COMODO
Creating Trust Online®

Comodo
Auto Discovery and Deployment Tool

Software Version 1.0

Administrator Guide

Guide Version 1.0.120418

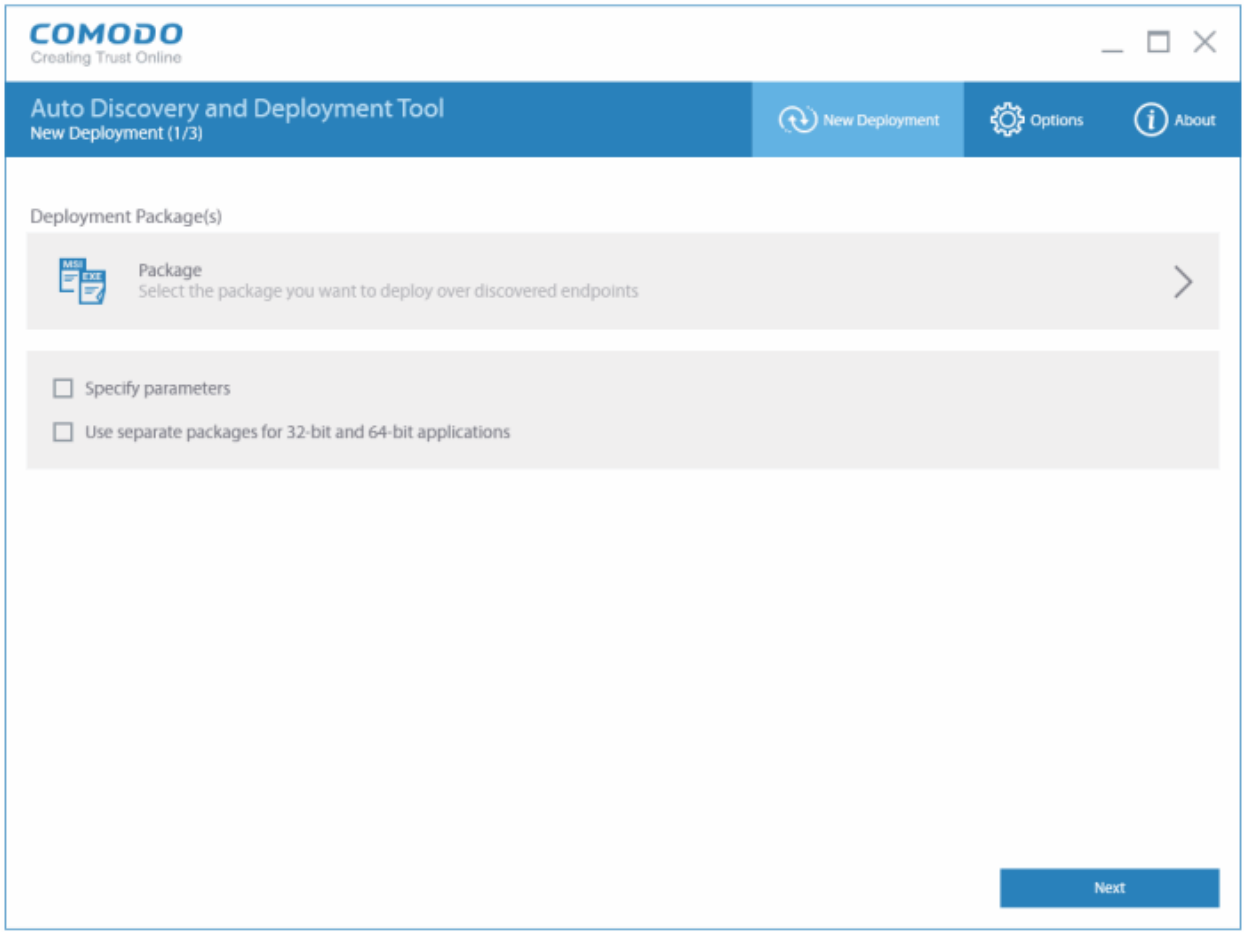
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Auto Discovery and Deployment Tool 3
1.1.Get Started with Comodo ADDT 4
2. Deploy Applications / Packages 5
2.1.Select Packages 5
2.2.Configure Deployment Options 6
2.2.1.Deploy Packages Using Active Directory 7
2.2.2.Deploy Packages to a Workgroup 11
2.2.3.Deploy Packages Using Network Addresses 14
3. CADDT Settings 17
4. About CADDT 19
About Comodo Security Solutions 21

1. Introduction to Comodo Auto Discovery and Deployment Tool

Comodo Auto Discovery and Deployment Tool (CADDT) allows network admins to remotely deploy applications to multiple endpoints via Active Directory, Workgroup or IP address/IP range/host name. Although primarily designed to allow Comodo ITSM customers to deploy the ITSM agent, the utility can be also be used to install any application remotely.



This guide will take you through the set up and ongoing usage of Comodo ADDT and is broken down into the following main sections:

- Introduction to Comodo ADDT
  - Get Started with Comodo ADDT
- Deploy Applications / Packages
- Select Packages
- Configure Deployment Options
  - Deploy Packages Using Active Directory
  - Deploy Packages Using Workgroup
  - Deploy Packages Using Network Addresses
- CADDT Settings
- About ADDT

1.1. Get Started with Comodo ADDT

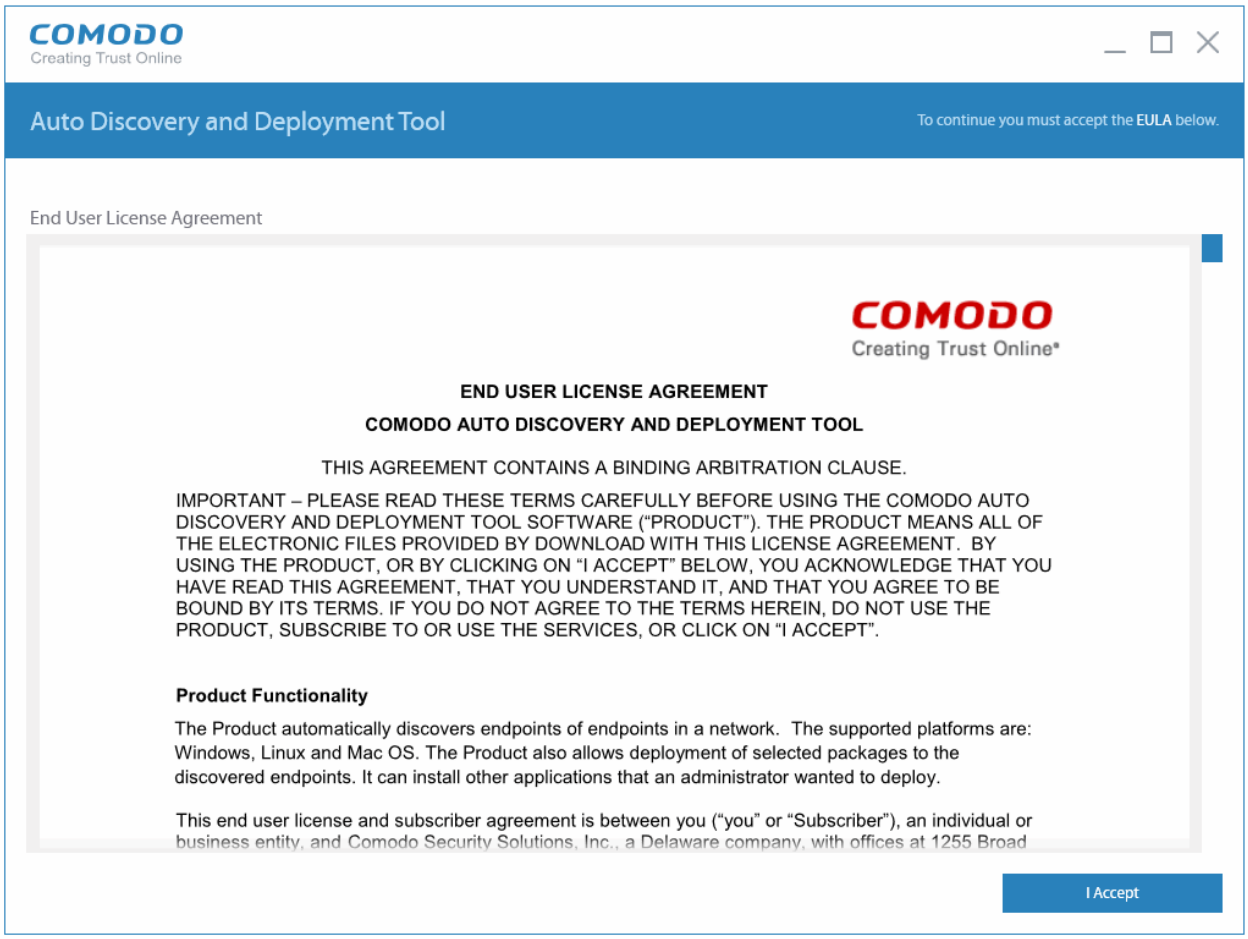
Comodo ADDT can be downloaded from the 'Tools' section of Comodo One.

- Login to Comodo One at one.comodo.com with your existing username and password.
- Click the 'Tools' (wrench) icon on the top navigation
- Select the 'Auto Discovery and Deployment' app then select 'Download'.
- Save the app to your local machine.

CADDT is a portable app which does not require installation. Simply double-click on ADDT.exe to run the application.

