rat

ITarian

Software Version 3.26

Network Assessment Tool Quick Start Guide

Guide Version 1.4.010820

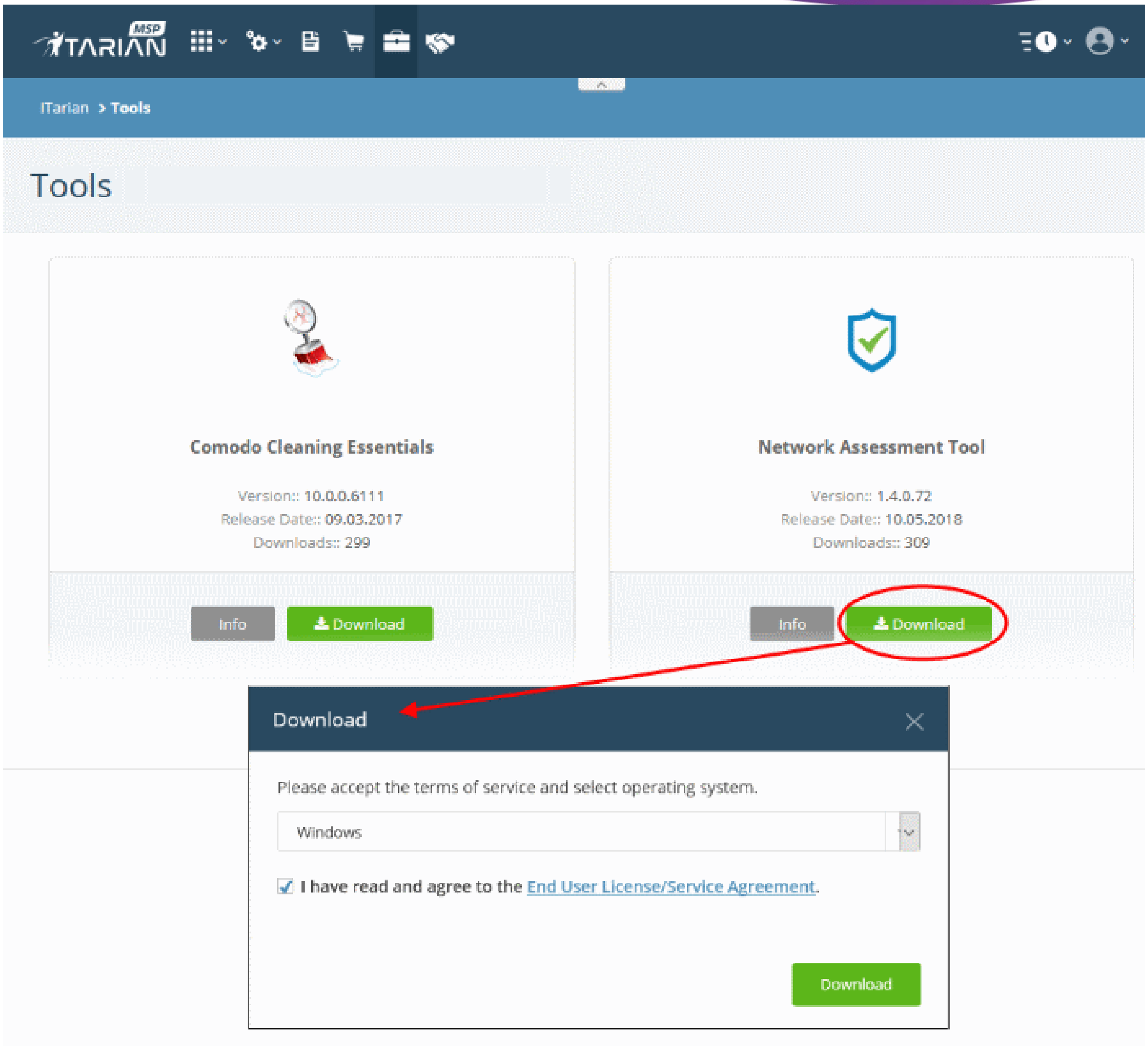
1255 Broad Street
Clifton, NJ 07013

Network Assessment Tool - 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 ITarian and download the NAT Tool

- Login to your ITarian 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.

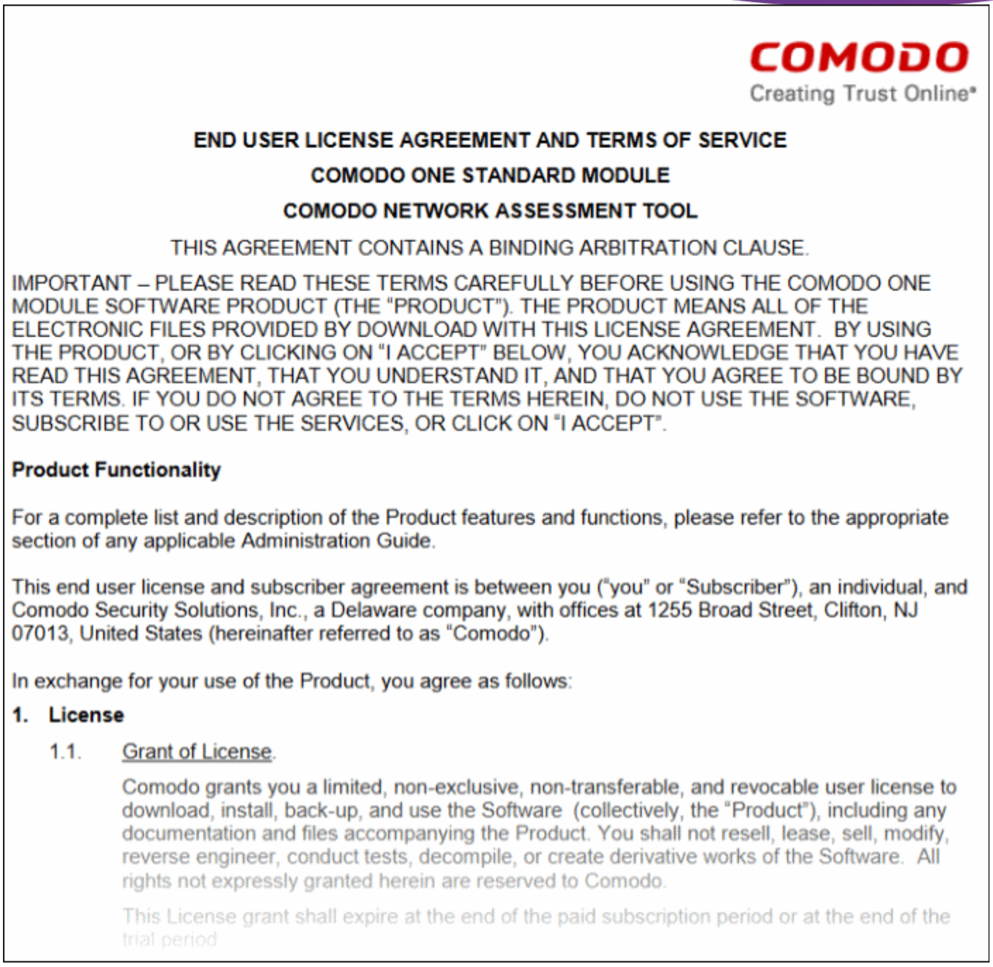
☑ I have read and agree to the End User License/Service Agreement.

