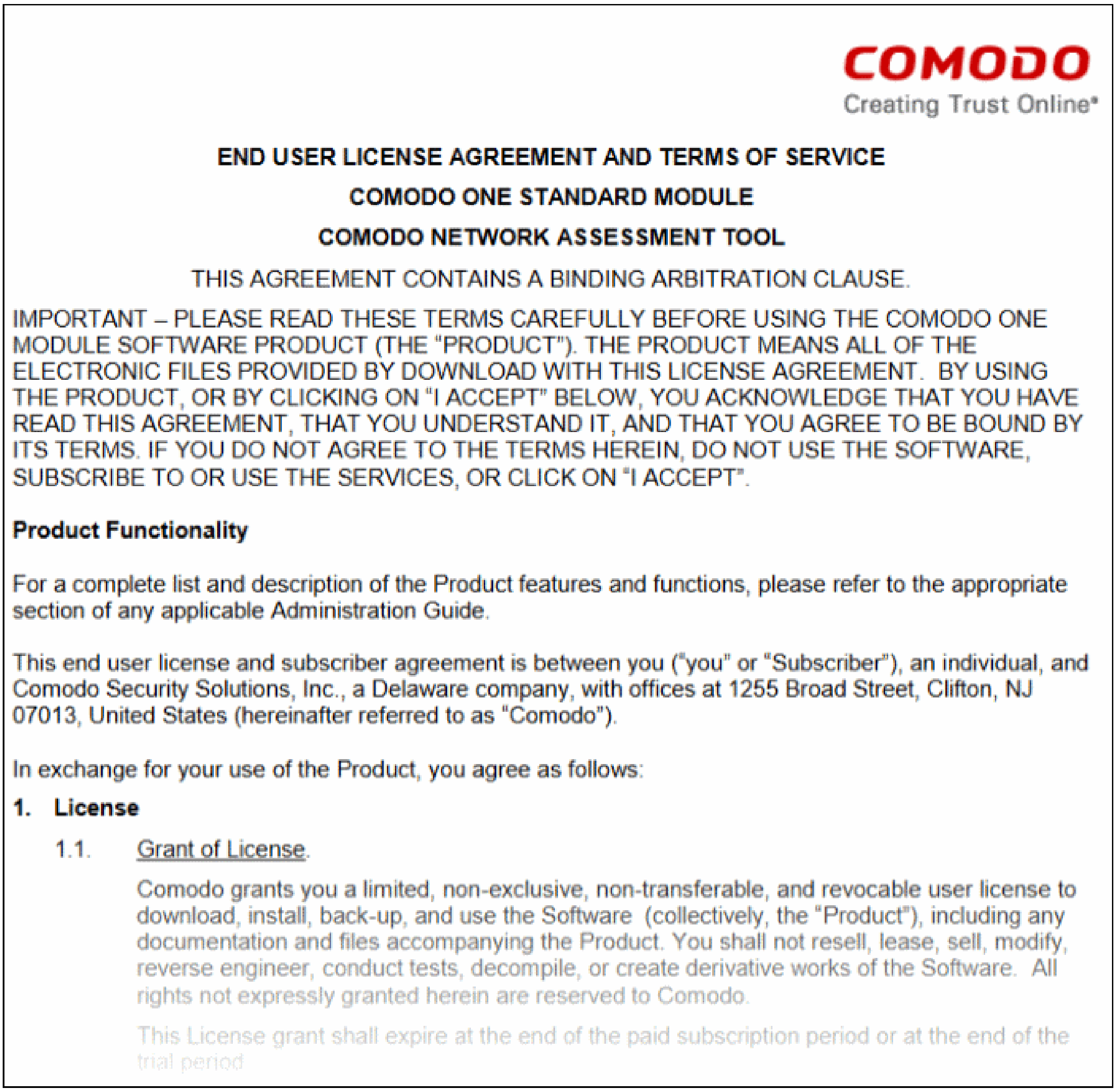
☑ I have read and agree to the End User License/Service Agreement.

- Agree to the end user license/service agreement
- Click 'Download'. Run the setup file to start the installer.
- The installation wizard takes you through the configuration of your first scan.
  - You can skip scan configuration and do it later if you wish.
- Note – You must have Network Mapper (NMAP) and Microsoft Baseline Security Analyzer (MBSA) installed on your management computer. The wizard will give you the opportunity to install this software if you do not

have it.

Step 1: End User License Agreement

Complete the initialization phase by reading and accepting the End User License Agreement (EULA).



COMODO
Creating Trust Online*

END USER LICENSE AGREEMENT AND TERMS OF SERVICE

COMODO ONE STANDARD MODULE

COMODO NETWORK ASSESSMENT TOOL

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.

IMPORTANT – PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONE MODULE SOFTWARE PRODUCT (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE ELECTRONIC FILES PROVIDED BY DOWNLOAD WITH THIS LICENSE AGREEMENT. BY USING THE PRODUCT, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT USE THE SOFTWARE, SUBSCRIBE TO OR USE THE SERVICES, OR CLICK ON "I ACCEPT".

Product Functionality

For a complete list and description of the Product features and functions, please refer to the appropriate section of any applicable Administration Guide.

This end user license and subscriber agreement is between you ("you" or "Subscriber"), an individual, and Comodo Security Solutions, Inc., a Delaware company, with offices at 1255 Broad Street, Clifton, NJ 07013, United States (hereinafter referred to as "Comodo").

In exchange for your use of the Product, you agree as follows:

1. License

1.1. Grant of License.

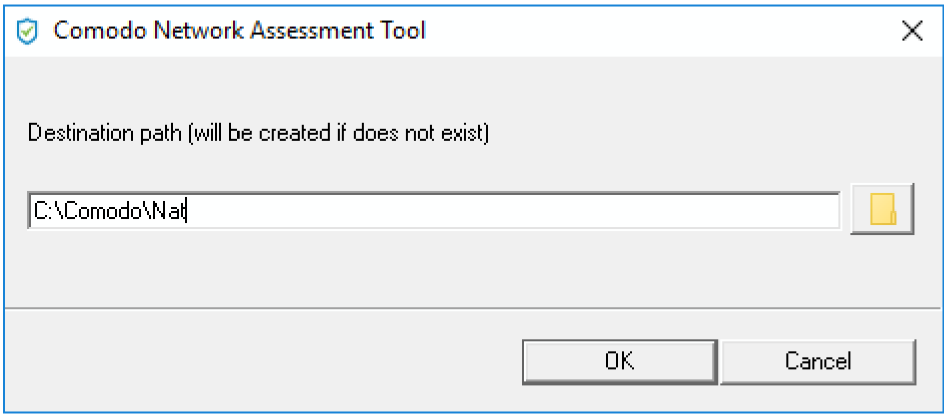
Comodo grants you a limited, non-exclusive, non-transferable, and revocable user license to download, install, back-up, and use the Software (collectively, the "Product"), including any documentation and files accompanying the Product. You shall not resell, lease, sell, modify, reverse engineer, conduct tests, decompile, or create derivative works of the Software. All rights not expressly granted herein are reserved to Comodo.

This License grant shall expire at the end of the paid subscription period or at the end of the trial period

- Read the agreement fully and click 'Accept' to continue. Click 'Decline' if you want to cancel the installation.

Step 2: Select Installation Folder

The next screen lets you choose the NAT installation folder:



Comodo Network Assessment Tool

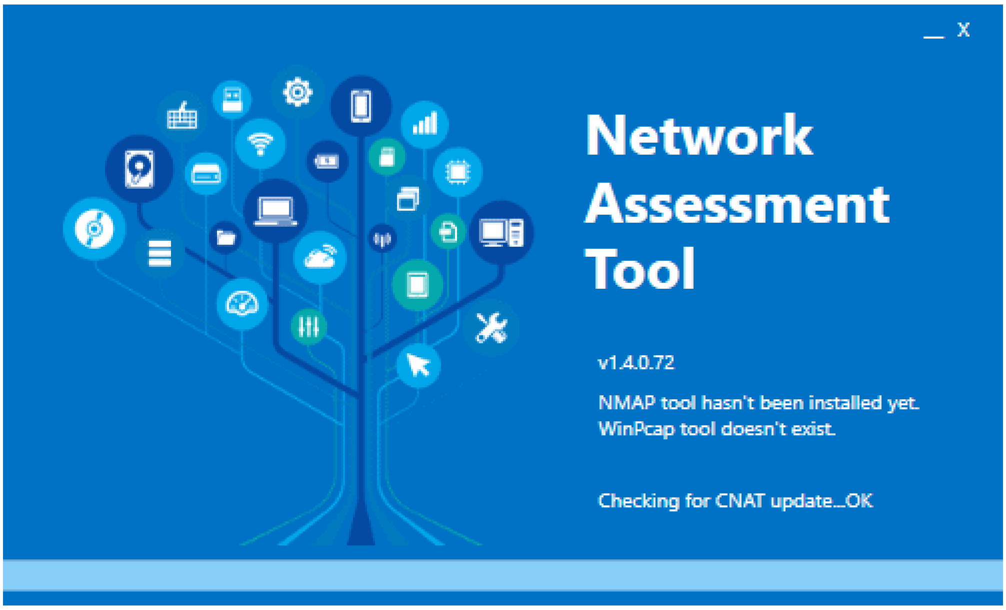
Destination path (will be created if does not exist)

C:\Comodo\Nat

- The default location is C:\Comodo\Nat. Click 'Browse' to choose a different location.
- Click 'OK' to start the installation

Step 3: Setup Progress

Installation will begin and progress shown as follows:

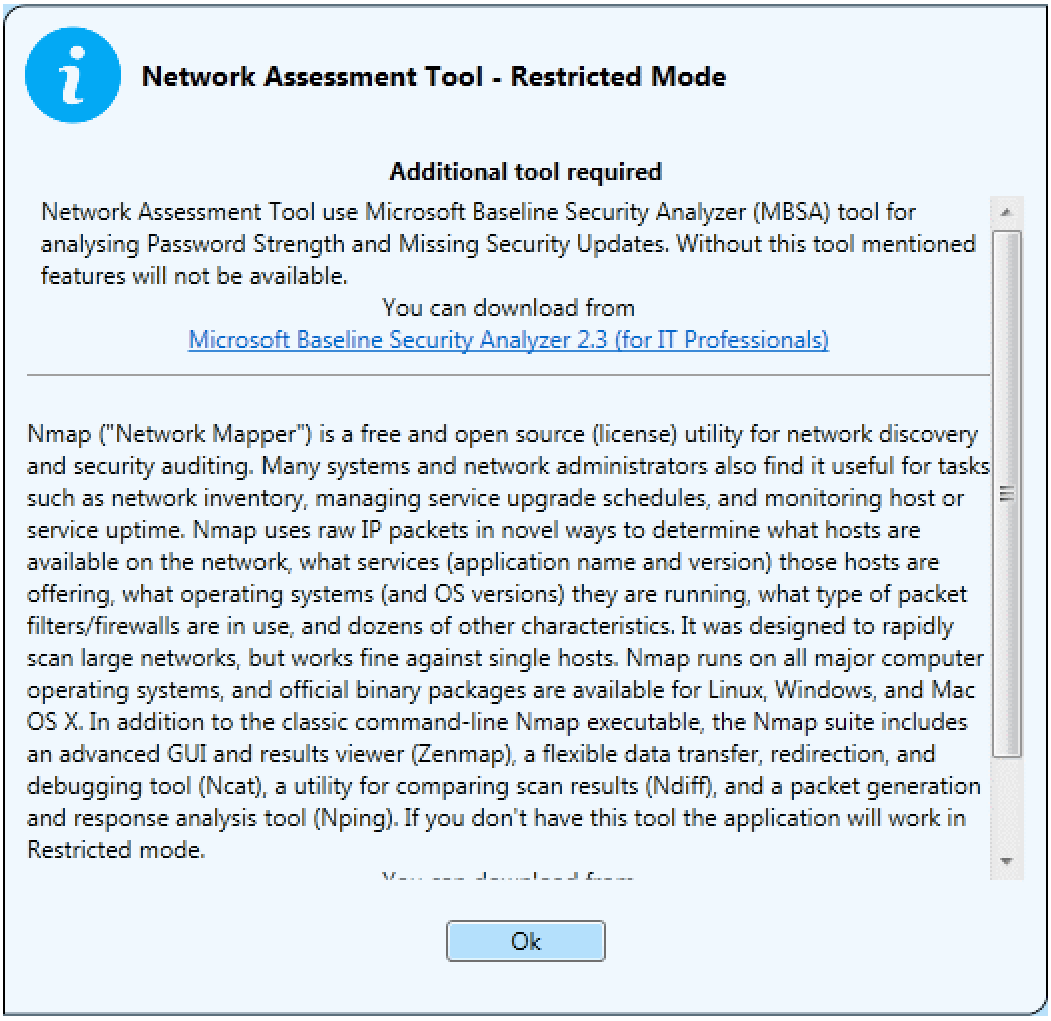


v1.4.0.72

NMAP tool hasn't been installed yet.
WinPcap tool doesn't exist.

Checking for CNAT update...OK

- The wizard will check whether MBSA and NMAP are installed and provide you download links if they are not:



Network Assessment Tool - Restricted Mode

Additional tool required

Network Assessment Tool use Microsoft Baseline Security Analyzer (MBSA) tool for analysing Password Strength and Missing Security Updates. Without this tool mentioned features will not be available.

