



## Comodo One Software Version 3.3

# Network Assessment Tool Quick Start Guide

Guide Version 1.3.101316

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

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'

#### COMODO Creating Trust Online



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 <sup>I</sup> 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.
- 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 <u>Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)</u>					
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 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 Assessme	ent Tool - First Run			х
#1 Please enter the o	default <b>IP Range</b> which will	be scanned		
Start IP Address:	10.108.51.1	]		
End IP Address:	10.108.51.255	]		
123			Previous	Next

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	х
#2 Network Assessment Tool can scan all your computers clientless	
Enable scanning for Workgroup : WORKGROUP (recommended)	
You can add/change Workgroups and Domains later!	
1 2 3 Previous Next	ן

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	1
#3	
Administrative Credentials are ne	eded to scan your computers
Windows Username:	*
Password:	*
Show Password	
Skip this step	
You can add/change Administrativ	/e Credentials later!
	Previous

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



Men The drop-down at top right contains options to configure the application	u bar controls to different on screens ate reports.	Main Config Allows you to a networks, initia credentials to a view scan prog depending on th from the	guration Area add and manage ate scans, enter ccess networks, gress and more, le screen chosen menu bar.	
Image: NAT v.1.3.0.d7d8bb5         Image: Configurations	canning Methods			
Active Directory Workgroup IP Address Active Directory Scanning  Enable Active Directory Scanni  Active Directory Scanni Active Directory Scanni Active Directory Scanni  Active Directory Scanni Active Directory S	Range ng ) Scan All Enabled Domain:	: Now		E
Enable DNS name mydlp.local Add OU Filter Enable OU Filter (objectCategory=computed) Thursday, March 10, 2016 Mode: Full	ter)	name :al		
Shows s	Task Bar canning mode and p	rogress 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

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

#### COMODO Creating Trust Online\*

⊘ NAT v.1.3.0.d7d8bb5	
Configurations	
Generate Report • Reports Wizard Reports Wizard Wizard Wizard Wizard Reports Canning Queue Scanning Details Methods Cr	redentials
Active Directory Workgroup IP Address Range	
Active Directory Scanning          Image: Construction of the second se	abled Domains Now
Enable DNS name	NetBios name
W mydlp.local	mydlp.local
+ Add OU Filter	
Enable OU Filter	
(objectCategory=computer)	
Thursday, March 10, 2016   Mode: Full 🤡	

 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.

( <del>-</del>	Add IP Range	Scan All E	nabled IP Ranges Now				
Enable	Start IP	End IP	Description	Time-out	Time-out	Credentials	
	10.108.51.11	10.108.51.21		0	0		
Marke	eting Team						•
	10.108.51.238	10.108.51.240	Test	0	0	bob	R <b>L</b> I

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	
			Ok Cancel

#### 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.

#### COMODO Creating Trust Online\*

Con	figurations			
te V	Vizard Scanning Queue Scanning Details	Scanning Methods		
dentials				
(+) <i>µ</i>	dd new Credential			
Enable	Туре	Name	Login	
	Windows	administrator@mydlp.local	administrator@mydlp.local	23
opings	Add new Mapping			

#### To add a new login credential

• click 'Add new Credential'