- 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 applications if you do not have them already.

- Double click on the setup file 🛡 to start the NAT installation wizard



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:

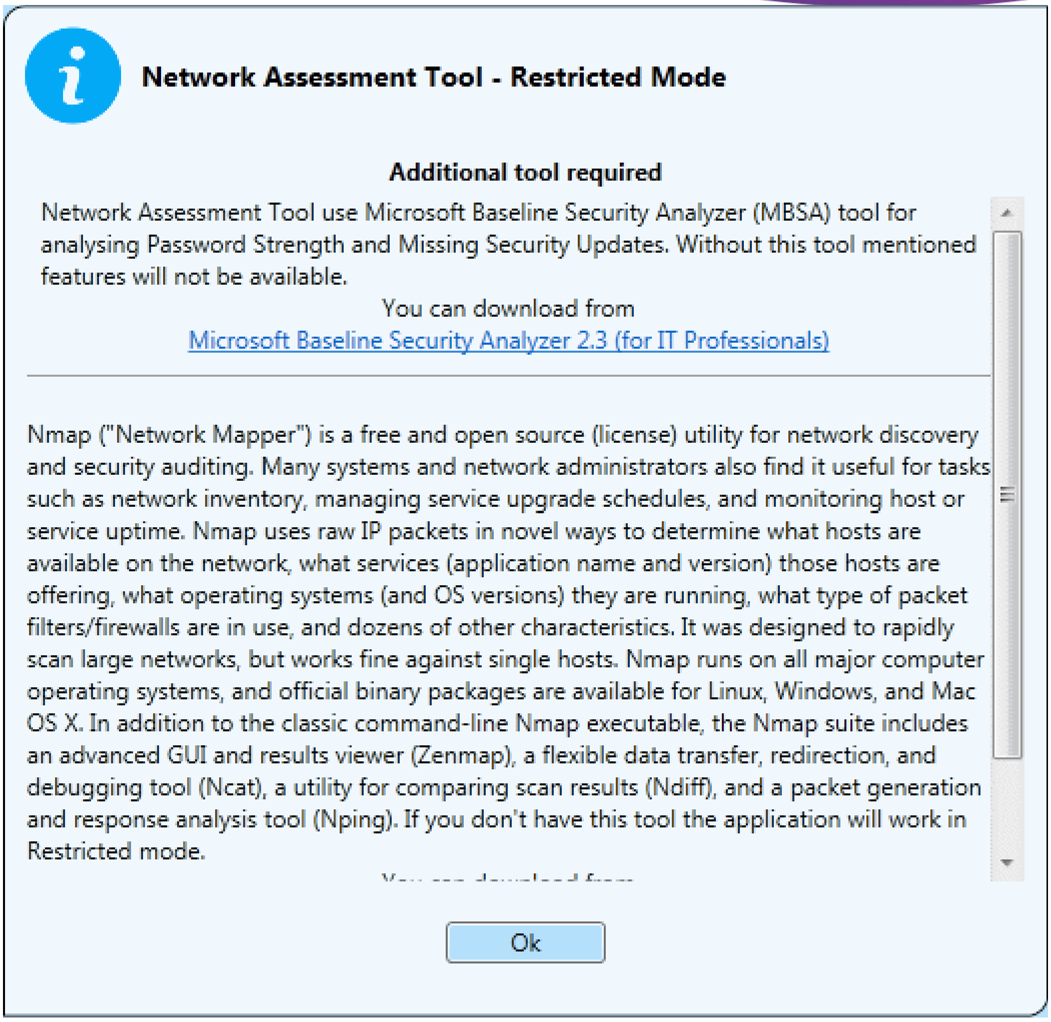
1. License

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

- 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

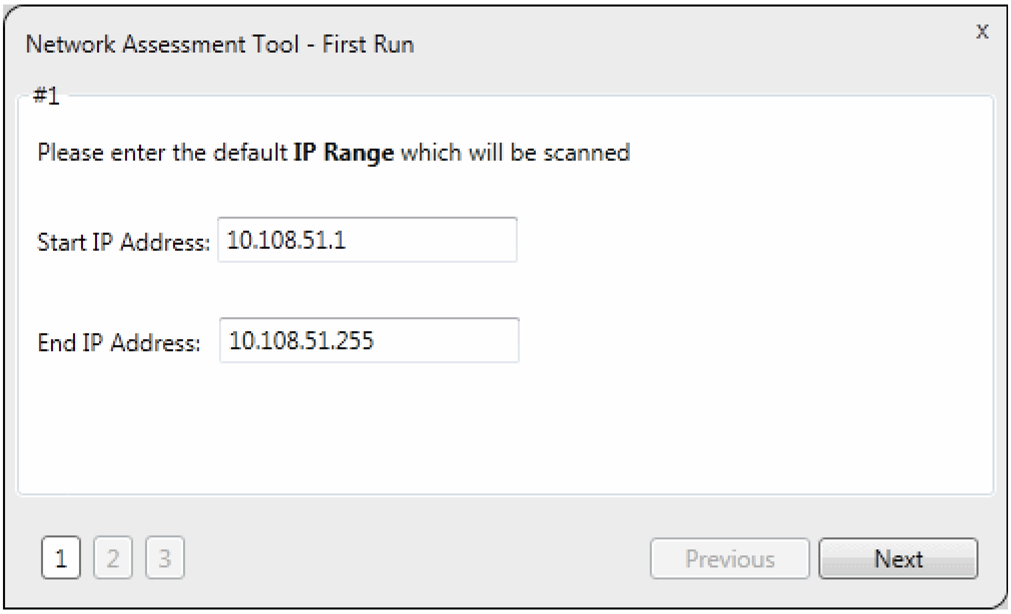
Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

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.

