Discovery and Deployment Tool Handbook

Table of Contents

Notices

The usage of the Discovery and Deployment Tool is subject to the Software License Agreement which is located at https://www.threatdown.com/legal/eula/ ("EULA") and are classified as "Optional item" as defined in the Optional Software Utilities, Beta Features and Beta Releases Section of the EULA. As stated in such Section of the EULA, Optional Items are provided "as is", and do not carry any warranties or maintenance or support; similarly, in no event shall we be liable for any damage arising from the use of Optional Items.

Products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal reference purposes only.

This document is provided "as-is." Information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

Windows is a registered trademark of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Third Party Project Usage

This software is made possible thanks in part to many open source and third-party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in software – as well as licenses for each – are available on Third party notices:
https://support.threatdown.com/hc/en-us/articles/4414986433683

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. We do not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

We do not warrant, guarantee, or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. We disclaim all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related thereto.

Introduction

The **Discovery and Deployment tool** assists you with the task of adding endpoints to your Nebula environment. It scans your network and identifies devices suitable for agent deployment. The tool identifies endpoints where the endpoint agent is already installed. Custom criteria are used to discover endpoints and provide a snapshot of your devices prior to deployment.

Once endpoints are identified, you may deploy agents to them. The tool downloads the latest MSI installer package then performs the deployment.

Let's go inside!

Usage Requirements

For the Discovery and Deployment tool to install software on endpoints in your network, your endpoints must meet certain requirements.

For the latest Nebula information, see Minimum requirements for Nebula.

For the latest OneView information, see Minimum requirements for OneView.

External Access Requirements and Exclusions

If your company's internet access is controlled by a firewall or other access-limiting device, you must grant access for endpoint agents to reach our services.

For Nebula access requirements, see Network access requirements for Nebula.

For OneView access requirements, see Network access requirements for OneView.

Program Modes

The Discovery and Deployment tool runs in either interactive (GUI) mode or command line mode. Information regarding command line mode is found in the **Command Line Reference** section located at the end of this handbook.

Before using the Discovery and Deployment tool, be aware of the following:

- The tool must be executed locally, from a Windows computer that has full access to your network endpoints. Attempting to run it from a network drive results in a failure.
- Command line mode has functional limitations when compared to the tool's GUI mode.
- Command line mode is better suited for use with third-party installation tools.
- Parameters specified in command line mode do not carry over to GUI mode.
- The most effective location to run the tool is on the same LAN network segment as your endpoints. This avoids potential routing and firewall issues.

Download and run the tool

To download the Discovery and Deployment tool, you'll need to log into Nebula or OneView.

1. Log in to Nebula or OneView.
2. Go to **Download Center**.
3. Go to **Advanced Tools**.
4. In the **Discovery and Deployment Tool** section, click the **Download** button.

The tool runs on a Windows computer with network visibility to your endpoints and external internet access.

1. Run the downloaded file, `EndpointAgentDeploymentTool.exe`.
2. The **User Account Control** screen displays. Click **Yes**.
3. The **Software License Agreement** displays. Click **I Agree**.
4. Enter your Nebula user credentials. If you are a OneView user, click **Sign in to OneView**, then enter your OneView user credentials. User accounts with Single Sign-On configured are not supported.
5. **Optional**: Configure proxy settings.
    a. Click the **Proxy Settings** link.
    b. Check **Use Proxy**.
    c. Enter your proxy information, then click **OK**.
6. Click **Sign in**.
    a. If you logged in with OneView credentials, select from a list which Site you would like to install/uninstall the endpoint agent on. Change this later with the drop-down menu at the top > **Change site**.
7. You're now logged into the Discovery and Deployment tool!

Note: Any proxy specifications entered here can propagate to endpoints deployed by the tool.

The Proxy Server Address must begin with **http://.**

The Discovery and Deployment tool has three primary functions:

Import Active Directory – Imports your Active Directory structure to group endpoints based on your existing Organizational Units (OUs).

Find endpoints – Discover endpoints based on your criteria, determine where agents are already installed, and deploy new agents according to your specifications. It can also remove unneeded resources from the search protection, such as printers and scanners.

Import Active Directory

The tool imports your Active Directory structure into Nebula or OneView. This enables you to quickly install agents and create groups in the cloud console that mimic your existing configuration.