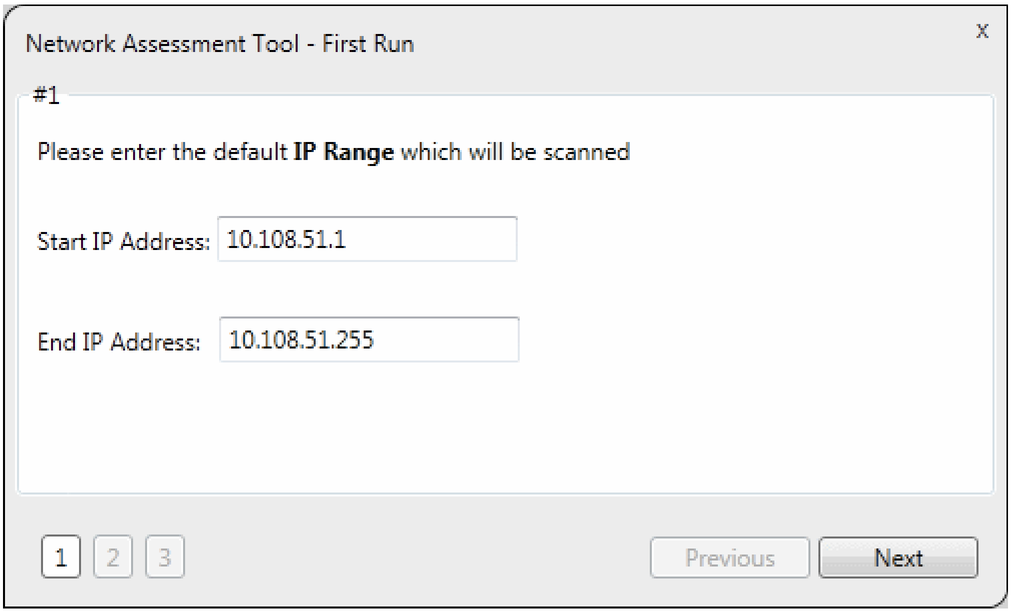
You can download from

Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping). If you don't have this tool the application will work in Restricted mode.

You can download from

- Install MBSA and/or NMAP as required. Please do this before continuing NAT installation.
- Click 'Ok' to continue NAT installation.
- The next step is configuration of your first scan:



Network Assessment Tool - First Run

#1

Please enter the default **IP Range** which will be scanned

Start IP Address: 10.108.51.1

End IP Address: 10.108.51.255

- Click 'Next' to continue with configuration.
- Close the dialog if you want to configure the scan later.
  - Click the 'Wizard' button on the menu bar to configure a scan at any time.

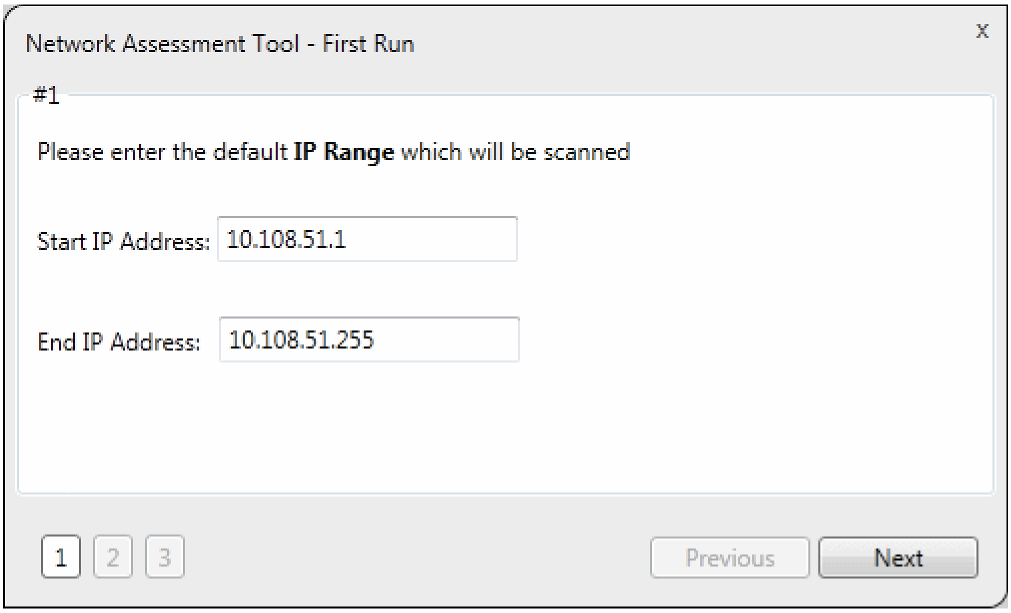
See **Configuration Wizard** for more details on the wizard.

1.4 Configuration Wizard

- The 'First Run' configuration wizard lets you configure your first network scan.
- You'll choose the IP range, enable/disable workgroup scans and provide admin credentials.
- Click 'Wizard' on the menu bar to start the wizard at any time.

Step 1 - Enter the IP Range

NAT identifies the network on which it is installed and populates the 'Start IP Address' and 'End IP Address'



Network Assessment Tool - First Run

#1

Please enter the default **IP Range** which will be scanned

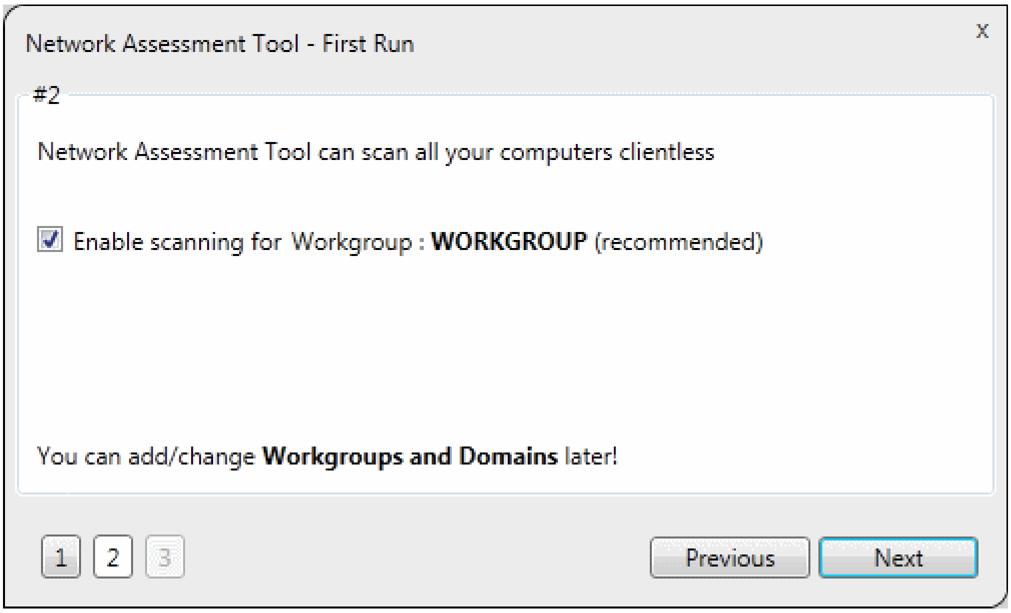
Start IP Address: 10.108.51.1

End IP Address: 10.108.51.255

You can change these addresses if required.

Step 2 - Enable Domain/Workgroup Scans

- NAT automatically identifies the workgroup or domain which your computer is connected to:



Network Assessment Tool - First Run

#2

Network Assessment Tool can scan all your computers clientless

☑ Enable scanning for Workgroup : **WORKGROUP** (recommended)

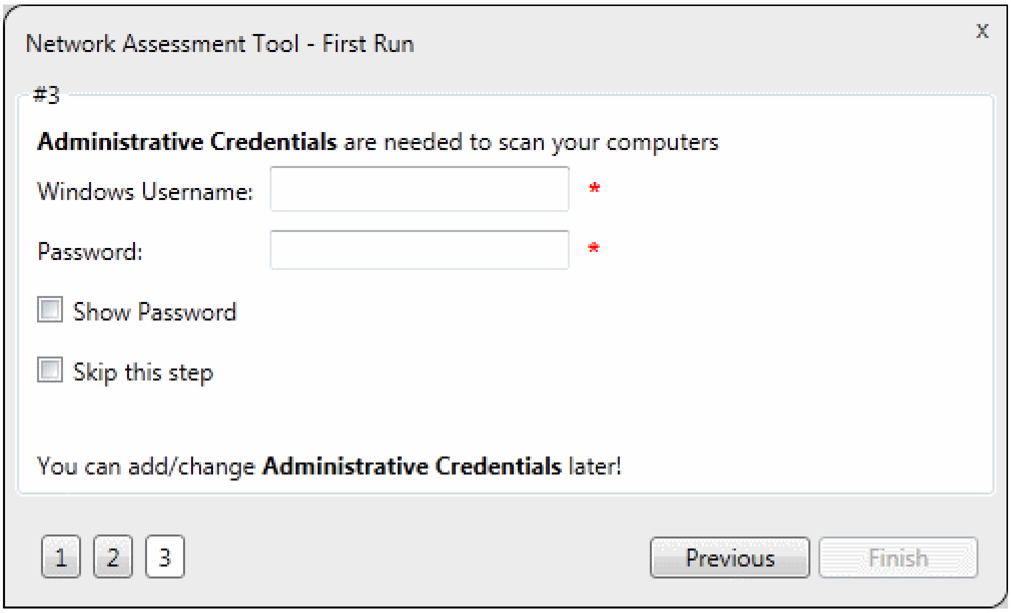
You can add/change **Workgroups and Domains** later!

- To automatically add your workgroup/domain, ensure 'Enable scanning Workgroup/Domain' is selected.

Tip: You can enable domain/workgroup scanning at any time. See **Network Management** for more details.

Step 3 - Admin Credentials

The next step is to provide login credentials for an account with network administrative privileges, for NAT to access the endpoints on your network for scanning.



Network Assessment Tool - First Run

#3

Administrative Credentials are needed to scan your computers

Windows Username: *

Password: *

□ Show Password

□ Skip this step

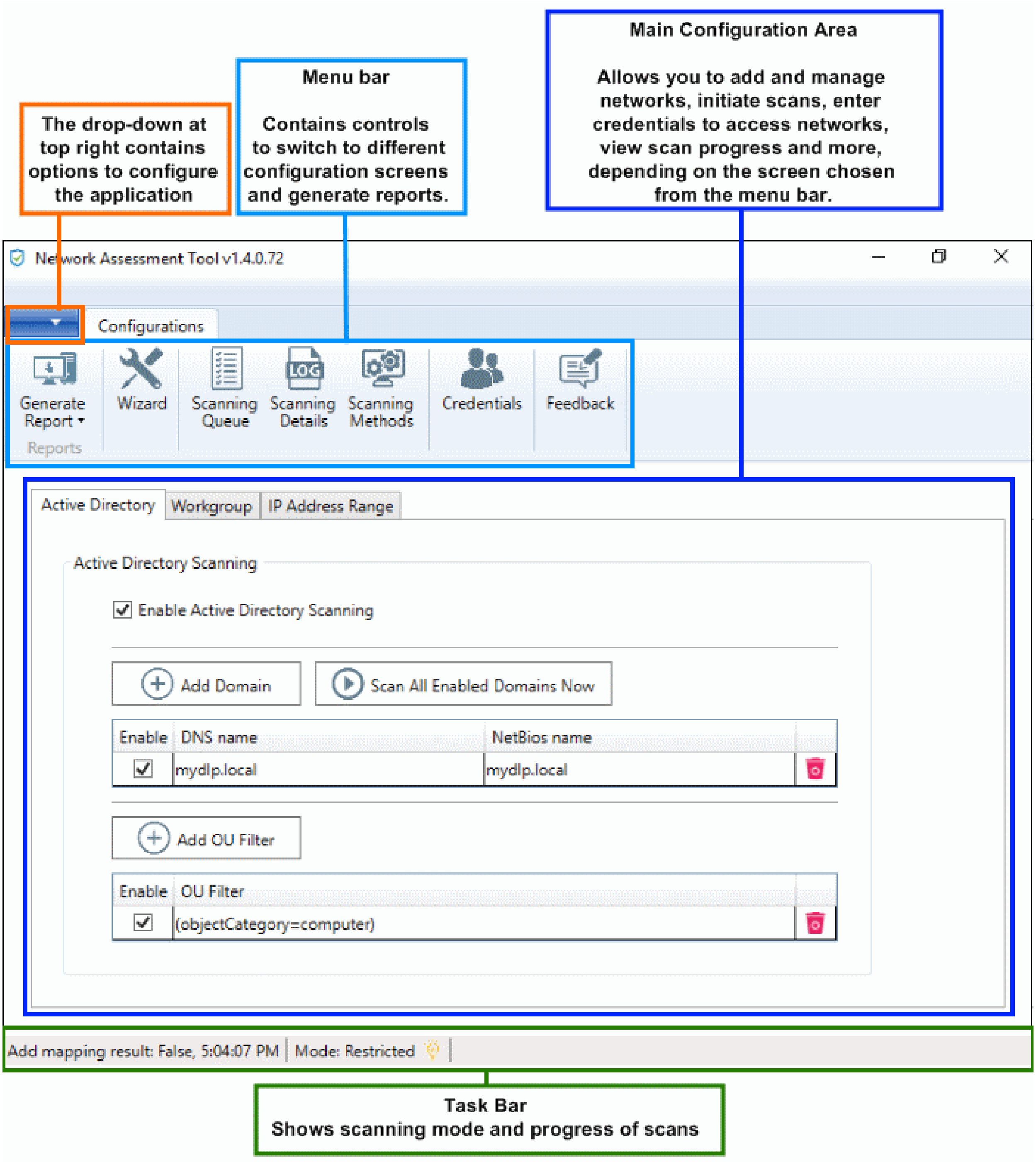
You can add/change **Administrative Credentials** later!

