COMODO
Creating Trust Online®

COMODO
one

Comodo One

Software Version 3.3

Network Assessment Tool Administrator Guide

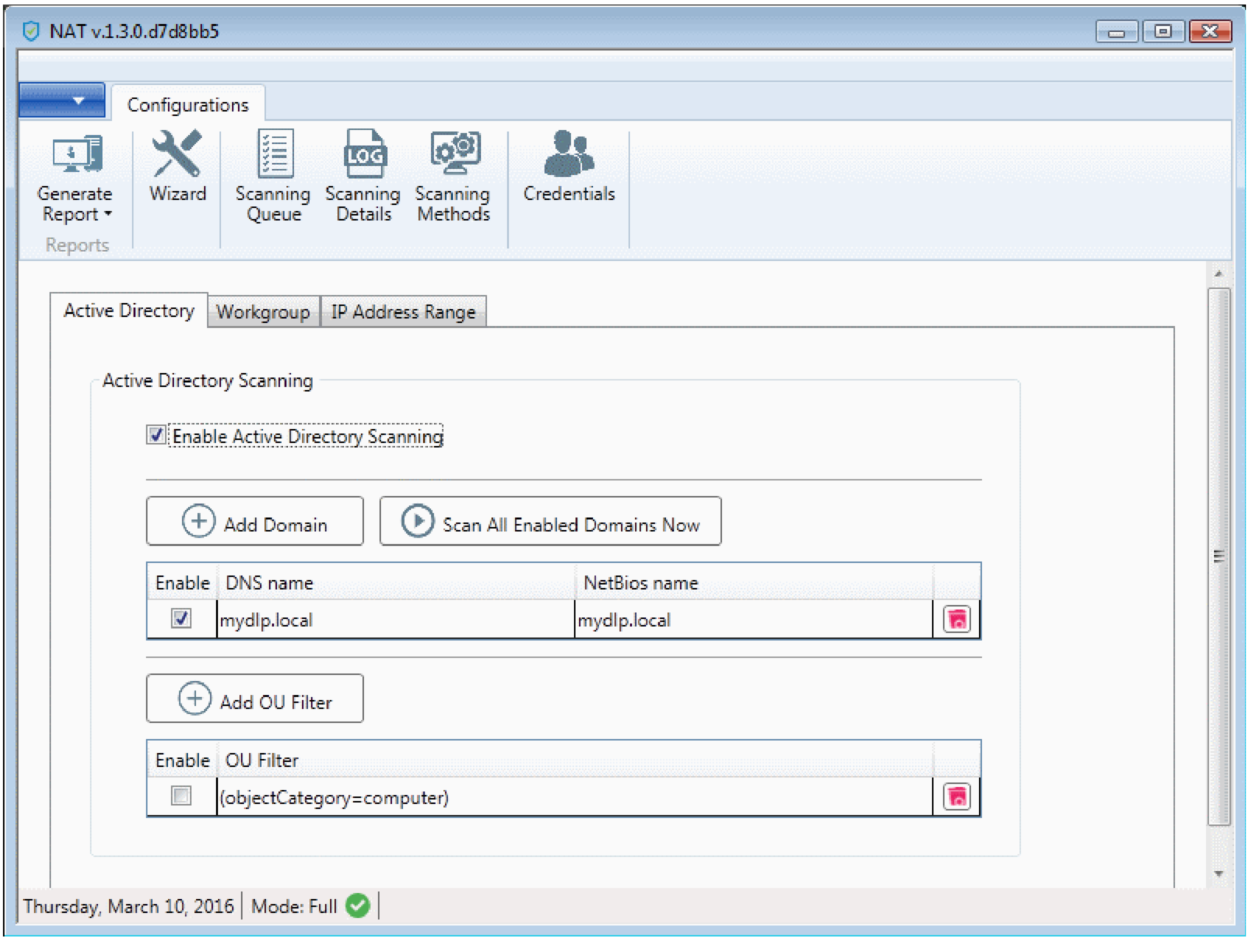
Guide Version 1.3.061218

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Network Assessment Tool

Comodo Network Assessment tool allows administrators to perform in-depth scans on client networks to identify a wide range of server, endpoint and network vulnerabilities. The tool will also prepare detailed risk reports for scanned networks along with a risk mitigation plan containing actionable advice to address each issue. Setup is easy with a simple wizard which allows users to import networks via Active Directory, Workgroup or IP range. This guide takes users 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)

Thursday, March 10, 2016 | Mode: Full ✓

Guide Structure

This guide is intended to take you through the installation, configuration and use of Comodo Network Assessment Tool and is broken down into the following main sections. The guide can be navigated using the bookmark links on the left.

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

1.1 Quick Start Guide

This tutorial briefly explains how an admin can setup Comodo Network Assessment Tool (NAT) and run assessment scans on the network.

Basic Setup:

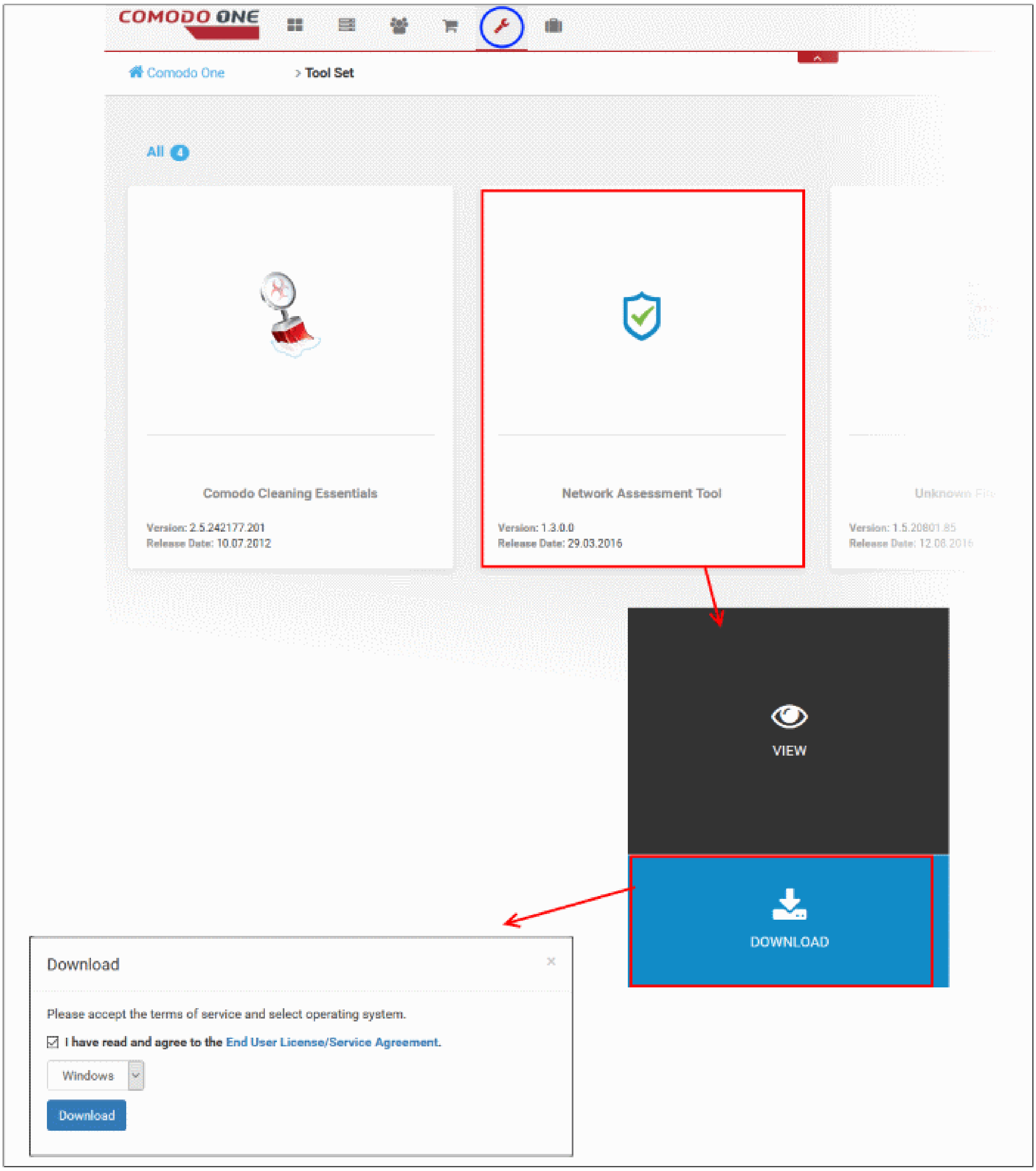
- Install the NAT tool and run the initial configuration wizard. The wizard allows you to enable scanning your domain/workgroup/IP Address Range, to which your computer is a member of and specify the administrative credentials for NAT to access the endpoints on your network.
- Add additional domains/workgroups/IP Address Ranges, accessible by your computer for scanning
- Enter login credentials with administrative privileges for the added networks and map them to respective networks

The guide will take you through the basic setup and usage of Comodo NAT. Click any link to go straight to the section you need help with.

- **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.
- Once logged-in, click 'Tool Set' at the top.
- Hover your mouse over Network Assessment Tool and click 'Download'



Download

Please accept the terms of service and select operating system.

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

Windows

Download

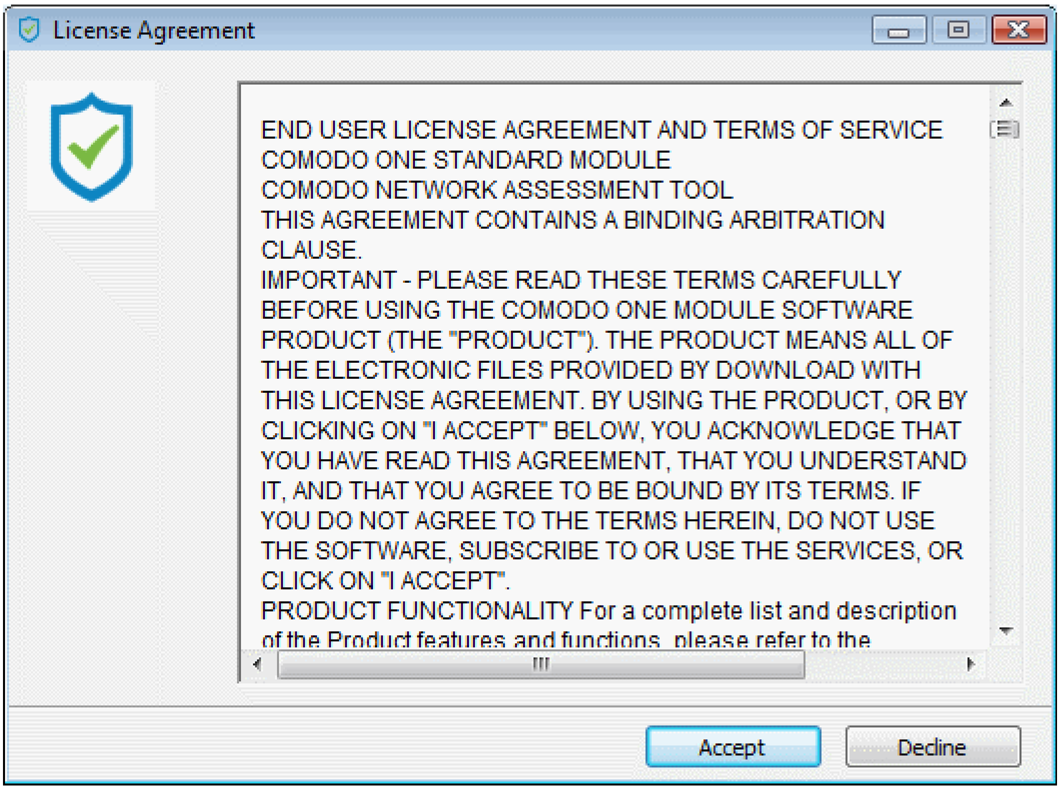
The 'Download' dialog will open.

- Click 'End User License/service Agreement', read the agreement and accept to it by selecting the EULA check box
- Click the 'Download' button to start the download of NAT setup file.

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 will allow you to download both applications if you do not have them already.

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

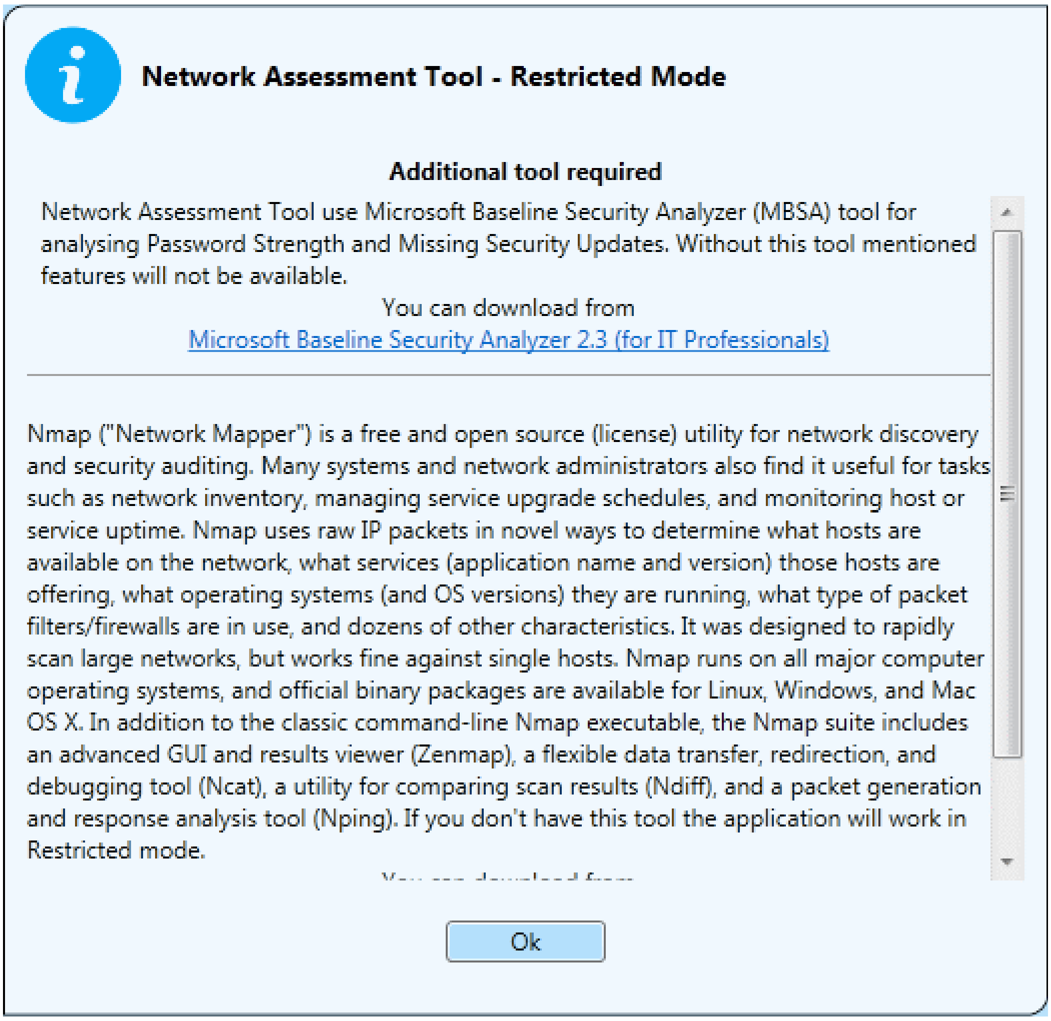


END USER LICENSE AGREEMENT AND TERMS OF SERVICE
COMODO ONE STANDARD MODULE
COMODO NETWORK ASSESSMENT TOOL
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.
IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONE MODULE SOFTWARE PRODUCT (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE 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

- 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**.
- If not available a dialog containing guidance and download links for the additional software will be displayed.



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)

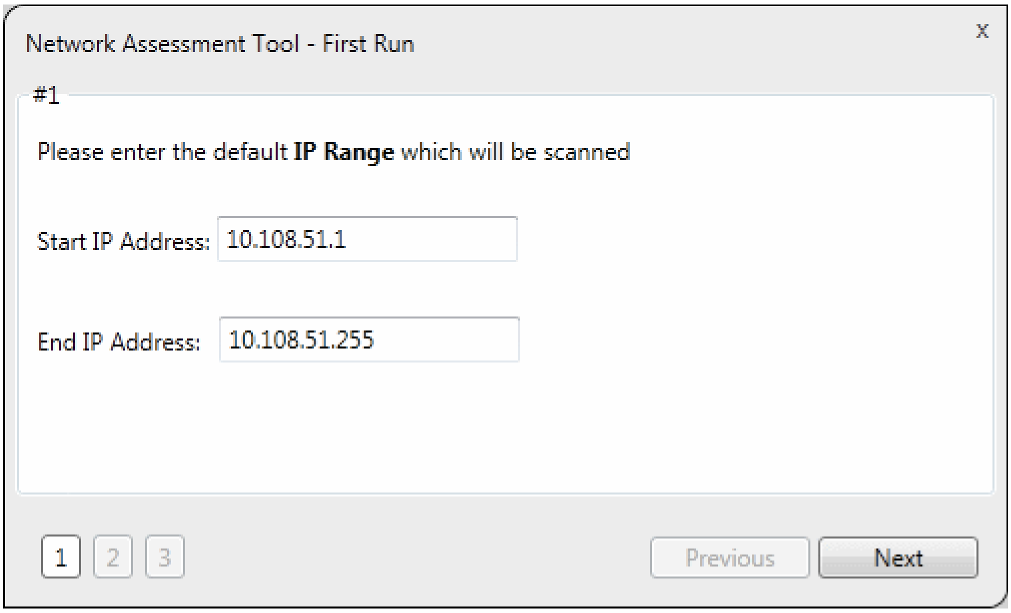
Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP 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

- You can download and install the Nmap tool and MBSA tool by clicking the respective links in the dialog.

Step 3 - Run Initial Configuration Wizard

On completion of installation and if the Nmap tool and MBSA tool are available, the initial configuration wizard will begin.



Network Assessment Tool - First Run

#1

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

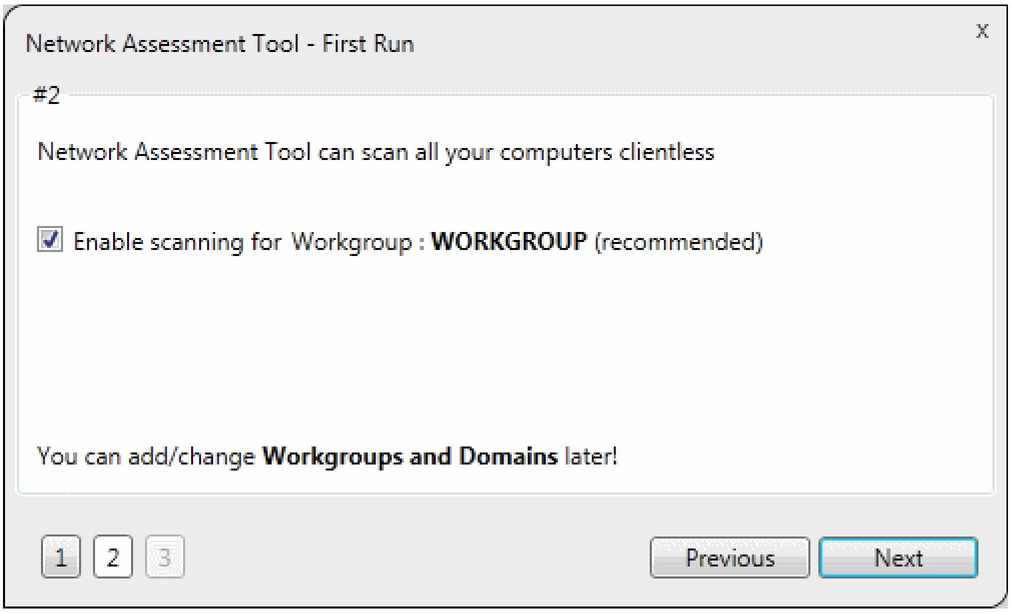
Start IP Address: 10.108.51.1

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 of your network to be scanned. Also, you can add and manage networks to be scanned to NAT. Refer to the section **Network Management** for more details.