The Discovery and Deployment tool supports a single Active Directory tree. Active Directory Forests are not supported.

1. Click **Import Active Directory**.
2. The tool uses your credentials to authorize access to the Domain Controller then displays Organizational Units from your Active Directory.
    - If you need to provide a different account, click **Change** at the bottom of the screen.
    - Filter specific OUs as needed using **Search** at the top of the screen.
3. Check the OUs to import.
4. Click **Preview** to show how the OUs appear in Nebula or OneView. A folder icon identifies groups.
5. Click **Apply**. This imports the selected OU as a Group.
6. You can now install agents on computers within the selected OU.

Discover Endpoints

The tool performs a series of checks on each endpoint to determine if it meets system requirements and is available for agent installation.

These checks require ports 135 and 445 to be accessible through the firewall for software probing. Allowing port 137 for the NetBIOS name service is optional.

Here's how we do it.

- Ping – Simple ICMP command to check response from the target endpoint. This is not always reliable because pings can be blocked at the endpoint or across your network.
- DNS – The IP address or hostname are searched on the DNS server the host machine uses. Recent endpoint activity is determined by checking the Time to Live (TTL) result.
- UDP Datagram – A small datagram is sent via UDP to the endpoint, and the tool checks for a response.
- TCP/IP Probe – Critical services checks are made to the endpoint IP using NETBIOS, HTTP, SSH, Telnet, or DNS. While some ports may not respond, it is likely that an online machine will respond to some of these tests. Any response is considered a success.
- Nmap – A powerful multi-purpose open source tool used for network discovery and security auditing. Much endpoint information can be found using this tool.

The following tests determine if an agent has been deployed to the endpoint.

- Remote Registry Detector – Checks if the registry service is available to perform agent installation.
- WMI Detector – Checks if Windows Management Instrumentation (WMI) is accessible for agent installation.
- Service Controller Detector – Retrieves a list of services running on the endpoint.
- Agent Status Check – Queries Nebula using endpoint identity information, looking for evidence of previous agent deployment.

Scan Network

When performing a scan for endpoints, three options are provided. Choose the option that works best for you.

- **Scan Active Directory** - looks for a list of machines in your domain. This is only available if Active Directory is used in your environment.
- **Select IP Range -** allows you to provide search information for endpoints in your network. All details that you enter are used in the search.
- **Import File** - Upload a text file with one endpoint per line.

Endpoint name format

When defining an endpoint via the **Select IP Range** or **Import File** method, you may use any combination of the following formats:

- IPv4 address
- IPv4 address range, like 10.10.10.34–10.10.10.106
- IPv4 address block in CIDR format, like 10.10.0.0/24
- IPv4 address block with mask, like 10.0.0.0/255.255.255.0
- Hostname
- FQDN
- IPv6 address

Below is a text file template for the **Import File** method:

Hostname
Hostname
IPv4 address
FQDN
IPv4 address

Perform the Network Scan

Note: To avoid potentially lengthy timeouts, scan small groups of endpoints at a time, such as 128 per scan.

You can also avoid unused or empty IP ranges for similar results.

1. From the **Home** screen, click **Find endpoints**.
2. Select the method to search for endpoints. Click **Change** to use different network credentials.
3. Enter required information based on the method you selected.

   The tool identifies endpoints that match your criteria and checks each endpoint to determine if the endpoint is online and an agent is already installed.
4. Click **Scan** to continue the search. If network credentials are required to scan the network, you may enter them here.
5. Once the scan begins, the **Deploy Endpoints** screen displays.

As the discovery scan runs, the screen shows matching endpoints discovered and their details. There are two key columns to pay attention to:

- **Status** refers to the current detected endpoint status.
- **Installed** indicates an endpoint agent has been detected on the endpoint.

Click on any field to sort or reverse the sort.

You can filter on-screen results by using the **Search** option. Enter an endpoint name or IP address, or use the search dropdown for additional filtering by endpoint status.

While the scan itself is extremely fast, probing – which detects status, agent status, and OS – takes additional time. The tool probes as many endpoints as possible in a linear fashion.

For example: If **Status** is online and **Installed** is ”?” (Unknown), this may indicate software detection cannot be performed on this online endpoint. It is also possible that missing or incorrect credentials were specified by the user.