- Enter the username and password of the network administrator in the respective fields and click 'Finish'.
- 'Skip this step' – Choose if you want to provide admin credentials later.
  - You can add admin accounts later by clicking the 'Credentials' button in the top-menu. See **Credentials Management** for more details.
- Click 'Finish' to finalize the configuration.

The '**NAT Admin Console**' will open.

1.5 The NAT Admin Console

The admin console allows you to run scans on networks, add network endpoints, generate reports and more.



The drop-down at top right contains options to configure the application

Menu bar

Contains controls to switch to different configuration screens and generate reports.

Main Configuration Area

Allows you to add and manage networks, initiate scans, enter credentials to access networks, view scan progress and more, depending on the screen chosen from the menu bar.

Network Assessment Tool v1.4.0.72

Active Directory Scanning

☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted

Task Bar

Shows scanning mode and progress of scans

The top-menu lets you access the following main areas:

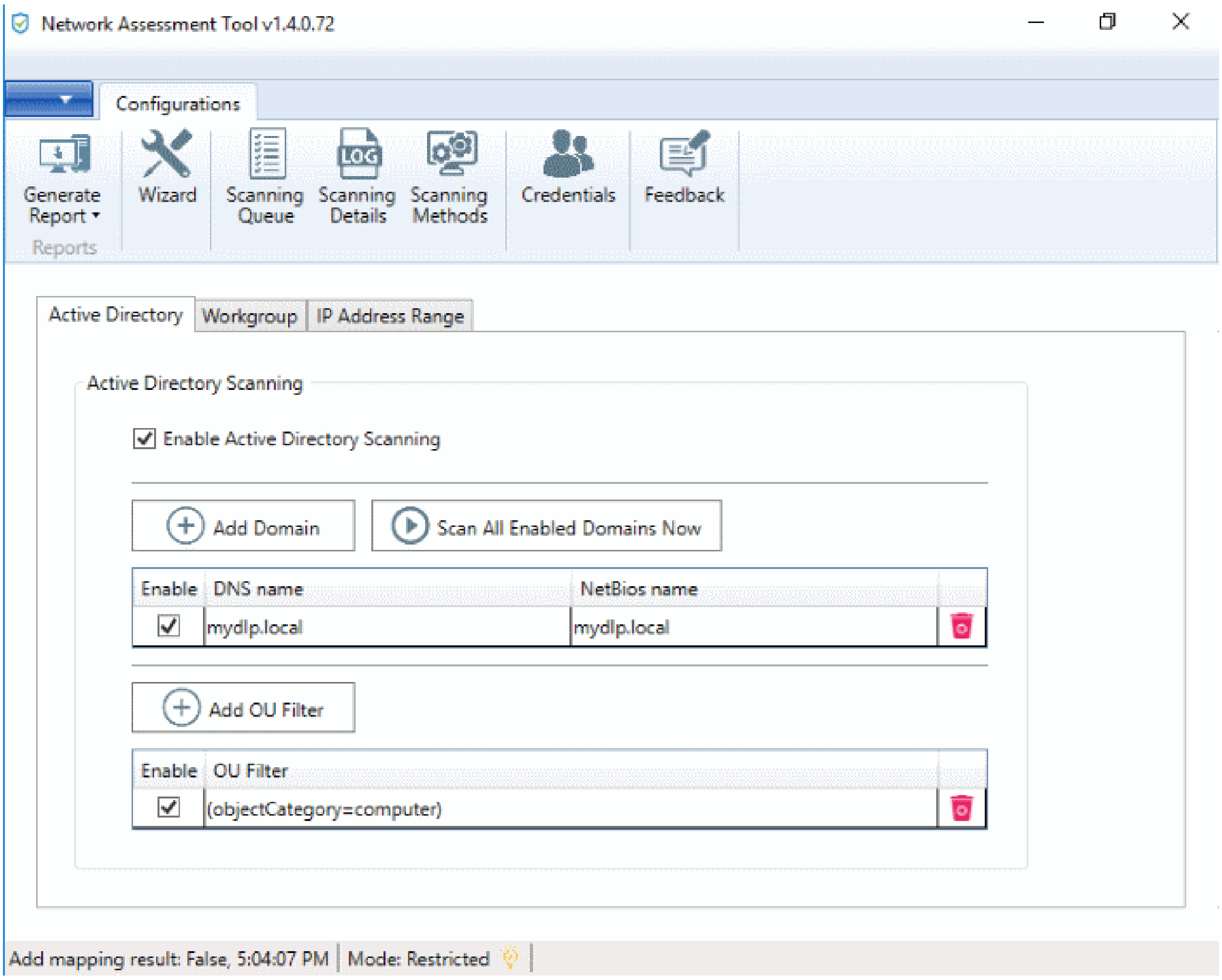
- **Generate Reports** - Create and download risk reports for your networks. You can also schedule reports.
- **Wizard** - Add networks and configure scans. You need to specify the default IP range that you wish to scan, a default domain to scan (optional) and an admin password for scanned endpoints.
- **Scanning Queue** - View progress of running scans and terminate unwanted scans.
- **Scanning Details** - View logs of the currently running and last run scans
- **Scanning Methods** - Add and manage domains, workgroups and IP ranges that you want to scan. Initiate

scans on selected networks.

- **Credentials** - Specify admin username and passwords to access target networks
- **Feedback** - Submit comments and suggestions on the product.

2 Network Management

- In order to run network assessment scans, you need to specify target networks and enter admin login details for those networks.
- The 'Scanning Methods' interface lets you add target networks via Active Directory, Workgroup or IP range.
- The 'Credentials' interface lets you specify admin usernames and passwords to access your networks.



☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Add mapping result: False, 5:04:07 PM | Mode: Restricted

See the following sections for more details:

- **Add Networks to be scanned**
- **Credentials Management**

2.1 Add Networks

Networks can be added using any of the following methods:

- **Domains** - Add Active Directory domains by specifying their DNS name and NetBios name. See **Adding Domains** for more details.
- **Workgroups** - Add workgroups by specifying the name of the workgroup. See **Adding a Workgroup** for

more details.

- **IP Address Range(s)** – Add Endpoints to be scanned can be specified by defining the IP range. See **Adding IP Address Range** for more details.

Add Domains

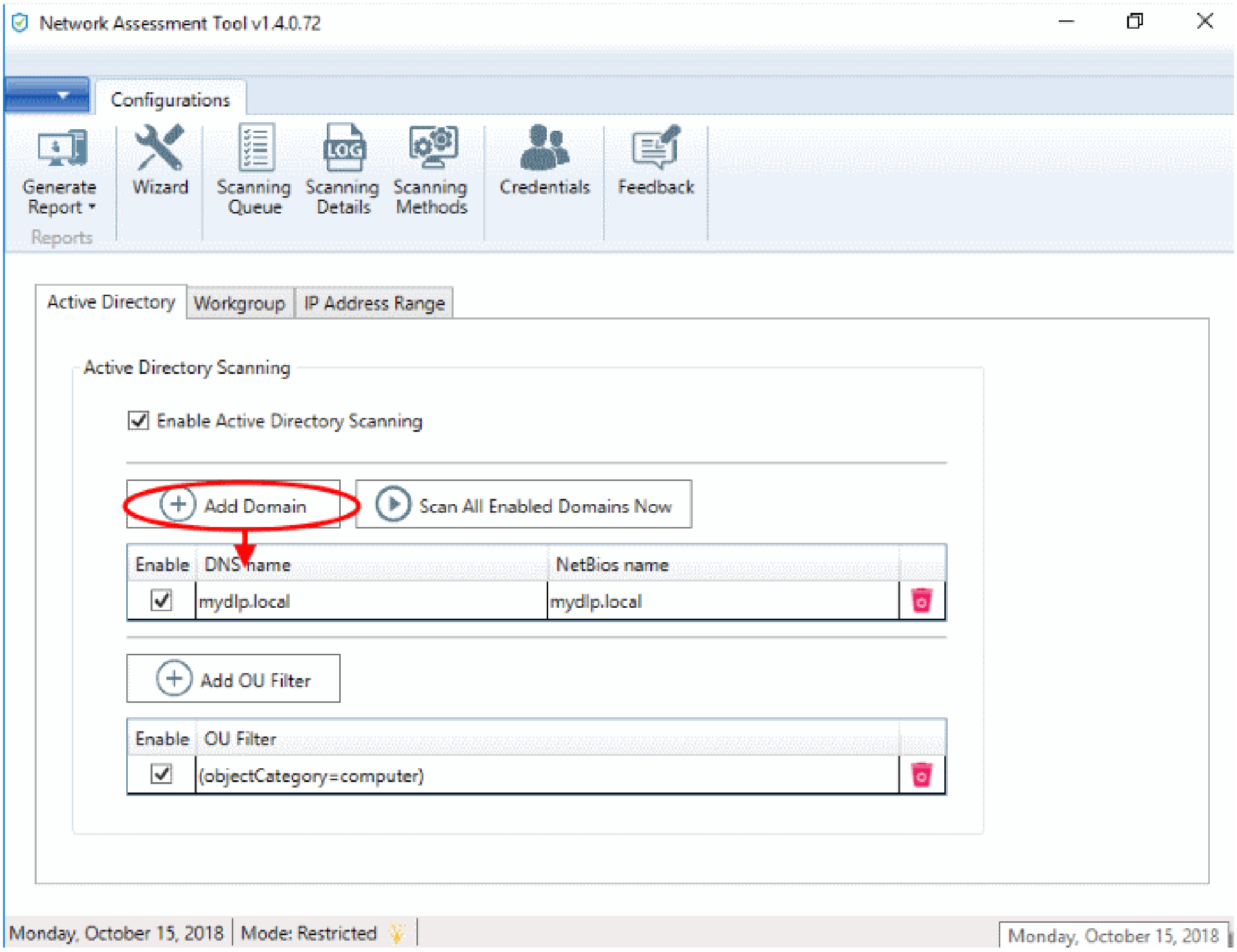
- You can add an AD domain by specifying its DNS domain name and NetBios name.
- If you want to scan only selected endpoints in the domain, you can add Organization Unit (OU) filters.
- Admin login details for the AD server need to be added in the 'Credentials' interface and mapped to the domain. See **Credential Management** for more details.

To add a domain

- Click 'Scanning Methods' from the menu bar and select the 'Active Directory' tab
- Ensure that the 'Enable Active Directory Scanning' check-box is selected
- Click 'Add Domain'

A new row will be added to the list of domains

- Enter the DNS name and NetBios name in the respective fields.



☑ Enable Active Directory Scanning

Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

- If you want to enable the domain for scanning, select the 'Enable' check-box beside the domain name

The domain will be added to the list.

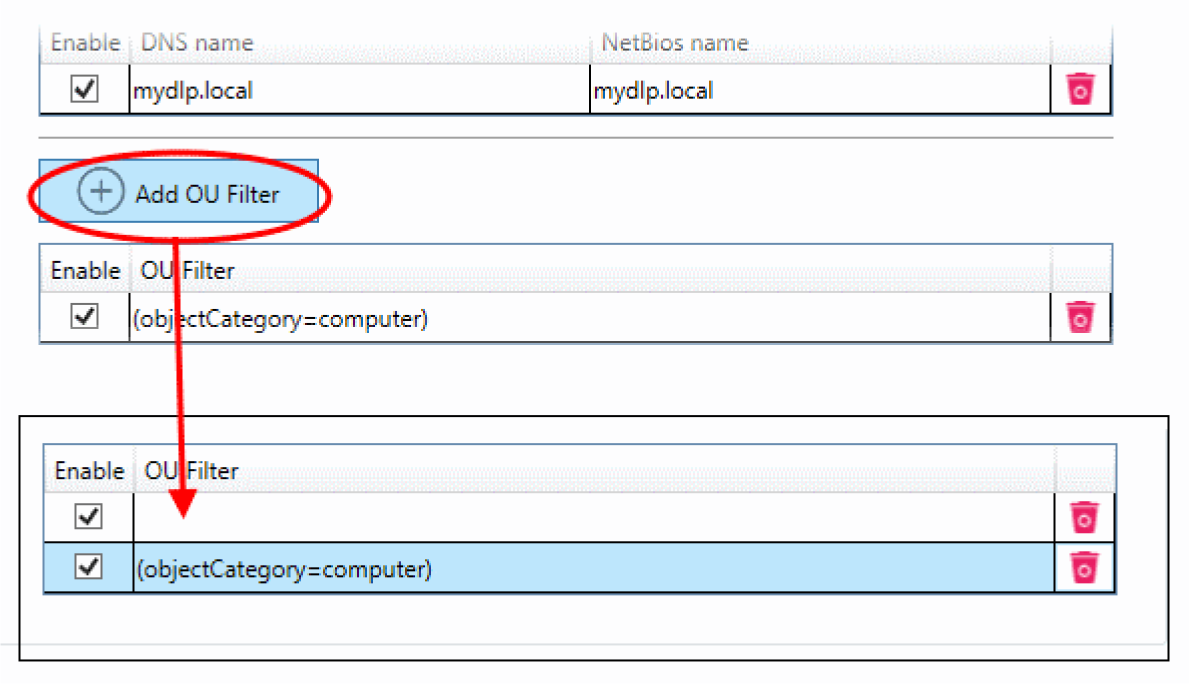
- To remove a domain click the trash can icon 🗑

To add an OU filter

- Click 'Add OU Filter'

A new row will be added to the list of filters.