- Click 'Next' to move to the next step.



Network Assessment Tool - First Run

#2

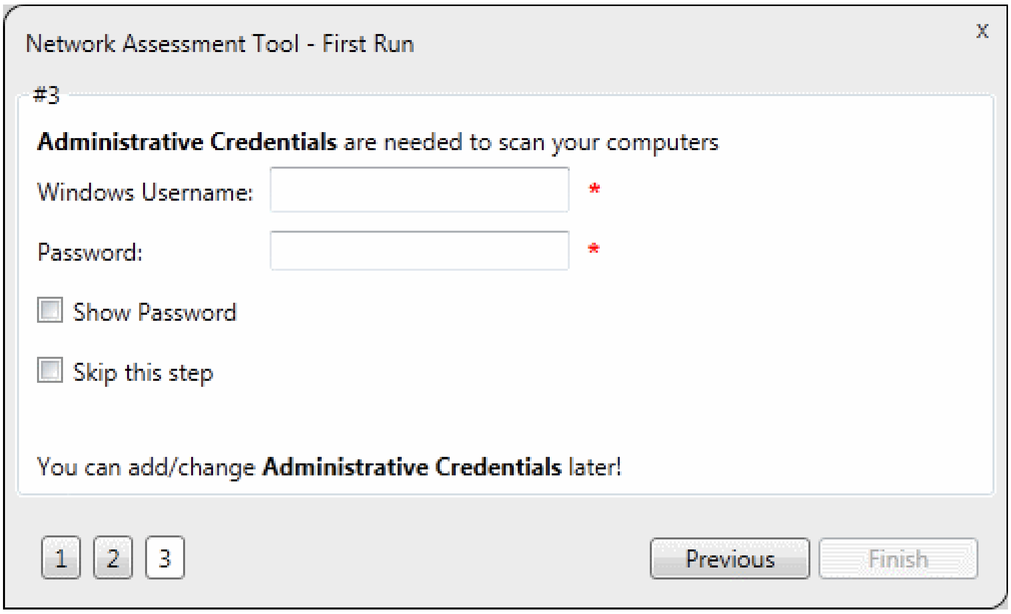
Network Assessment Tool can scan all your computers clientless

☑ 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 a member of and displays it.

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



Network Assessment Tool - First Run

#3

Administrative Credentials are needed to scan your computers

Windows Username: *

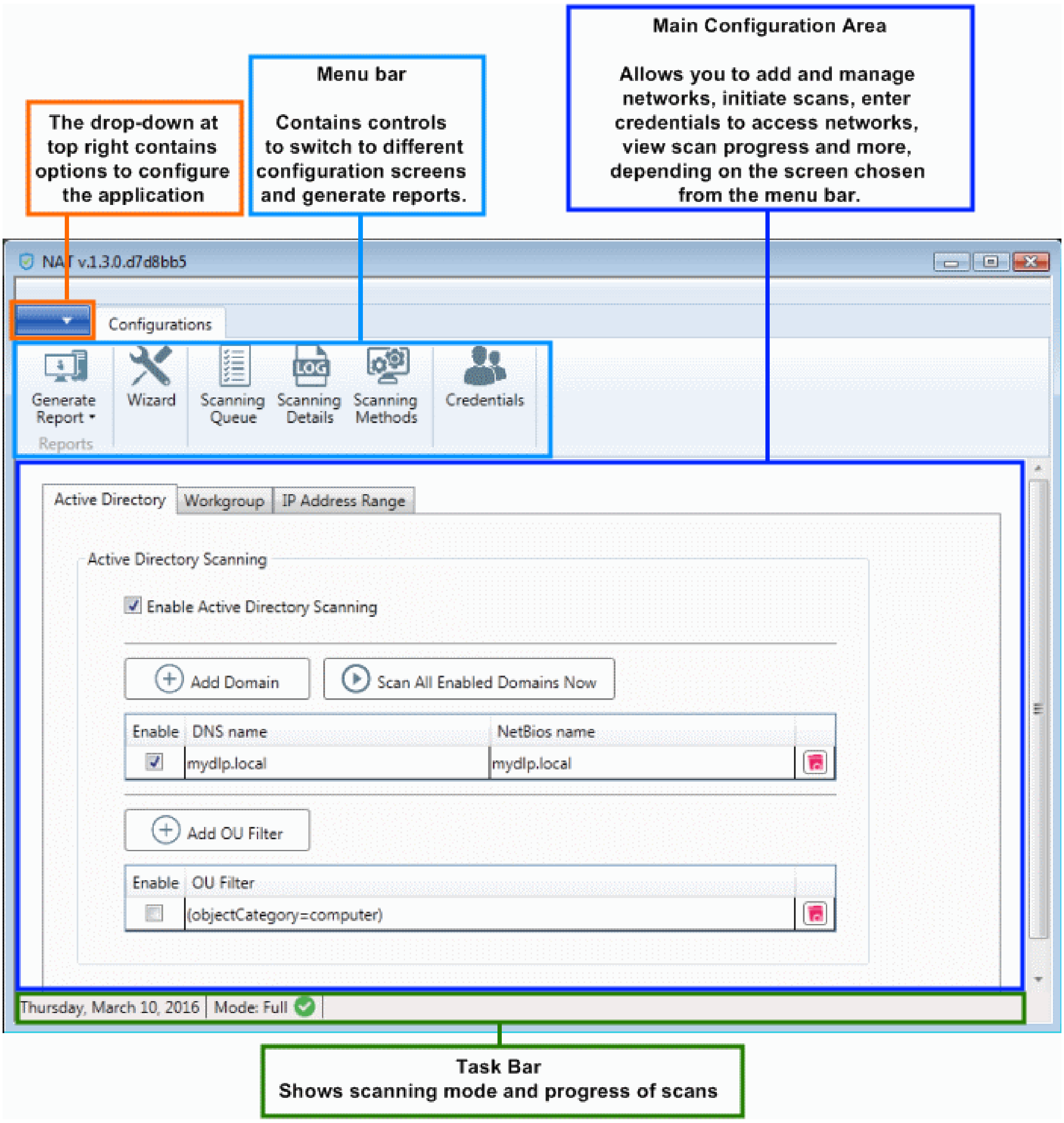
Password: *

□ Show Password

□ Skip this step

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

- Enter an username and password of the machines on the target network and click 'Finish'.
- NAT will immediately begin scanning your network and the main interface will open:


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.
NAT v.1.3.0.d7d8bb5
Configurations
Generate Report
Reports
Wizard
Scanning Queue
Scanning Details
Scanning Methods
Credentials
Active Directory
Workgroup
IP Address Range
Active Directory Scanning
☑ Enable Active Directory Scanning
Add Domain
Scan All Enabled Domains Now
Add OU Filter
Thursday, March 10, 2016
Mode: Full
Task Bar
Shows scanning mode and progress of scans

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

Enable	OU Filter
□	(objectCategory=computer)

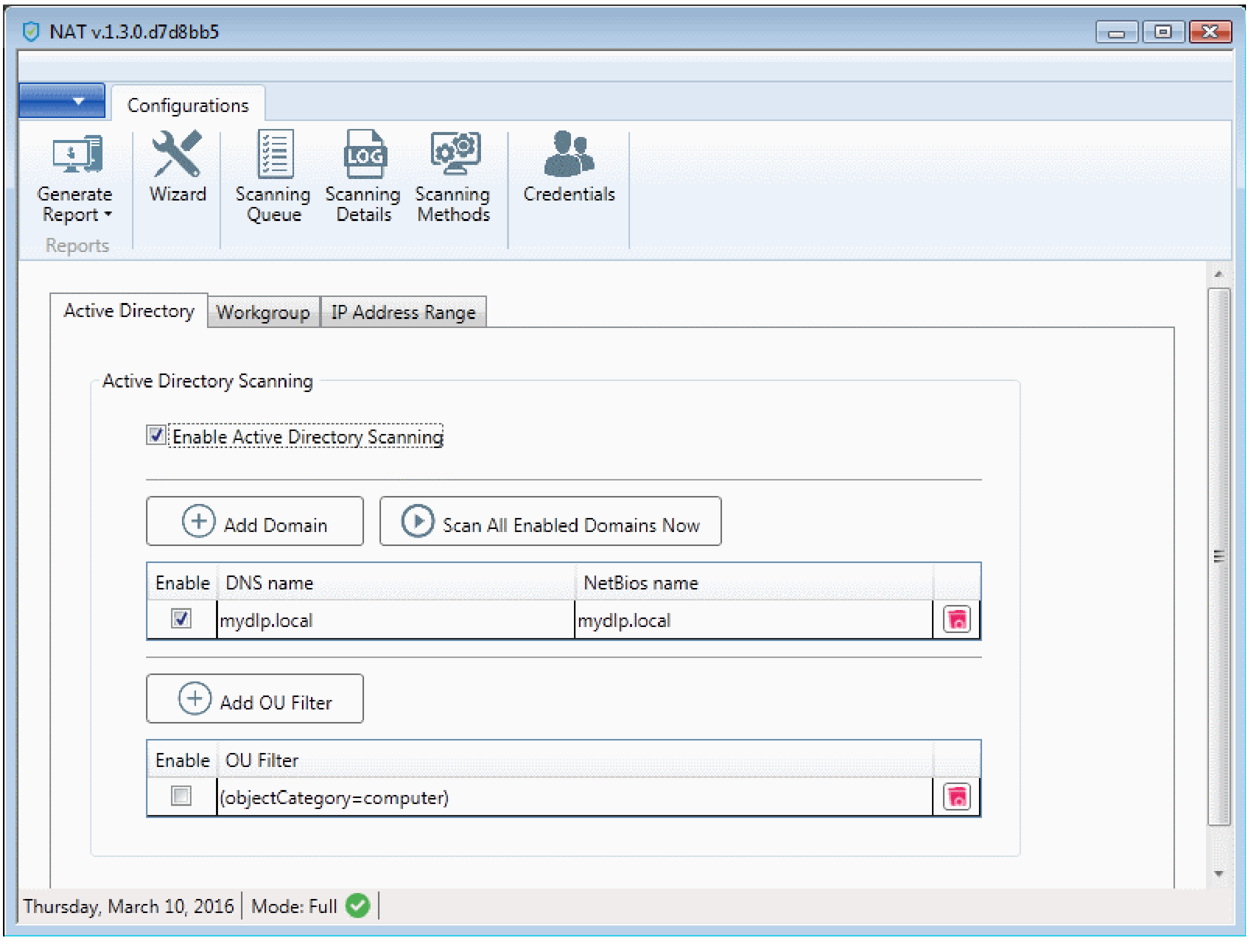
- To view scan progress, click the 'Scanning Queue' button
- To generate reports on completion of scan, click 'Generate Report'.

Step 4 - Add Networks

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

To add a network:

- Click 'Scanning Methods' from the menu bar



☑ Enable Active Directory Scanning

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

Enable	OU Filter
□	(objectCategory=computer)

- Select the any one of the tabs from 'Active Directory', 'Workgroup' and 'IP Address Range' depending on the network type you wish to add.

To add a domain

- Click the 'Active Directory' tab, ensure that the 'Enable Active Directory Scanning' check-box is selected and click 'Add Domain'

  A new row will be added to the list

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

To add a workgroup

- Click the 'Workgroup' tab, ensure that the 'Enable Workgroup Scanning' check-box is selected and click 'Add Workgroup'

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

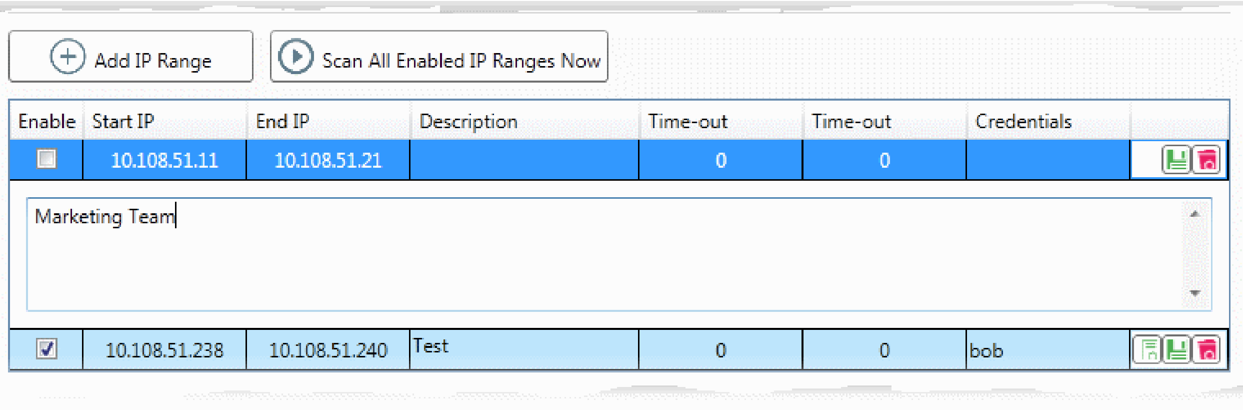
- Enter the name of the workgroup to be added.

To add an IP Address Range

- Click the 'IP Address Range' tab, ensure that the 'Enable IP Address Range Scanning' check-box is selected and click 'Add IP Range'

  A new row will be added to the list of IP Address Ranges.

- 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.
- 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.

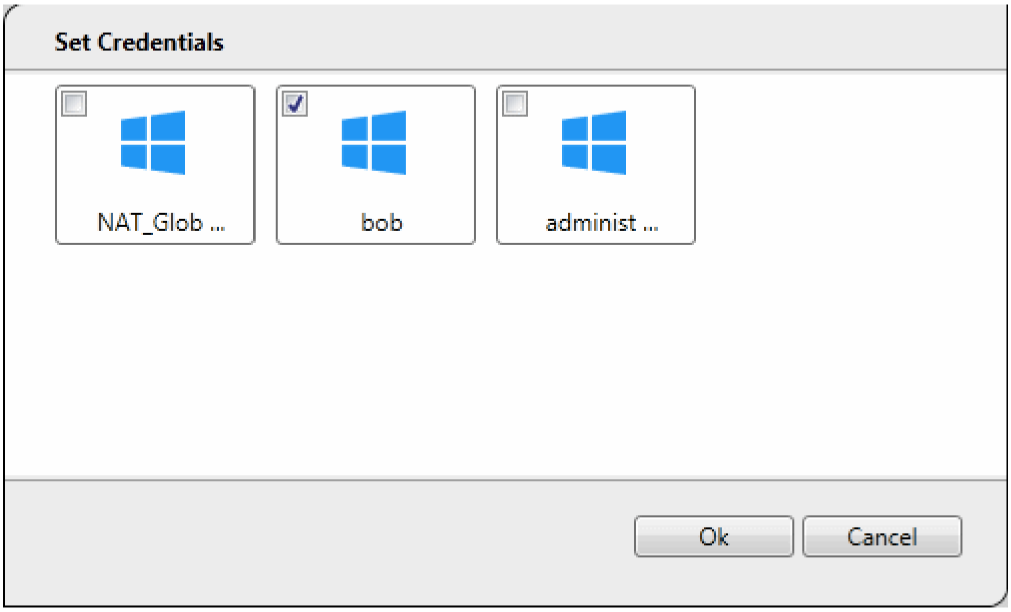


Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials
□	10.108.51.11	10.108.51.21		0	0	
Marketing Team						
☑	10.108.51.238	10.108.51.240	Test	0	0	bob

- Click the 'Save' button 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. NAT stores the credentials entered in the initial configuration wizard. You can add more credentials for different administrative accounts from the Credentials interface. Refer to **Step 5 - Add Credentials and Map to Respective Networks** for more details.

- Click the 'Add Credential' button at the right of the row and choose the credentials to be mapped to the IP address range. You can choose more than one credential, if different endpoints in the IP address range can be accessed with respective credentials.

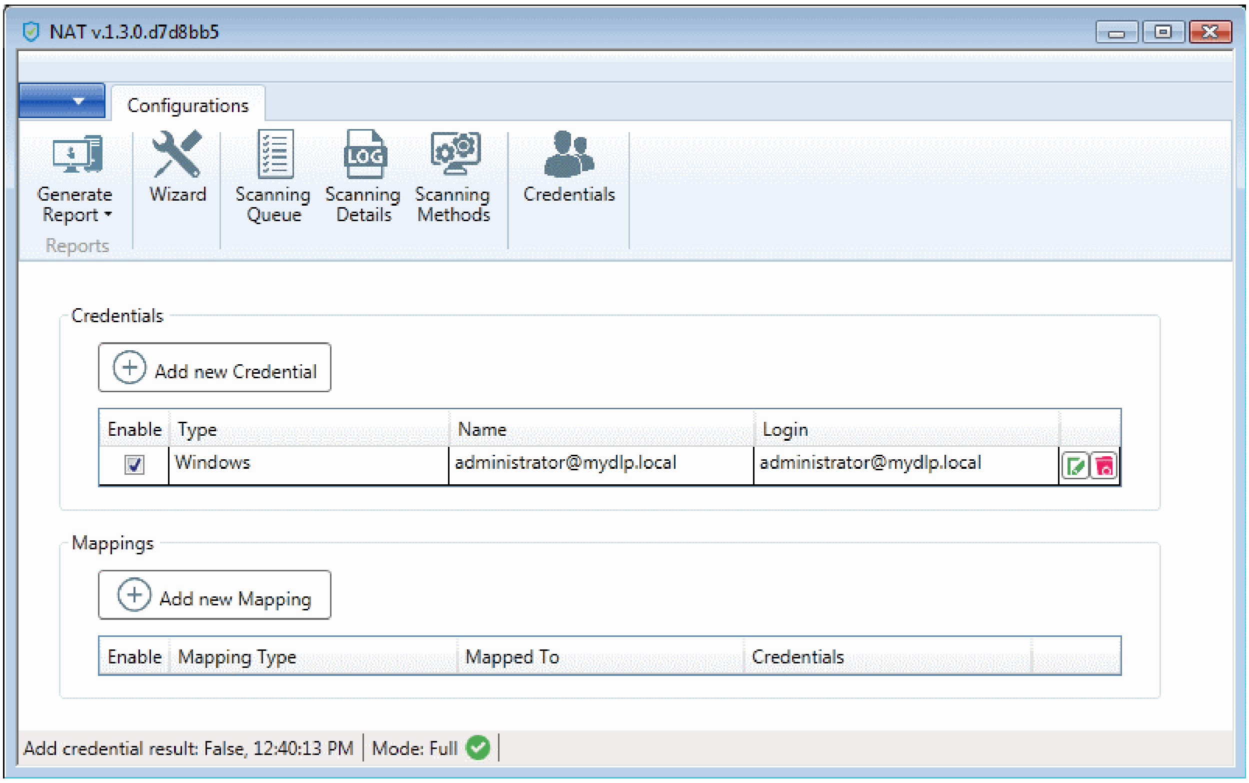

Set Credentials

□ NAT_Glob ...
☑ bob
□ administ ...