Once running

- First read and agree to the End User License Agreement (EULA):



- Click the 'I Accept' button to open the utility

Comodo ADDT is a lightweight application which is compatible with the following operating systems:

- Windows 10 (32bit and 64bit)
- Windows 8 (32bit and 64bit)
- Windows 7 (32bit and 64bit)
- Windows Vista (Home/Business/Ultimate) (32bit and 64bit)
- Windows 2008 Server (32bit and 64bit)

2. Deploy Applications / Packages

You can deploy applications to remote endpoint in two short steps:

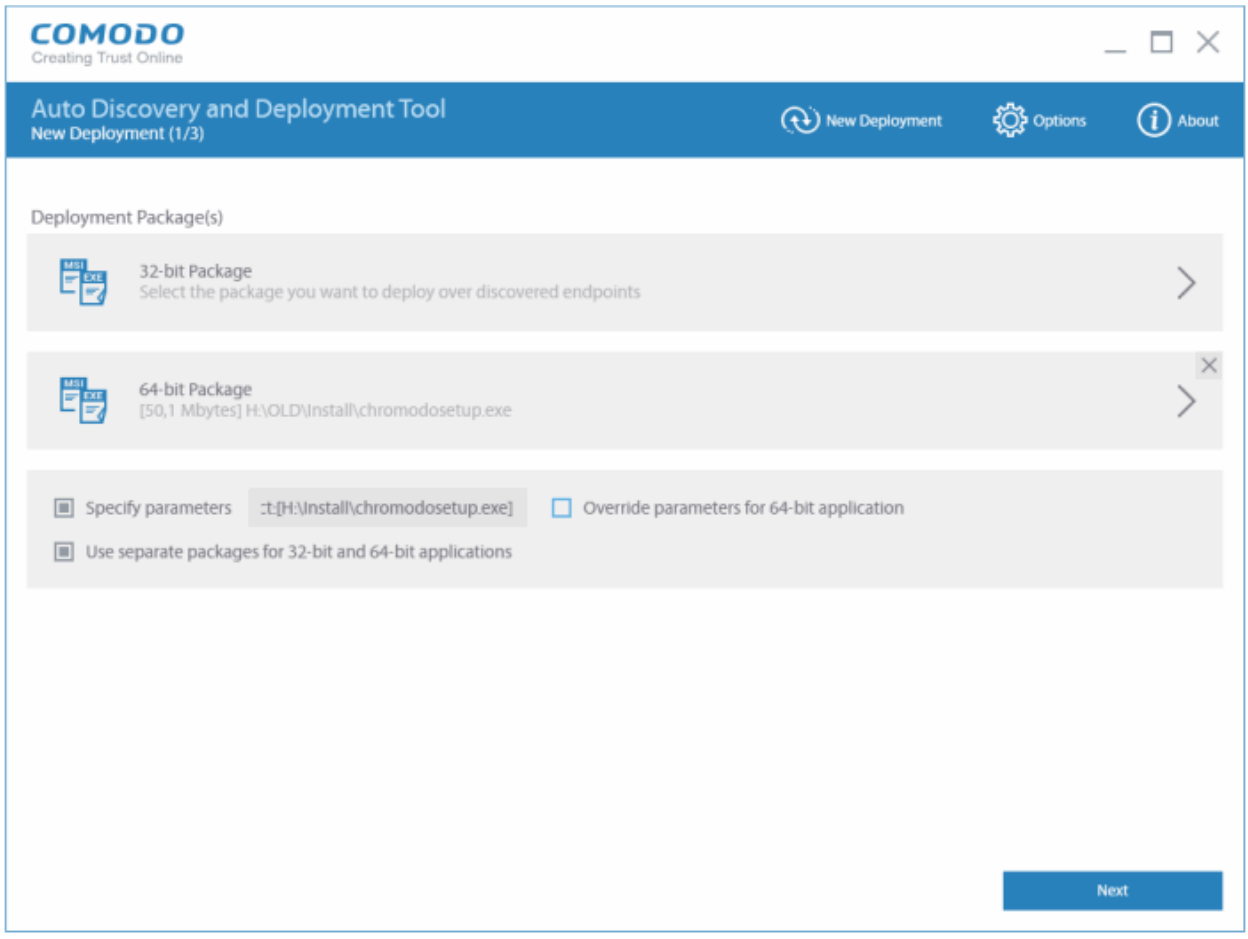
1. Select the packages to be deployed to discovered endpoints:
   - Select the application that you wish to deploy.
   - Optional – add command line parameters/switches to modify installer behavior.
   - Optional – specify different installers for 32 bit and 64 bit operating systems. Comodo ADDT will detect the endpoint OS type and deploy the appropriate package.
2. Specify target endpoints using Active Directory, Workgroup or Network Addresses

Refer to the following sections for more details:

- **Select Packages**
- **Configure Deployment Options**

2.1. Select Packages

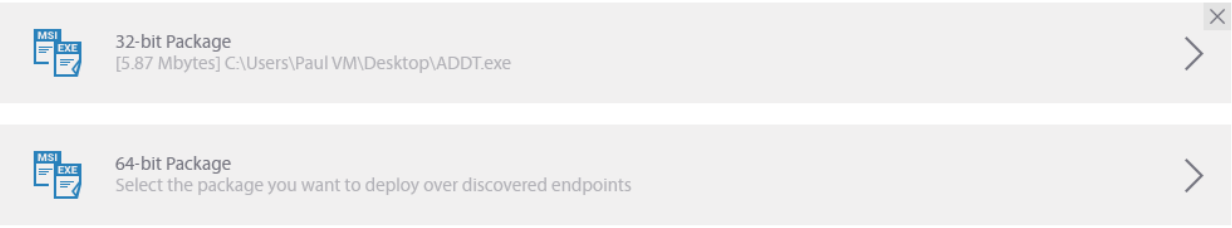
After starting Comodo ADDT and agreeing to the EULA, the application will open at the 'New Deployment' page. This page allows you to select the applications you wish to install and specify basic installation settings:



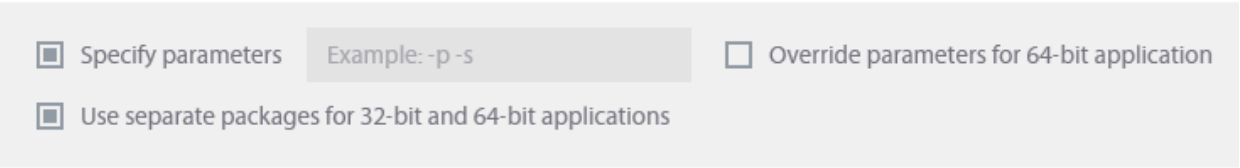
Package – Choose the package you wish to deploy to your remote endpoints. You can install any .msi. or exe package. Comodo ITSM users who want to deploy the agent and client can download it by logging into ITSM and clicking Devices > Bulk Installation Package > Offline Package. More details on this can be found at **https://help.comodo.com/topic-399-1-786-10851-Enroll-Windows-Devices-by-Installing-the-ITSM-Agent-Package.html**

Specify Parameters (Optional) - The parameters field allows you to enter command line switches which modify the behavior of the installer. The switches you can use depend on the type of installer used by your application. For more information, see **https://support.microsoft.com/en-us/kb/912203** and **http://unattended.sourceforge.net/installers.php**

Use separate packages for 32 bit and 64 bit applications – Enable this setting if you wish to specify different installers for 32 bit and 64 bit operating systems. Comodo ADDT will detect the OS of the target endpoint and deploy the appropriate package. If enabled, you will be given the opportunity to upload separate installers as shown below:



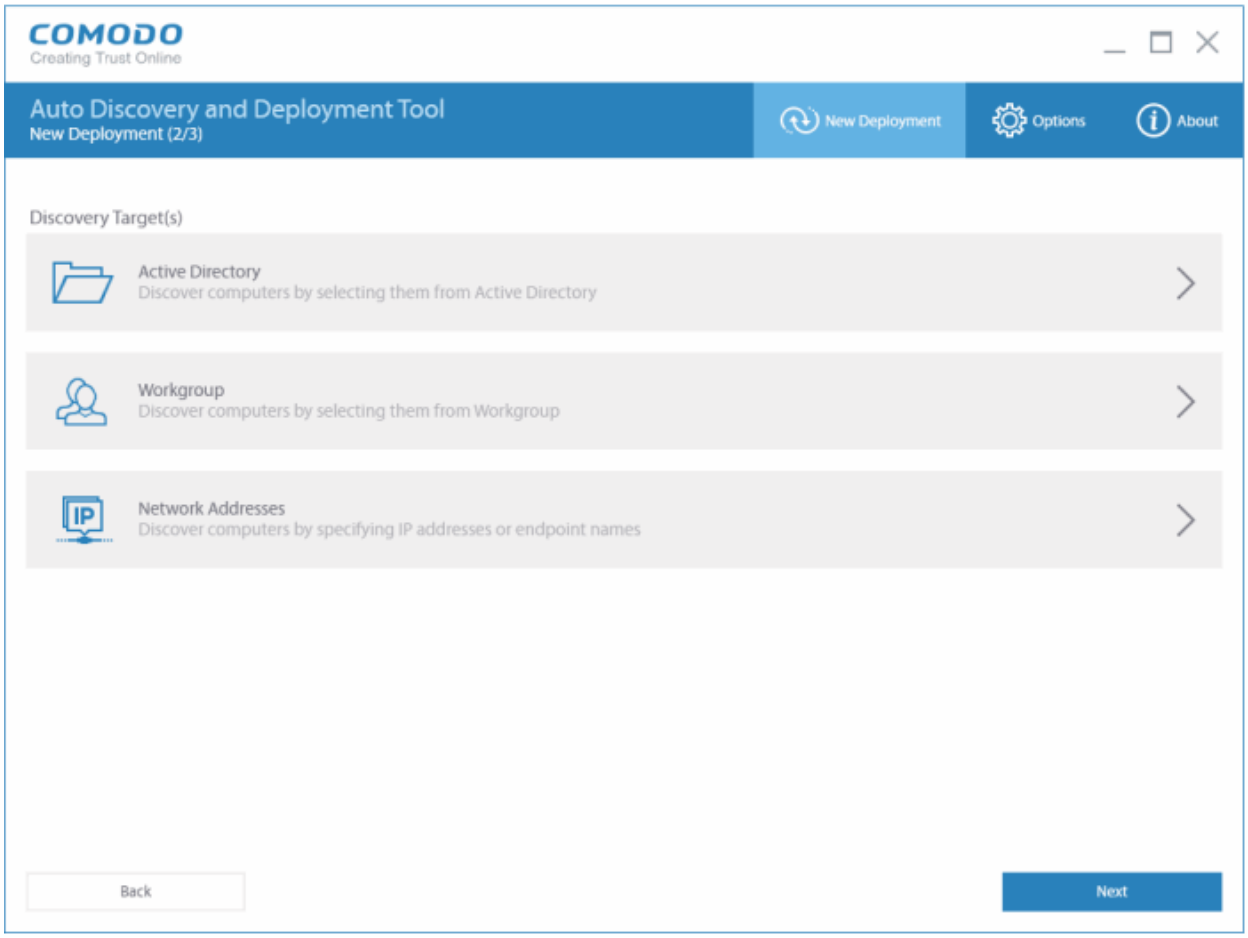
- If both 'Specify Parameters' and 'Use Separate...' are enabled, you will be given the option to disable your parameters/switches for 64-bit applications:



After uploading your installers and configuring your settings, click 'Next' to proceed to step 2 – deployment.