- Enter the OU filter in the new row.



Enable	DNS name	NetBios name
☑	mydlp.local	mydlp.local

Enable	OU Filter
☑	(objectCategory=computer)

Enable	OU Filter
☑	
☑	(objectCategory=computer)

- If you want to enable the filter, select the 'Enable' check-box

The filter will be added to the list.

- To remove a filter, click the trash can icon

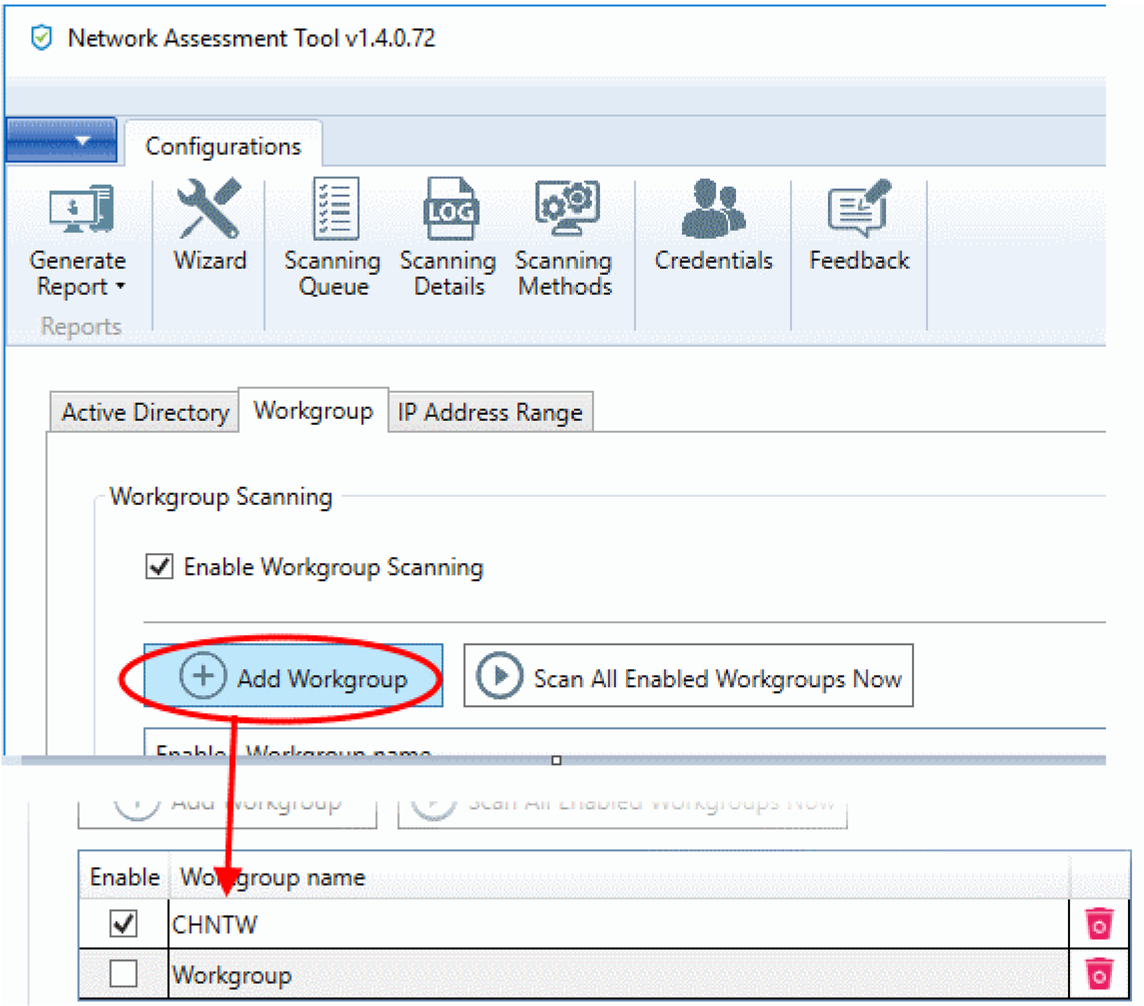
Adding a Workgroup

In order to scan endpoints in a workgroup, 'Workgroup Scanning' has to be enabled in NAT. You can add a workgroup by specifying its name. You must then add an admin password for the domain n the 'Credentials' area and map it to the workgroup. See **Credential Management** for more details on this.

To add a workgroup

- Click 'Scanning Methods' from the menu bar and select the 'Workgroup' tab
- Ensure that 'Enable Workgroup Scanning' check-box is selected
- Click 'Add Workgroup'

A new row will be added to the list of workgroups.



☑ Enable Workgroup Scanning

Enable	Workgroup name	
☑	CHNTW	🗑
□	Workgroup	🗑

- Enter the name of the workgroup you want to add
- Click the trash can icon 🗑 to remove a work-group

Adding IP Address Range

You can add endpoints within a network by specifying their IP address range. In order to scan those endpoints, 'IP Address Range Scanning' has to be enabled in NAT. The login credentials for the endpoints in the network with administrative privileges are to be added in the 'Credentials' interface and mapped to the IP range from the 'Scanning Methods' interface to enable NAT to scan the endpoints in it. See **Credential Management** for more details. The credentials mapping can also be done through the 'Scanning Methods' interface.

Prerequisite - For mapping the login credentials for the network from the 'Scanning Methods' interface, the credentials should have been added to NAT through the 'Credentials' interface. See **Credential Management** for more details

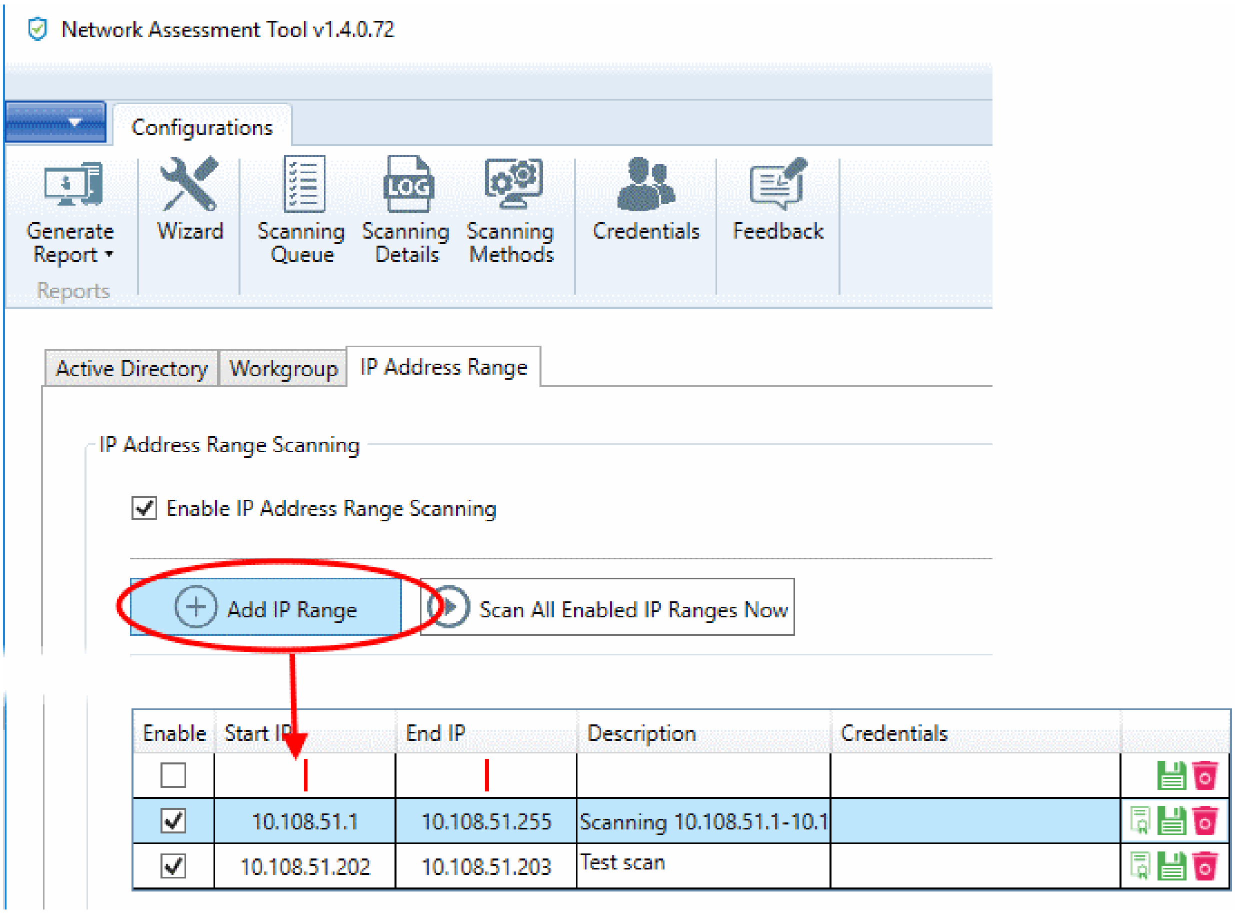
To add an IP Address Range

- Click 'Scanning Methods' on the menu bar and select the 'IP Address Range' tab

The list of IP address ranges added to NAT will be displayed.

- Ensure that 'Enable IP Address Range Scanning' checkbox is selected
- Click 'Add IP Range'

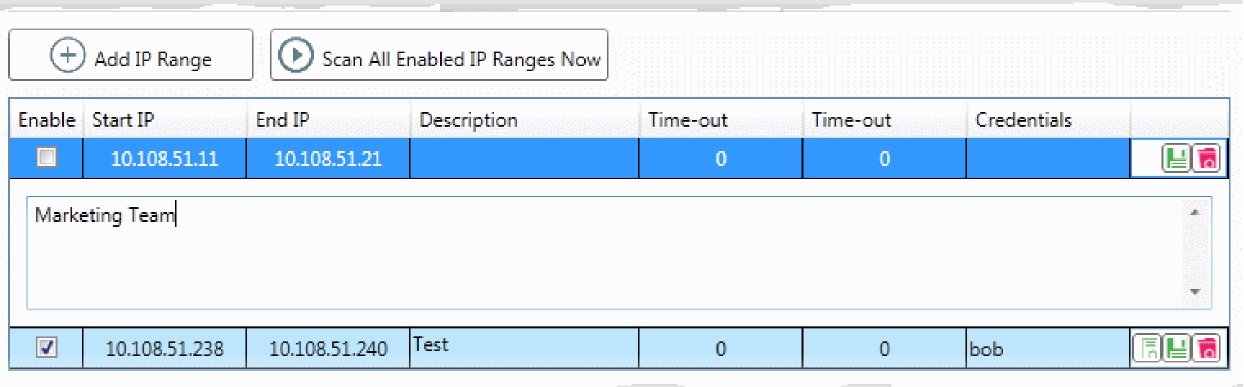
A new row will be added to the list of IP address ranges.



☑ Enable IP Address Range Scanning

Enable	Start IP	End IP	Description	Credentials	
☐					
☑	10.108.51.1	10.108.51.255	Scanning 10.108.51.1-10.1		
☑	10.108.51.202	10.108.51.203	Test scan		

- Enter the start IP address and the end IP address in the respective fields
- Enter a description for the IP address range in the textbox that appears below the row.



Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials	
☐	10.108.51.11	10.108.51.21		0	0		

Marketing Team

Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials	
☑	10.108.51.238	10.108.51.240	Test	0	0	bob	

- Enter the time out period for WMI so as to skip scanning the endpoints that are not responsive for the period specified in this field.