You can download from

Step 3 - Run Initial Configuration Wizard

The configuration wizard begins once NAT installation is complete:



Network Assessment Tool - First Run

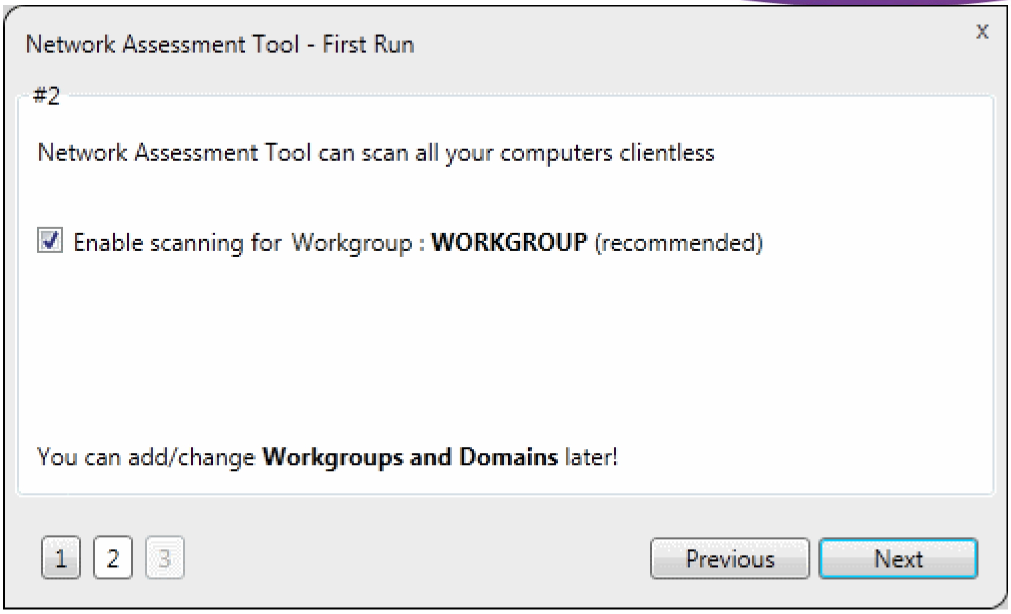
#1

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 identifies the network on which it is installed and populates the 'Start IP Address' and 'End IP Address'
- If required, you can change the start and end IP addresses to a different target network.
- Click 'Next' to move to the next step.



Network Assessment Tool - First Run

#2

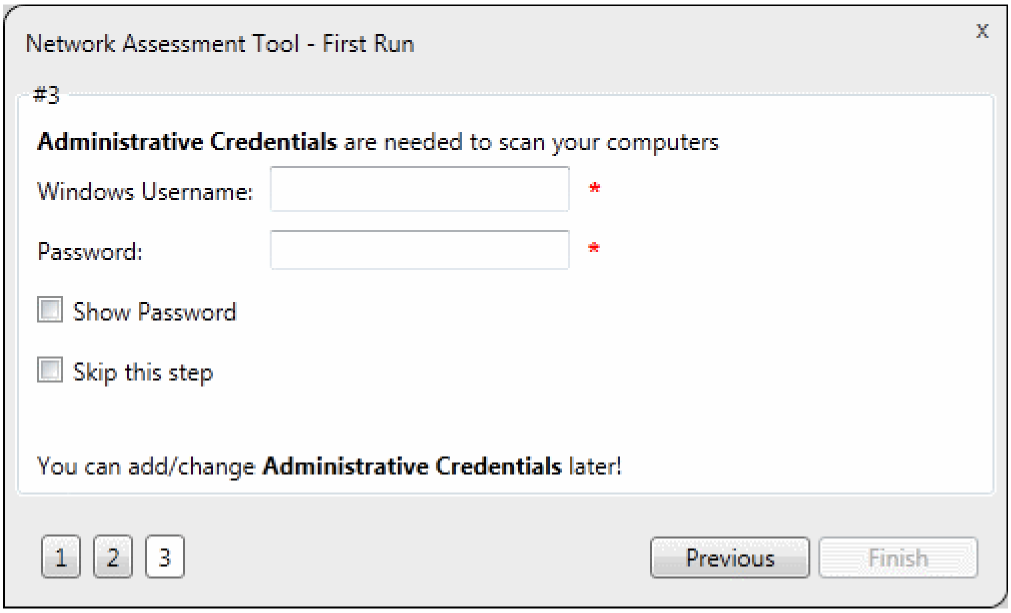
Network Assessment Tool can scan all your computers clientless

☑ 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 connected.