2.2. Configure Deployment Options

After adding your package, the next step is to deploy the package to your target endpoints. Comodo ADDT provides three ways of doing this:

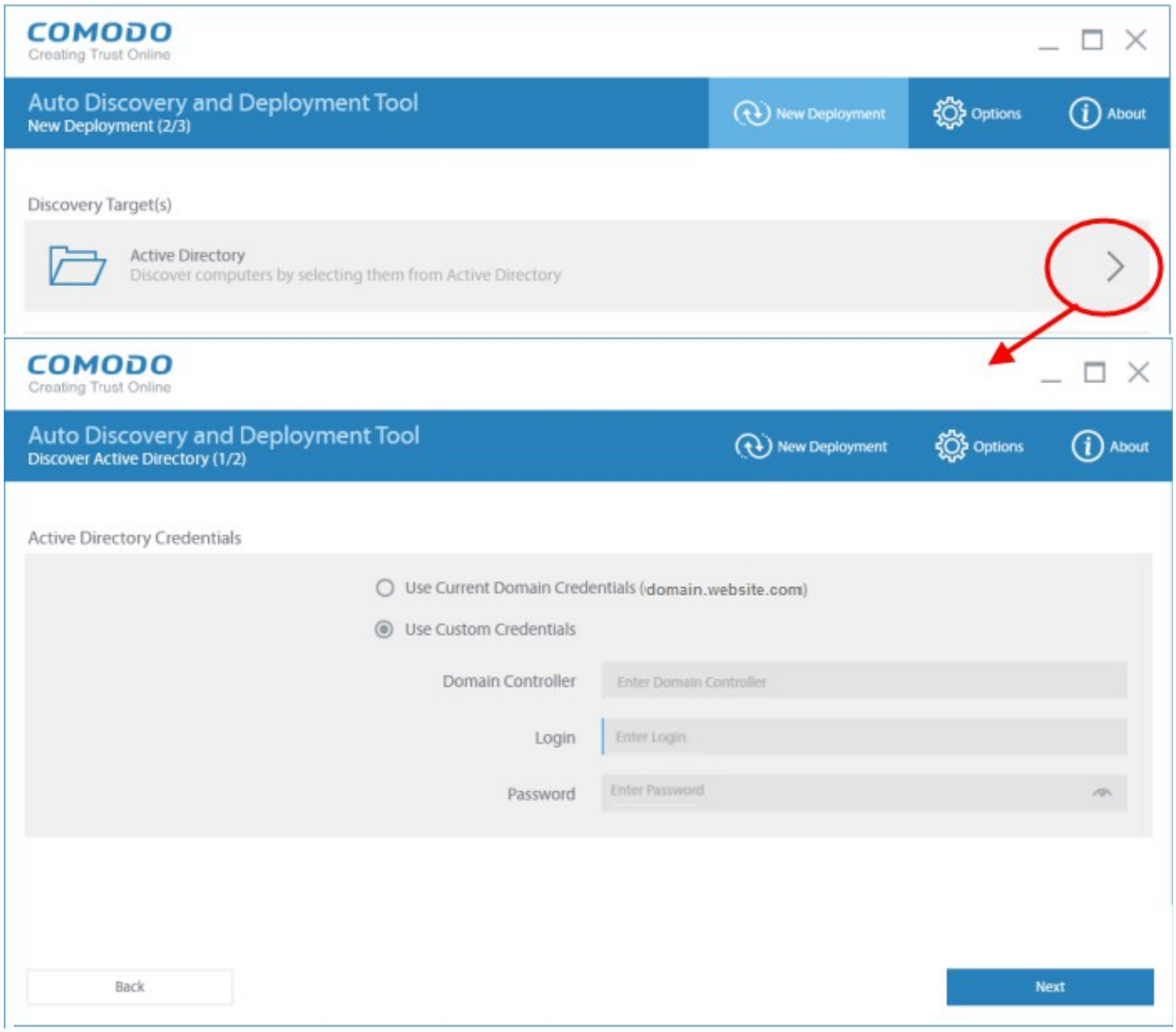


- **Active Directory** - Import and deploy certificates to large numbers of endpoints using Active Directory
- **Workgroup** – Import and deploy certificates to endpoints which belong to a workgroup.
- **Network Address** – Import and deploy certificates to endpoints by specifying host name / IP address or IP range.

2.2.1. Deploy Packages Using Active Directory

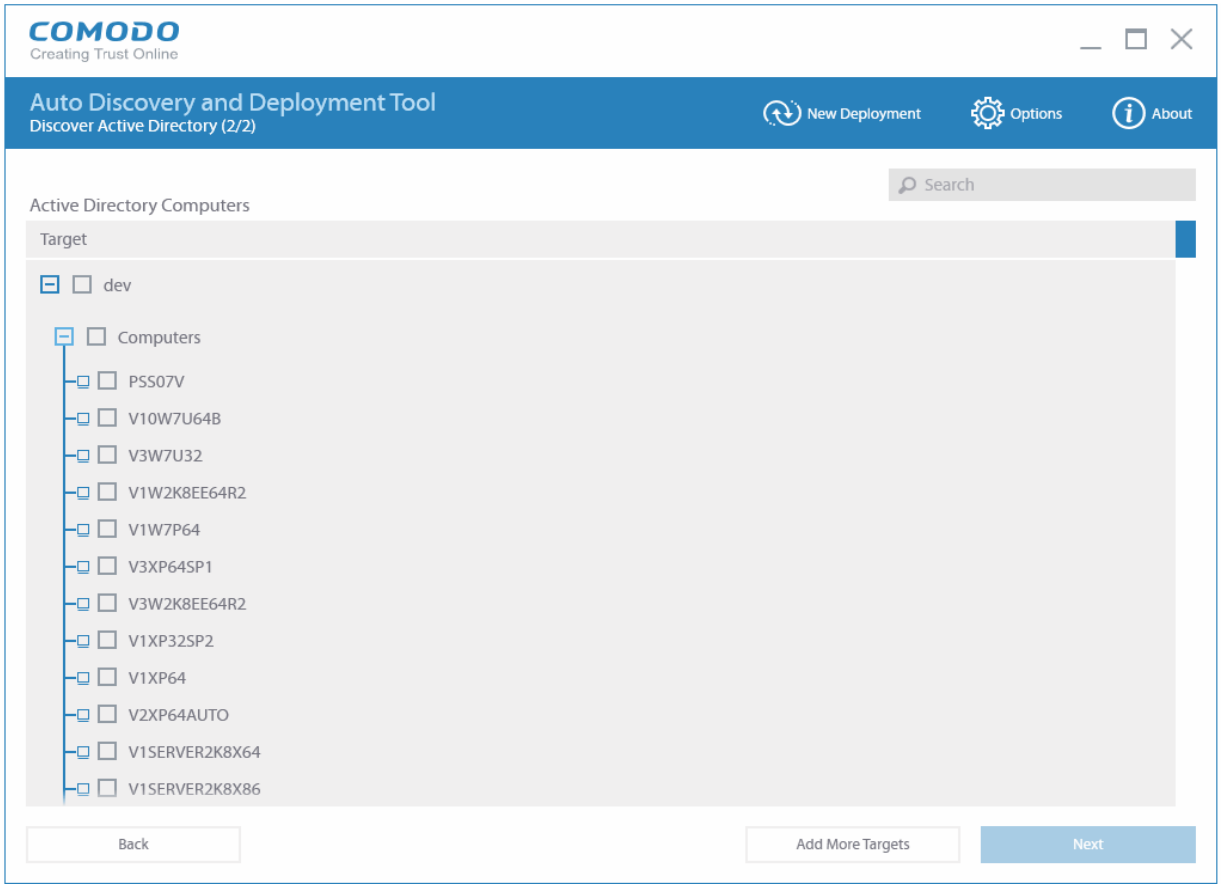
The 'Active Directory' method allows administrators to deploy packages to endpoints from the current domain or a custom domain. To get started:

- If you haven't done so already, upload your packages as shown in **step 2.1**
- Select 'Active Directory' in the 'Discovery Targets' window:

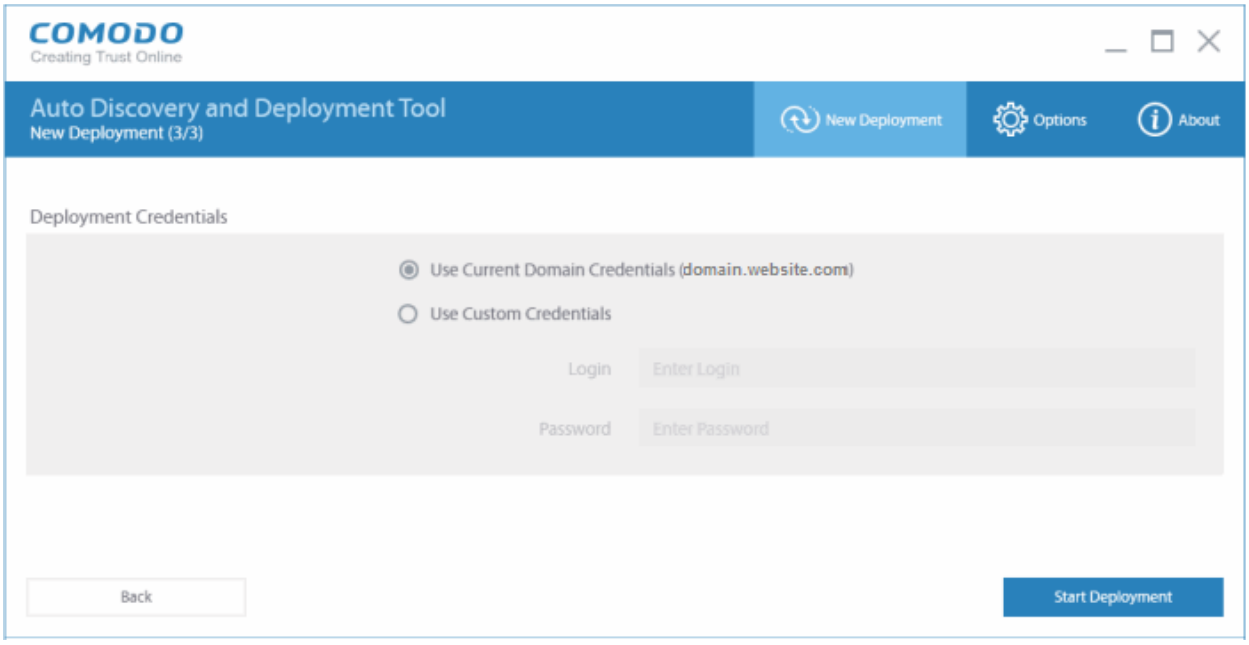


- Select whether you want to use your current credentials or custom credentials
  - Enter the name of your Active Directory domain controller
  - Enter an administrator username and password
  - Click 'Next'