COMODO Creating Trust Online\*

Configurations   Wizard   Scanning   Queue   Scanning   Queue   Details   Credentials   Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Credentials Enable Type Name Login administrator@mydlp.local administrator@mydlp.local administrator@mydlp.local et new credential pe: Windows Constrained Subset Name is required field. me: Source Constrained Constr			
Wizard Image: Scanning Scanning Scanning Methods   Credentials   Credentials   <	Configurations		
Add new Credertial     Enable Type     Name   Login     administrator@mydlp.local     administrator@mydlp.local     administrator@mydlp.local     et new credential     pe:   Windows     © User Name is required field.   me:   ② User Name is required field.   gin:   ssword:     *	te Wizard Scan Qu	ining Scanning Scanning Methods Credentials	
Wirdows administrator@mydlp.local     Wirdows administrator@mydlp.local     t new credential     e: Windows     Windows     • Windows <th>+ Add new Cred</th> <th>ertial</th> <th>1 a size</th>	+ Add new Cred	ertial	1 a size
Windows administrator@mydlp.local   et new credential     be:   Windows   Windows   ©   User Name is required field.   me:   ©   Login is required field.   gin:   isword:   nfirm Password:	Enable Type	Name	Login
et new credential  pe: Windows  Subser Name is required field.  me:  Subser Name is required field.  gin:  ssword:  nfirm Password:  *	Vir dows	administrator@mydlp.lo	cal administrator@mydlp.loca
ssword:	Windows	administrator@mydlp.lo	cal administrator@mydlp.loca
gin: ssword: nfirm Password:	et new credential	Windows Subser Name is required field.	cal administrator@mydlp.loca
ssword:	et new credential	Windows User Name is required field.	cal administrator@mydlp.loca
nfirm Password:	iet new credential rpe: ame: ogin:	Windows User Name is required field.  Kogin is required field.	cal administrator@mydlp.loca
	Jet new credential //pe: ame: bgin: assword:	Windows  User Name is required field.   Login is required field.	cal administrator@mydlp.loca

The 'Set new credential' dialog will open.

Set new credential dialog - Form parameters		
Form Element	Description	
Туре	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	

Ok

Cancel

- 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.

Apply Mapping Rul	2	]
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.

#### COMODO Creating Trust Online\*

•	Configura	ations						
enerate eport •	Wizard	Scanning Sca Queue D	anning Scanning Methods	Credentials				
Active	Directory Address R	Workgroup IP ange Scanning	Address Range					
Active	Directory Address F	Workgroup IP ange Scanning : IP Address Rang	Address Range					
Active	Address F	Workgroup IP ange Scanning E IP Address Rang Add IP Range	9 Address Range ge Scanning	Enabled IP Ranges Now	D			
Active	Address F	Workgroup IP ange Scanning e IP Address Rang Add IP Range Start IP	e Scanning Scan All E End IP	Enabled IP Ranges Now Description	D Time-out	Time-out	Credentials	
Active	Address F Address F Enable	Workgroup IP ange Scanning – e IP Address Rang Add IP Range Start IP 10.108.51.238	e Scanning Scan All E End IP 10.108.51.240	nabled IP Ranges Now Description Test	Time-out 0	Time-out 0	Credentials Bob Smith	

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

#### COMODO Creating Trust Online

⊘ NAT v.1.3.0.d7d8bb5	-		
Configurations			
Generate Report • Reports	nning Scanning Methods Credentials		
Scanserver BOBSMITH-PC is running Total scanned: 7 Scan service started at 3/14/2016 5:30 Scanning Information	):49 PM		
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	- Windows co Processin In Queue	mputer scanning g: 0 : 0	
Status Target	Status	Target	
10.108.50.21			
10.108.50.22			
10.108.50.23			
10.108.50.24			
10.108.50.25			
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

Ø NAT v.1.3.0.d7d8bb5	
Configurations	
Wizard     Scanning     Scanning     Scanning       Wizard     Scanning     Scanning     Scanning       Queue     Details     Methods	
Client Risk Report           Image: Network Management Plan           Active Directory         Workgroup           IP Address Range	

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

## About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.	Comodo CA Limited			
1255 Broad Street	3rd Floor, 26 Office Village, Exchange Quay, Trafford			
Clifton, NJ, 07013	Road, Salford, Greater Manchester M5 3EQ,			
United States	United Kingdom.			
Email: EnterpriseSolutions@Comodo.com	Tel : +44 (0) 161 874 7070			
	Fax : +44 (0) 161 877 1767			

For additional information on Comodo - visit http://www.comodo.com.