Step 5 - Add Credentials and Map to Respective Networks

The next step is to add login credentials of network administrator accounts to NAT and map them to the networks, for NAT to access the endpoints in the scanned network(s). If different endpoints in a single network require different access credentials, you can add all the credentials and map them to the single network, so that , so that NAT can access each endpoint with the respective credential.

- Click 'Credentials' from the menu bar.



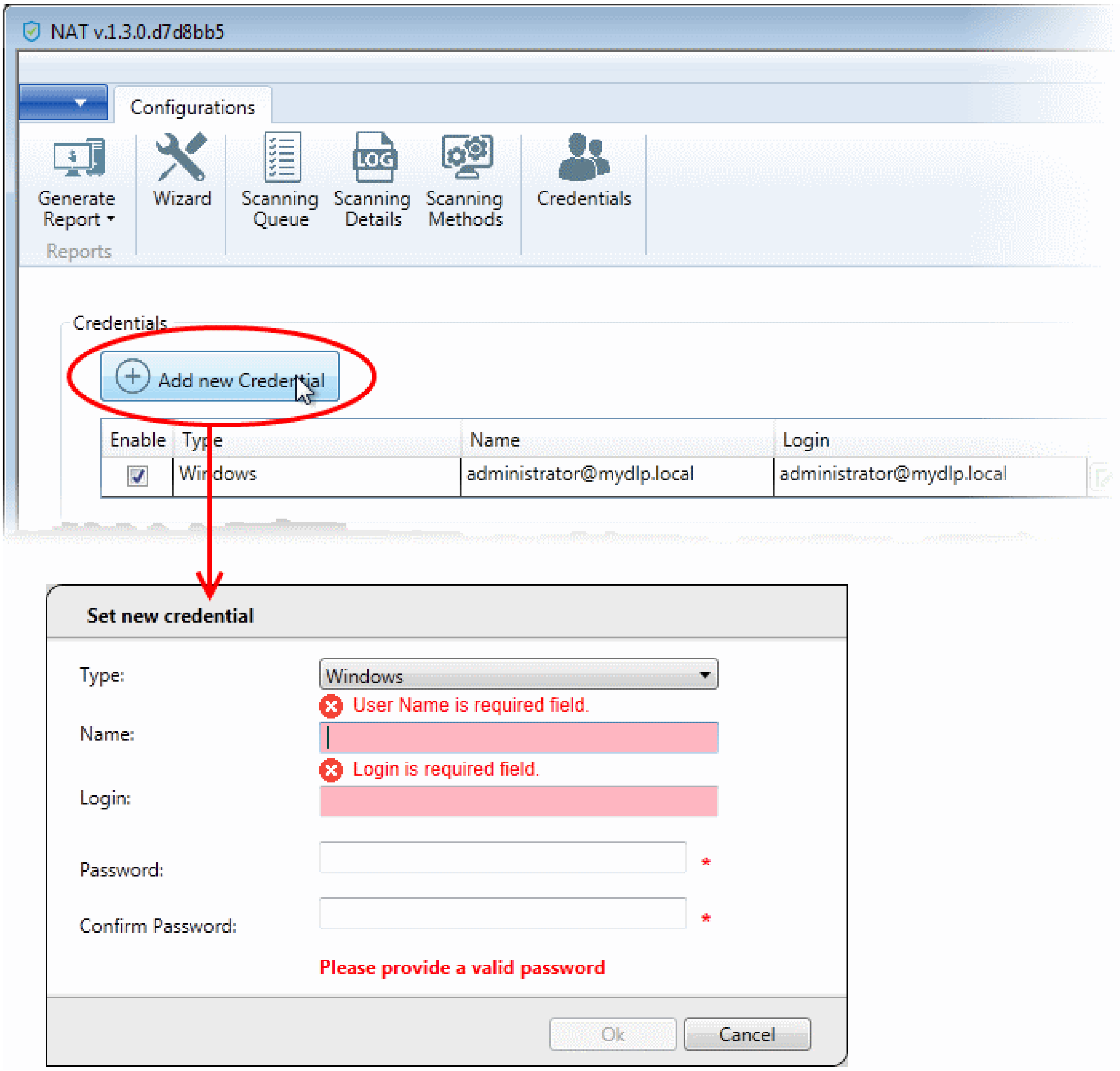
Enable	Type	Name	Login
☑	Windows	administrator@mydlp.local	administrator@mydlp.local

Enable	Mapping Type	Mapped To	Credentials

Add credential result: False, 12:40:13 PM | Mode: Full

To add a new login credential

- click 'Add new Credential'



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

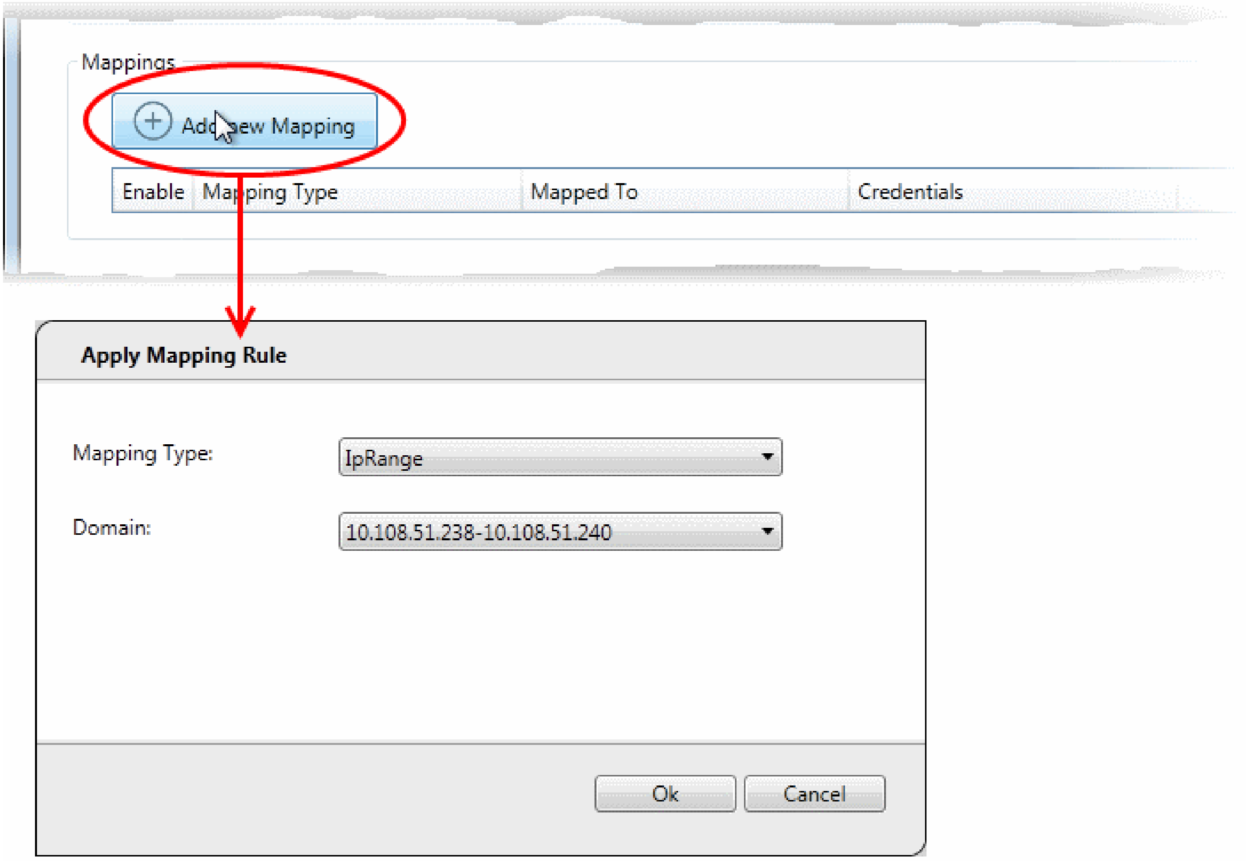
Set new credential dialog - Form parameters	
Form Element	**Description**
Type	Choose the operating system of the endpoints for which the credential is set
Name	Enter a name to identify the account, for example, the name of the administrator
Login	Enter the username of the account
Password	Enter the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

To map credentials to a network

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

The 'Apply Mapping Rule' wizard will open.



Mapping Type: IpRange

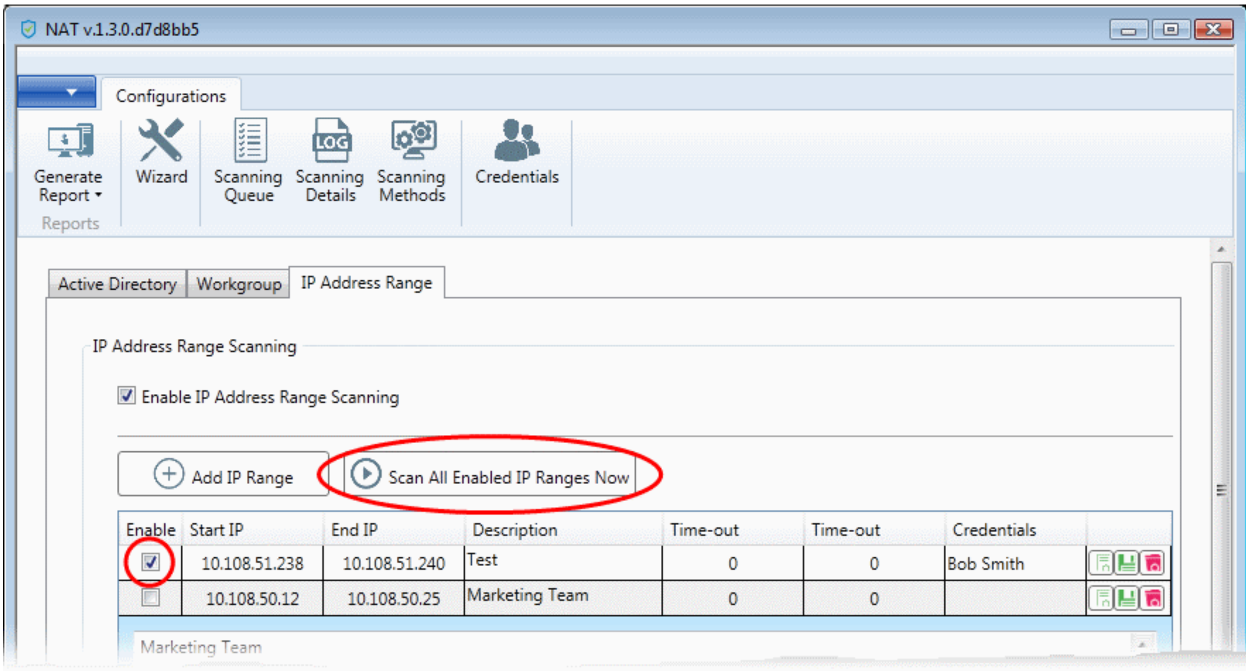
Domain: 10.108.51.238-10.108.51.240

- Mapping Type - Choose the type of the network to which the credentials are to be mapped. The available choices 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'
- Repeat the process to map the credentials to different networks as needed

Step 6 - Run a Scan

- Click 'Scanning Methods' from the menu bar
- Choose the type of network on which the scan is to be initiated, by selecting the respective tab.
  - Active Directory - To run the assessment scan on endpoints in a domain
  - Workgroup - To run the assessment scan on endpoints in a workgroup
  - IP Address Range - To run the assessment scan on endpoints that fall within the specified IP address range in the network
- Ensure that the network(s) to be scanned are enabled and those that need not be scanned are not enabled
- Click 'Scan All Enabled Domains Now', 'Scan All Enabled Workgroups Now' or 'Scan All Enabled IP Ranges Now' as appropriate to the network type chosen.



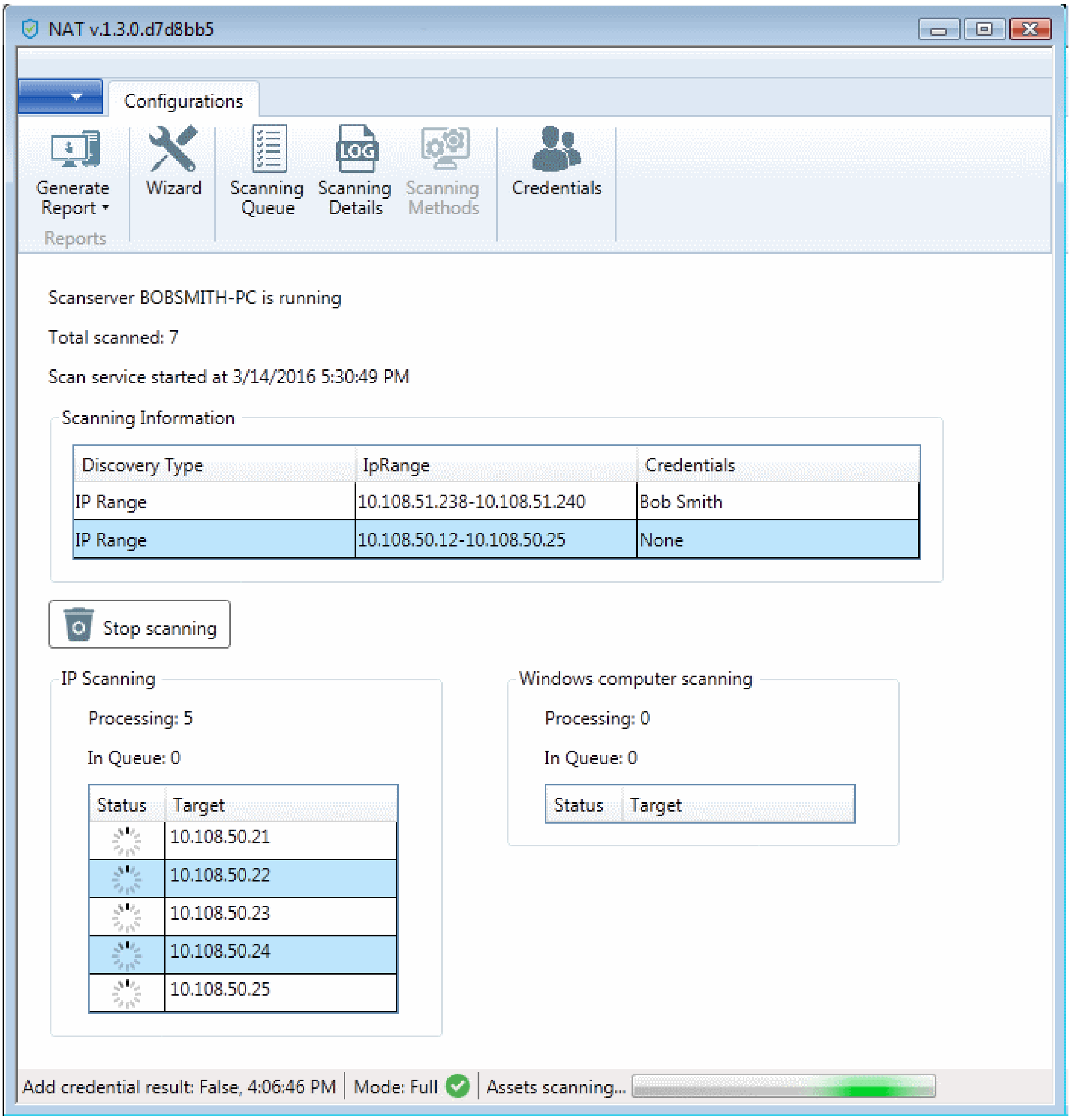
☑ Enable IP Address Range Scanning

Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials
☑	10.108.51.238	10.108.51.240	Test	0	0	Bob Smith
□	10.108.50.12	10.108.50.25	Marketing Team	0	0	

Marketing Team

The scan will be started. You can view the progress of the scan from the 'Scanning Queue' interface.

- Click 'Scanning Queue' from the menu bar



Scanserver BOBSMITH-PC is running

Total scanned: 7

Scan service started at 3/14/2016 5:30:49 PM

Scanning Information

Discovery Type	IpRange	Credentials
IP Range	10.108.51.238-10.108.51.240	Bob Smith
IP Range	10.108.50.12-10.108.50.25	None

IP Scanning

Processing: 5

In Queue: 0

Status	Target
	10.108.50.21
	10.108.50.22
	10.108.50.23
	10.108.50.24
	10.108.50.25

Windows computer scanning

Processing: 0

In Queue: 0

Status	Target

Add credential result: False, 4:06:46 PM | Mode: Full ✓ | Assets scanning...

- **Scanning Information** - Displays details about currently running scans on domain(s), Workgroup(s) and IP Address Range(s).
- **IP Scanning** - Displays the list of IP addresses discovered on the currently scanned network using Network Mapper (Nmap).
- **Windows Computer Scanning** - Displays a list of hostnames/IP addresses being scanned using Windows Management Instrumentation(WMI) and Microsoft Baseline Security Analyzer (MBSA)

- To terminate the scan, click 'Stop Scanning'.

The successful completion of scanning will be indicated.

Step 7 - Generate Reports

You can generate assessment reports after the completion of each scan.

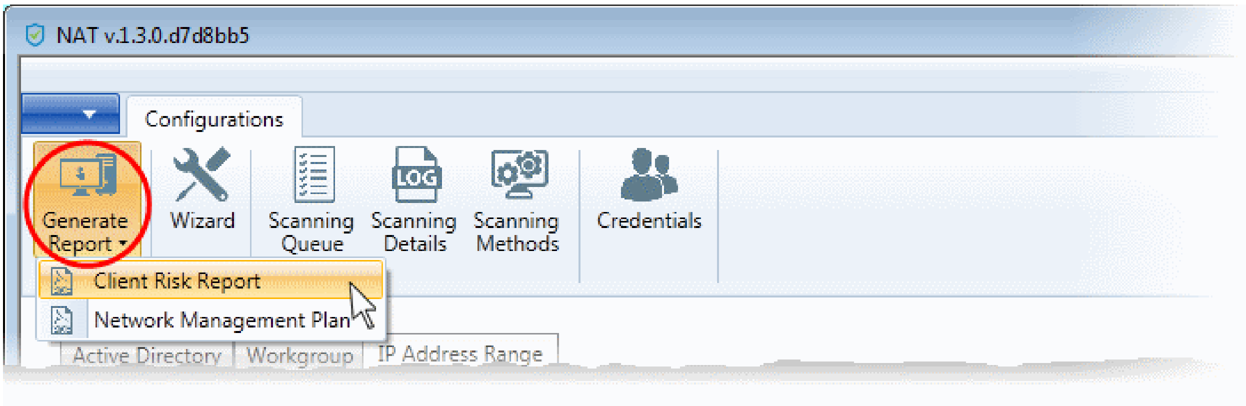
NAT can generate two types of reports:

- Client Risk Report - Contains details on discovery scans performed on the network, details on network assets, issues identified, storage status on the discovered endpoints and more.