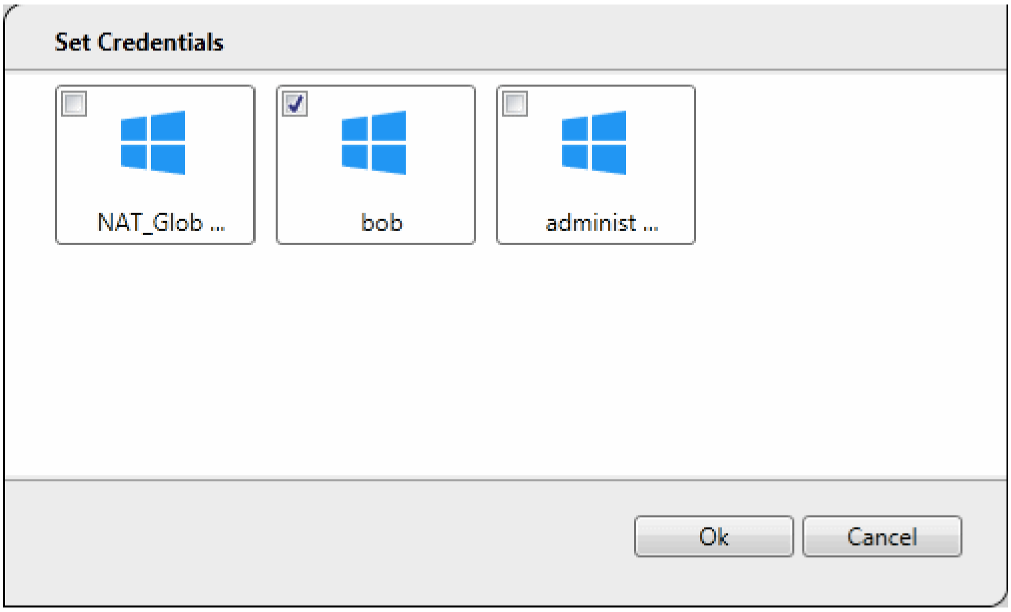
Note: NAT uses Windows Management Instrumentation (WMI) and Microsoft Baseline Security Analyzer (MBSA) to scan the endpoints identified at the given IP addresses by the Network Mapper (NMAP) tool.

- Click 'Save' 💾 at the right of the row to add the IP address range.

The next step is to map login credentials to the IP address range.

- Click 'Add Credential' 📄 at the right of the row.

The 'Set Credentials' dialog will appear with a list of credentials added to NAT.



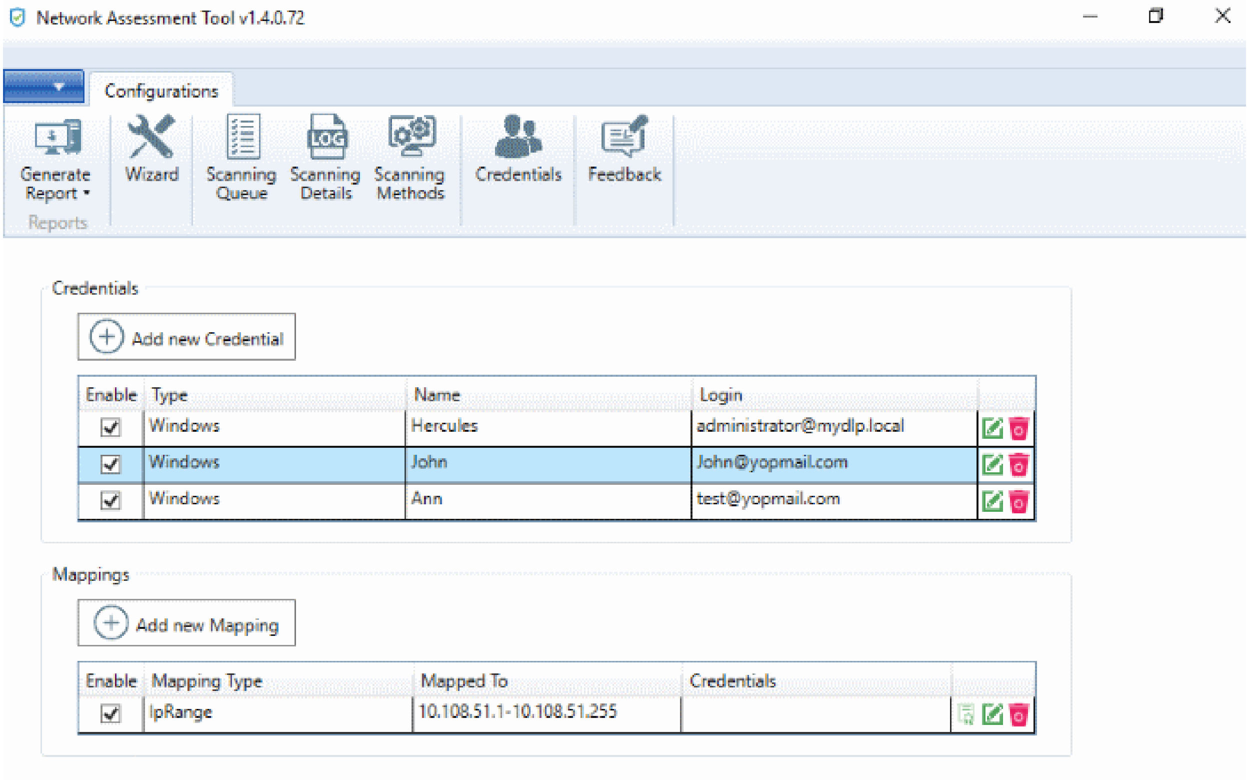
- Click 'Ok' after choosing the credentials to apply to the IP address range
- Click the trash can icon 🗑 to remove an address range

2.2 Credentials Management

- You need to provide admin login details for your target networks in order for NAT to scan them.
- You can map credentials to specific networks. NAT uses the appropriate credentials to access each network.

The 'Credentials' interface allows you to add and map login credentials for the networks.

- Click 'Credentials' on the menu bar



Enable	Type	Name	Login	
☑	Windows	Hercules	administrator@mydlp.local	✎ 🗑
☑	Windows	John	John@yopmail.com	✎ 🗑
☑	Windows	Ann	test@yopmail.com	✎ 🗑

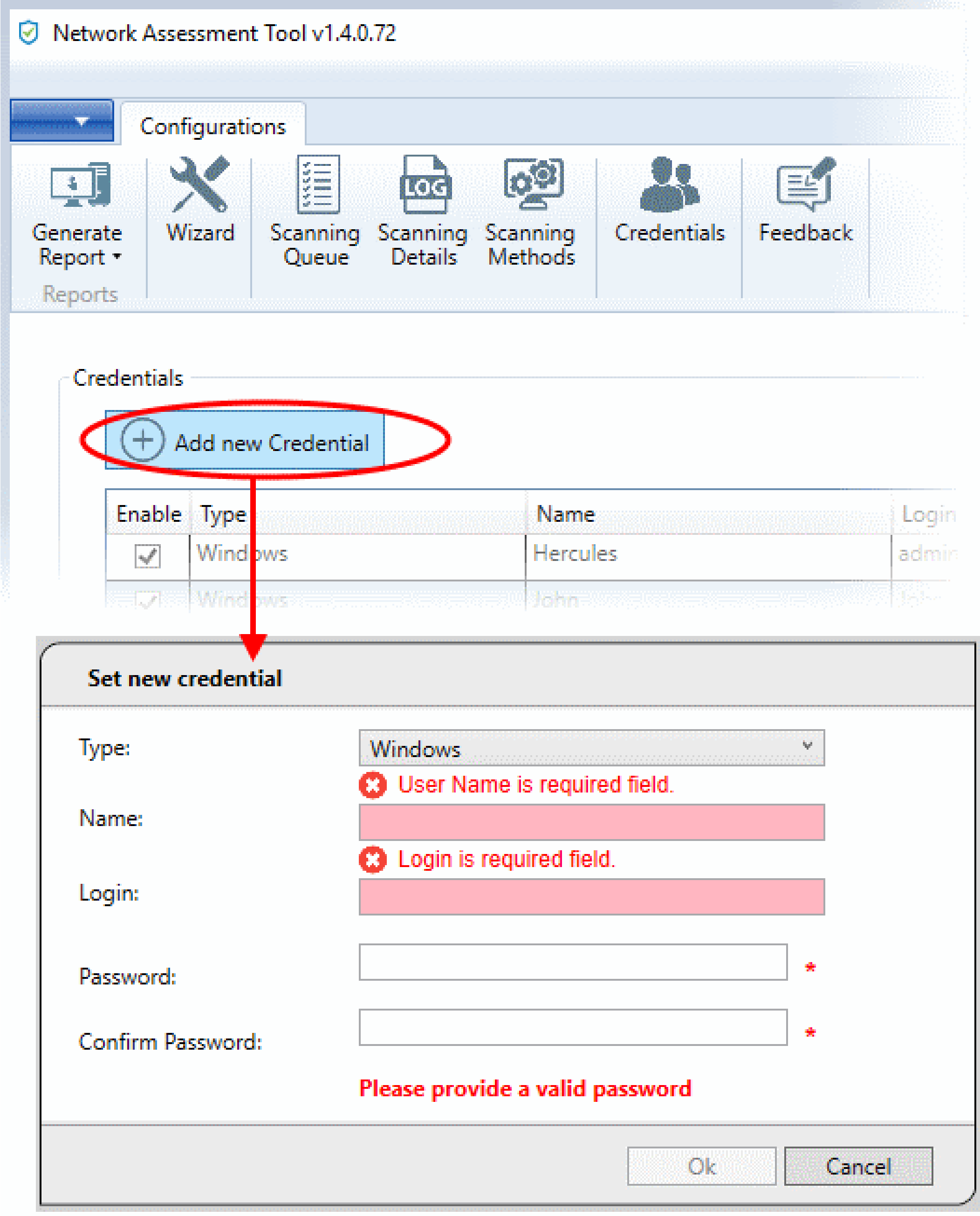
Enable	Mapping Type	Mapped To	Credentials	
☑	IpRange	10.108.51.1-10.108.51.255		✎ 🗑

See the following sections for more details:

- **Adding login credentials**
- **Mapping credentials to a network**

To add a new login credential

- Click 'Add new Credential' from the 'Credentials' interface



The 'Set new credential' dialog will open.

Set new credential dialog - Form parameters	
Form Element	**Description**
Type	Choose the operating system of the endpoints for which the credential is set
Name	Enter a name to identify the account, for example, the name of the administrator

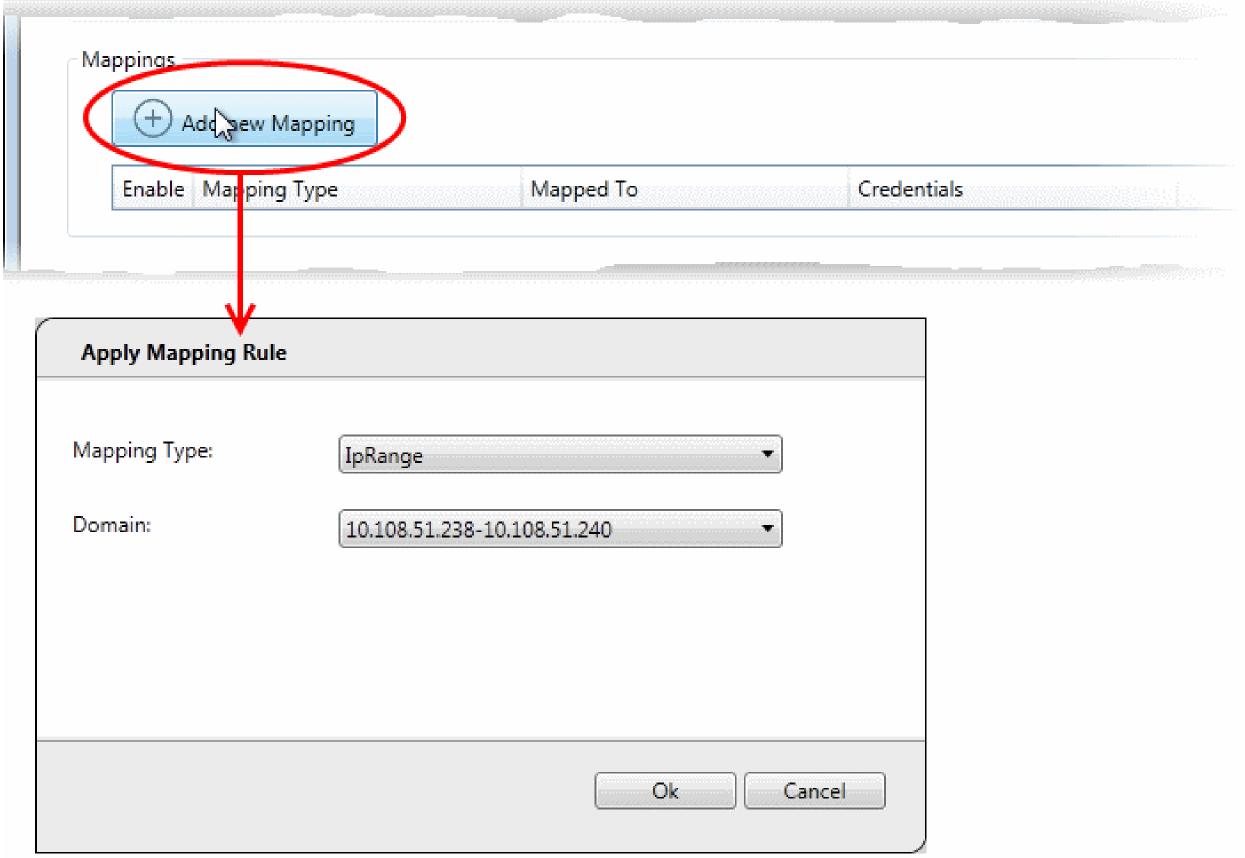
Login	Enter the username of the account
Password	Enter the password of the account.
Confirm Password	Re-enter the password of confirmation

- Click 'Ok' to add the credential
- Repeat the process to add more credentials
- Click 'Edit' ✎ at the right of the row to edit a credential and enter the new values in the 'Set new credential' dialog. The process is similar to adding a new credential.
- Click the trash can icon 🗑 to remove a credential

To add a new mapping of credential to a network

- Click 'Add new Mapping' in the 'Credentials' interface:

The 'Apply Mapping Rule' wizard will open.