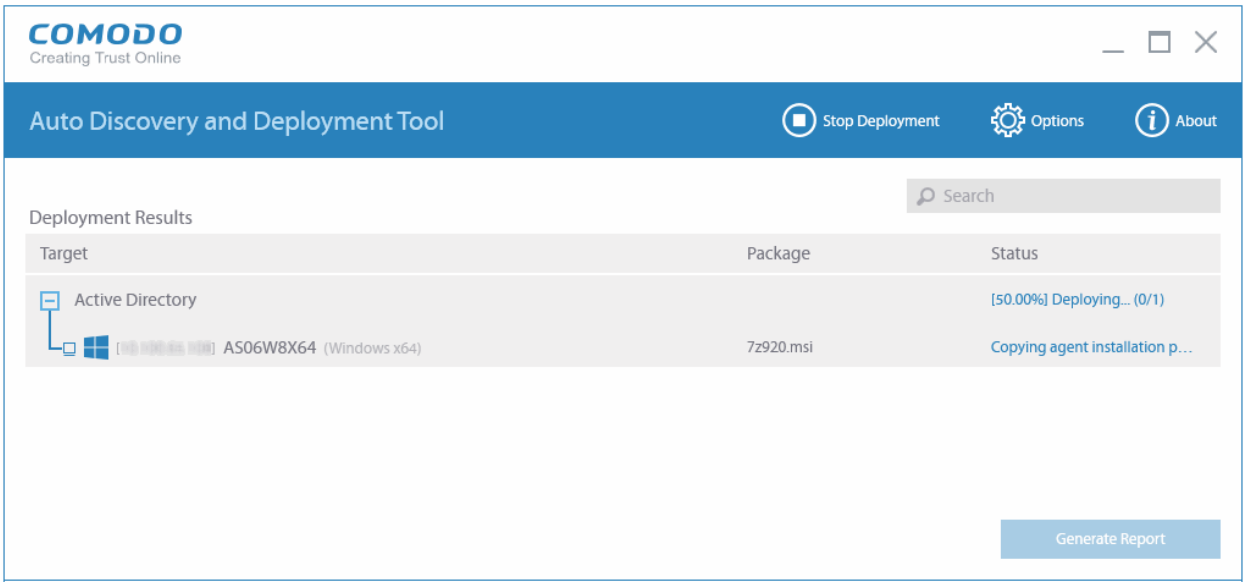
A list of all endpoints in the directory will be displayed:



- Select all target endpoints to which you want to deploy your package
- To search for a particular endpoint, type the name of the endpoint in the search window
- To add more targets, click the 'Add More Targets' on the bottom of the interface. You will be taken to the Discovery Target(s) interface
- Click 'Next' to move onto stage 3 – Deployment Credentials:

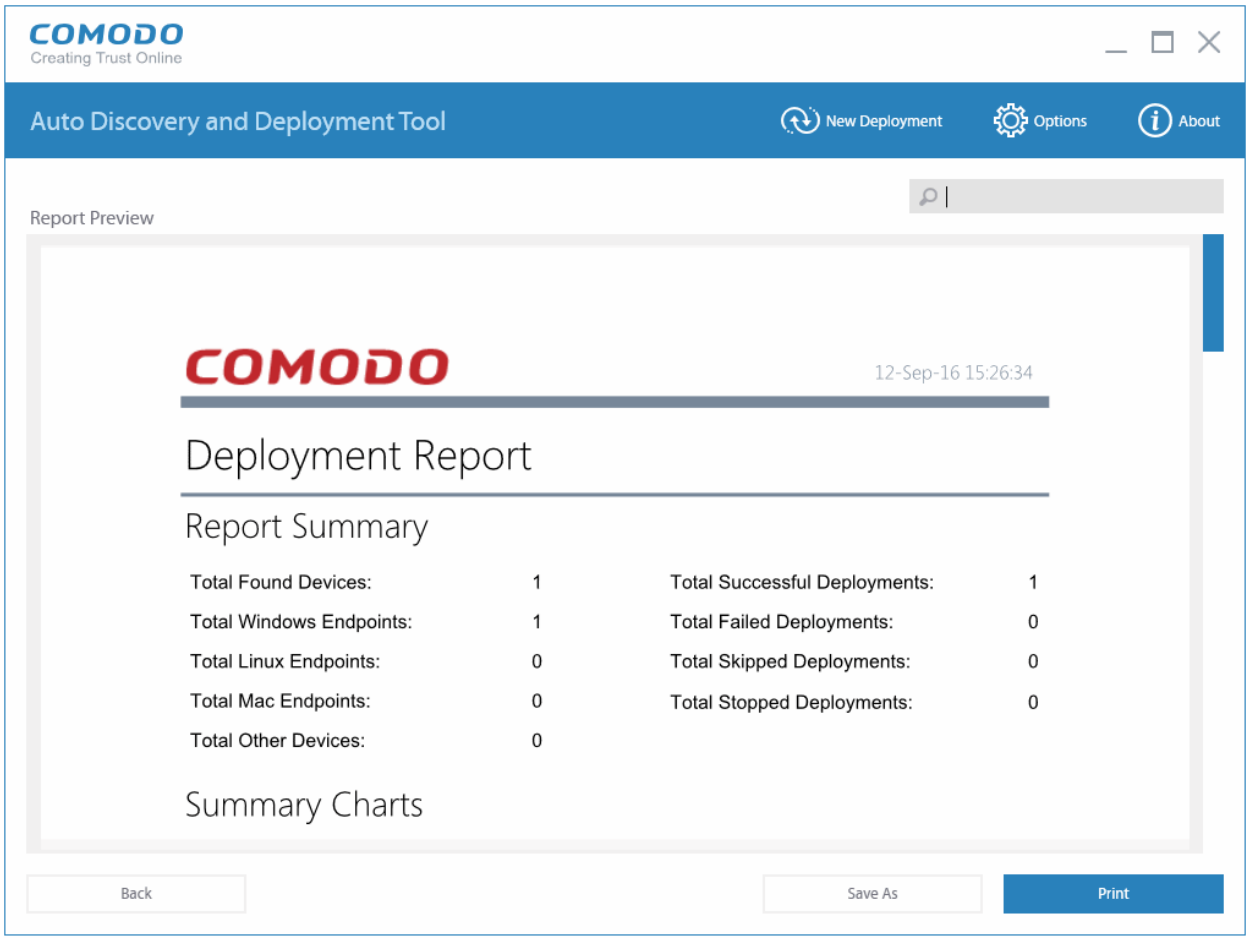


- Use your current administrator credentials to deploy the package, or select 'Use Custom Credentials' and enter an administrators username and password



- Click 'Start Deployment' to initiate the operation. You will see a screen indicating deployment progress. The length of time it takes to deploy the packages depends on the quantity of endpoints and network traffic conditions.
- Click the 'Stop Deployment' button to should you wish to abort the operation
- Once deployment is complete, click the 'Generate Report' button

Scroll down to view the full report.



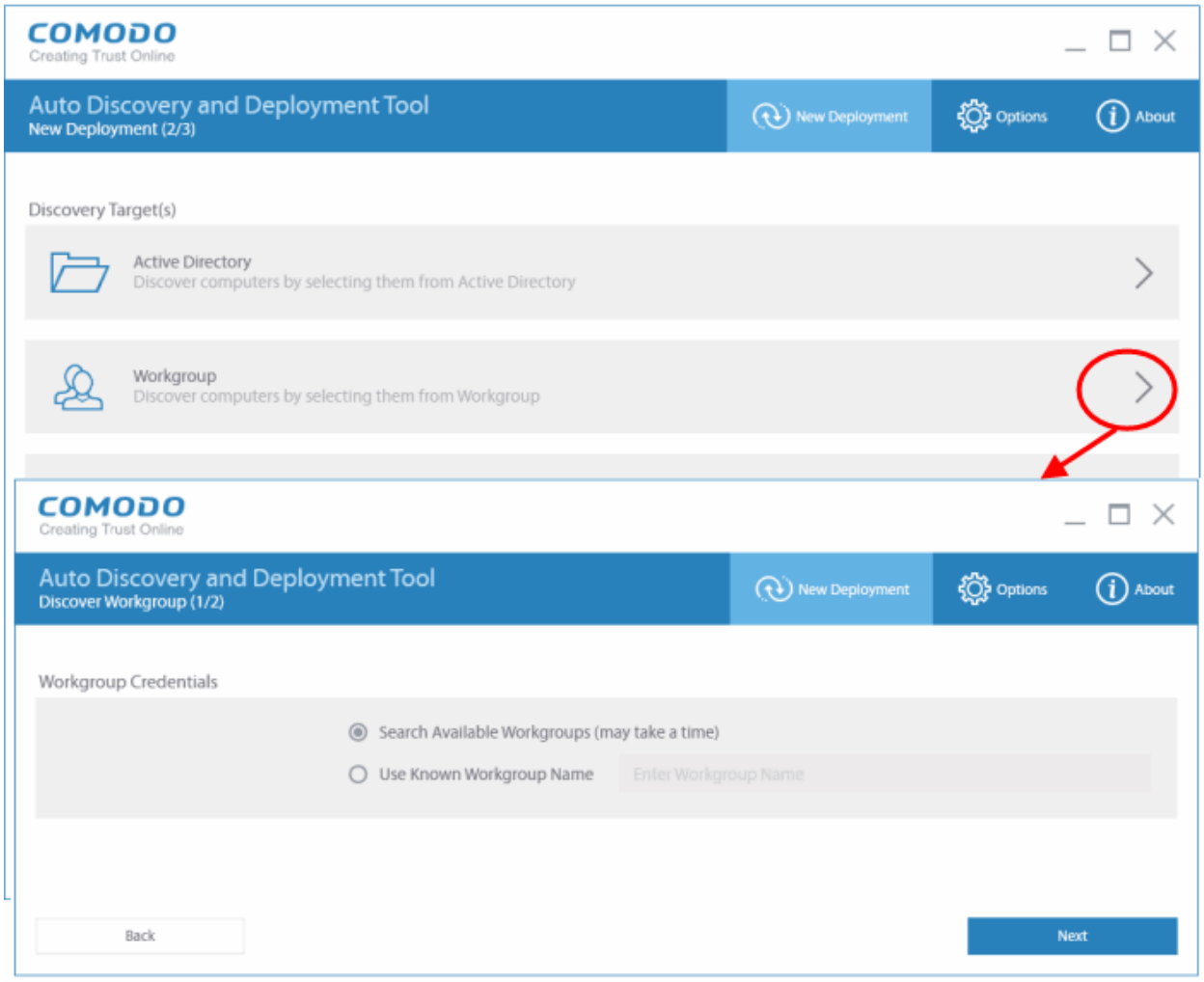
- **Report Summary** – Provides details about the number of devices to which the package was deployed, the date and time of the deployment, and the number of successful/failed deployments
- **Summary Charts** – Displays endpoints by OS type and the status of the deployment
- **Discovered by Active Directory** – Overall summary of scan results, including the number of discovered devices, the OS breakdown of discovered devices and the quantity of deployments which were successful, unsuccessful, skipped or failed.