- Network Management Plan - Contains remediation advice for items listed in the risk report.

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.

1.2 System Requirements

The list below shows supported operating systems and hardware requirements for computer on which NAT is to be installed.

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

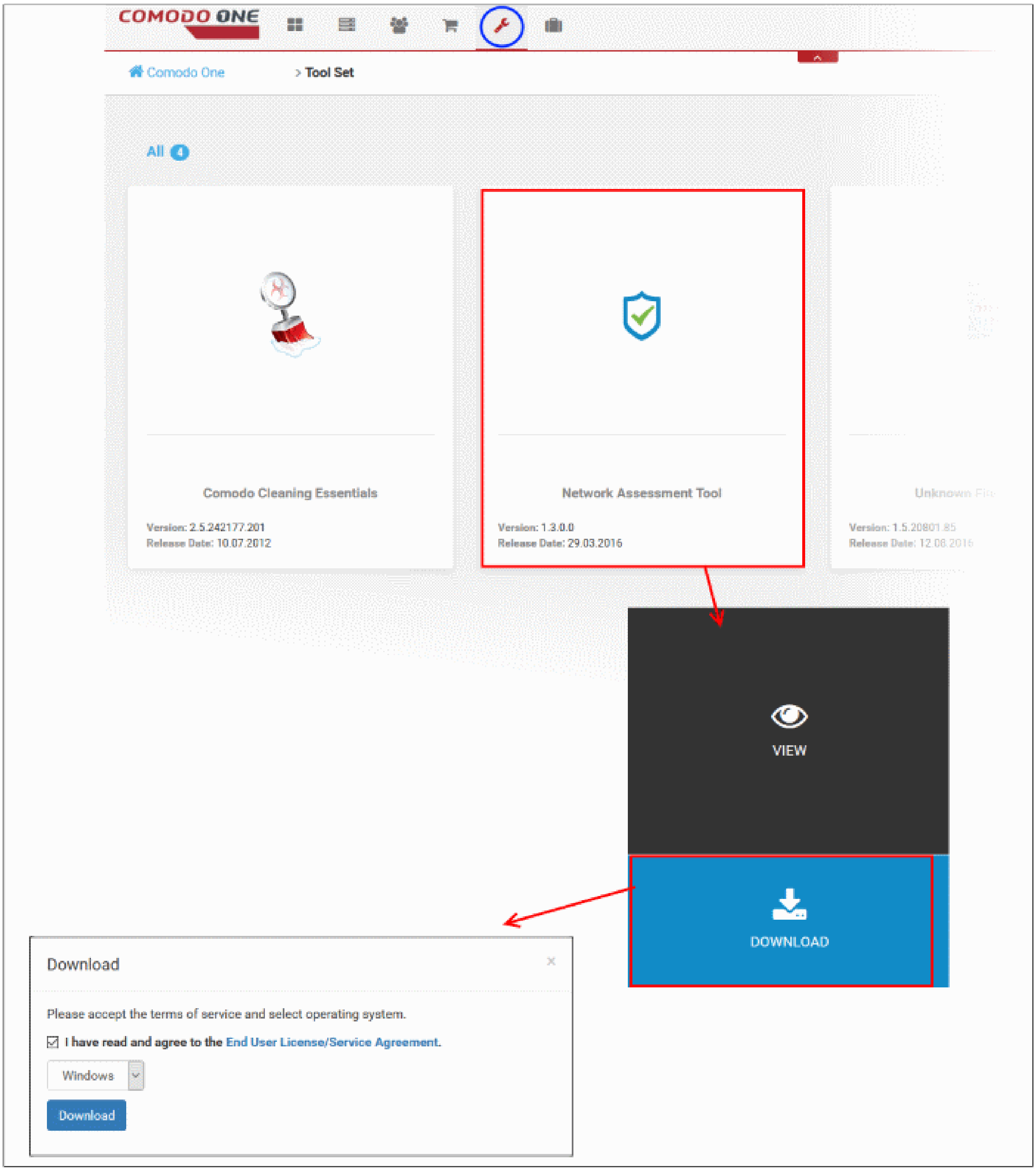
- Processor - Single core 1 GHz or better

1.3 Downloading and Installing Network Assessment Tool

Comodo Network Assessment Tool (NAT) can be downloaded from the 'Tools Set' interface of Comodo One console.

To download the NAT setup

- Login to your Comodo One account at https://one.comodo.com/app/login.
- Once logged-in, click 'Tool Set' at the top.
- Hover your mouse over Network Assessment Tool and click 'Download'



Comodo Cleaning Essentials
Version: 2.5.242177.201
Release Date: 10.07.2012

Network Assessment Tool
Version: 1.3.0.0
Release Date: 29.03.2016

Unknown File
Version: 1.5.20801.85
Release Date: 12.08.2016

Download ×

Please accept the terms of service and select operating system.

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

Windows

Download

The 'Download' dialog will open.

- Click 'End User License/service Agreement', read the agreement and accept to it by selecting the EULA check box
- Click the 'Download' button to start the download of NAT setup file.

After downloading the NAT setup file, the next step is to install it in your system. The installation wizard guides you through the installation and on successful installation, the configuration wizard will continue for initial configuration of the network to be scanned and the credentials to be used to access the network endpoints.

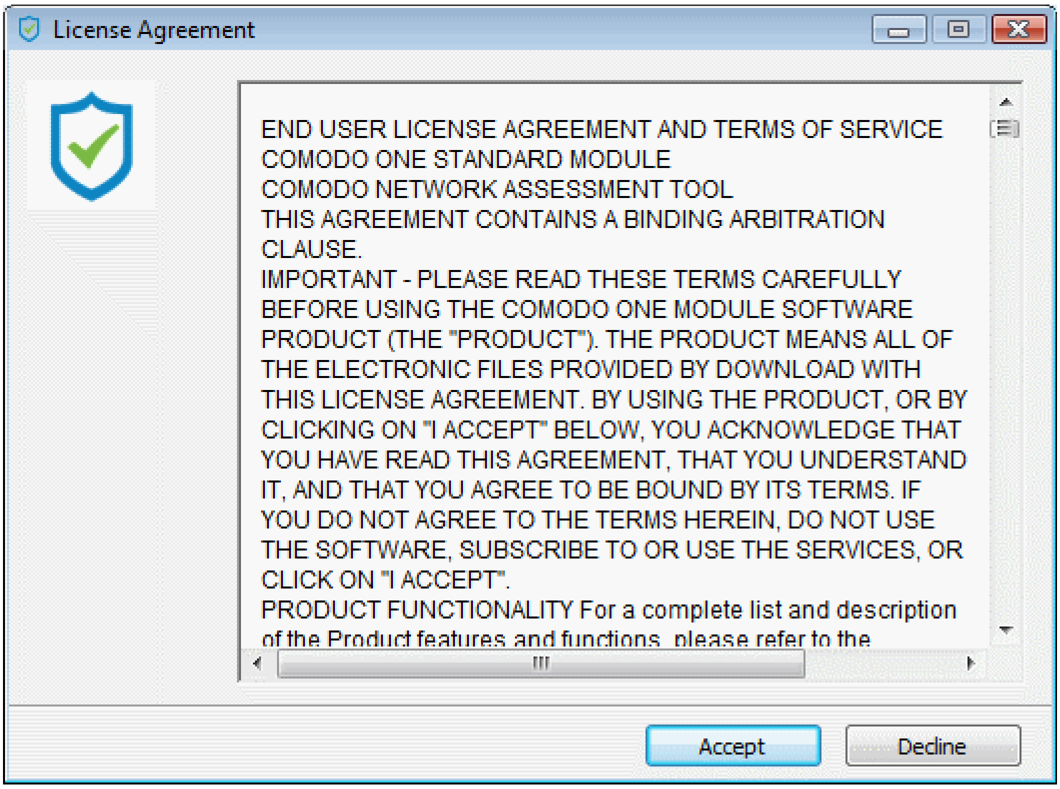
Tip: You can skip the initial configuration wizard if you do not want to do it at this stage and can start the configuration wizard at a any time, by clicking 'Wizard' from the menu bar. Refer to the section **Configuration Wizard** for more details.

Prerequisite - NAT requires Network Mapper (NMAP) and Microsoft Baseline Security Analyzer (MBSA) installed on the same machine on which it is installed. If not installed, the installation wizard will guide you on downloading and installing those applications.

- To start the installation wizard, double click on the setup file

Step 1: End User License Agreement

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

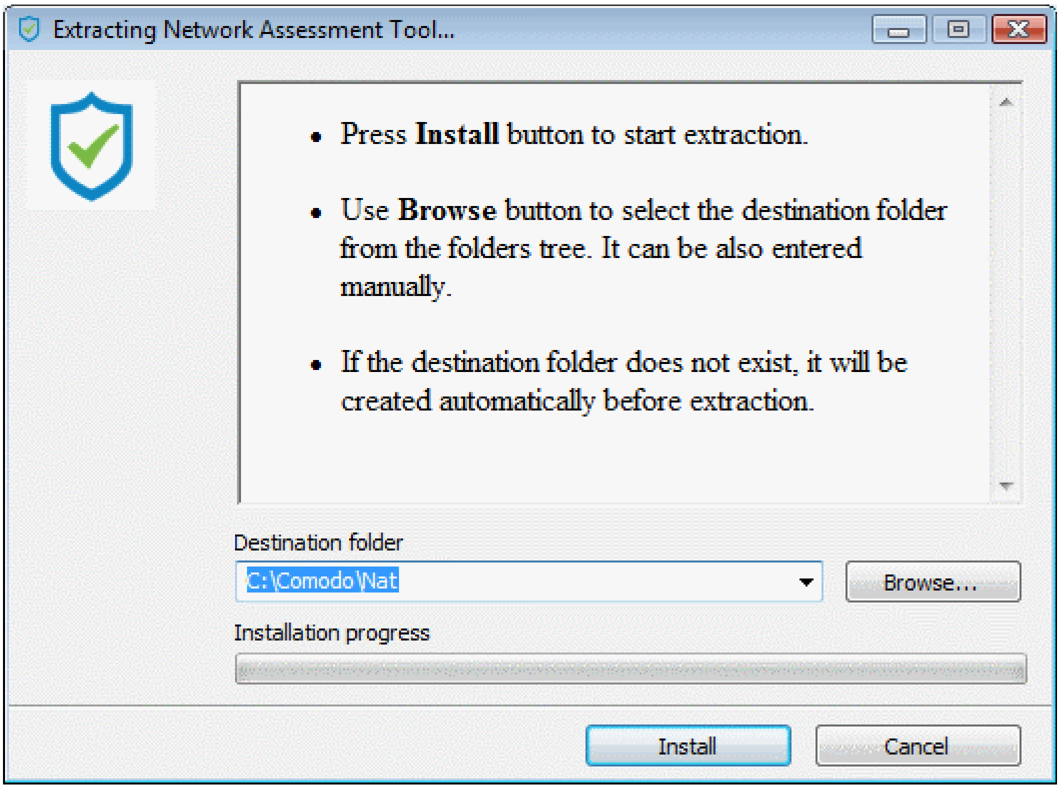


END USER LICENSE AGREEMENT AND TERMS OF SERVICE
COMODO ONE STANDARD MODULE
COMODO NETWORK ASSESSMENT TOOL
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.
IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE COMODO ONE MODULE SOFTWARE PRODUCT (THE "PRODUCT"). THE PRODUCT MEANS ALL OF THE 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

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

Step 2: Select Installation Folder and Start Installation

The next screen allows you to select the destination folder in your hard drive for installing NAT.



Extracting Network Assessment Tool...

- Press **Install** button to start extraction.
- Use **Browse** button to select the destination folder from the folders tree. It can be also entered manually.
- If the destination folder does not exist, it will be created automatically before extraction.

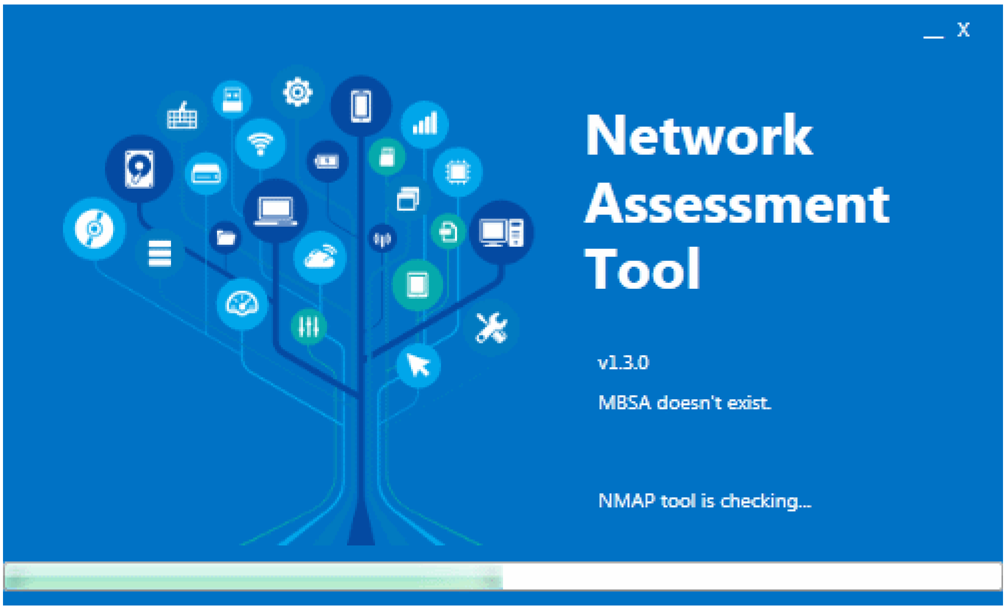
Destination folder: C:\Comodo\Nat

Installation progress

- By default the NAT is installed at C:\Comodo\Nat. If you want to install the application in a location other than the default, click 'Browse' to choose a different location.
- Click 'Install' to start the installation

Step 3: Setup Progress

Installation will begin and the progress will be displayed.



Network Assessment Tool

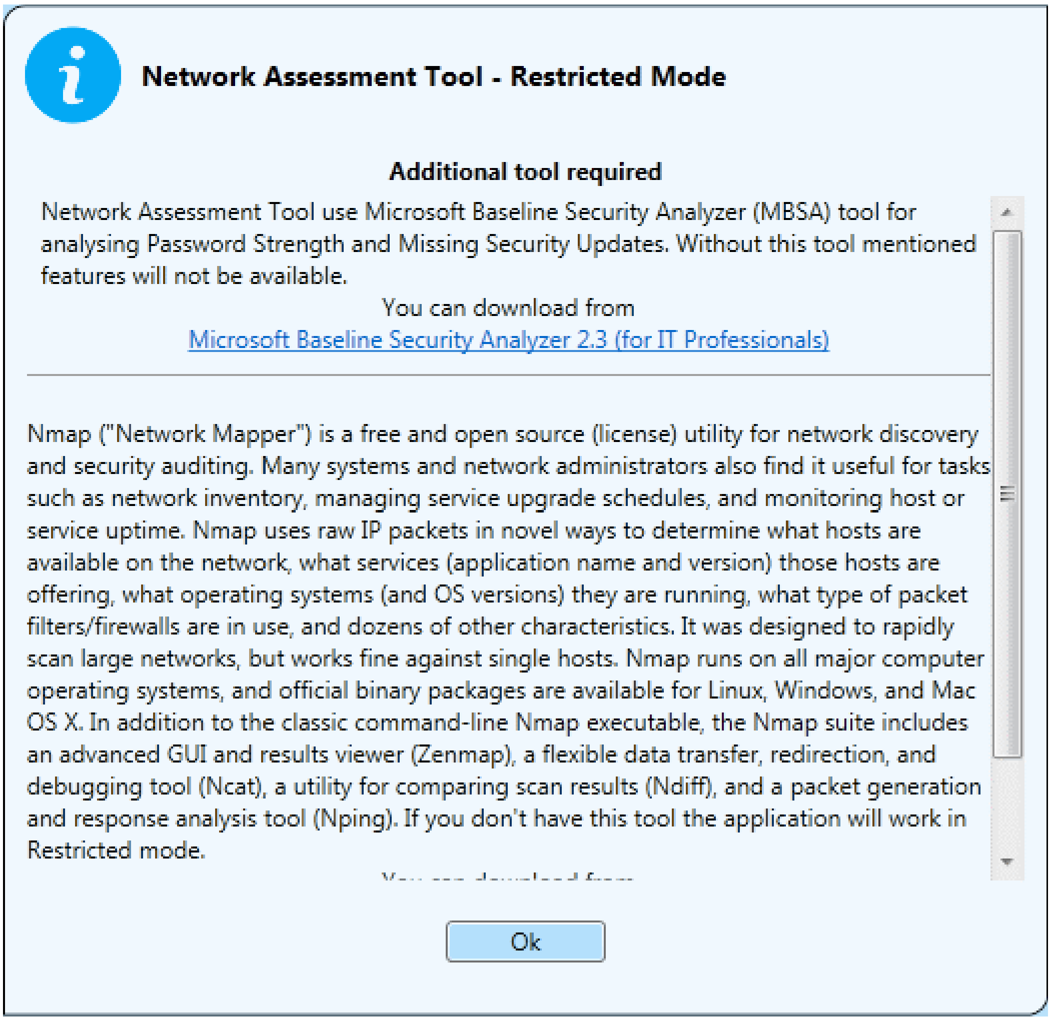
v1.3.0

MBSA doesn't exist.

NMAP tool is checking...

During the progress, 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**.
- If not available, the following dialog will be displayed. The dialog contains guidance on downloading and installing the additional software.



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.

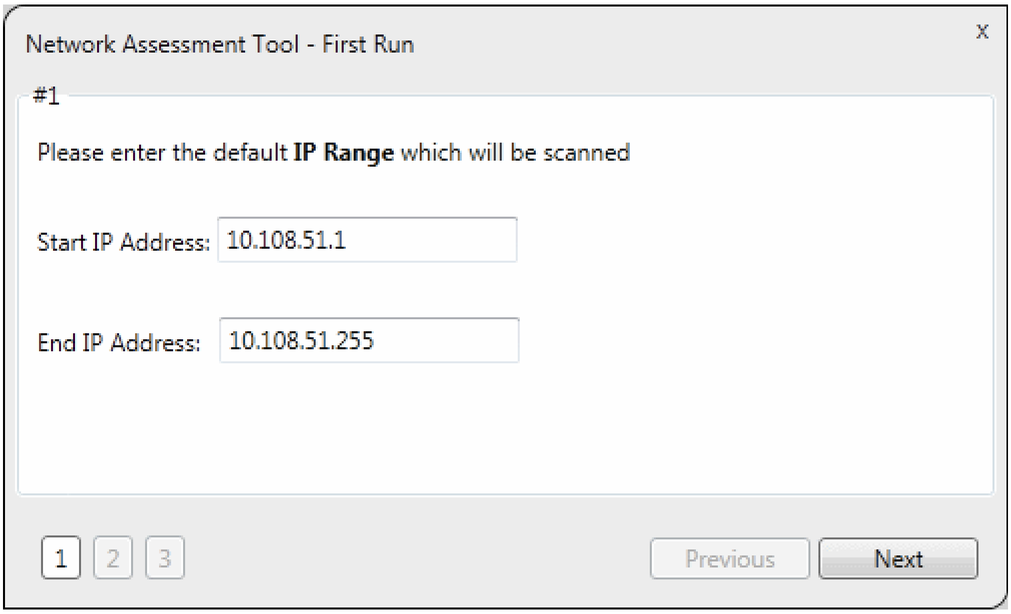
You can download from

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 the setup files for MBSA and Nmap by clicking the links in the dialog and install them in your machine. Once installed, click Ok to continue the installation.
- On completion, the initial configuration wizard will begin.