Scan Active Directory

Note: Active Directory scans cannot discover Mac endpoints if they are not registered and/or managed by Active Directory. Use one of the other scan options.

Active Directory scans use similar search and AD filter criteria, with the following differences:

- **Search process** – This queries Active Directory for the endpoint list instead of scanning using network criteria.
- **Name** – Displays the full FQDN name.
- **Domain** – Displays Active Directory domain name.

Filtering by Active Directory

If you used the scan active directory method, click on the funnel icon to display the filter window. This filter allows you to drill down and select OUs from your Active Directory structure.

- Check the Organizational Units (OUs) from your Active Directory list.
- Click on **Apply Filter** to apply your OU selection to the scan results.
- You can use both a filter and the **Search** option at the same time.

Before you deploy

Review the following information before you deploy.

Windows endpoints belonging to workgroups

Domain administrators can override User Account Control (UAC) settings on domain endpoints. If an endpoint is a member of a workgroup, additional steps are required.

For more information, read Microsoft's Description of User Account Control and remote restrictions in Windows Vista article.

Remote deployment tips

For best results, follow these tips before you begin deployment.

- Administrator credentials are required to perform remote deployment. A domain account will suffice if the target endpoint is:
    - part of the domain.
    - the domain account used is part of the local administrators group.
- Credentials should be in the form:

  `<IP>\username`

  Or

  `<hostname>\username`
- Files are copied to the `ADMIN$` share on the destination Windows endpoints.
- Access on port 137 must be enabled on the destination Windows endpoints.
- Remote access (SSH) must be enabled on the destination Mac endpoints.
- The installer will not uninstall our consumer product. You should remove this from your Mac endpoints ahead of installation.
- The installer will download the latest Protection Updates.
- The tool must be able to reach our servers to download the latest MSI install package. It also downloads the account token, which is a unique identifier used when software package updates are available.
- If the tool has trouble locating target endpoints, run it from a local LAN segment endpoint to bypass any firewall or network issues.

Technical deployment information for Windows endpoints

The following is technical information related to how Nebula and OneView perform Windows agent deployment. This information may be used for troubleshooting, or just understanding how deployment works behind the scenes. **No action is necessary**.

Deployment Methods

We use a Windows construct called **Named Pipes** to communicate with Windows endpoints. Local admin credentials are used, and ports 137 and 445 need to be accessible. Three files: `EAInstall.bat`, `EAUninstall.bat` and `MBExec.exe` are transferred to the endpoint to either `ADMIN$` or `IPC$`, based on availability. One of the two must be available for this method to succeed.

Deployment with Windows Methods (WMI)

Note: The WMI protocol has specific firewall requirements to allow two-way communication over random ports. For more information, see this Microsoft article.

Windows Management Instrumentation (WMI) is another method we use. It is typically used when our primary method is unsuccessful. If you already use WMI onsite, it will likely be your best choice for deployment.

WMI Deployment uses the `ADMIN$` share. This share is used as a temporary home for files that we retrieve for updating and installing on the endpoint. You may need to enable Remote Management of the endpoint to successfully access the `ADMIN$` share.

Deployment with Windows Methods requires the following:

- Run the Discovery and Deployment Tool as an administrator, using the `-WMIOnly` switch.
- The username for the workstation you run the tool from must match the username on the target endpoint.
- Endpoint port 135 must be available through the firewall.

Deployment outside of your local network

Do not use the Discovery and Deployment Tool to deploy agents to endpoints outside of your local network, including endpoints over VPN. In doing so, ports opened for deployment remain open after deployment is complete, creating a security risk on that endpoint.

Deploying Windows endpoint agents

Deploy on Windows endpoints

Now that you have identified the devices on your network, you may begin deployment.

1. Check the devices you want to install on.
2. Click the **Deploy** button.
3. Monitor the deployment process using the **Tasks** tab. See the Monitor deployment with the Tasks tab section for more information on Tasks.

Deploying Mac endpoint agents

Local Deployment for Mac

To install the endpoint agent manually:

1. From the desired Mac endpoint, run the Endpoint Agent installer.
2. When installation finishes, your Mac displays a **System Extension Blocked** message. Click **OK**.
3. Go to **Security & Privacy** > General tab. Click the **Allow** button.