- Click 'Save' to save the report in .pdf format or click 'Print' to print the report

2.2.2. Deploy Packages to a Workgroup

The 'Workgroup' method allows administrators to deploy packages to multiple endpoints within a workgroup. To get started:

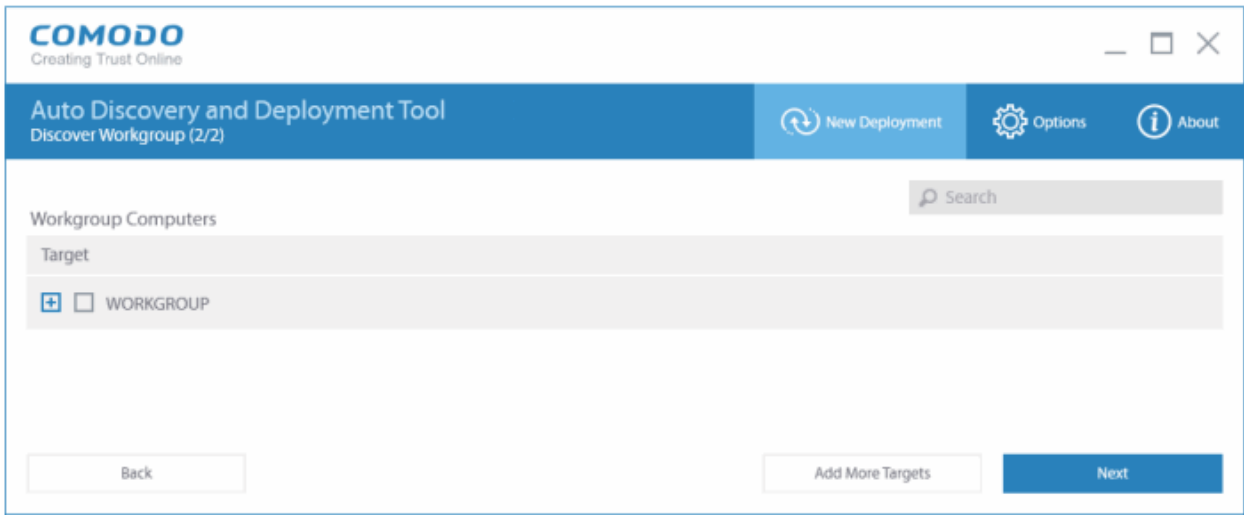
- If you haven't done so already, upload your packages as shown in **step 2.1**
- Select 'Workgroup' in the 'Discovery Targets' window:



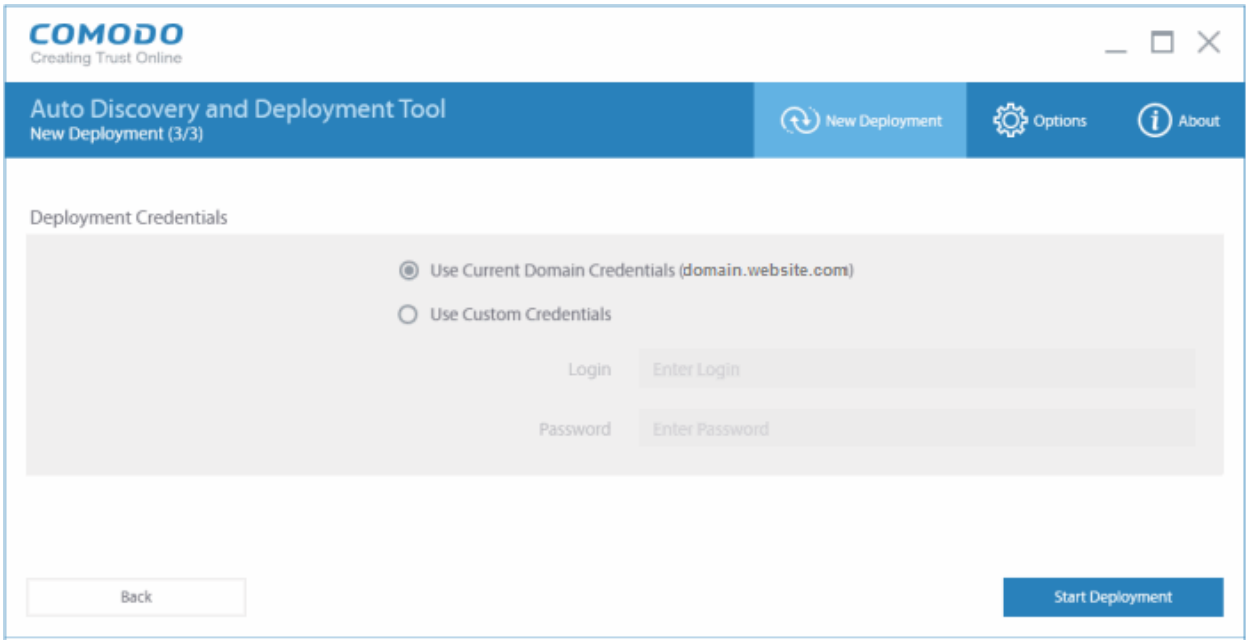
- Search Available Workgroups (may take time) – Automatically discover Workgroups detected on the local network
- Use Known Workgroup Name – Manually specify a Workgroup name. Enter the domain name of your Workgroup

- Click 'Next'

A list of all discovered workgroups will be displayed.

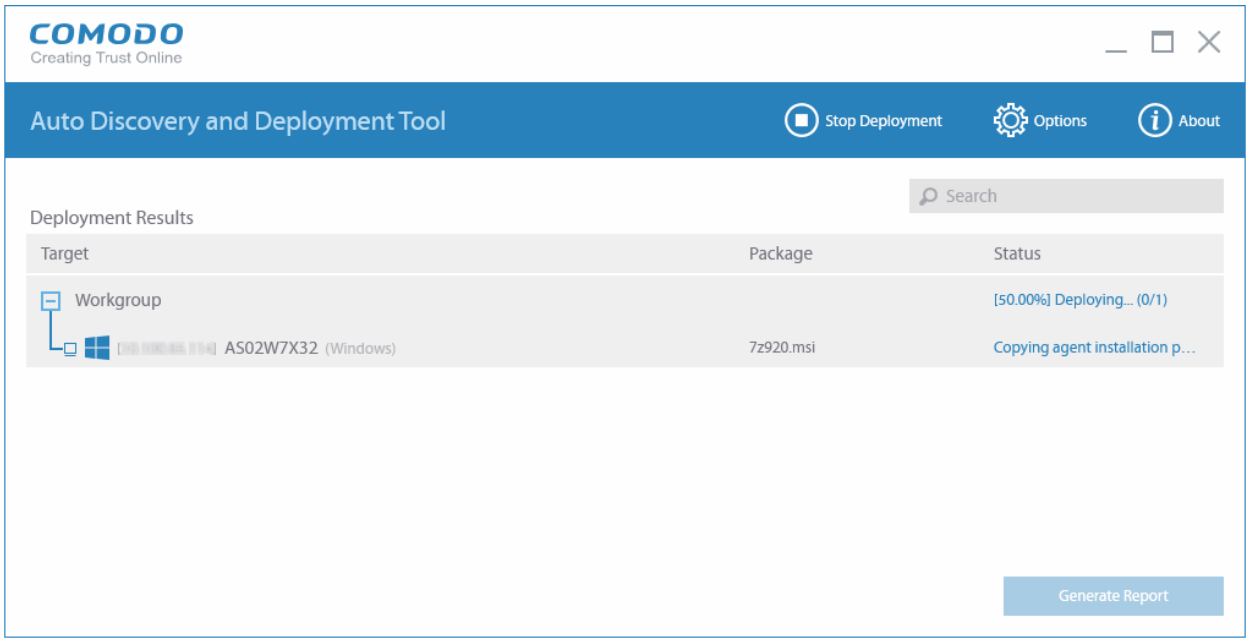


- Select all target endpoints to which you want to deploy your package
- To search for a particular endpoint, type the name of the endpoint in the search window
- To add more targets, click the 'Add More Targets' on the bottom of the interface. You will be taken to the Discovery Target(s) interface
- Click 'Next' to move onto stage 3 – Deployment Credentials:



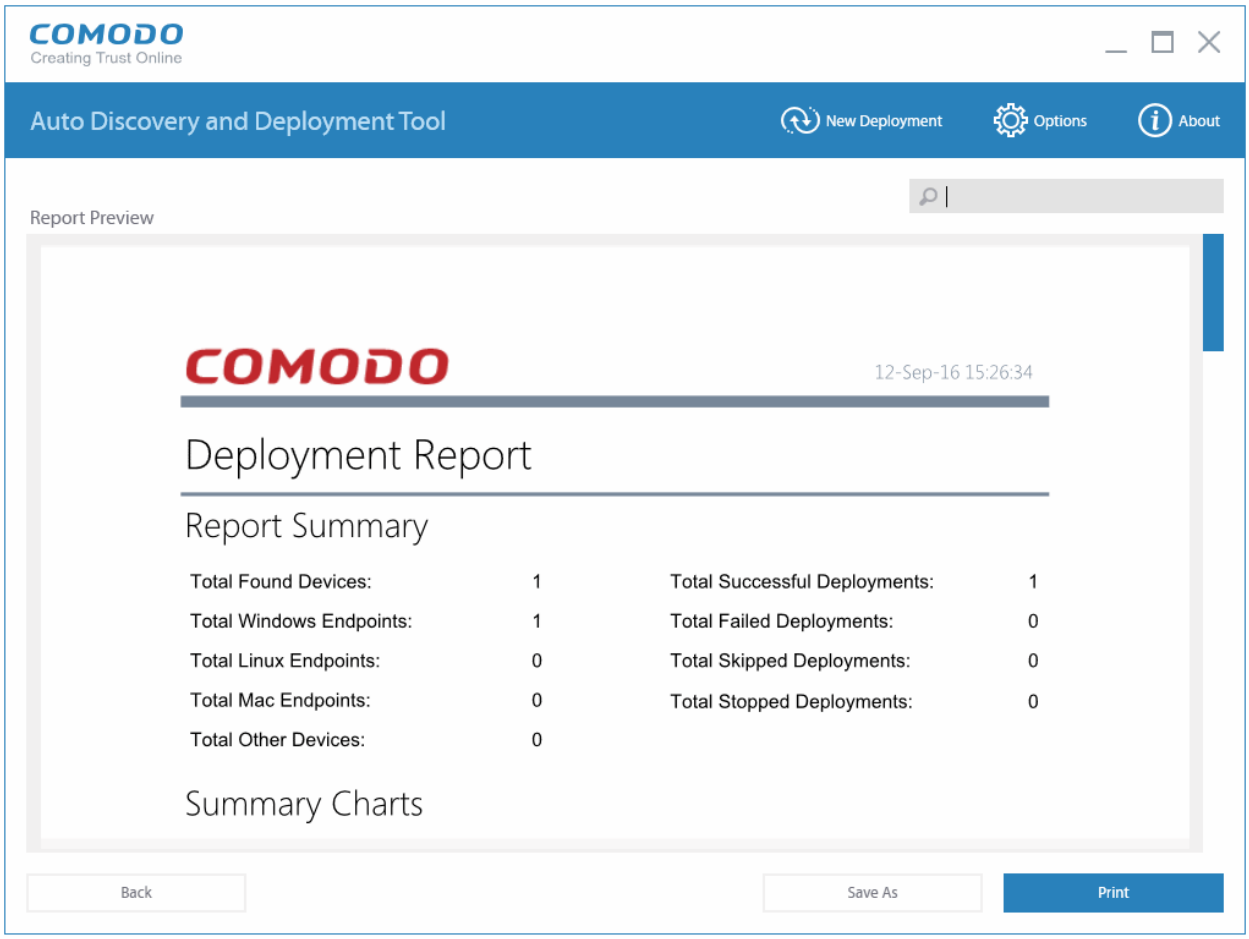
- Use your current administrator credentials to deploy the package, or select 'Use Custom Credentials' and enter an administrators username and password

- Click 'Start Deployment' to initiate the operation. You will see a screen indicating deployment progress. The length of time it takes to deploy the packages depends on the quantity of endpoints and network traffic conditions.



- Click the 'Stop Deployment' button to should you wish to abort the operation
- Once deployment is completed, click the 'Generate Report ' button

Scroll down to view the full report.



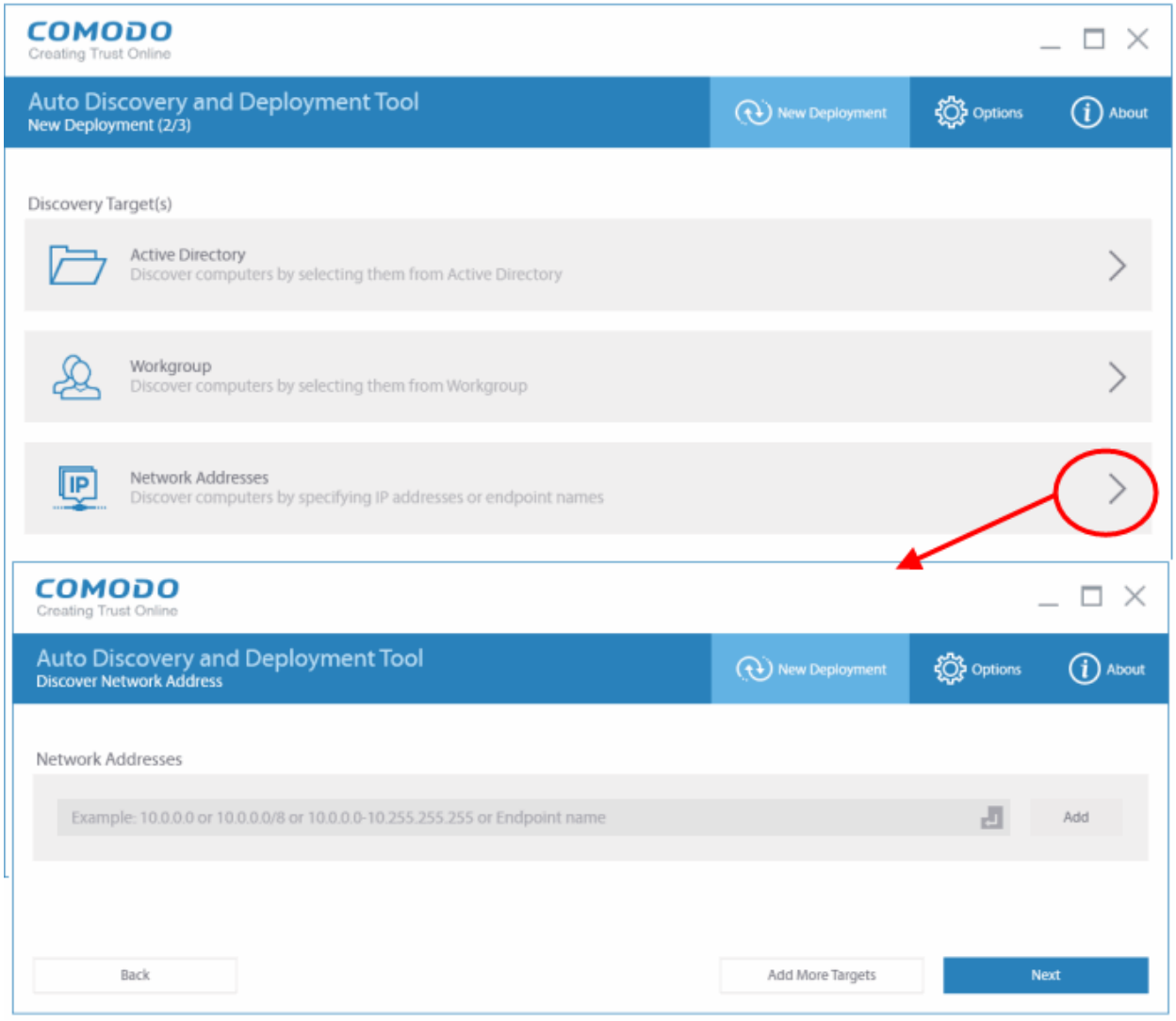
- **Report Summary** – Provides details about the number of devices to which the package was deployed, the date and time of the deployment, and the number of successful/failed deployments
- **Summary Charts** – Displays endpoints by OS type and the status of the deployment
- **Discovered by Workgroup** – Overall summary of scan results, including the number of discovered devices, the OS breakdown of discovered devices and the quantity of deployments which were successful, unsuccessful, skipped or failed.

- Click 'Save' to save the report in .pdf format or click 'Print' to print the report

2.2.3. Deploy Packages Using Network Addresses

The 'Network Addresses' method allows administrators to deploy packages to endpoint by specifying IP addresses, IP ranges or hostnames.