Initial Configuration wizard



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 continue the wizard by clicking Next or choose to skip the wizard by closing the dialog. You can start the wizard at any time by clicking 'Wizard' from the menu bar.

Refer to the next section **Configuration Wizard** for more details on the wizard.

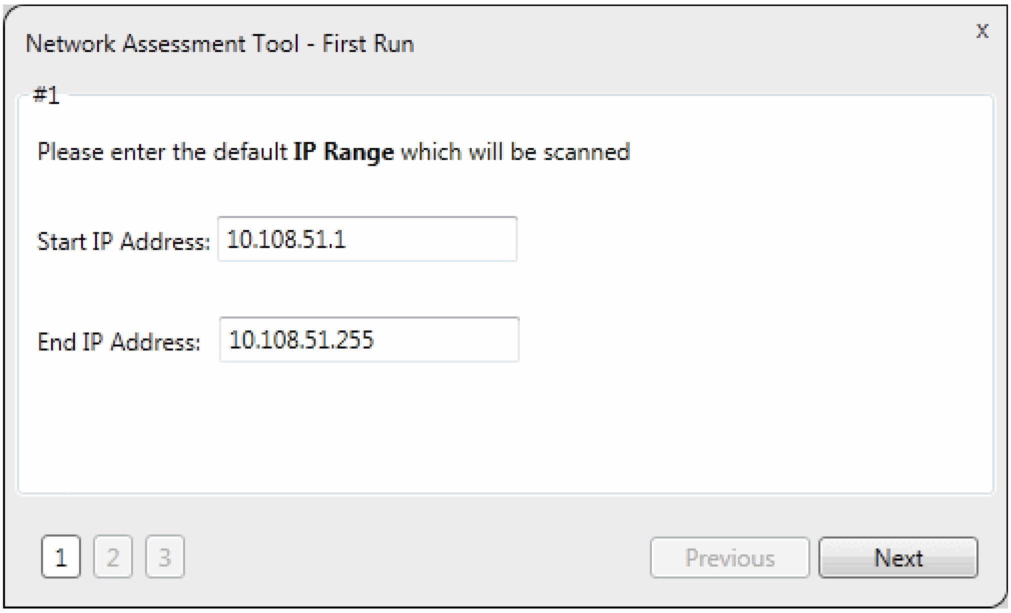
1.4 Configuration Wizard

The First Run configuration wizard allows you to configure the network to be scanned, credentials with administrative privileges to access the endpoints in the network and basic configuration parameters.

The wizard is automatically started on completion of installation. If you have chosen to skip the wizard during installation or you wish to reconfigure the initial configuration, you can start the wizard at any time by clicking 'Wizard' from the menu bar.

Step 1 - Entering 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

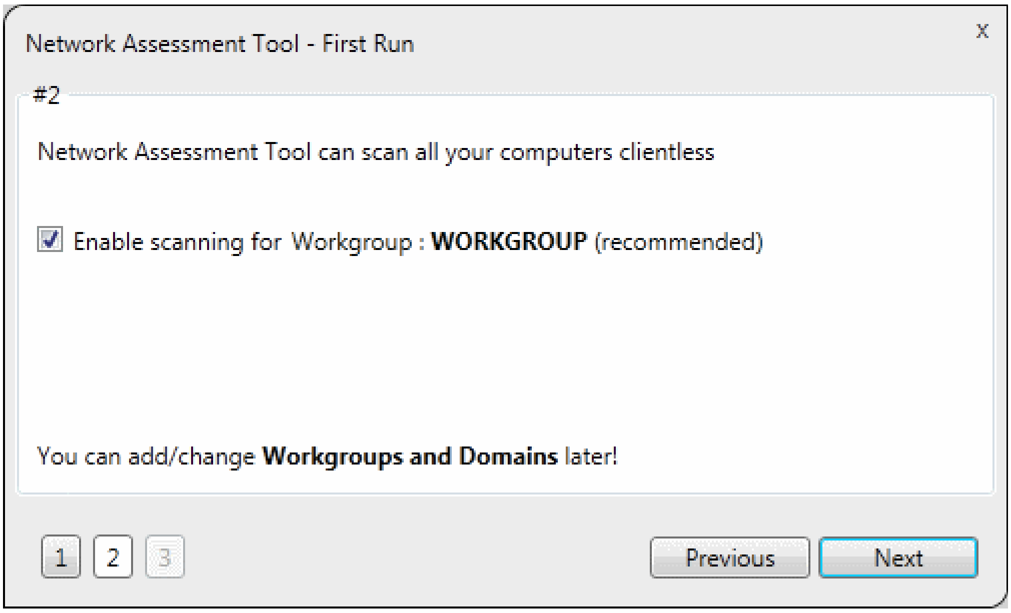
Start IP Address: 10.108.51.1

End IP Address: 10.108.51.255

If required, you can change the Start and End IP Addresses of your network to be scanned. Also, you can add and manage networks to be scanned to NAT. Refer to the section **Network Management** for more details.

Step 2 - Enabling Domain/Workgroup Scanning

The next step allows you to enable scanning your workgroup and domain. NAT automatically identifies the workgroup or domain to which your computer is a member of and displays it.



Network Assessment Tool - First Run

#2

Network Assessment Tool can scan all your computers clientless

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

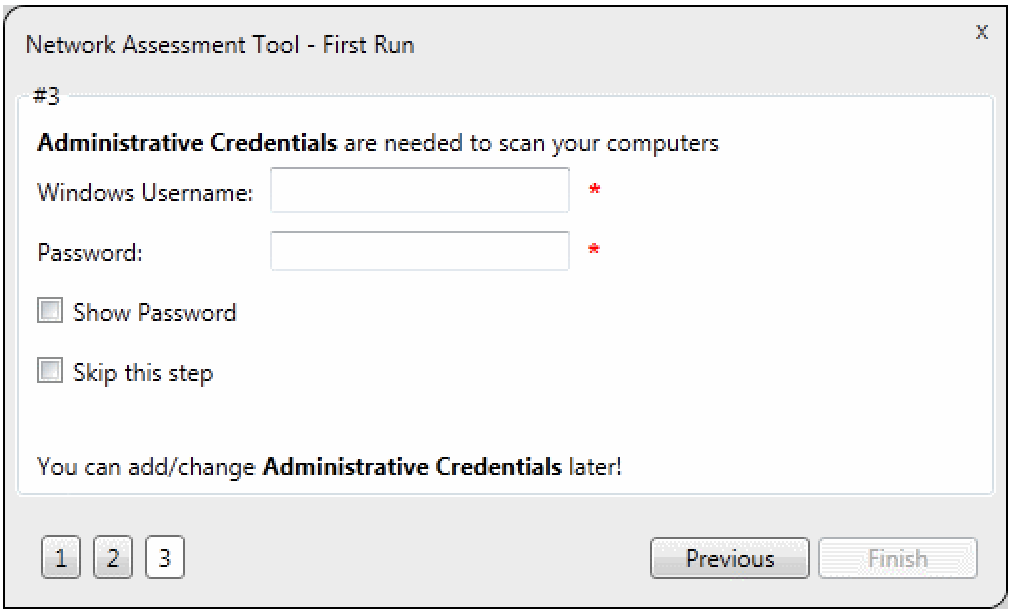
You can add/change **Workgroups and Domains** later!

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

Tip: You can enable domain/workgroup scanning at a later time too. Refer to the section **Network Management** for more details.

Step 3 - Administrative 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

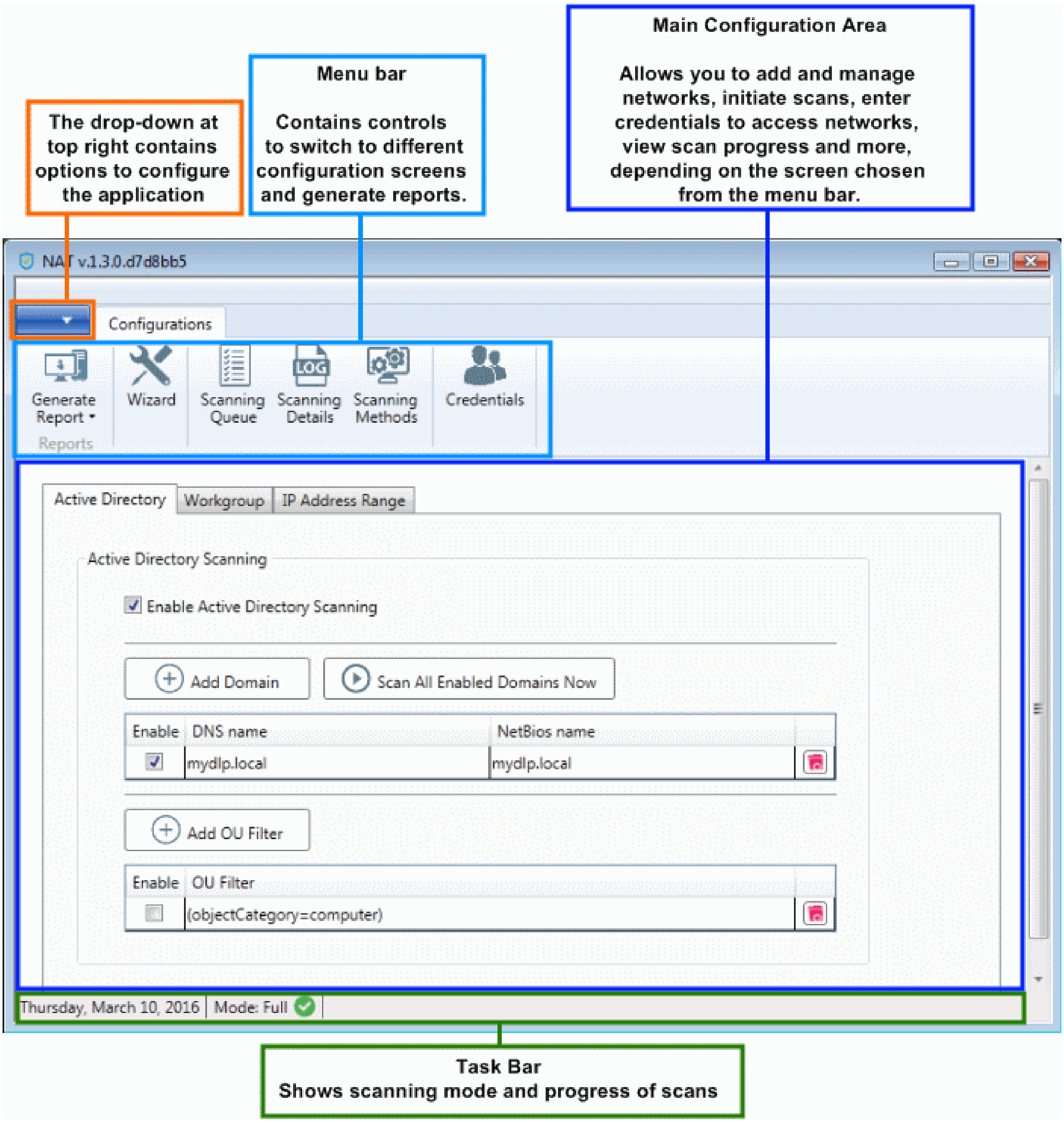
You can add/change **Administrative Credentials** later!

- Enter the username and password of the network administrator in the respective fields and click 'Finish'.
- If you want to provide the administrative credentials at a later time, select 'Skip this step' and click Finish. You can enter the credential and map it to your network through the 'Credentials' interface. Refer to the section **Credentials Management** for more details.

The **NAT Administrative Console** will open.

1.5 The NAT Administrative Console

The Administrative Console is the nerve center of Comodo Network Assessment Tool (NAT), allowing administrators to add network endpoints, initiate scans, generate reports and more. NAT scans each endpoint in the network and generates reports on vulnerabilities and a management plan to address identified issues.



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.

Task Bar

Shows scanning mode and progress of scans

☑ Enable Active Directory Scanning

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

Enable	OU Filter
□	(objectCategory=computer)

Thursday, March 10, 2016 | Mode: Full

The console consists of the following main areas that can be selected from the menu bar - 'Generate Reports', 'Wizard', 'Scanning Queue', 'Scanning Details', 'Scanning Methods' and 'Credentials'.

Main Functional Areas

- **Generate Reports** - Allows you to download Client Risk Reports and Network Management plans for the last scan.
- **Wizard** - Allows you to complete initial configuration of the NAT tool. 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** - Displays the progress of currently running scans and allows you to terminate unwanted

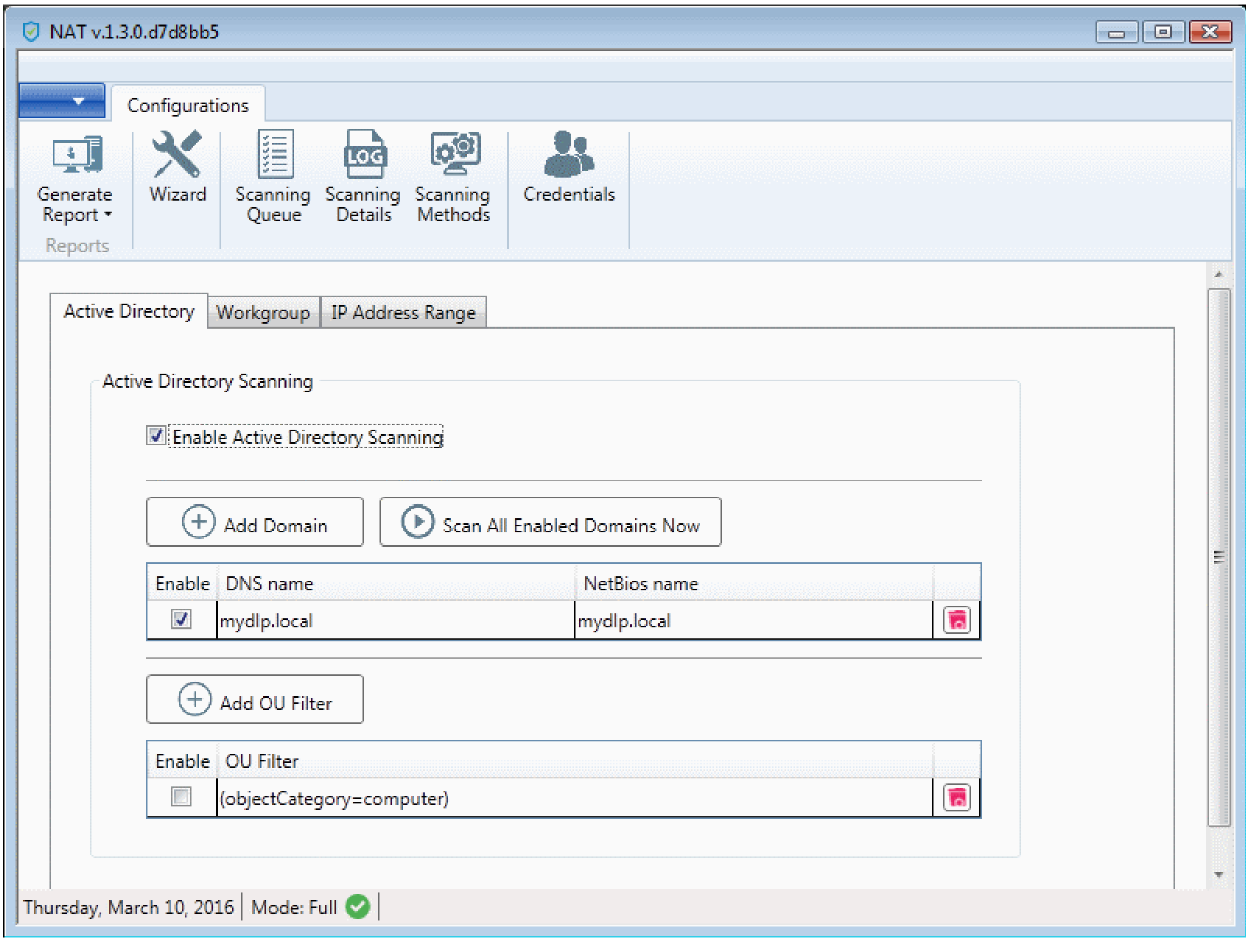
scans.

- **Scanning Details** - Displays a log of the currently running and last run scans
- **Scanning Methods** - Allows you to add and manage domains, workgroups and IP ranges to be scanned and initiate scans on selected network resources
- **Credentials** - Allows you to enter login credentials to be used by the NAT tool to access network resources

2 Network Management

In order to run network assessment scans, you need to specify target networks and enter administrator login credentials for those networks.

The 'Scanning Methods' interface allows you add target networks via Active Directory, Workgroup and IP range. The 'Credentials' interface allows you enter administrative account credentials and to map them to respective network(s).



☑ Enable Active Directory Scanning

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

Enable	OU Filter
□	(objectCategory=computer)

Refer to the following sections for more details:

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

2.1 Adding Networks to be Scanned

Networks can be added using any of the following methods:

- **Domains** - Active Directory domains can be added by specifying their DNS name and NetBios name. Refer to **Adding Domains** for more details.

- **Workgroups** - Workgroup can be added by specifying the Workgroup name. Refer to **Adding a Workgroup** for more details.
- **IP Address Range(s)** - Endpoints to be scanned can be specified by defining the IP range. Refer to **Adding IP Address Range** for more details.