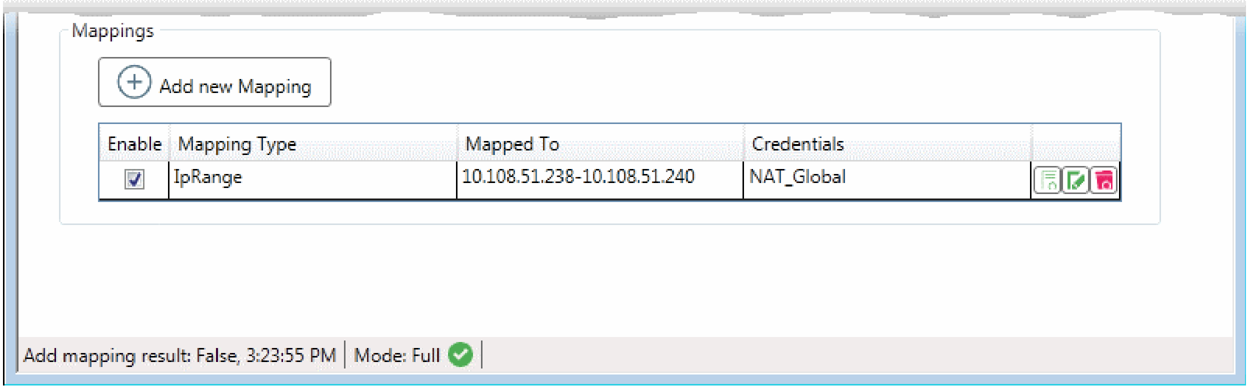


Mapping Type: IpRange

Domain: 10.108.51.238-10.108.51.240

  - Mapping Type - Choose the type of the network to which the credentials are to be mapped. The available options are 'IP Range', 'Domain' and 'Workgroup'.
  - Domain - The drop-down displays the networks added to NAT and fall under the type chosen from the 'Type' drop-down. Choose the network to which the credential is to be applied
- Click 'Ok'

The network will be added to the 'Mappings' list, mapped with the default credentials that was specified through the initial configuration wizard.

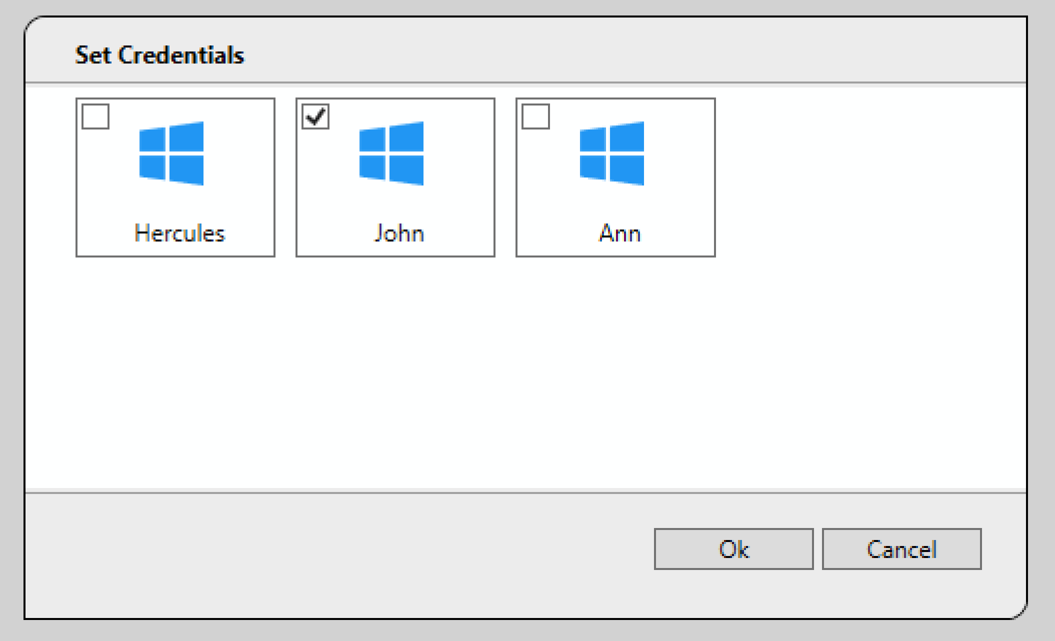


Enable	Mapping Type	Mapped To	Credentials
☑	IpRange	10.108.51.238-10.108.51.240	NAT_Global

Add mapping result: False, 3:23:55 PM | Mode: Full

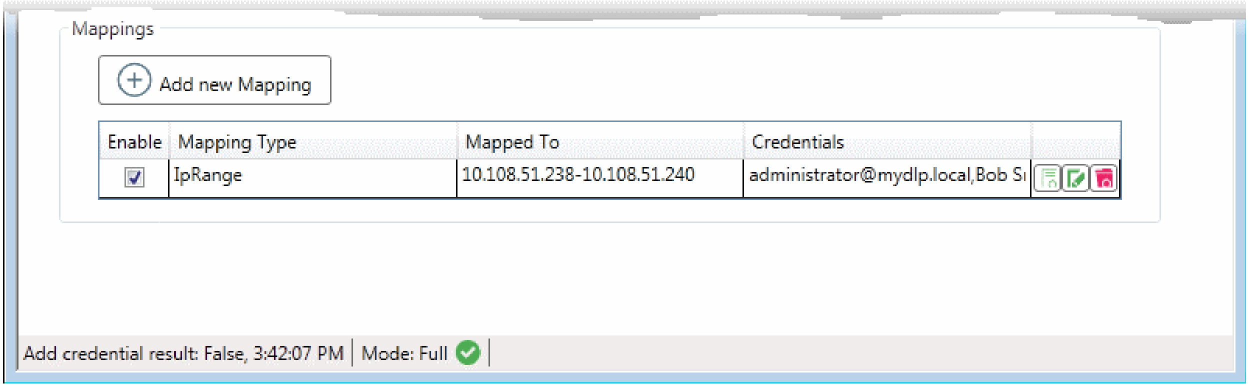
- Click 'Add Credential' at the right end of the row, to change the credential for the network.

The 'Set Credentials' dialog will appear.



- Select the credential(s) to be applied to the network and click 'Ok'.

Note: You can select more than one credential for a network, if it contains endpoints that can only be accessed by using respective credentials.



Enable	Mapping Type	Mapped To	Credentials
☑	IpRange	10.108.51.238-10.108.51.240	administrator@mydlp.local,Bob Sı

Add credential result: False, 3:42:07 PM | Mode: Full

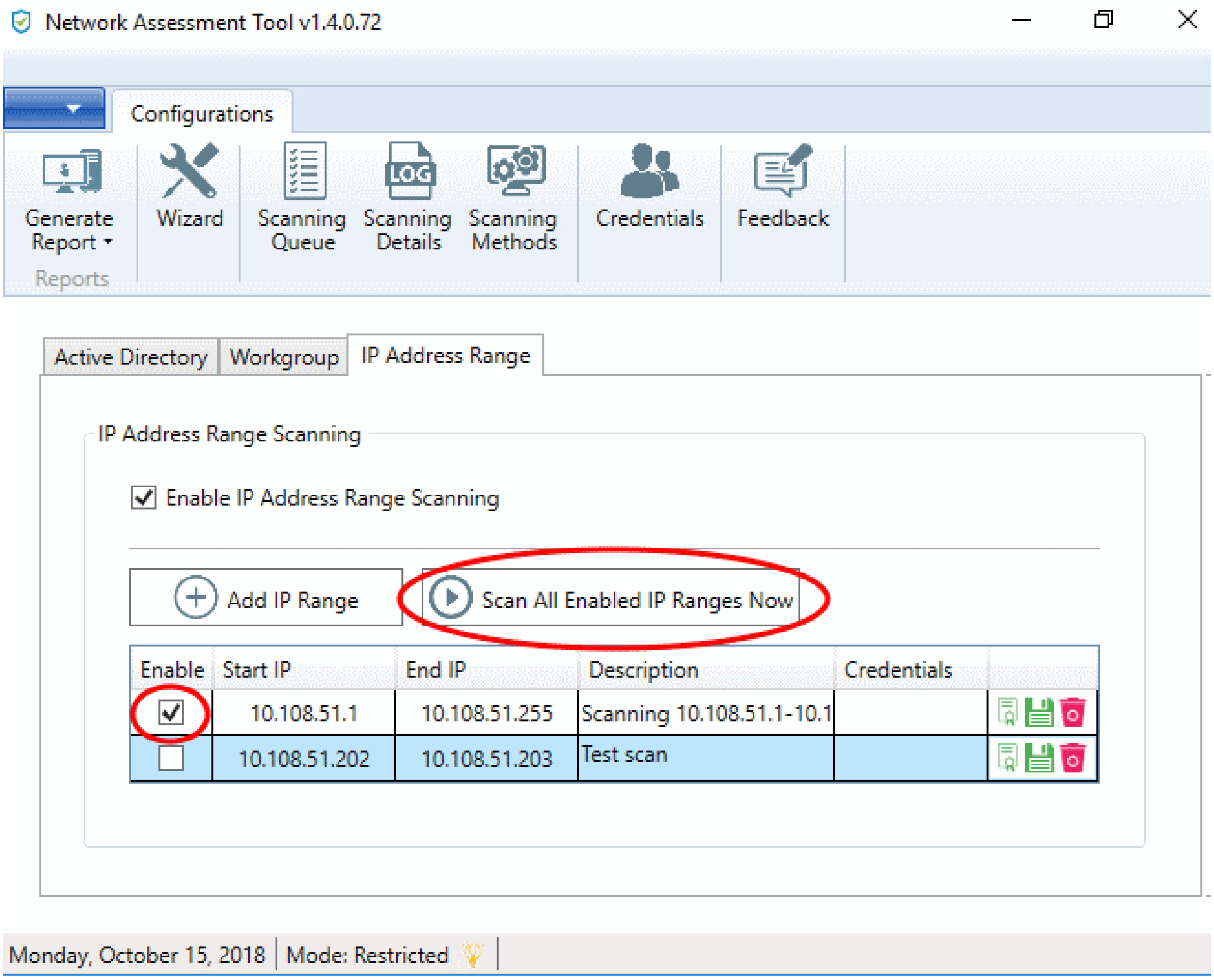
- To add new credential(s) to the same network, click 'Add Credential' at the right end of the row and repeat the process.
- Click 'Edit' at the right of the row, to edit the network and change the network type and the network. The process is similar to adding a network mapping.
- Click the trash can , to remove a mapping from the list.

3 Run Network Assessment Scan

- You can run assessment scans on networks at anytime. You can also generate reports on the scan afterwards.
    - You can view the progress of scans and terminate scans from the 'Scanning Queue' interface.
    - You can view a log of scans from the 'Scanning Details' interface.

To initiate a scan

- Click 'Scanning Methods' on the menu bar
- Choose the type of network on which the scan will run:
    - Active Directory
    - Workgroup
    - IP Address Range
- Ensure target networks are enabled. Disable those you do not wish to scan.
- Click 'Scan All Enabled... Now'



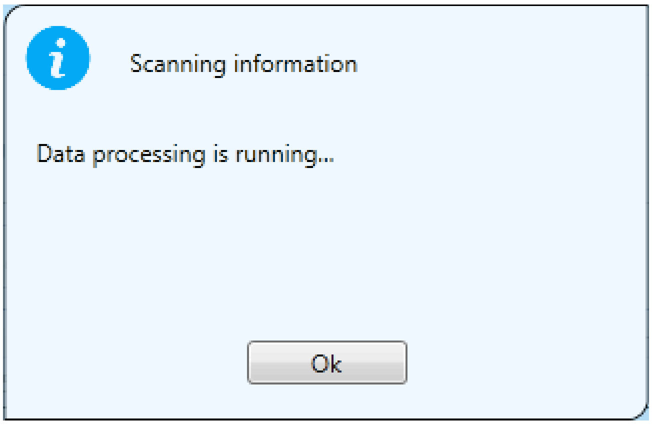
IP Address Range Scanning

☑ Enable IP Address Range Scanning

Enable	Start IP	End IP	Description	Credentials
☑	10.108.51.1	10.108.51.255	Scanning 10.108.51.1-10.1	
☐	10.108.51.202	10.108.51.203	Test scan	

Monday, October 15, 2018 | Mode: Restricted

The scan will start:



Scanning information

Data processing is running...

- You can view the scan progress of scan in the 'Scanning Details' interface.