- If you haven't done so already, upload your packages as shown in **step 2.1**
- Select 'Network Addresses' in the 'Discovery Targets' window:



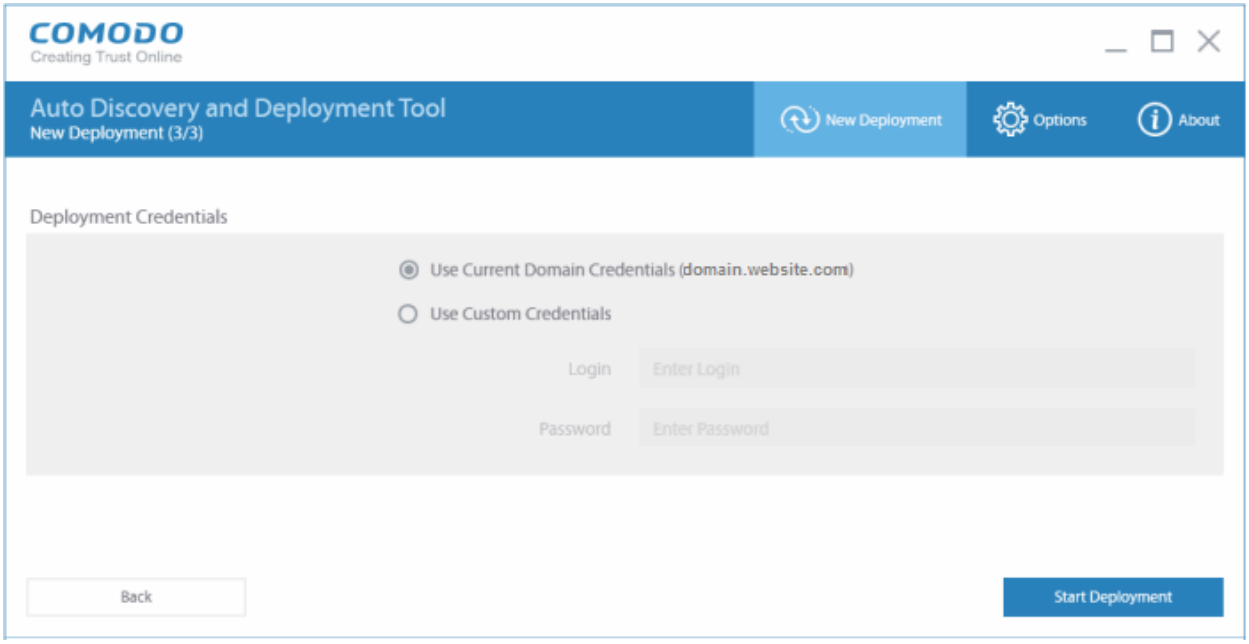
- Network Address: Enter the IP address, IP range or host name as shown below:
  - IP – 10.0.0.1

- IP Range – 10.0.0.1-10.0.0.5
- IP Subnet – 10.0.0.0/24 or 10.0.0.0/255.255.255.0
- hostname-pc

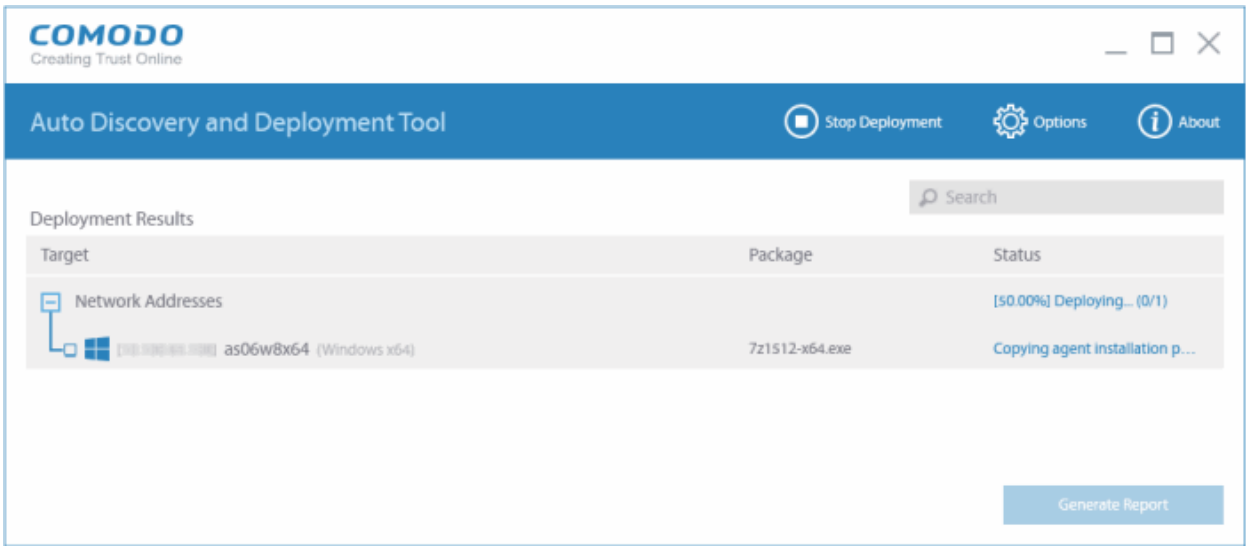
- Click the 'Add' button
- Click 'Add More Targets' to add more endpoints
- To delete an item from the list, click the 'X' beside it

Click 'Next' to go to stage 3 – Deployment Credentials.

- Select whether you want to use your current credentials or custom credentials. You must enter an administrator password to deploy packages to target endpoints:



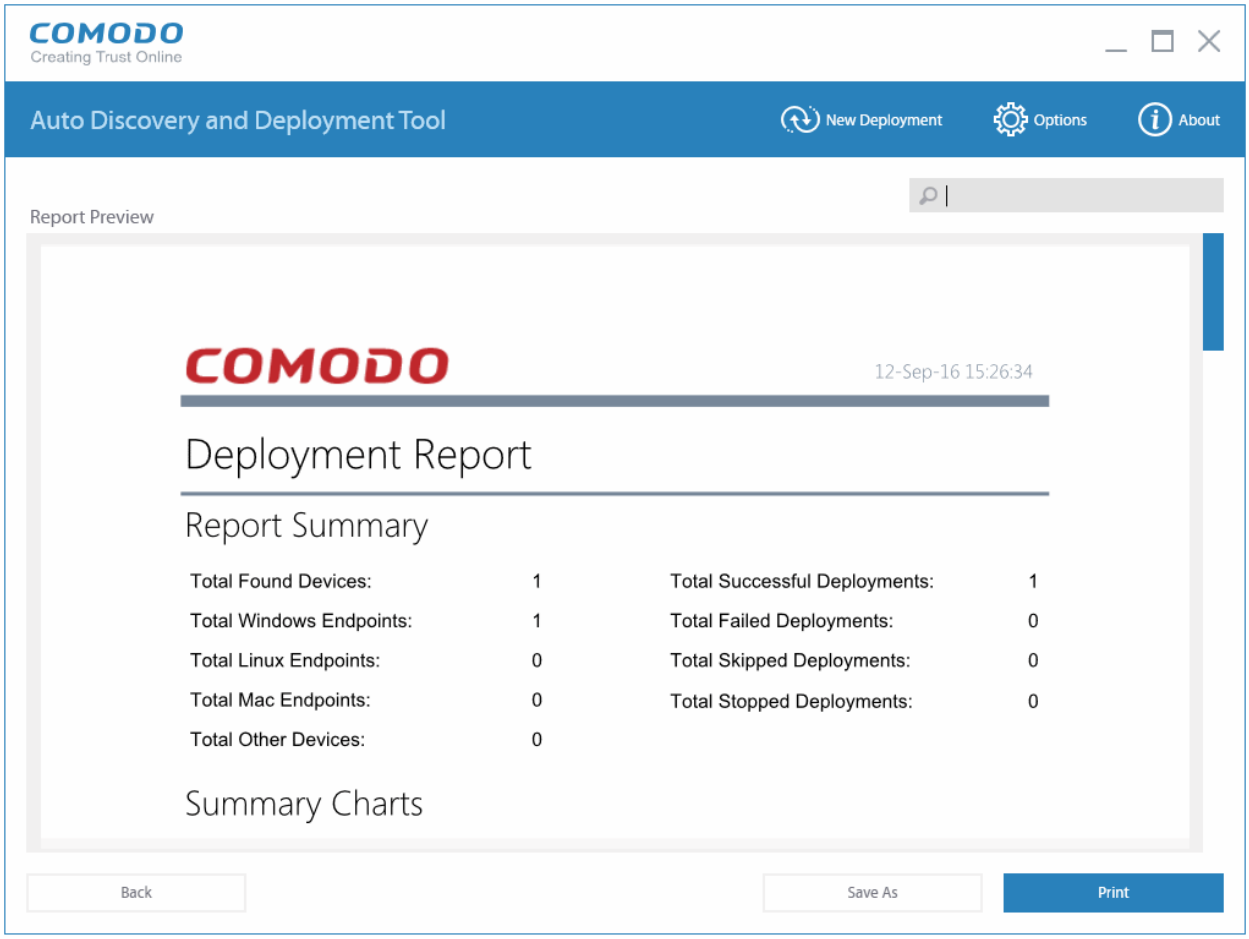
- Click the 'Start Deployment' button to begin the operation. You will see a screen indicating deployment progress. The length of time it takes to deploy the packages depends on the quantity of endpoints and network traffic conditions.



- To search for a particular host, type the name of the endpoint in the search window
- Click the 'Stop Deployment' button to discontinue the deployment process and confirm it in the 'Stop Deployment' dialog.

- Once deployment is completed, click the 'Generate Report' button

Scroll down to view the full report.