Adding Domains

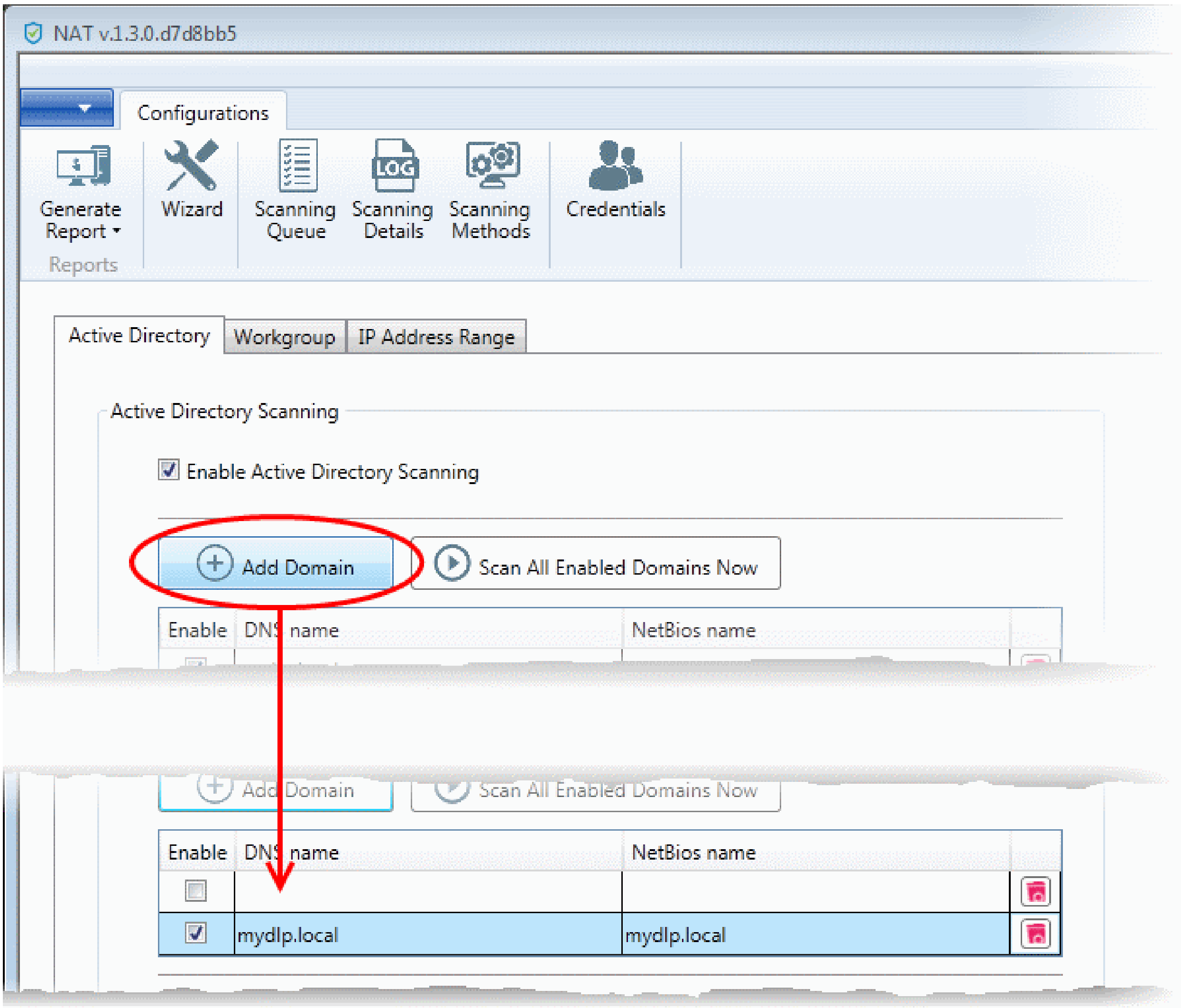
In order to scan the endpoints in an Active Directory domain, Active Directory scanning has to be configured in NAT. You can add an AD domain by specifying its DNS domain name and NetBios name. If you want to scan only selected endpoints in the domain, you can add Organization Unit (OU) filters. The login credentials for the AD server are to be added in the 'Credentials' interface and mapped to the domain to enable NAT to scan. 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

- 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.

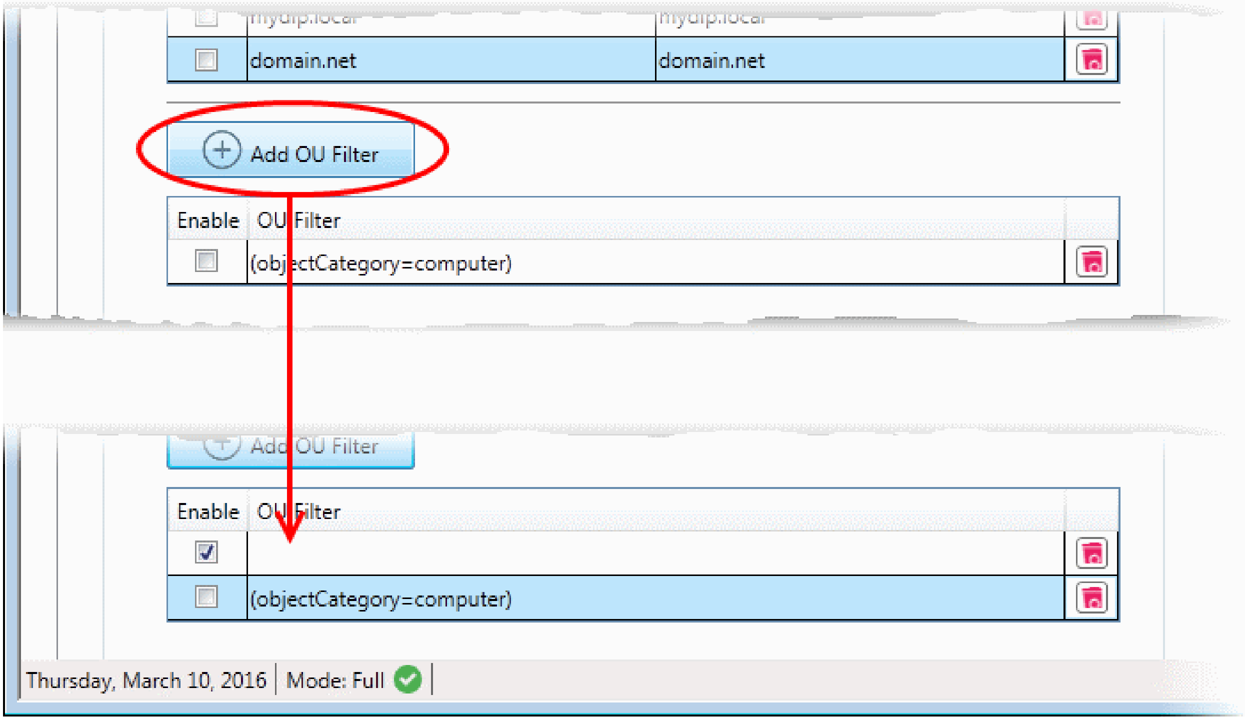
- To remove a domain click the thrash can icon

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.



- 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 thrash can icon

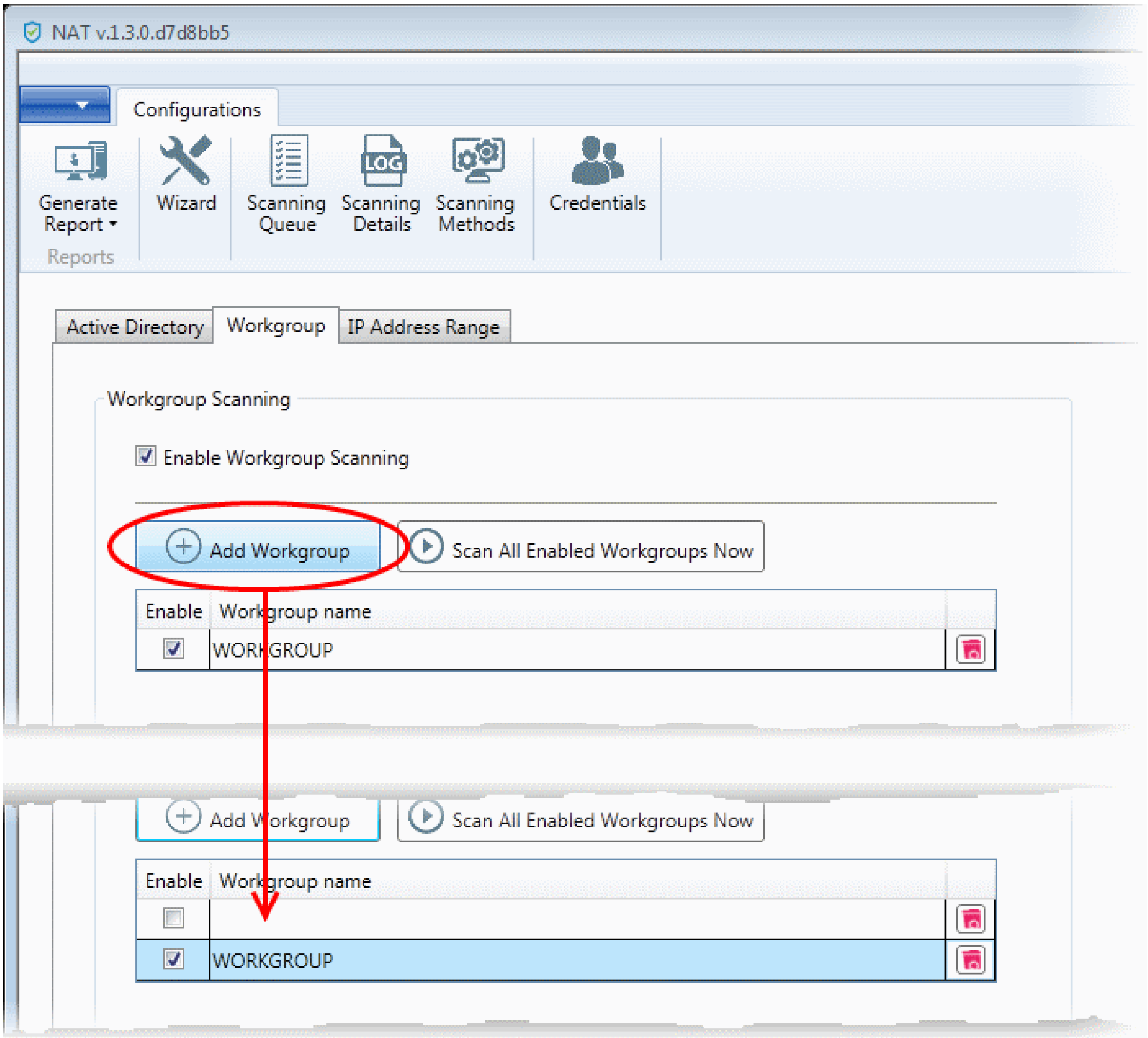
Adding a Workgroup

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.



- Enter the name of the workgroup to be added.
- To remove a work-group, click the thrash can icon 🗑

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

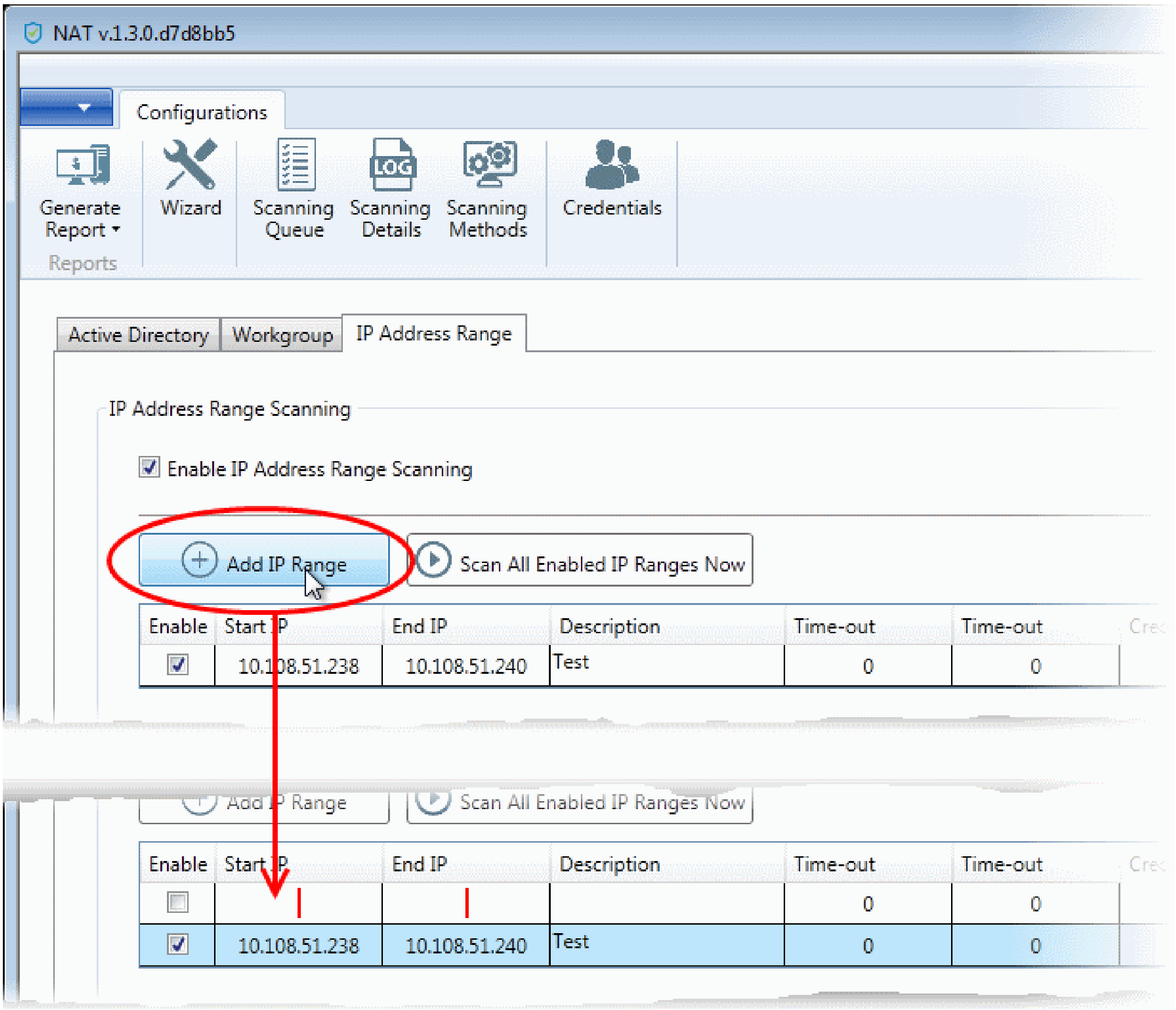
To add an IP Address Range

- Click 'Scanning Methods' from 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.

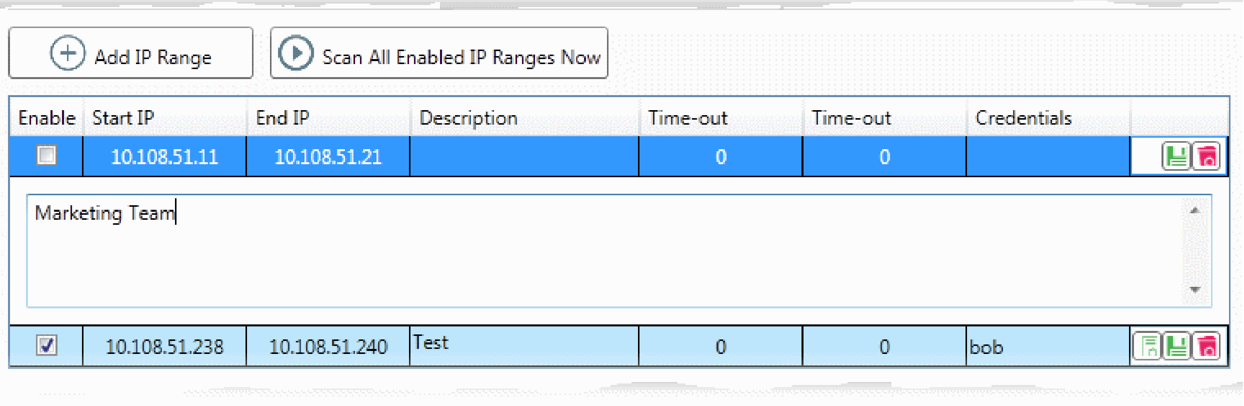


☑ Enable IP Address Range Scanning

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

Enable	Start IP	End IP	Description	Time-out	Time-out	Cre
□				0	0	
☑	10.108.51.238	10.108.51.240	Test	0	0	

- 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						
☑	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.

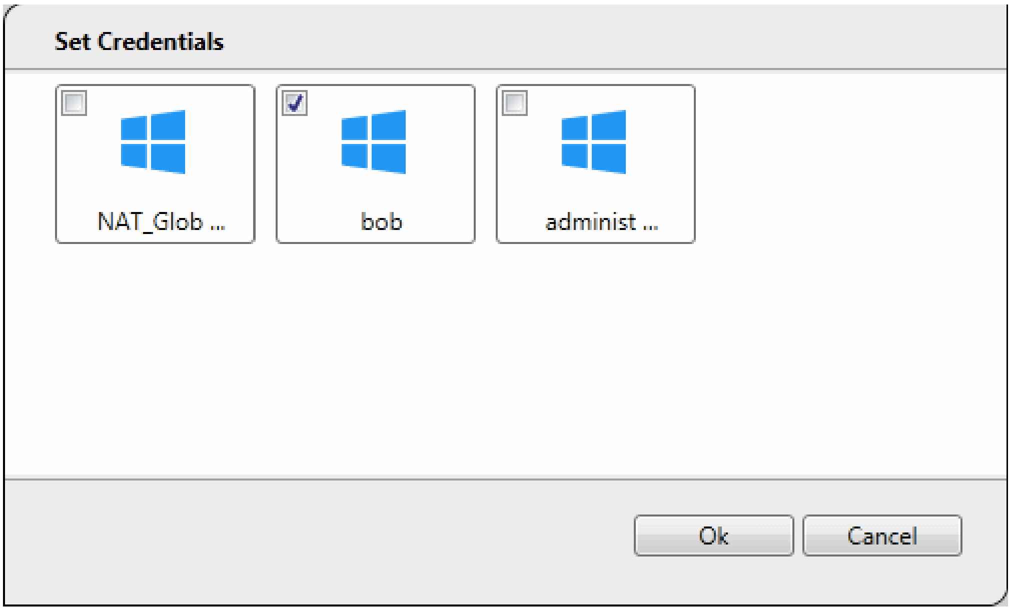
Note: NAT uses Windows Management Instrumentation (WMI) and Microsoft Baseline Security Analyzer (MBSA) to scan the endpoints identified at the given IP addresses by the Network Mapper (NMAP) tool.

- Click the 'Save' button 💾 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 the 'Add Credential' button at the right of the row.