- 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: *

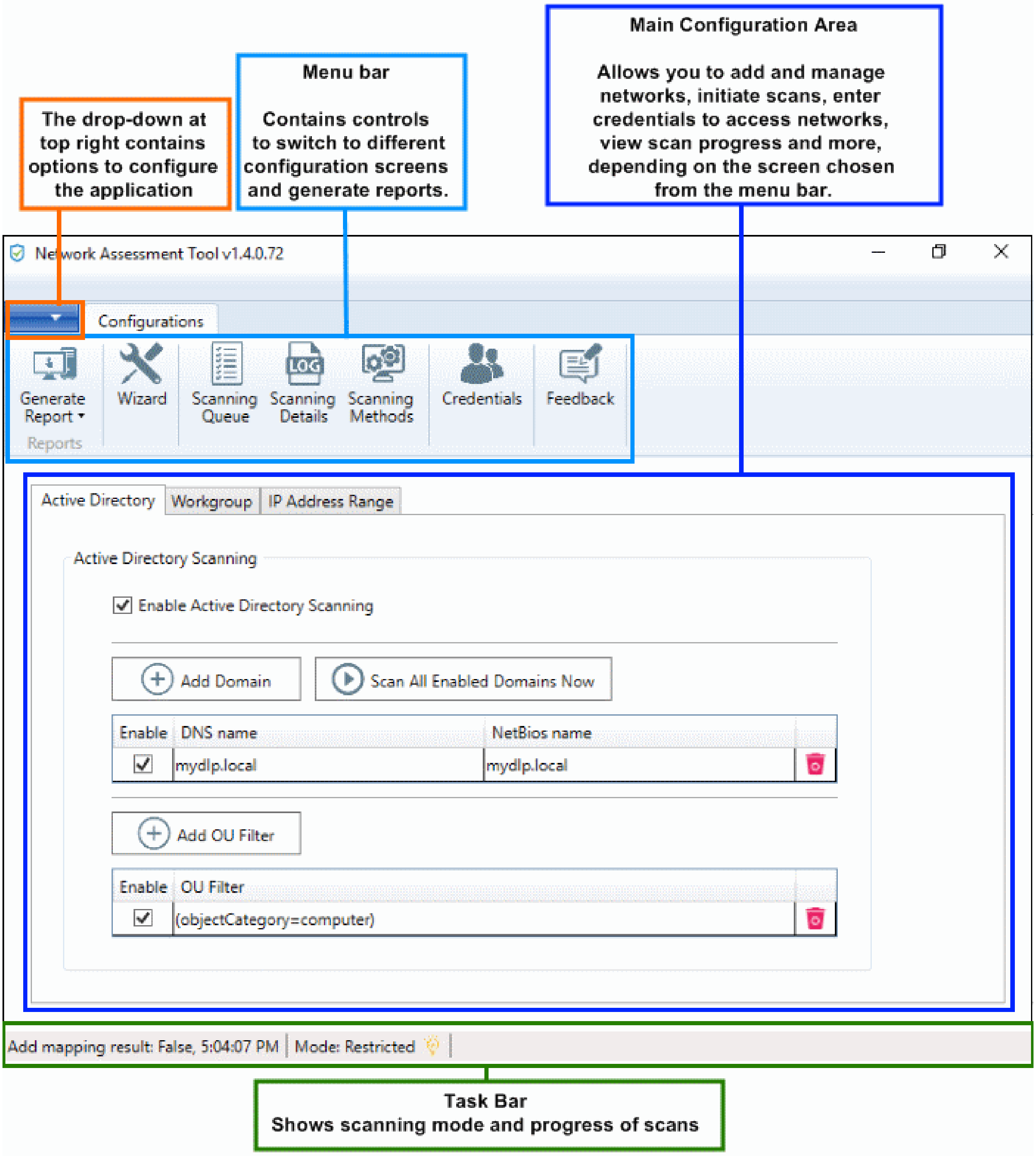
Password: *

□ 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:



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

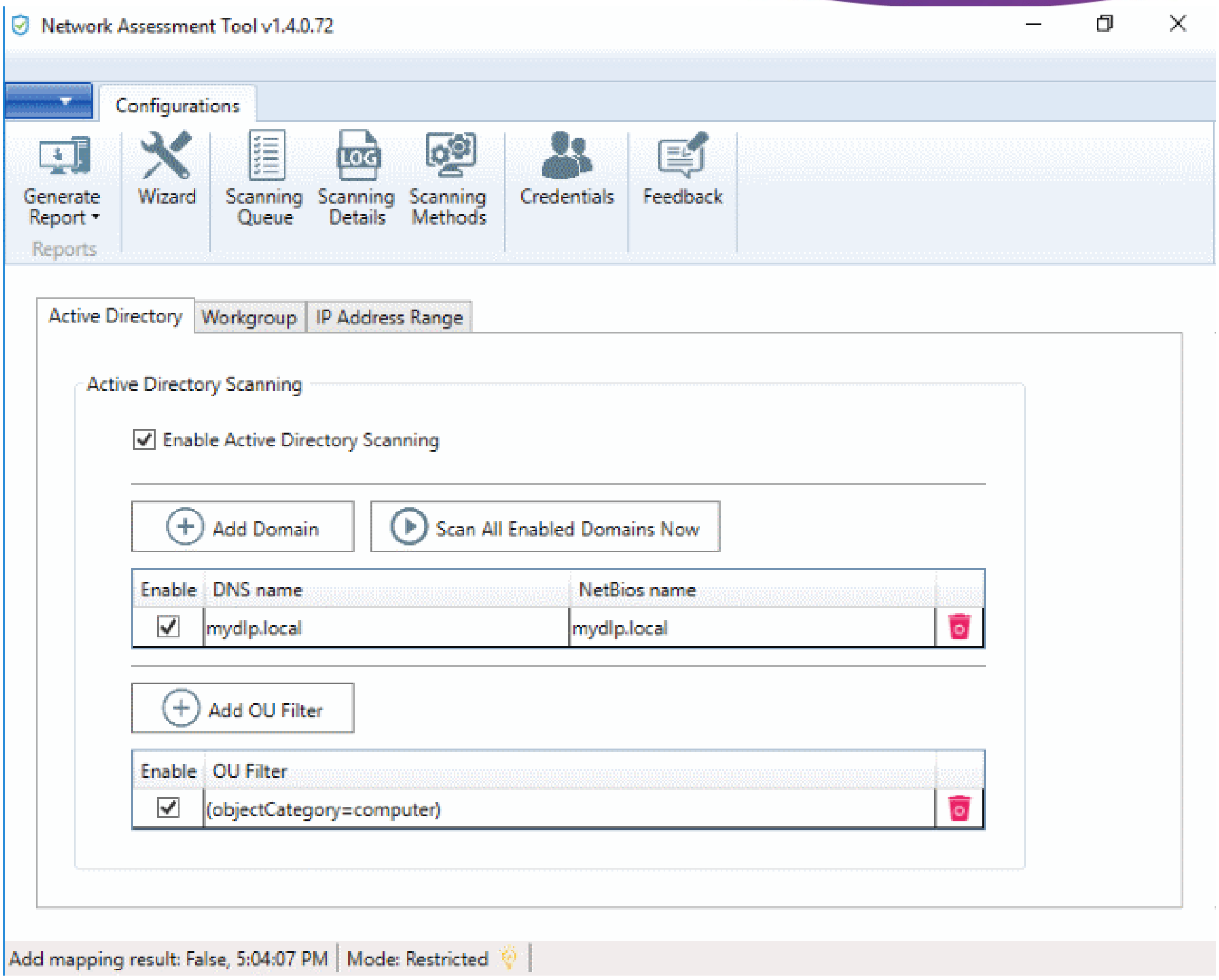
- To view scan progress, click the 'Scanning Queue' button
- To generate reports on completion of scan, click 'Generate Report'.