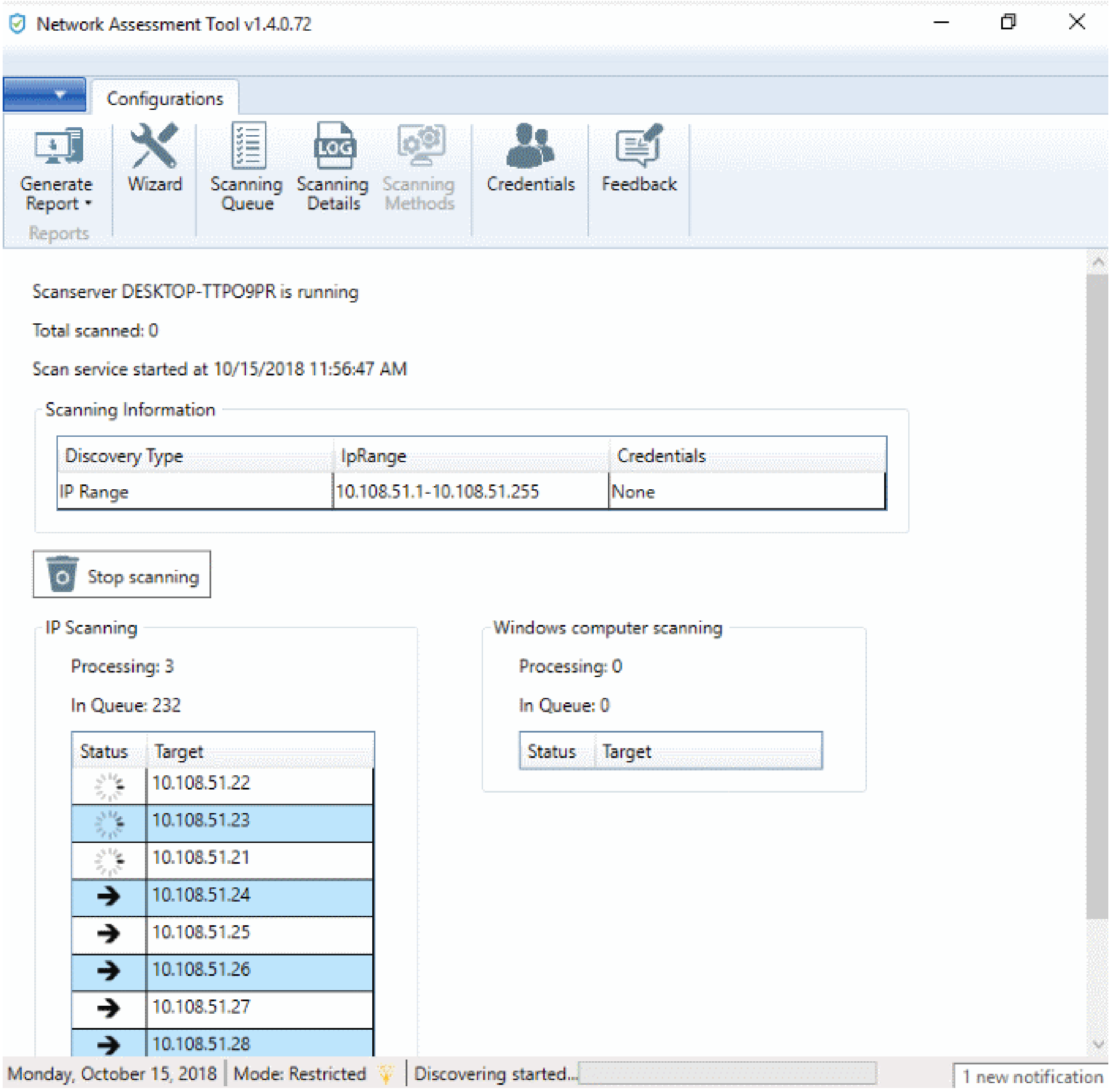
See the following sections for more help:

- **Viewing Scan Progress**
- **Viewing Scan Logs**

3.1 View Scan Progress

The 'Scanning Queue' interface allows you to view the progress of scans and to terminate unwanted scans.

- Click 'Scanning Queue' on the menu bar



Scanserver DESKTOP-TTPO9PR is running

Total scanned: 0

Scan service started at 10/15/2018 11:56:47 AM

Scanning Information

Discovery Type	IpRange	Credentials
IP Range	10.108.51.1-10.108.51.255	None

IP Scanning

Processing: 3

In Queue: 232

Status	Target
	10.108.51.22
	10.108.51.23
	10.108.51.21
→	10.108.51.24
→	10.108.51.25
→	10.108.51.26
→	10.108.51.27
→	10.108.51.28

Windows computer scanning

Processing: 0

In Queue: 0

Status	Target

Monday, October 15, 2018 | Mode: Restricted | Discovering started...

- **Scanning Information -** Displays all domains, workgroups and IP addresses currently being scanned.
- **IP Scanning -** Shows IP addresses discovered on the current network using Network Mapper (Nmap).
- **Windows Computer Scanning -** Shows hostnames/IP addresses being scanned using Windows Management Instrumentation(WMI) and Microsoft Baseline Security Analyzer (MBSA)

- Click 'Stop Scanning' if you want to terminate a scan.

You can create reports for recently run scan in the 'Generate Reports' area. See **Generate Reports** for more details.

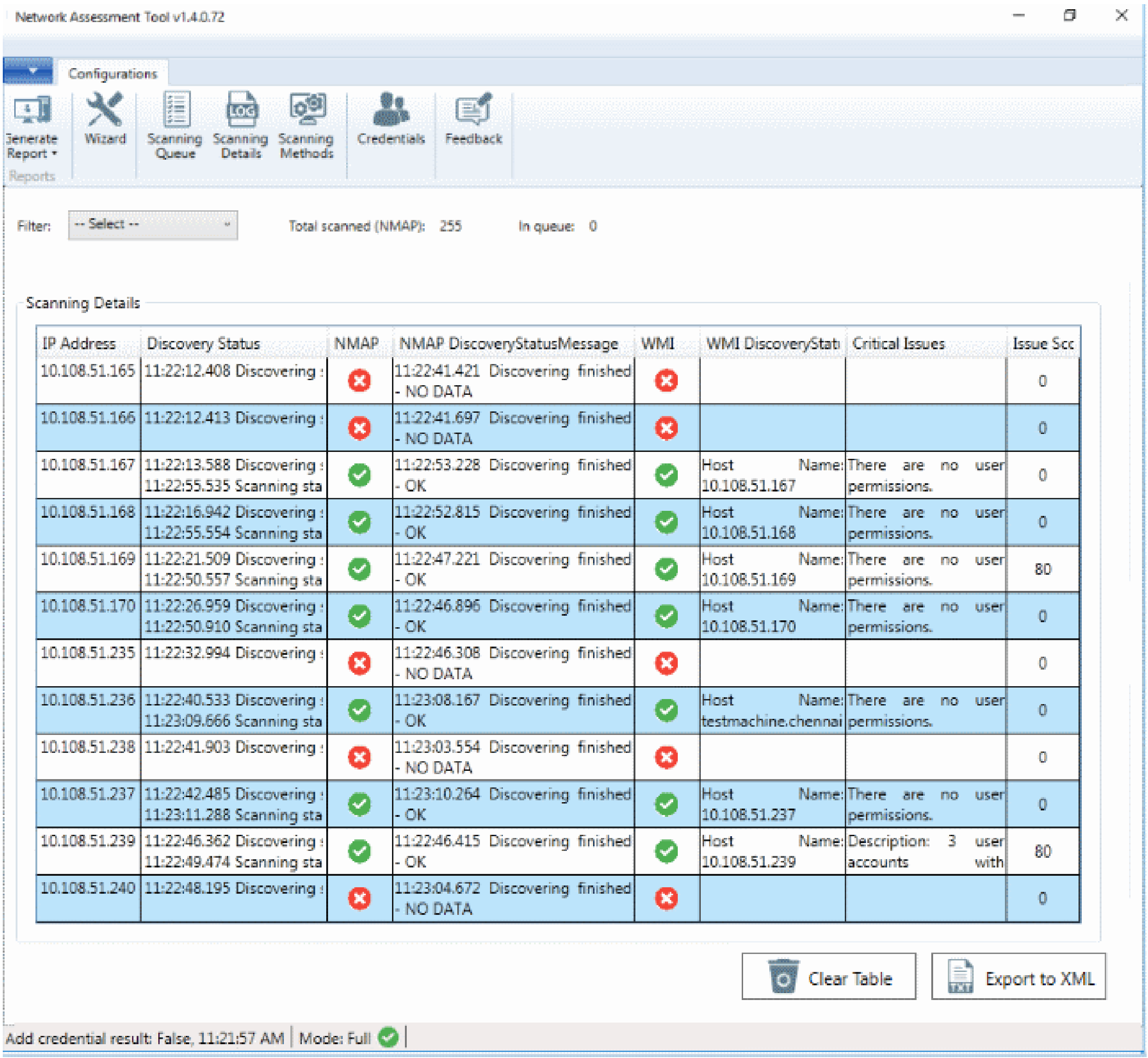
3.2 View Scan Logs

- The 'Scanning Details' interface lets you view logs of currently running and recent scans.
- The logs provide information on the IP address scanned as per the domain, workgroup or the IP address range chosen for scanning, endpoints discovered at the IP addresses, a summary of critical issues identified from the endpoints and the issue score of the endpoints.

- The logs can also be saved as an XML file for later analysis.

> **Note**: The 'Scanning Details' interface will be available only if logging is enabled for the NAT application. See **Configuring Network Assessment Tool** for more details.

- To view the scan logs, click 'Scanning Details' from the menu bar.



Filter: -- Select --   Total scanned (NMAP): 255   In queue: 0

Scanning Details

IP Address	Discovery Status	NMAP	NMAP DiscoveryStatusMessage	WMI	WMI DiscoveryStat	Critical Issues	Issue Scc
10.108.51.165	11:22:12.408 Discovering :	✗	11:22:41.421 Discovering finished - NO DATA	✗			0
10.108.51.166	11:22:12.413 Discovering :	✗	11:22:41.697 Discovering finished - NO DATA	✗			0
10.108.51.167	11:22:13.588 Discovering : 11:22:55.535 Scanning sta	✓	11:22:53.228 Discovering finished - OK	✓	Host Name: 10.108.51.167	There are no user permissions.	0
10.108.51.168	11:22:16.942 Discovering : 11:22:55.554 Scanning sta	✓	11:22:52.815 Discovering finished - OK	✓	Host Name: 10.108.51.168	There are no user permissions.	0
10.108.51.169	11:22:21.509 Discovering : 11:22:50.557 Scanning sta	✓	11:22:47.221 Discovering finished - OK	✓	Host Name: 10.108.51.169	There are no user permissions.	80
10.108.51.170	11:22:26.959 Discovering : 11:22:50.910 Scanning sta	✓	11:22:46.896 Discovering finished - OK	✓	Host Name: 10.108.51.170	There are no user permissions.	0
10.108.51.235	11:22:32.994 Discovering :	✗	11:22:46.308 Discovering finished - NO DATA	✗			0
10.108.51.236	11:22:40.533 Discovering : 11:23:09.666 Scanning sta	✓	11:23:08.167 Discovering finished - OK	✓	Host Name: testmachine.chennai	There are no user permissions.	0
10.108.51.238	11:22:41.903 Discovering :	✗	11:23:03.554 Discovering finished - NO DATA	✗			0
10.108.51.237	11:22:42.485 Discovering : 11:23:11.288 Scanning sta	✓	11:23:10.264 Discovering finished - OK	✓	Host Name: 10.108.51.237	There are no user permissions.	0
10.108.51.239	11:22:46.362 Discovering : 11:22:49.474 Scanning sta	✓	11:22:46.415 Discovering finished - OK	✓	Host Name: 10.108.51.239	Description: 3 user accounts with	80
10.108.51.240	11:22:48.195 Discovering :	✗	11:23:04.672 Discovering finished - NO DATA	✗			0

Add credential result: False, 11:21:57 AM | Mode: Full ✓

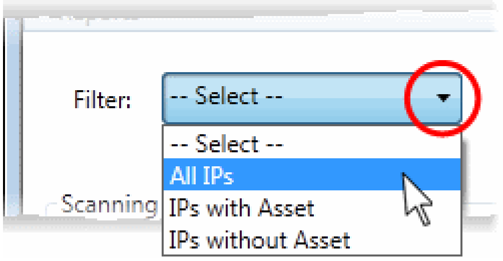
Scanning Details - Column Descriptions	
Column Header	**Description**
IP Address	Indicates the IP address scanned
Discovery Status	Indicates the precise time at which the IP address was scanned for assets and the status
NMAP	Indicates whether an asset, like an endpoint, server or any other network device was identified at the IP address by NMAP tool.
NMAP Discovery Status Message	Indicates the precise time NMAP tool was running discovery scan on the IP address and displays the result of the scan.
WMI	Indicates whether an asset, like an endpoint, server or any other network device was

	identified at the IP address by WMI tool.
WMI Discovery Status Message	Indicates the precise time WMI tool was running discovery scan on the IP address and displays the result of the scan.
Critical Issues	Displays a summary of critical issues identified at the endpoint, at the IP address.
Issue Score	Displays the score assigned to the endpoint by NAT, based on issues identified at the endpoint. Larger the score, larger the number of issues found at the endpoint.

Sort and Filter Options:

- Clicking on any column header sorts the events based on the alphabetical order of entries in that column

The 'Filter' drop-down at the top left allows you to filter the scanning details based on discovery of assets at the IP addresses scanned. The available options are:



- All IPs - Displays the scanning details from all IP addresses scanned
- IPs with Asset - Displays the scanning details only from those IP addresses at which network assets were discovered
- IPs without Asset - Displays the scanning details only from those IP addresses at which no network assets were discovered

Save Logs:

You can generate an XML file from the currently displayed logs and save it for analysis at a later time.