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



- Choose the credential(s) to be applied to the IP address range and click 'OK'
- To remove an IP Address Range, click the thrash can icon

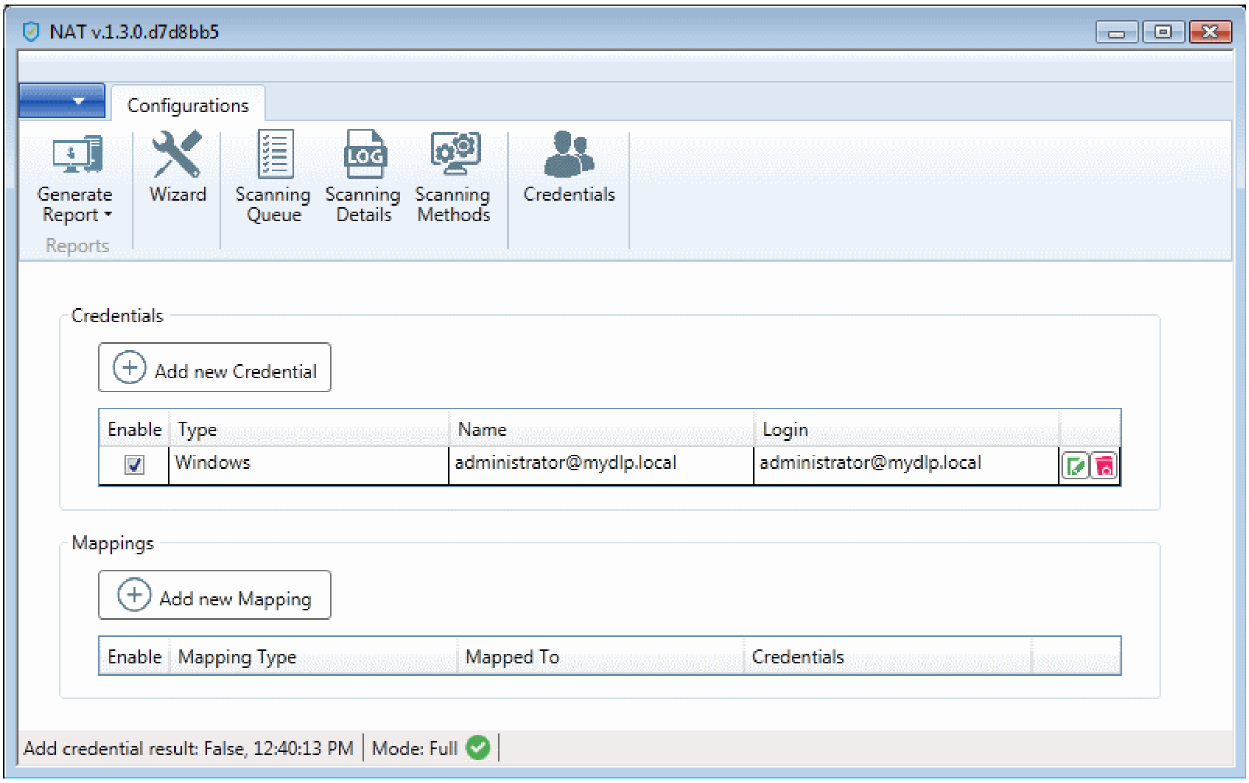
2.2 Credentials Management

The Network Assessment Tool requires login credentials of the network administrator, in order to scan the endpoints. You can add the credentials of all the networks and map them to appropriate network. NAT uses the appropriate credentials to access each network.

If different endpoints in a single network require different access credentials, you can add all the credentials and map them to the single network, so that , so that NAT can access each endpoint with the respective credential.

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

- To access the 'Credentials' interface, click 'Credentials' from the menu bar.



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

Enable	Mapping Type	Mapped To	Credentials

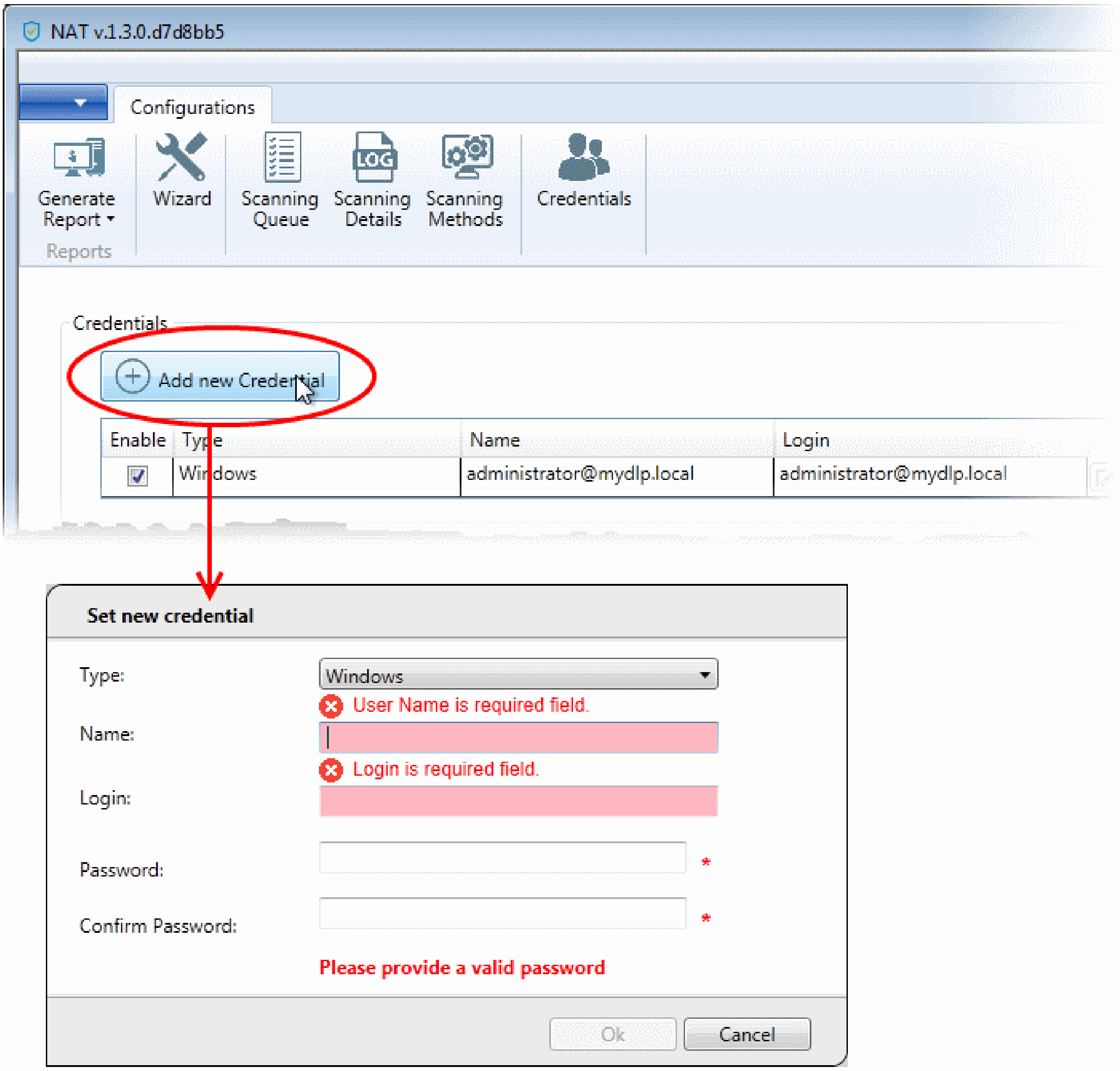
Add credential result: False, 12:40:13 PM | Mode: Full ✓

The following sections explain on:

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

To add a new login credential

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



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

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 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

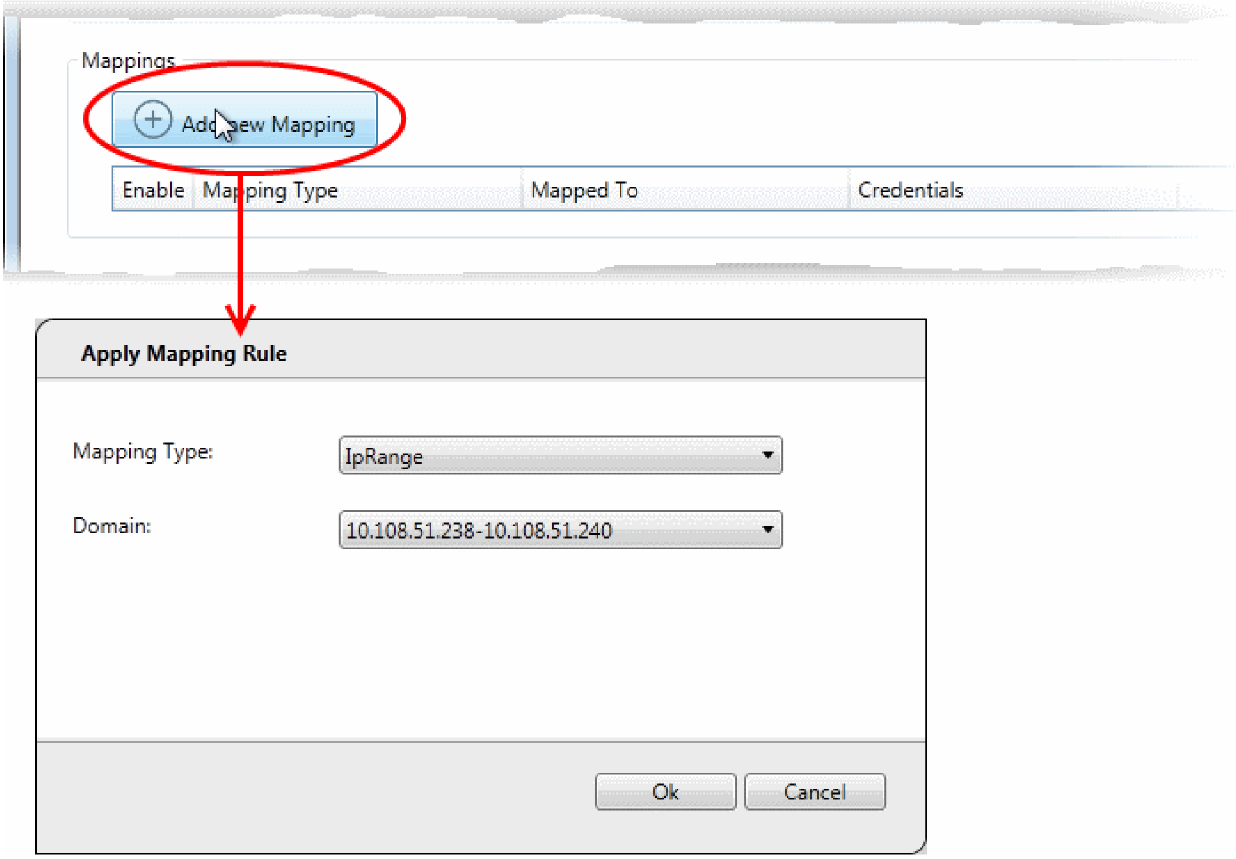
- Click 'OK' to add the credential
- Repeat the process to add more credentials
- To edit a credential, click the 'Edit' button ✎ at the right of the row and enter the new values in the 'Set new credential' dialog. The process is similar to adding a new credential.

- To remove a credential, click the thrash can icon 🗑 .

To add a new mapping of credential to a network

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

The 'Apply Mapping Rule' wizard will open.



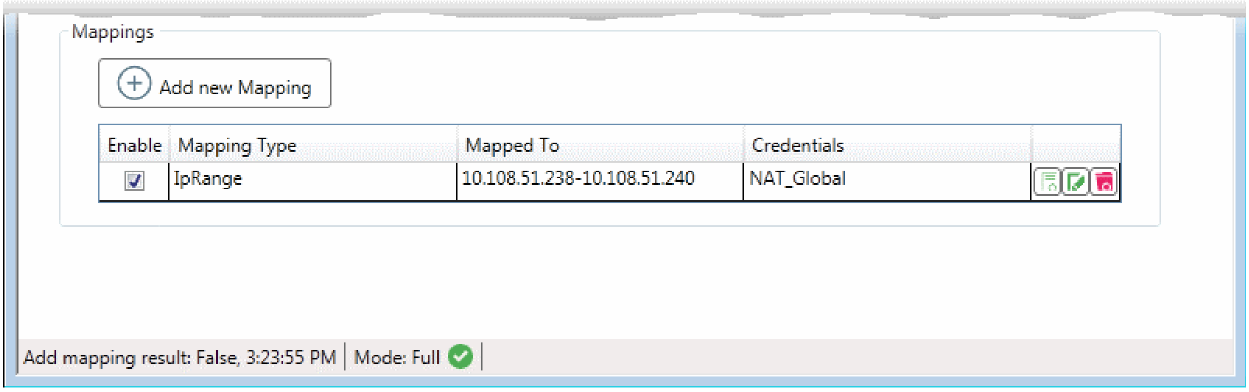
Mapping Type: IpRange

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 choices 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.

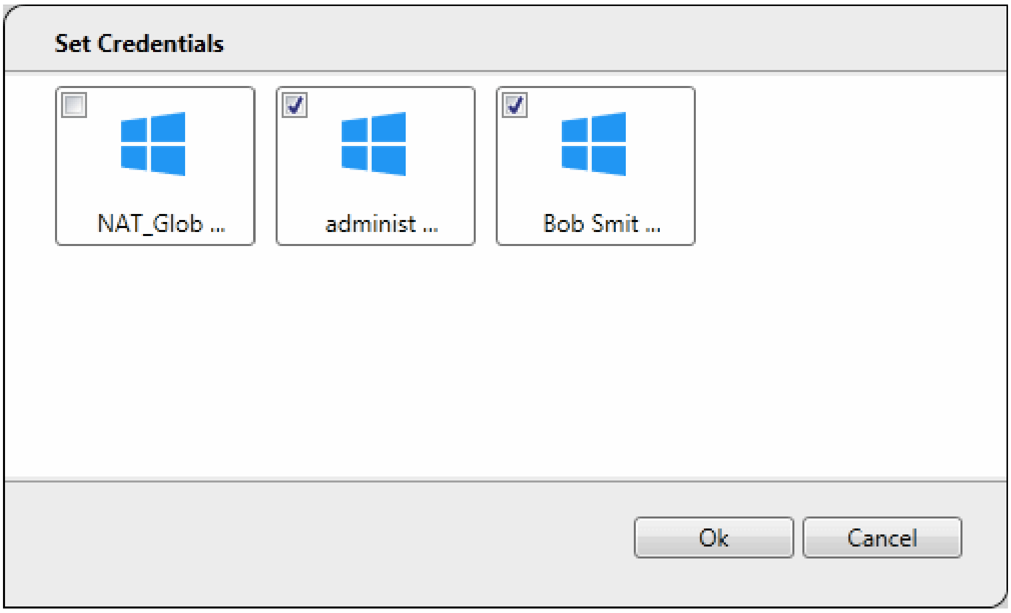


Enable	Mapping Type	Mapped To	Credentials	
☑	IpRange	10.108.51.238-10.108.51.240	NAT_Global	

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

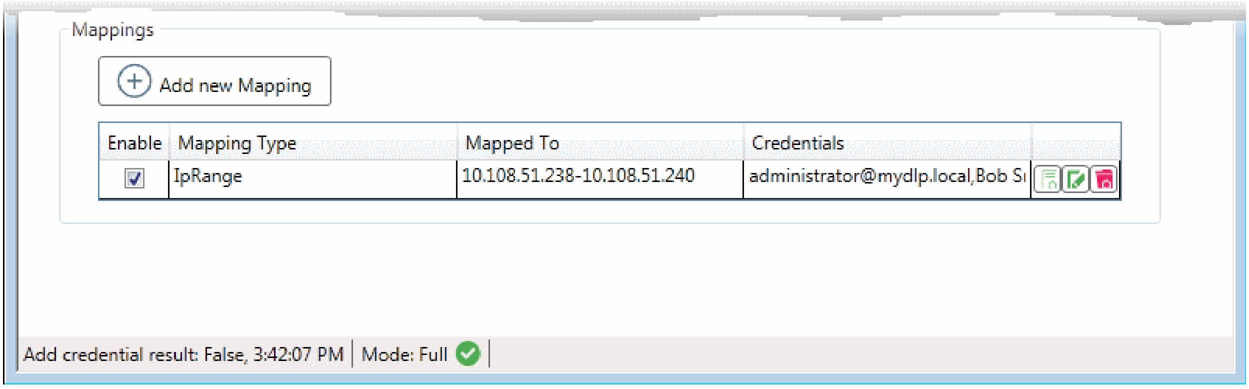
- To change the credential for the network, click the 'Add Credential' button at the right end of the row.

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 Si

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

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

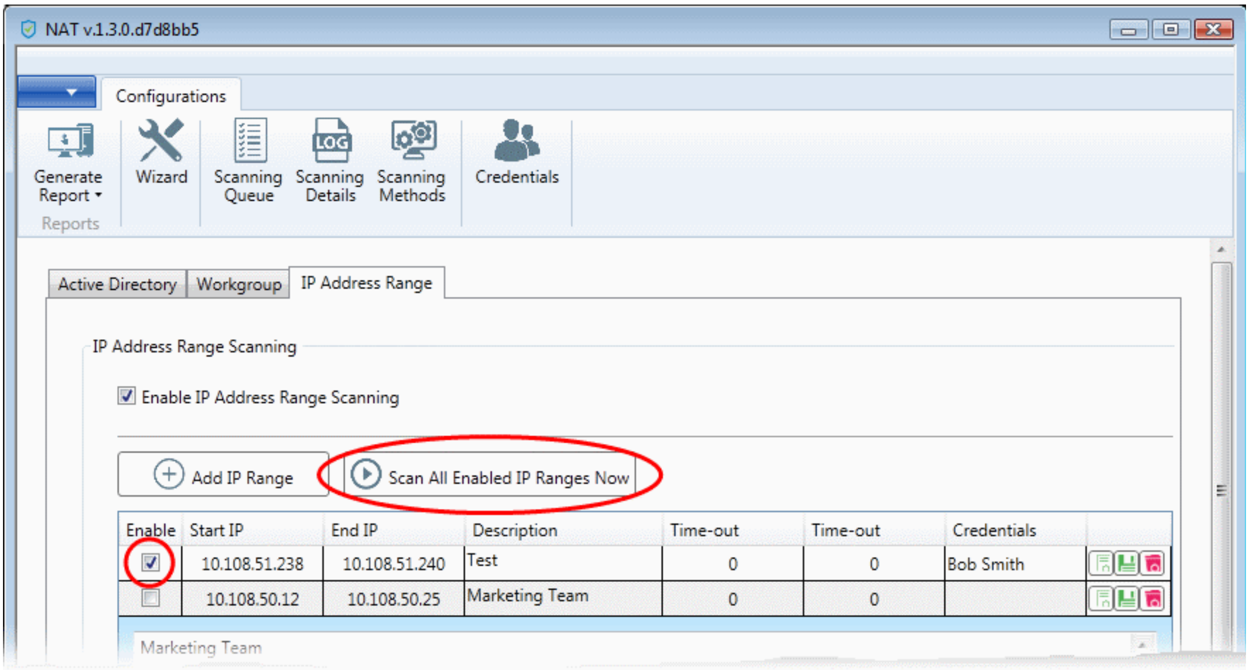
3 Running Network Assessment Scan

The administrator can run assessment scans on endpoints on a network at anytime for the network(s) added to NAT and appropriate login credentials with administrative privileges are mapped to them. Upon successful completion of a scan, the reports can be generated and downloaded to assess the network assets, identified vulnerabilities and the proposed management plan.

The 'Scanning Methods' interface allows you to initiate scanning on a selected networks one by one. You can view the progress of scans and terminate scans from the 'Scanning Queue' interface. Also, you can view a log of scans from the 'Scanning Details' interface.

To initiate a scan

- Click 'Scanning Methods' from the menu bar
- Choose the type of network on which the scan is to be initiated, by selecting the respective tab.
  - Active Directory - To run the assessment scan on endpoints in a domain
  - Workgroup - To run the assessment scan on endpoints in a workgroup
  - IP Address Range - To run the assessment scan on endpoints that fall within the specified IP address range in the network
- Ensure that the network(s) to be scanned are enabled and those that need not be scanned are not enabled
- Click 'Scan All Enabled Domains Now', 'Scan All Enabled Workgroups Now' or 'Scan All Enabled IP Ranges Now' as appropriate to the network type chosen.