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' from the menu bar



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

- 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

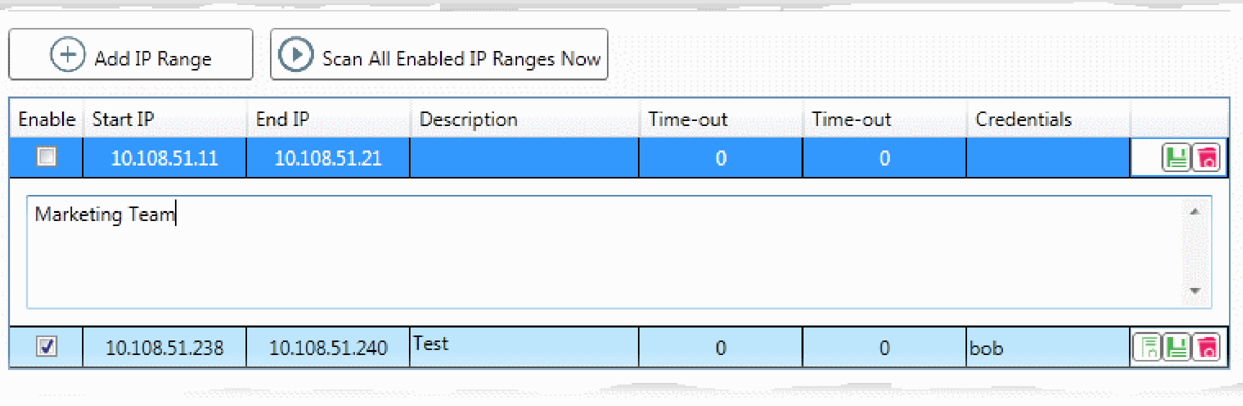
Add an IP Address Range

- 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

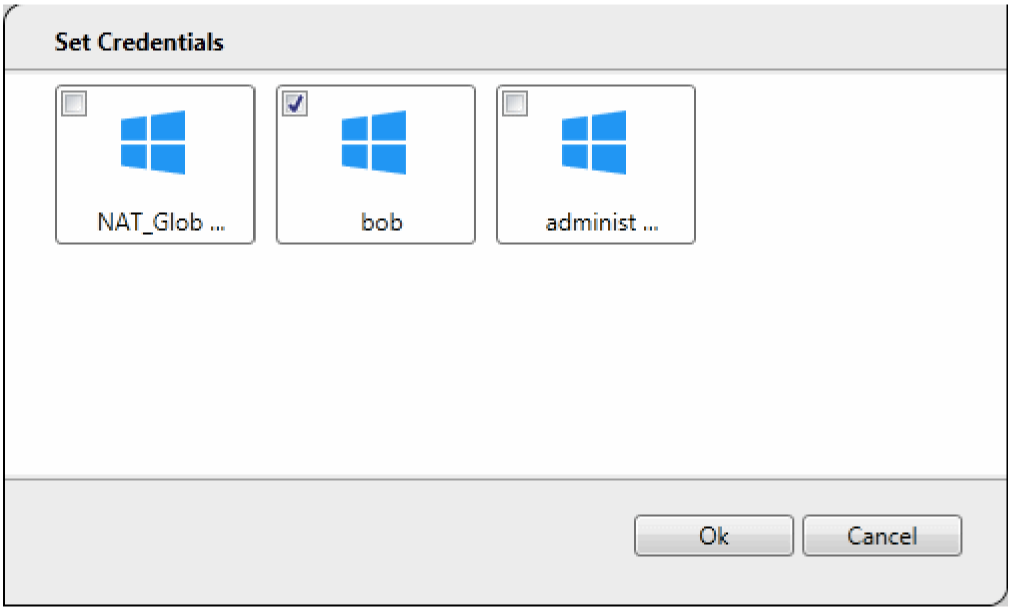
- Time out period - Skip scans on endpoints that do not respond in the set time.



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

- 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.



Set Credentials

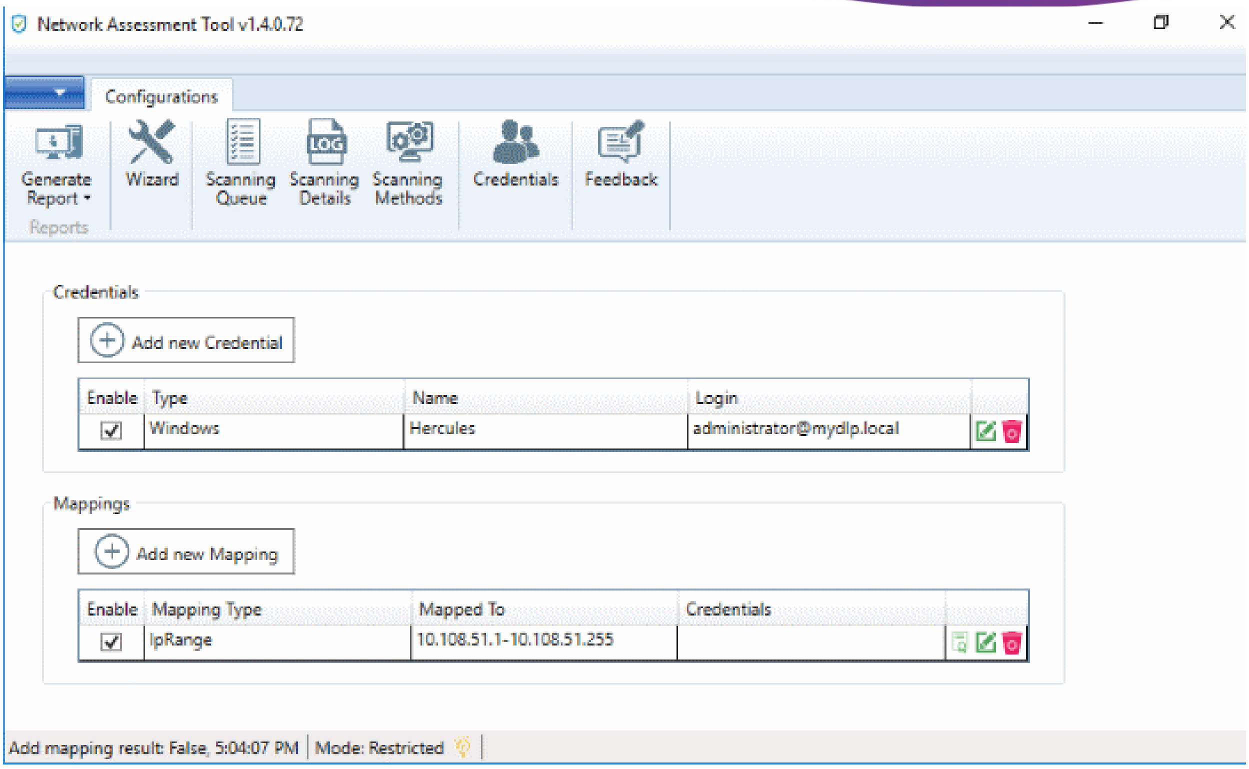
☐ NAT_Glob ...