To save the logs

- Use the filter to view the scan details you want to save as XML file
- Click 'Export to XML' and save the generated .xml file on your computer

4 Generate Reports

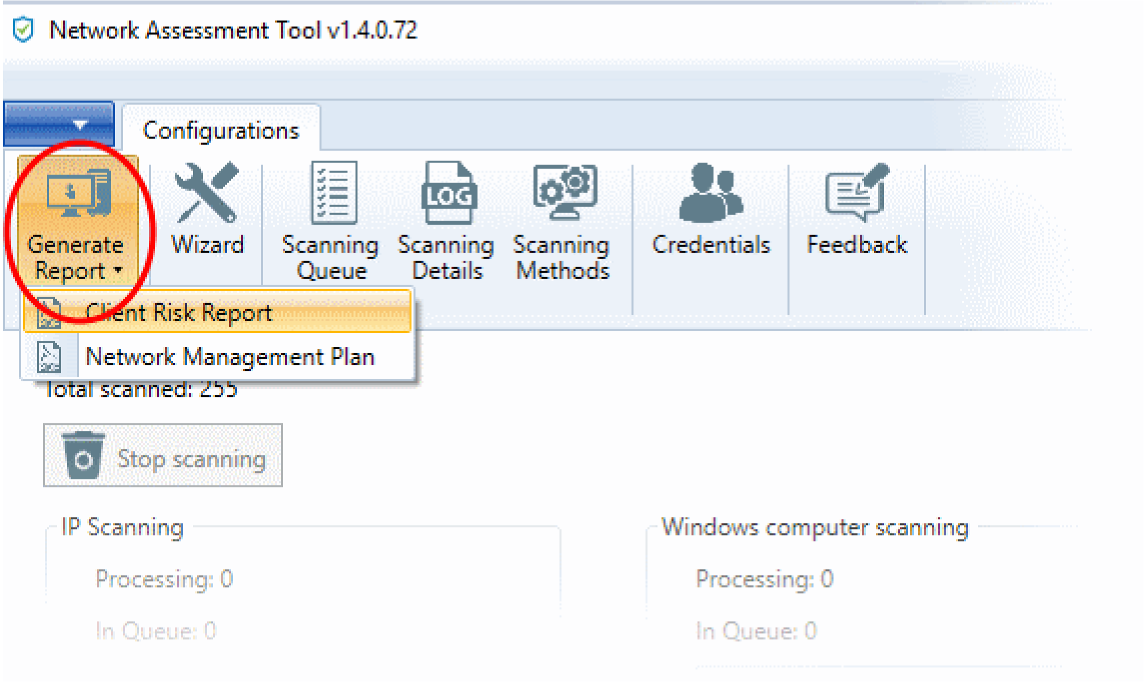
- Admins can generate assessment reports on the network last scanned.

NAT can generate two types of reports:

- Client Risk Report - An report on discovered network assets, issues identified, and more.
- Network Management Plan – Help to remediate issues found on scanned endpoints.

To download reports from the last scan

- Click 'Generate Report' from the menu bar
- Choose the report type from the drop-down

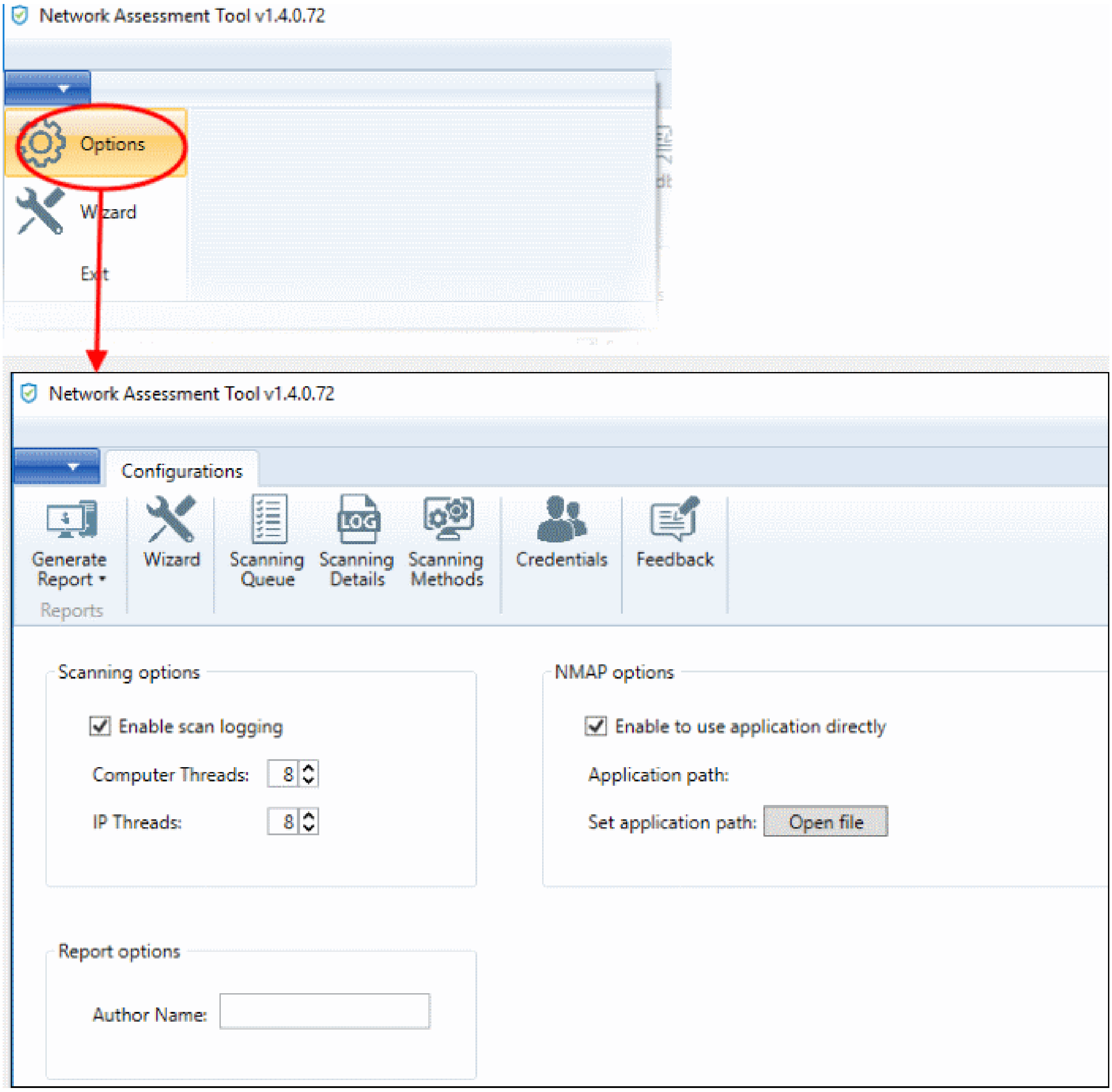


NAT will start generating the report and on completion you will be able to download and save the report on your computer in pdf format.

Tip: The cover page of the report contains the 'Author Name' that indicates the person that generated the report, with a label 'Prepared by' . You can configure the author name to be displayed on the cover page from the configuration panel. See **Configuring Network Assessment Tool** for more details.

5 Configure Network Assessment Tool

- Click the blue drop-down arrow at the top left and choose 'Options'



Scanning options

☑ Enable scan logging

Computer Threads: 8

IP Threads: 8

NMAP options

☑ Enable to use application directly

Application path:

Set application path:

Report options

Author Name:

Scan Options

- NAT uses Network Mapper (NMAP) to discover endpoints in the IP addresses covered by the network being scanned and Windows Management Instrumentation (WMI) and Microsoft Baseline Security Analyzer (MBSA) to scan the identified endpoints.
- The parameters under 'Scanning Options' allow you to configure the number of threads that can be used by NMAP for discovery and number of threads that can be used by WMI and MBSA for scanning endpoints. You can also enable or disable logging of the scan details.
  - **Enable scan logging** - Allows you to enable or disable logging of scan details of IP addresses discovered by the domain, workgroup or the IP address range. The logs of currently running or the last run scan can be viewed from the 'Scanning Details' interface. See **Viewing Scan Logs** for more details.
  - **Computer Threads** - Choose the number of threads to be used for scanning endpoints/IP addresses in the network
  - **IP Threads** - Choose the number of threads to be used for discovering endpoints/IP addresses in the network

NMAP Options

As a prerequisite, NAT requires NMAP installed on the same computer to discover the endpoints/IP addresses covered by the network. Upon every scan execution, NAT checks for the NMAP installation. If NMAP is installed on its default location (C:\Program Files\Nmap), NAT can identify the application. If NMAP is installed on a different location, you need to manually specify the installation location of NMAP.

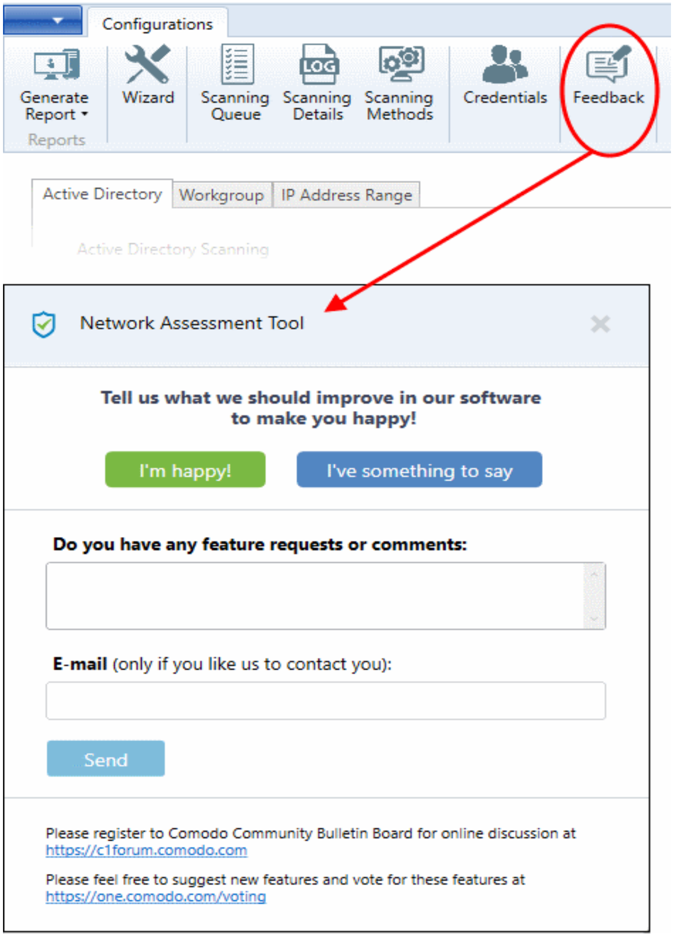
- **Enable to use application directly -** Allows you to enable or disable NAT to use NMAP installed on your computer, at a location different from the default path. If enabled, click 'Open File' and navigate to the installation location of NMAP application, select the application and click 'Open'.

Report Options

- **Author Name -** Allows you to specify the name of the person that runs the scans and generates the network assessment reports. The name will appear beside 'Prepared by:' in the cover pages of client risk report and management plan, generated by NAT.

6 Feedback

- The feedback tab allows you to post your remarks on the NAT software.
- Enter issues/improvements/modifications you want in the tool.
  - **Do you have any feature requests or comments -** Enter your recommendations/comments in this text field
  - **Email -** Enter your email id if you want the Comodo One support team to contact you.



Network Assessment Tool

Tell us what we should improve in our software to make you happy!

Do you have any feature requests or comments:

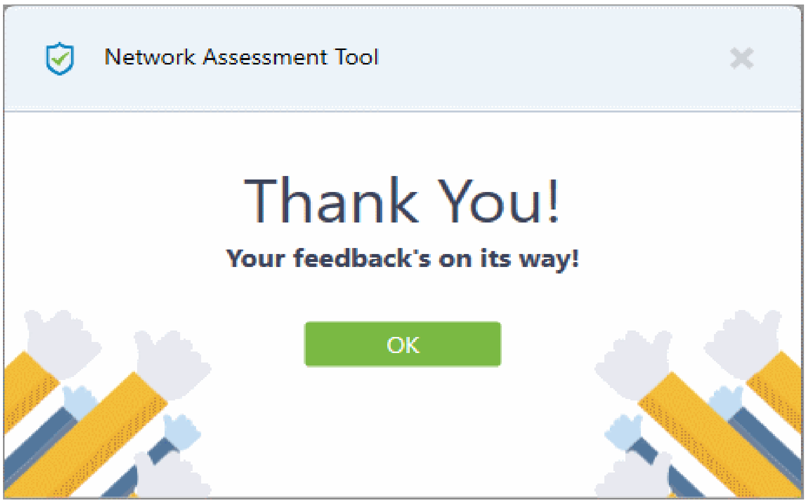
E-mail (only if you like us to contact you):

Please register to Comodo Community Bulletin Board for online discussion at https://c1forum.comodo.com

Please feel free to suggest new features and vote for these features at https://one.comodo.com/voting

- Click 'Send' after you have entered your email address.

A 'Thank You' screen will be displayed



Thank You!

Your feedback's on its way!

- Click 'OK' to go back to the NAT interface.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**