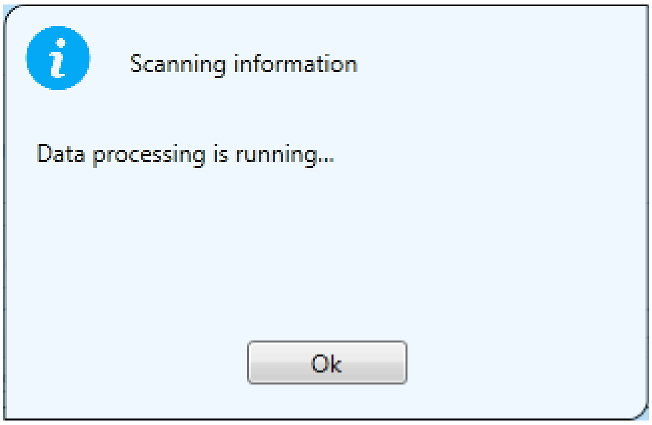


☑ Enable IP Address Range Scanning

Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials	
☑	10.108.51.238	10.108.51.240	Test	0	0	Bob Smith	
□	10.108.50.12	10.108.50.25	Marketing Team	0	0		

Marketing Team

The scan will be started.


Scanning information

Data processing is running...

- Repeat the process to initiate the scan on required networks

You can view the progress of scan from the Scanning Details interface.

The following sections explain on

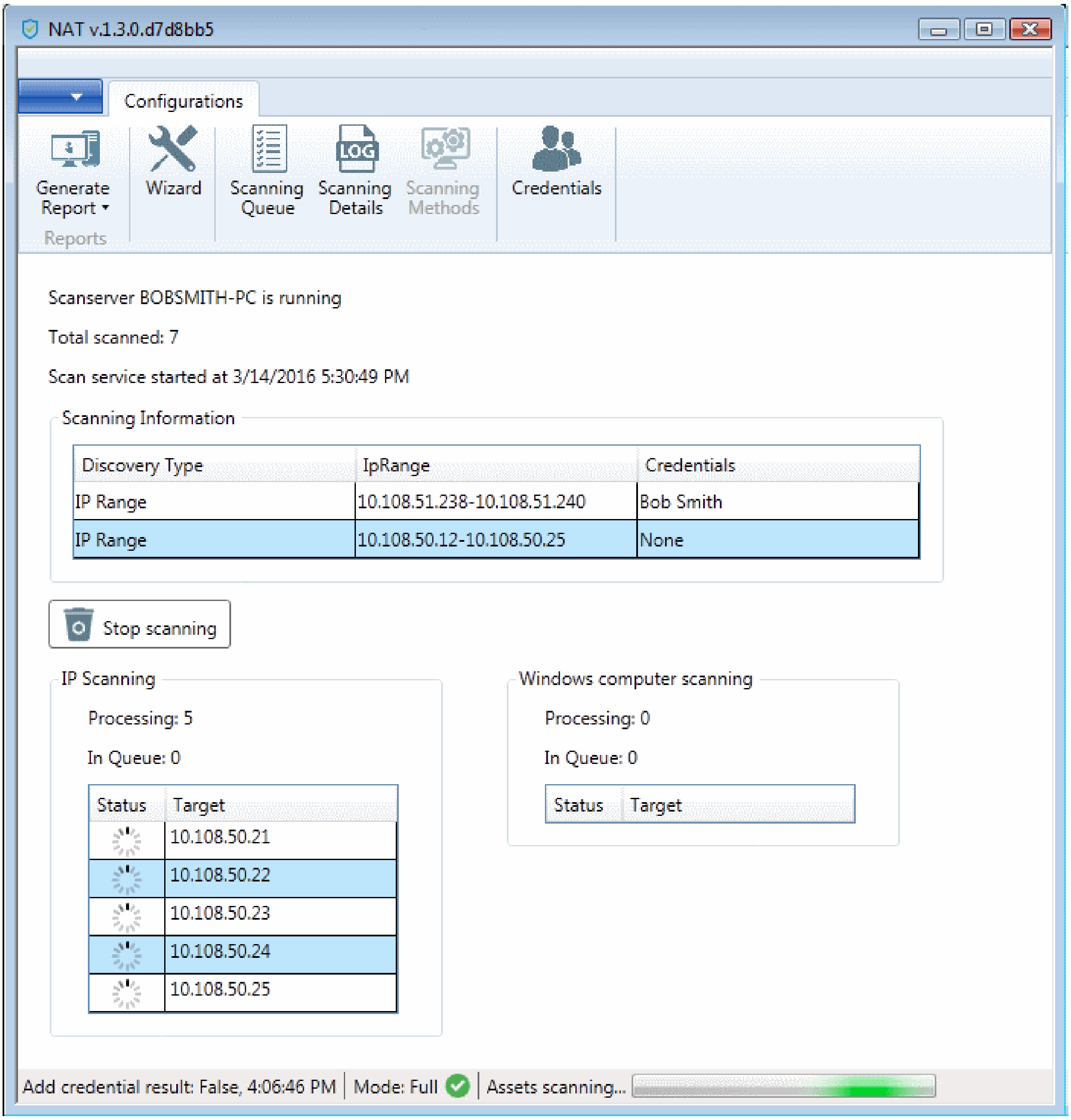
- **Viewing Scan Progress**
- **Viewing Scan Logs**

3.1 Viewing Scan Progress

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

To view the scan progress

- Click 'Scanning Queue' from the menu bar



Scanserver BOBSMITH-PC is running

Total scanned: 7

Scan service started at 3/14/2016 5:30:49 PM

Scanning Information

Discovery Type	IpRange	Credentials
IP Range	10.108.51.238-10.108.51.240	Bob Smith
IP Range	10.108.50.12-10.108.50.25	None

IP Scanning

Processing: 5

In Queue: 0

Status	Target
	10.108.50.21
	10.108.50.22
	10.108.50.23
	10.108.50.24
	10.108.50.25

Windows computer scanning

Processing: 0

In Queue: 0

Status	Target

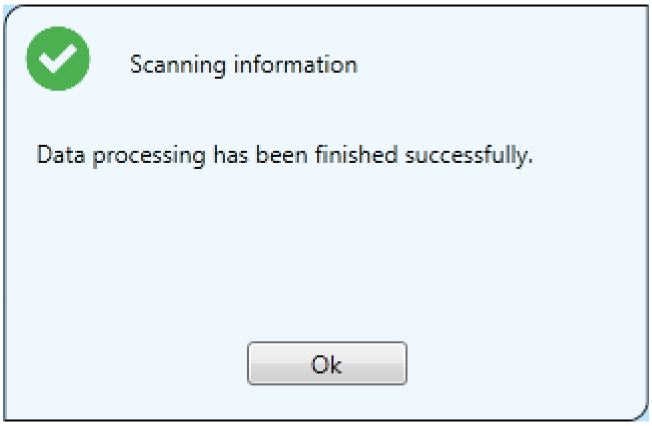
Add credential result: False, 4:06:46 PM | Mode: Full ✓ | Assets scanning...

- **Scanning Information -** Displays the domain(s), Workgroup(s) and IP Address Range(s) currently scanned.
- **IP Scanning -** Displays the list of IP addresses discovered at the currently scanned network using Network Mapper (Nmap).
- **Windows Computer Scanning -** Displays the list of hostnames/IP addresses being scanned using Windows Management Instrumentation(WMI) and Microsoft Baseline Security Analyzer

(MBSA)

- To terminate the scan, click 'Stop Scanning'.

The successful completion of scanning will be indicated.



Scanning information

Data processing has been finished successfully.

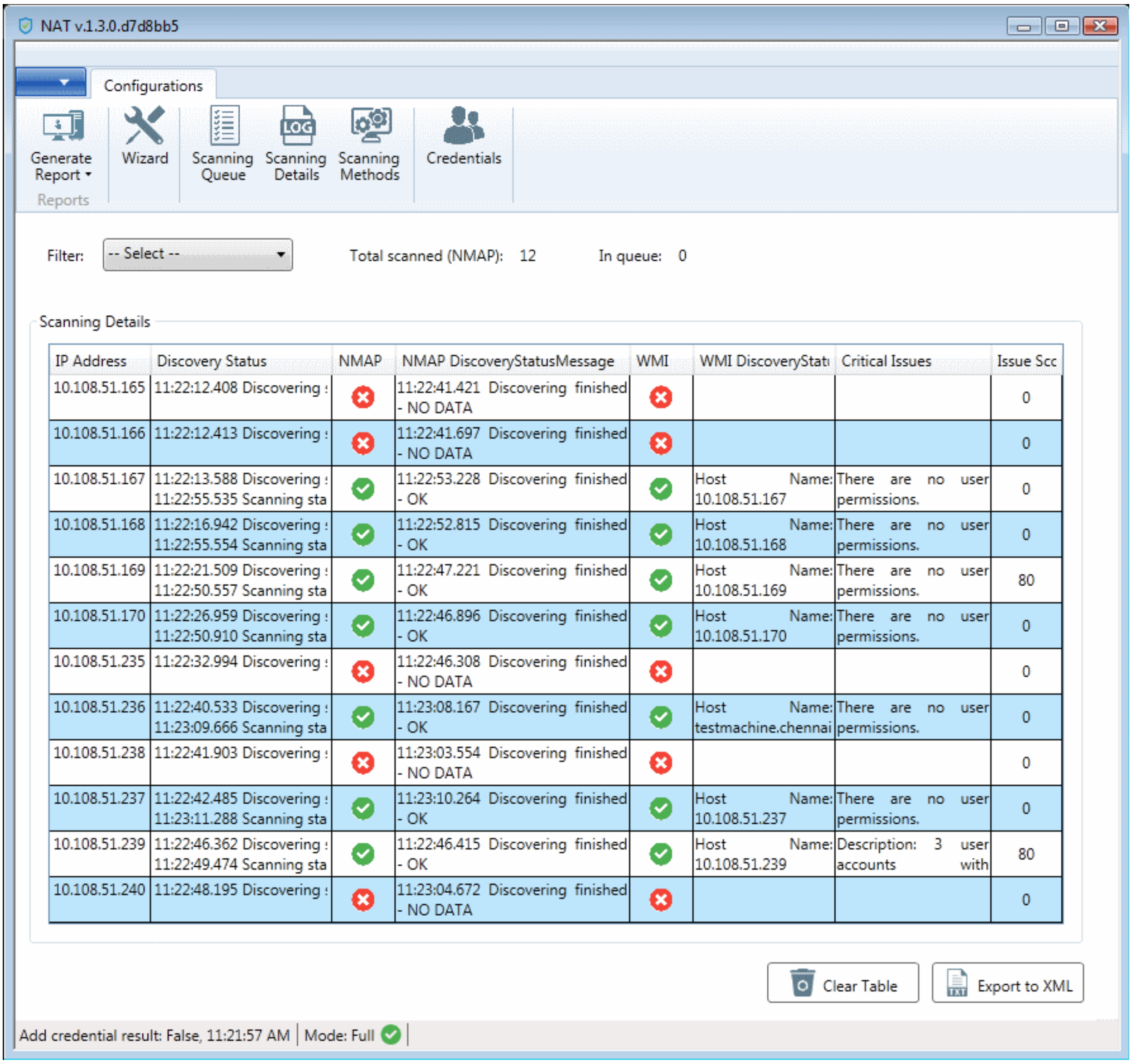
The reports can be generated and downloaded for the scan from the Generate Reports interface. Refer to the section **Generate Reports** for more details.

3.2 Viewing Scan Logs

The 'Scanning Details' interface allows the administrator to view the logs of the currently running and last run 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. Refer to the section **Configuring Network Assessment Tool** for more details.

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



Filter: -- Select -- Total scanned (NMAP): 12 In queue: 0

Scanning Details

IP Address	Discovery Status	NMAP	NMAP DiscoveryStatusMessage	WMI	WMI DiscoveryStatı	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 ✓

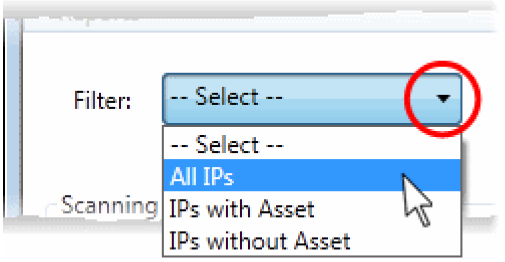
Scanning Details - Column Descriptions	
Column Header	**Description**
IP Address	Indicates the IP address scanned
Discovery Status	Indicates the precise time at which the IP address was scanned for assets and the status
NMAP	Indicates whether an asset, like an endpoint, server or any other network device 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.

Sorting and Filtering 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

Saving the 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

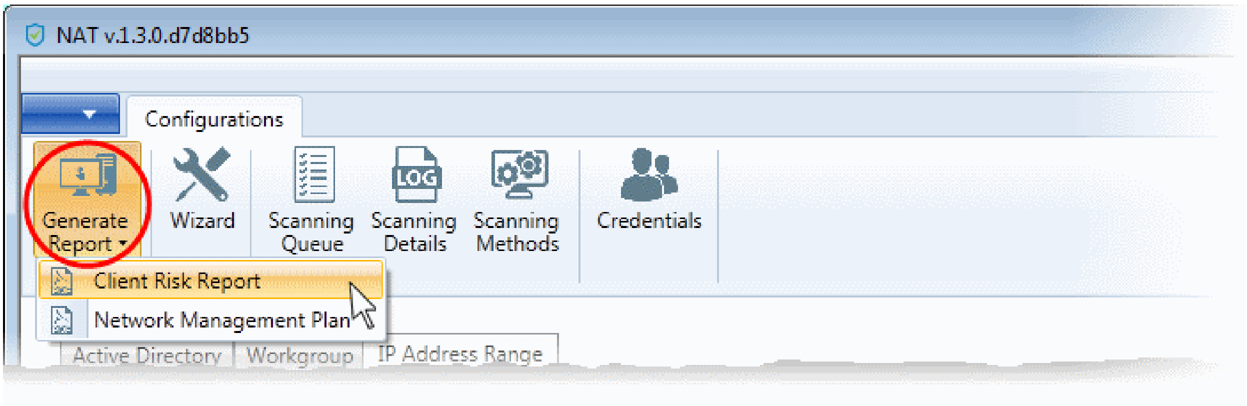
The administrator can generate assessment reports on the network last scanned. The reports help administrators to obtain details on the assets discovered from the Domain, Workgroup or the IP Address Range scanned, issues found at the scanned endpoints, risks detected on the network and a management plan to resolve the issues and mitigate the risks.

NAT can generate two types of reports:

- Client Risk Report - Contains details on discovery scans performed on the network, details on network assets, issues identified, storage status on the discovered endpoints and more.
- Network Management Plan - Contains guidance on remediation measures for mitigating risks and resolve issues identified from the 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.

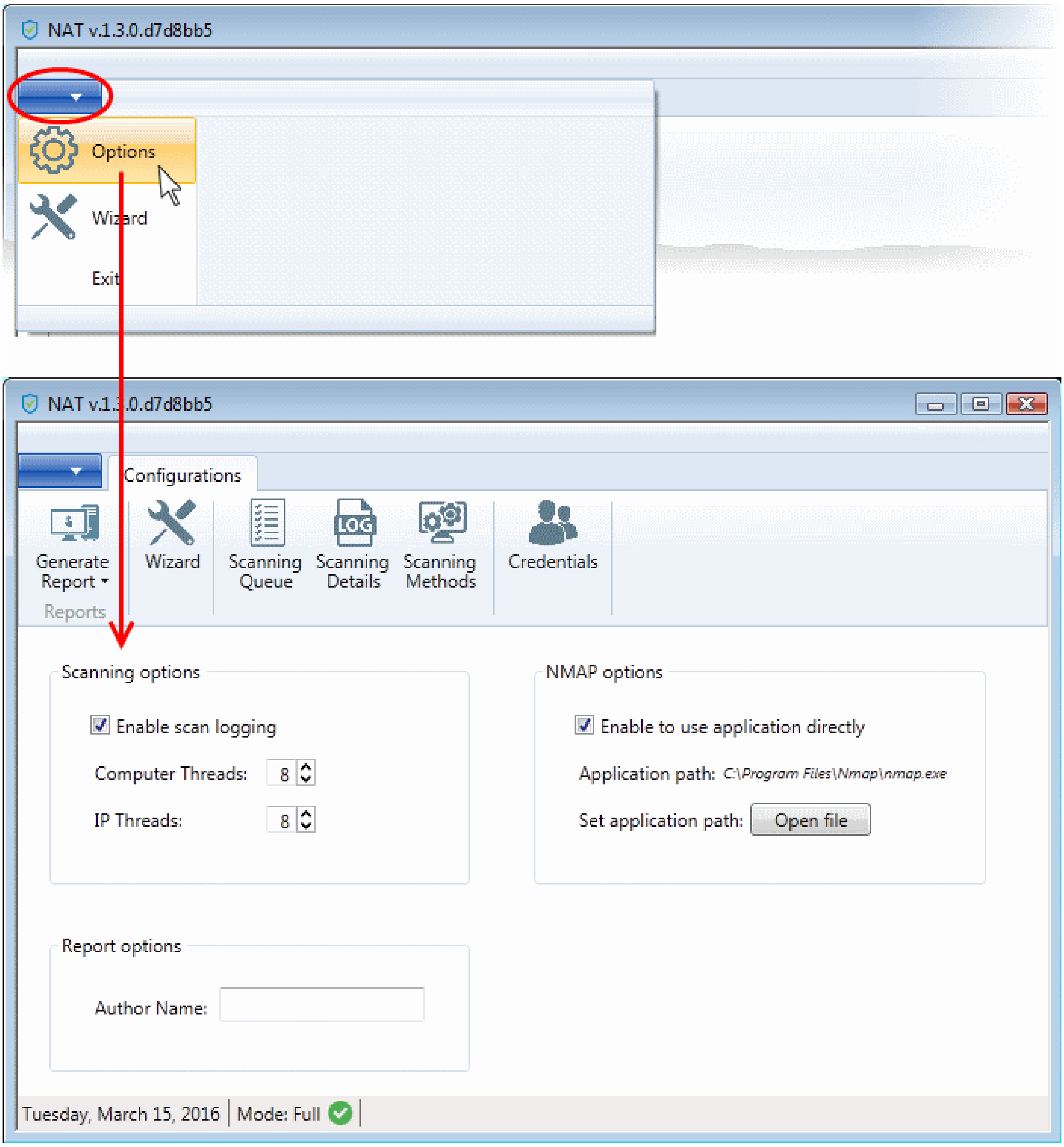
Tip: The cover page of the report contains the 'Author Name' that indicates the person that generated the report, with a label 'Prepared by' . You can configure the author name to be displayed on the cover page from the configuration panel. Refer to the section **Configuring Network Assessment Tool**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

5 Configuring Network Assessment Tool

You can configure the miscellaneous settings concerning the overall behavior of the application from the 'Configuration' interface.

To open the configuration interface

- 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: C:\Program Files\Nmap\nmap.exe

Set application path: Open file

Report options

Author Name:

Tuesday, March 15, 2016 | Mode: Full ✓

Scanning 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 scanning details of IP addresses covered by the domain, workgroup or the IP address range being scanned. The logs of currently running or the last run scan can be viewed from the Scanning Details interface. Refer to the section **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 location. 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.

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 : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**