☑ bob

☐ administ ...

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:



Credentials

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

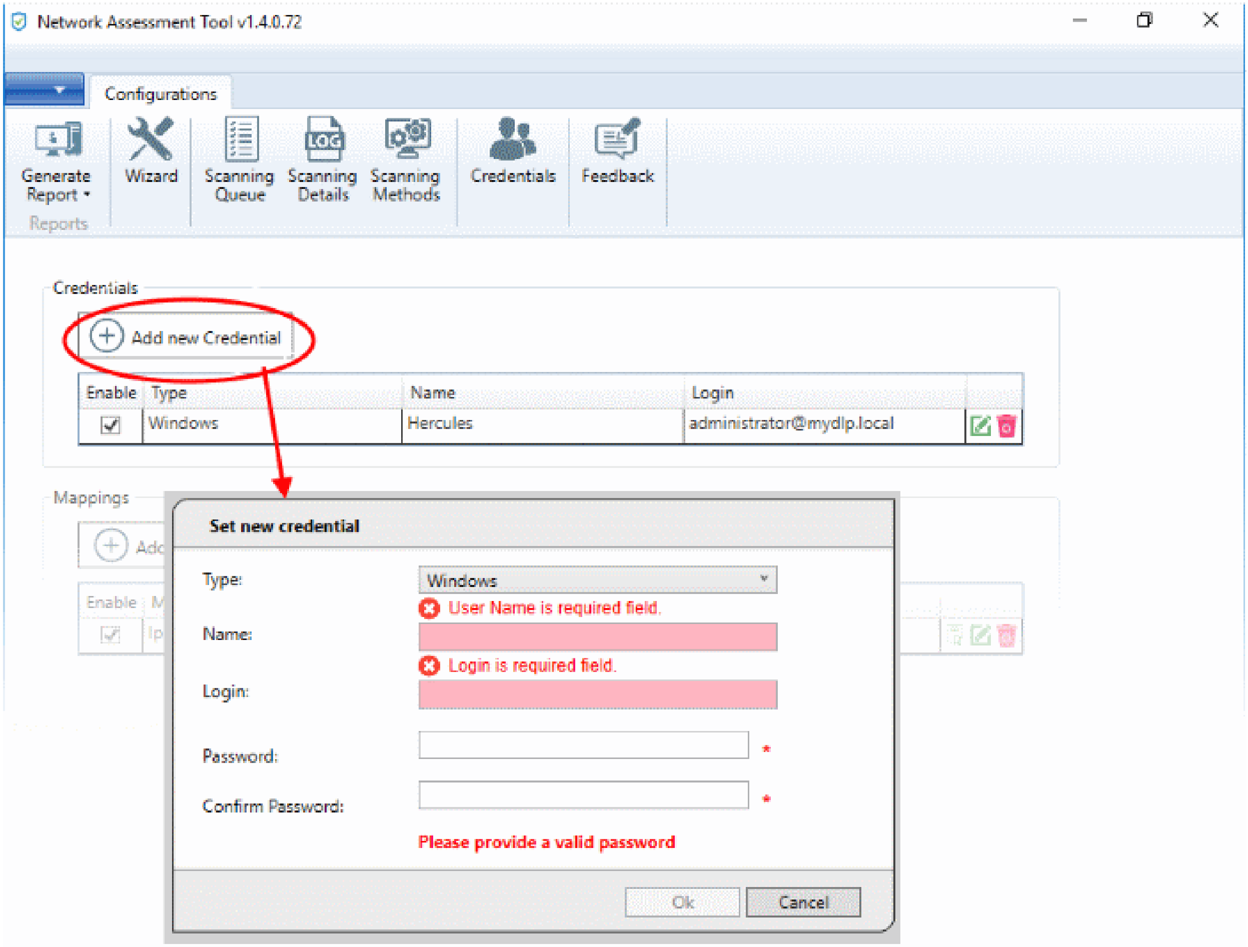
Mappings

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'