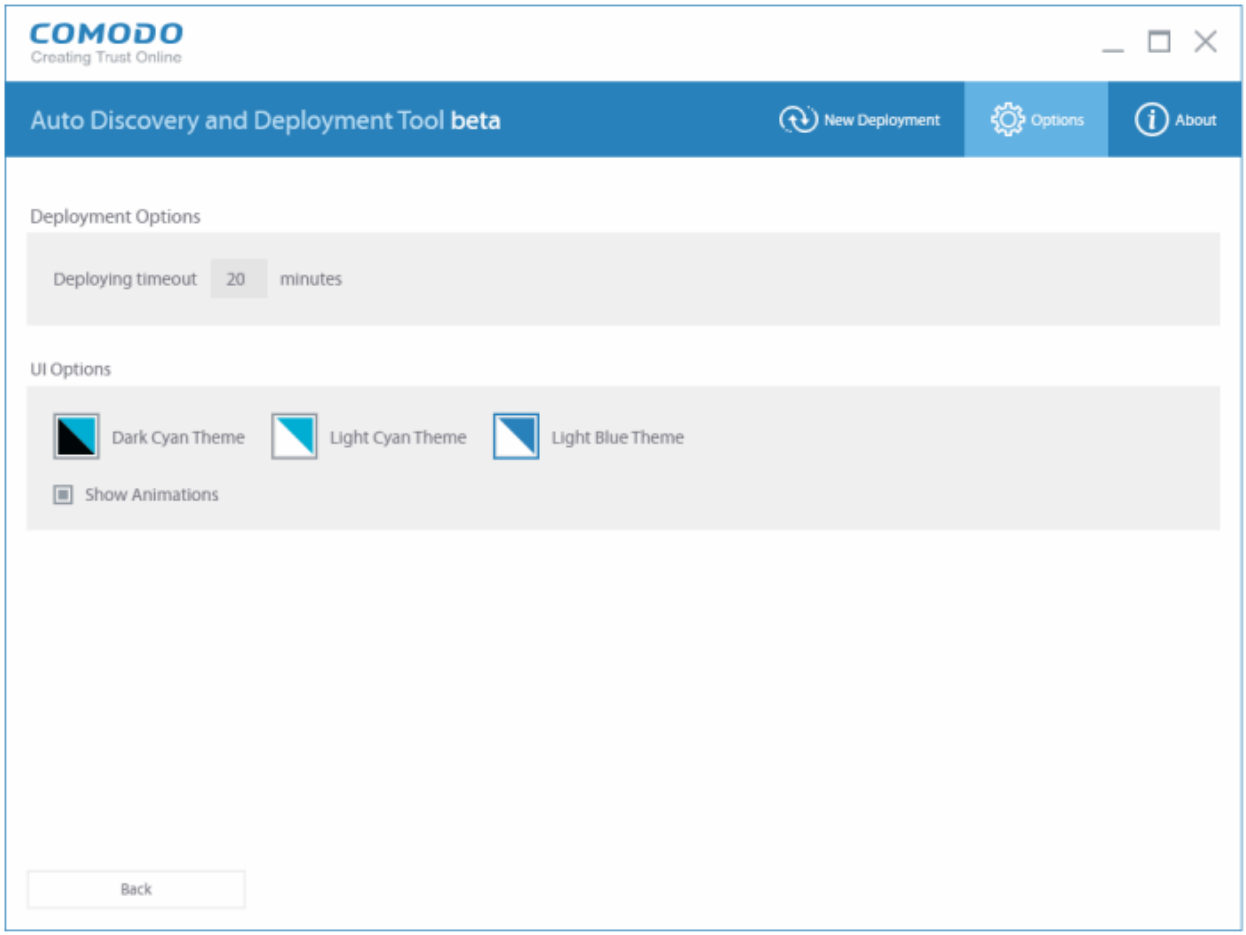
- **Report Summary** – Provides details about the number of devices to which the package was deployed, the date and time of the deployment, and the number of successful/failed deployments
- **Summary Charts** – Displays endpoints by OS type and the status of the deployment
- **Discovered by Network Address** – Overall summary of scan results, including the number of discovered devices, the OS breakdown of discovered devices and the quantity of deployments which were successful, unsuccessful, skipped or failed.

- Click 'Save' to save the report in .pdf format or click 'Print' to print the report

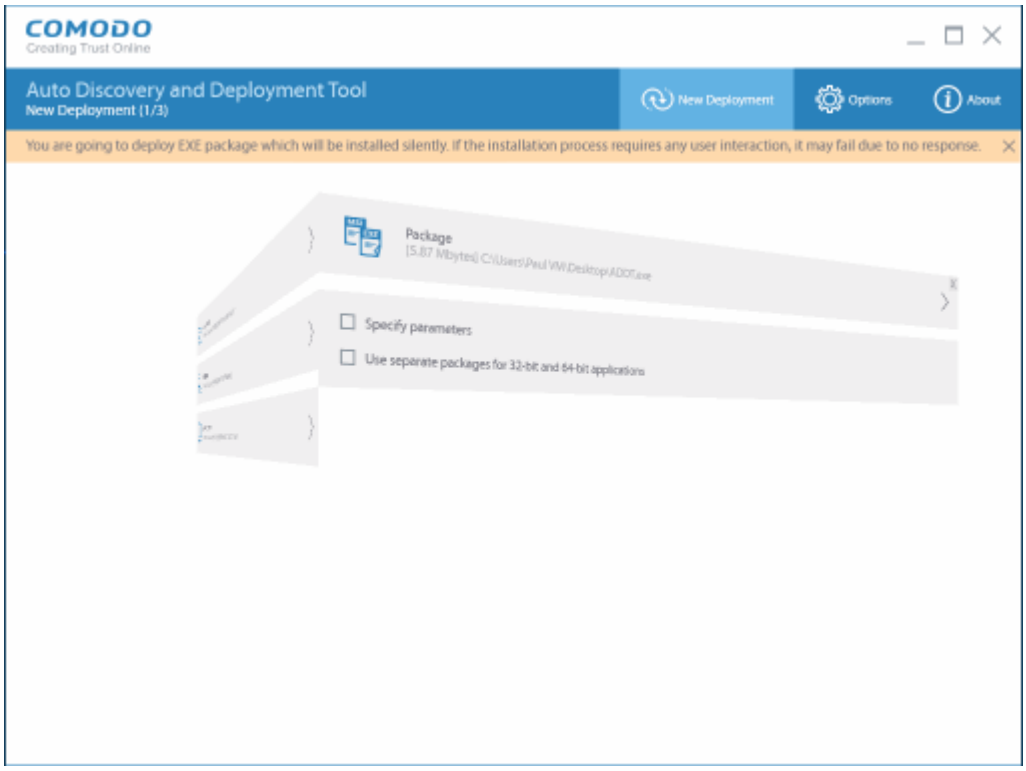
3. CADDT Settings

The 'Options' area in the Comodo Auto Discovery and Deployment Tool allows you to configure deployment and user interface settings.

To access the settings area, simply click the 'Options' link in the title bar.



- Deployment timeout (Default = 20 minutes) – Set the maximum amount of time the deployment should take.
- UI Options – Specify the user interface theme. Choose from Dark Cyan Theme, Light Cyan Theme, Light Blue Theme (Default)
- Show Animations – Show Animations – If enabled, CADDT will display transition animations when the administrator moves between stages or clicks a button in the top menu. (Default = Enabled)

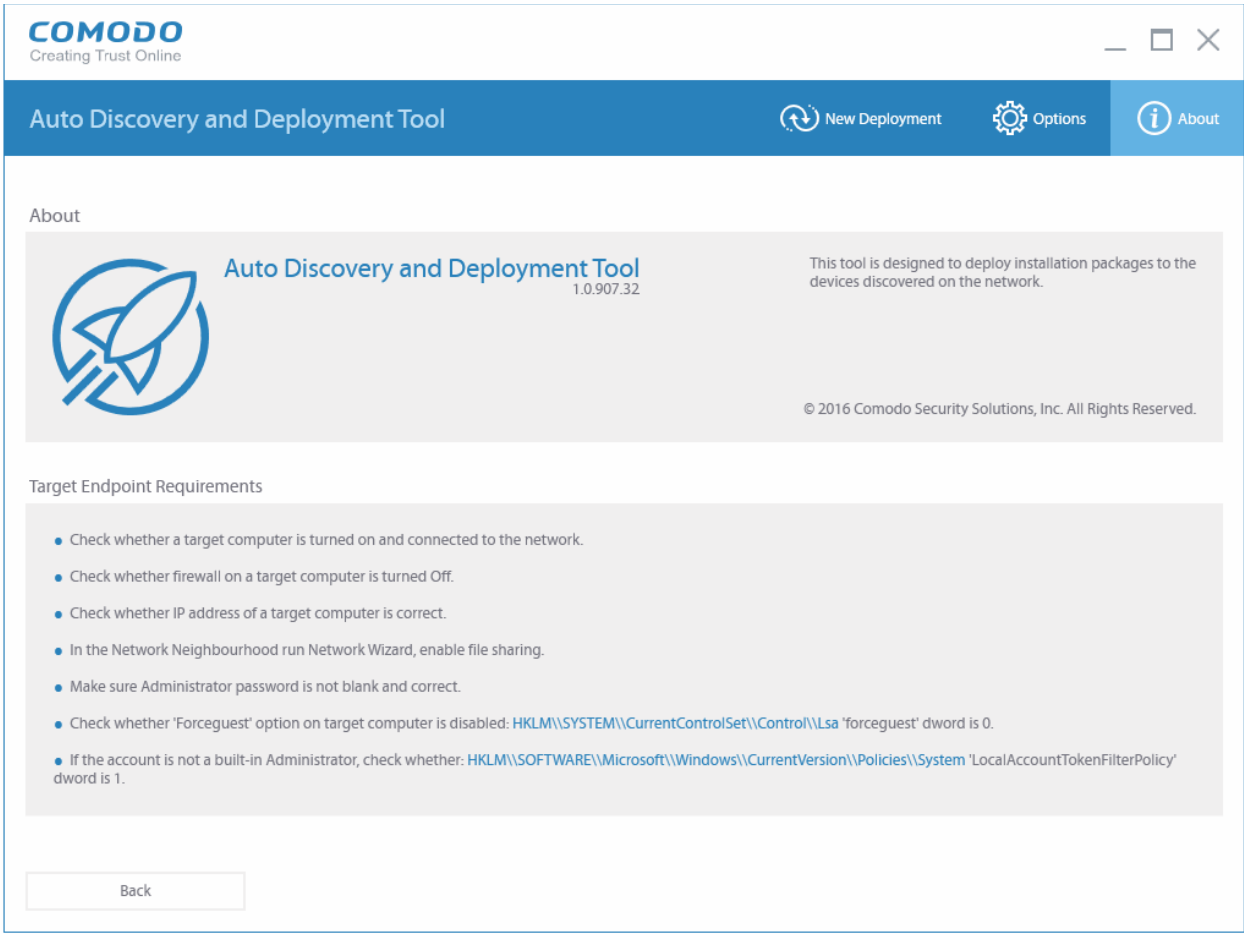


- Click the 'Back' button to return to the 'main deployment interface'

4. About CADDT

The 'About' area interface provides the details of the product, its version number and the target Endpoint requirements.

To view the utility details and requirements, click 'About' from the menu bar.


COMODO
Creating Trust Online
Auto Discovery and Deployment Tool
New Deployment
Options
About
About
Auto Discovery and Deployment Tool
1.0.907.32
This tool is designed to deploy installation packages to the devices discovered on the network.
© 2016 Comodo Security Solutions, Inc. All Rights Reserved.
Target Endpoint Requirements
Check whether a target computer is turned on and connected to the network.
Check whether firewall on a target computer is turned Off.
Check whether IP address of a target computer is correct.
In the Network Neighbourhood run Network Wizard, enable file sharing.
Make sure Administrator password is not blank and correct.
Check whether 'Forceguest' option on target computer is disabled: HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa 'forceguest' dword is 0.
If the account is not a built-in Administrator, check whether: HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System 'LocalAccountTokenFilterPolicy' dword is 1.
Back

About Comodo Security Solutions

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

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

About Comodo Cybersecurity

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

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**