Credentials

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

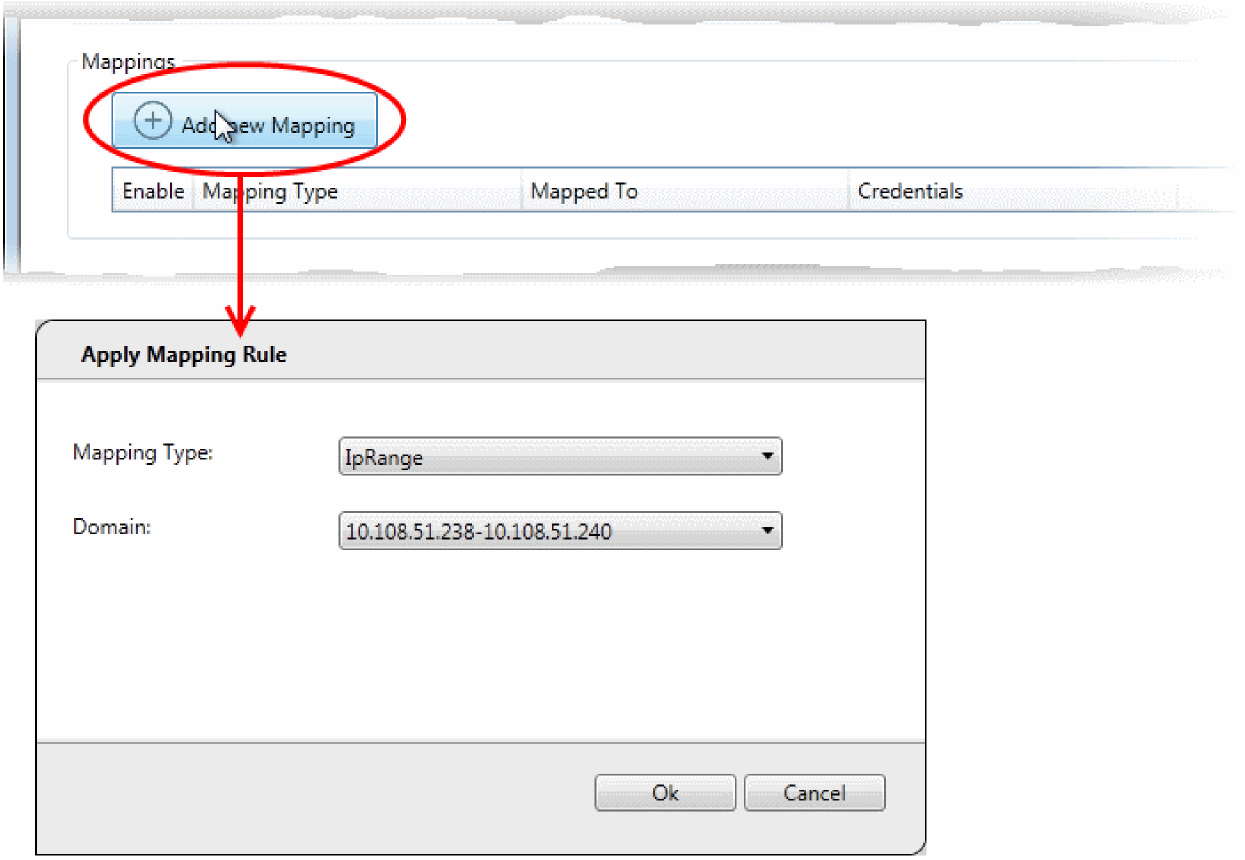
The 'Set new credential' dialog will open.

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:



Mapping Type: IpRange

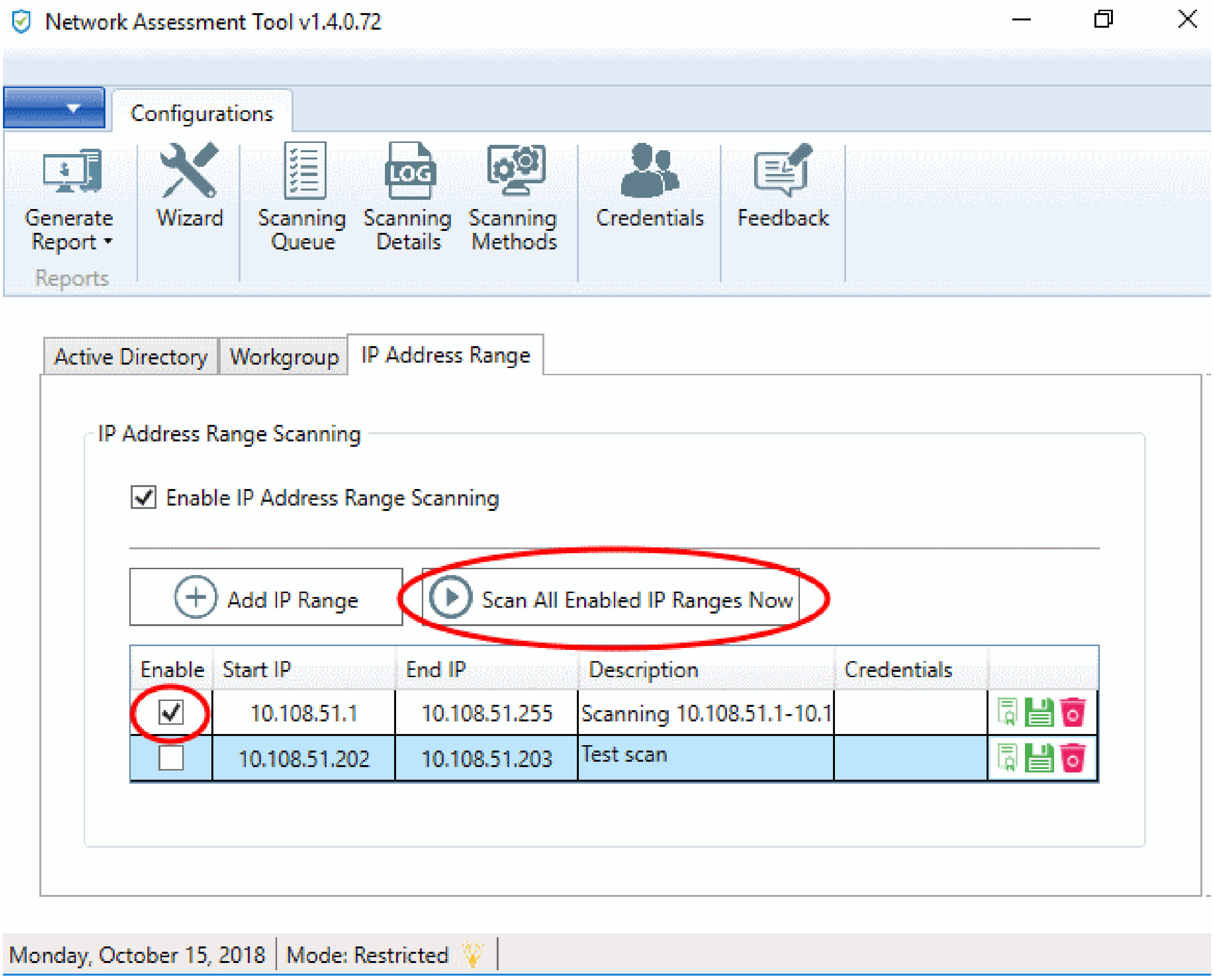
Domain: 10.108.51.238-10.108.51.240

- 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':

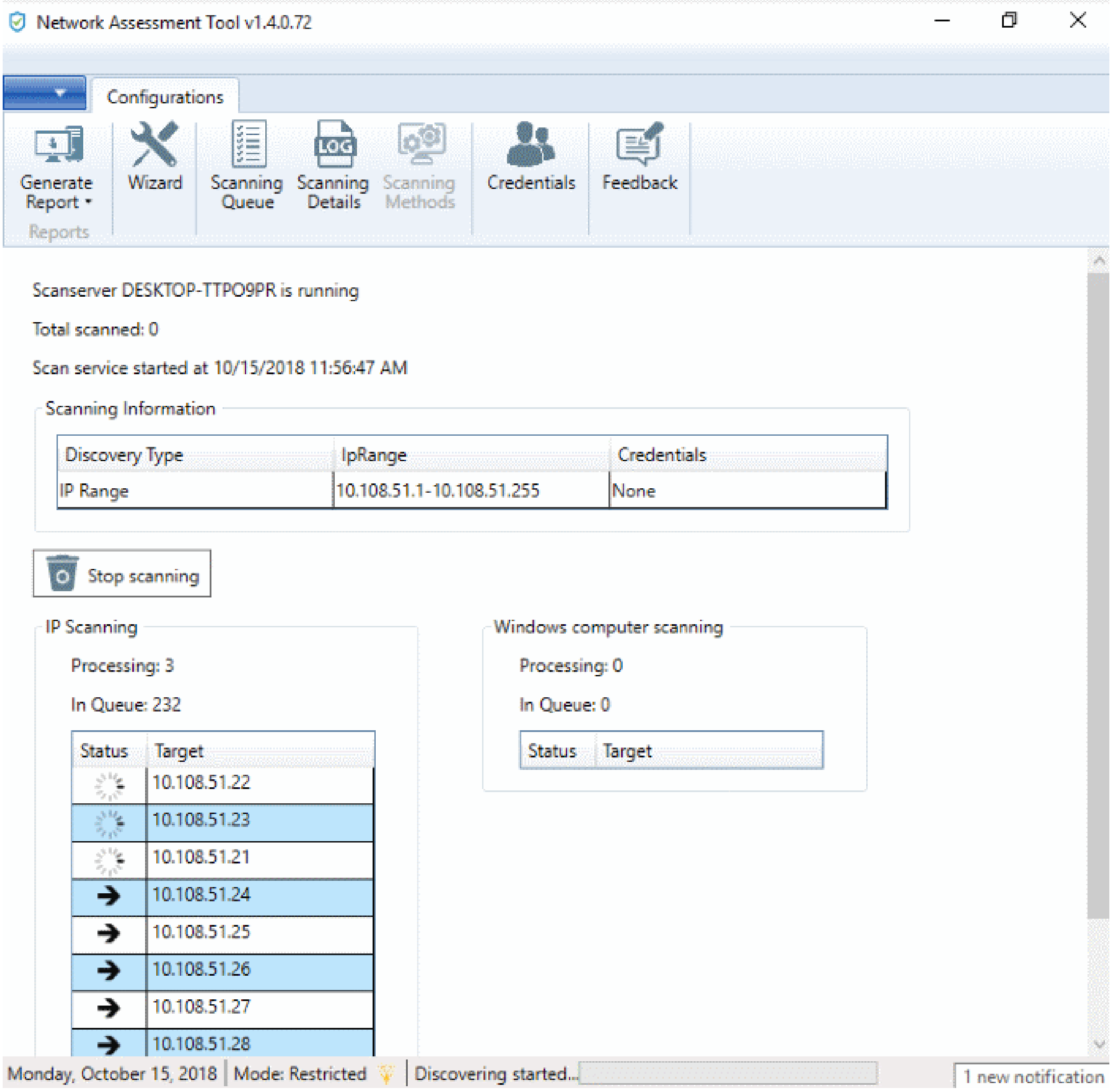


☑ Enable IP Address Range Scanning

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).

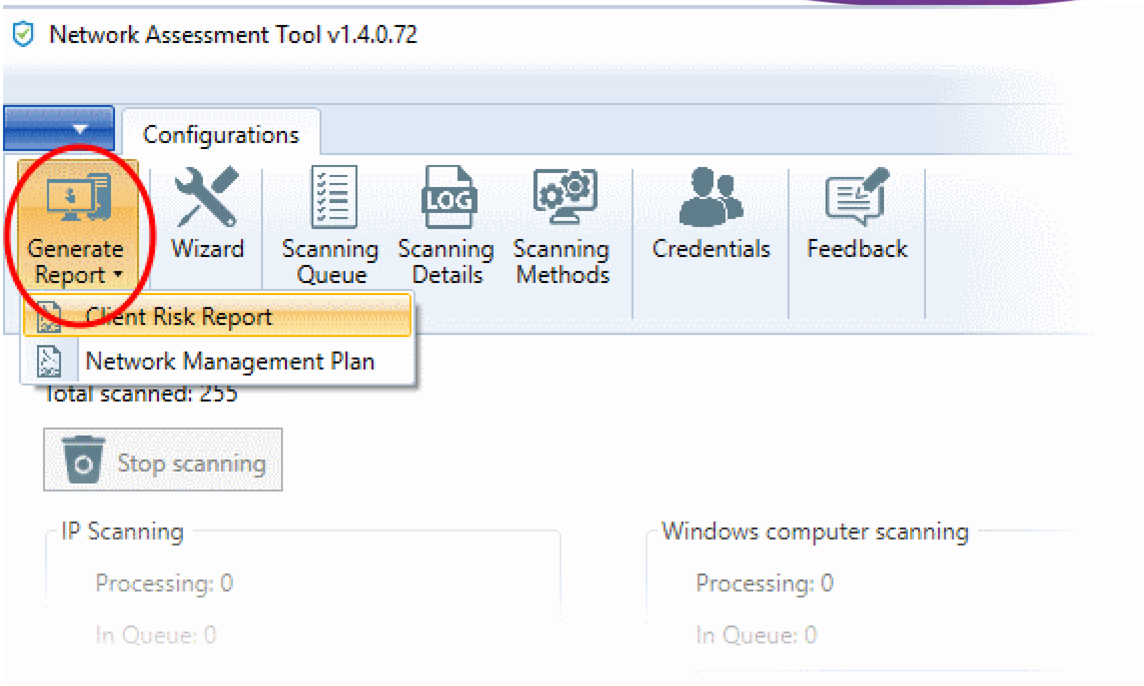
Step 7 - Generate Reports

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 generate the report in .pdf format.

About ITarian

The comprehensive and powerful ITarian IT operating platform helps you simplify operations, boost productivity, and better utilize IT resources. It includes all the essential IT management tools, including remote monitoring and management, remote access and control, service desk and ticketing, and patch management. For free.

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.

1255 Broad Street

Clifton, NJ 07013

United States

https://www.itarian.com

Sales - **sales@itarian.com** / 833-579-3572

Support - **support@itarian.com** / 877-422-3865