You must locally click the **Allow** button in order to finish the installation and enable real-time protection. Clicking **Allow** via screen sharing or scripted actions does not work. The **Allow** button disappears after 30 minutes. Restart the Mac to display the **Allow** button again.

Remote Deployment for macOS 11 and above

Computers with macOS 11 or later require deployment of a kernel extension policy to the endpoint.

The kernel extension policy must:

- Have a filename of `com.apple.syspolicy.kernel-extension-policy`
- Be delivered via a user-approved MDM server.

Example policy file:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
 <dict>
  <key>AllowUserOverrides</key>
  <false/>
  <key>AllowedTeamIdentifiers</key>
  <array>
   <string>GVZRY6KDKR</string>
  </array>
  <key>AllowedKernelExtensions</key>
  <dict>
   <key>GVZRY6KDKR</key>
   <array>
    <string>com.malwarebytes.mbam.rtprotection</string>
   </array>
  </dict>
 </dict>
</plist>
```

Take note of the key value, **GVZRY6KDKR**. This key is specific to the real-time protection kernel extension. You may add additional keys for other applications you wish to install that require kernel extensions.

Alternative Method

You may bypass clicking **Allow** during manual install if your endpoint meets these requirements.

- Not enrolled in DEP
- Is enrolled in DEP but doesn't have a DEP-deployed MDM

To whitelist the kernel extension, perform the following steps:

1. Restart the endpoint in **Recovery Mode**.
2. Open the **Terminal**.
3. Enter the following command:

```
spctl kext-consent add GVZRY6KDKR
```

This whitelists the kernel extension on that machine. You can utilize this technique with NetBoot, NetInstall, and NetRestore images.

For more information on macOS Recovery, see the following Apple article.

- About macOS Recovery

Additional Information

For more information, refer to the following articles.

- User Approved Kernel Extension Loading
- Kernel Extension Policy
- Create a NetBoot, NetInstall, or NetRestore volume

Monitor deployment in the tasks tab

Once deployment is underway, use the **Tasks** tab to monitor deployment progress.

This tab is divided into two sections. The left side of the **Tasks** screen shows a quick status of install/uninstall activity. Click a category to expand it for additional information.

The right side of the **Tasks** screen shows each Host Name, IP Address, Status, and a link to the current logs. There are two log types:

- a log for each endpoint deployment
- a log for the tool itself, located at `C:\ProgramData\ThreatDown Discovery and Deployment\Logs\ea-pushdeploy-log.txt`

Status values:

- **Running –** Installation is currently being performed.
- **Success –** Installation has successfully completed.
- **Failure –** Installation failed. Click **View Log** to see the reason for the failure.
- **Queued –** Endpoints are waiting for sufficient resources to become available to run the install process.

Tip: If the endpoint agent fails to install, verify all unmanaged or consumer products are removed from the endpoint.

Uninstall and Repair endpoint agent

With the endpoint agent installed, your devices are now protected. If you run into an issue that requires you to remove or repair the endpoint agent, this can be done with the Discovery and Deployment tool. This should be used as a last resort when the standard removal and repair process is unsuccessful.

Uninstall endpoint agent

Uninstalling the endpoint agent from the Discovery and Deployment tool allows you to remotely remove endpoints. This includes endpoints that are unable to communicate with Nebula. The Tamper Protection password is not required when uninstalling with this method.

1. Check the devices you want to uninstall on.
2. Click the **Uninstall** button.
3. Monitor the task using the **Tasks** tab.

Common messages and errors

There are many messages that may display on screen or in the Discovery and Deployment Tool log files. This section of the handbook acts as a reference for clarifying messages that may appear.

Waiting for Deployment Resources Try Again

The deployment tool places installers into the following directory:

`x:\ProgramData\ThreatDown Discovery and Deployment\RemotePush\`

The request for these installers will show as queued until these files finish downloading:

- `Setup.MBEndpointAgent.msi`
- `Setup.MBEndpointAgent.x64.msi`

ErrorMessage:System.IO.IOException: An attempt was made to logon, but the network logon service was not started

In order to authenticate users and services, the Microsoft service **Netlogon** maintains a secure channel between the target endpoint and the domain controller.

- If Netlogon is stopped, the endpoint may not authenticate users and services, and the domain controller cannot register DNS records.
- If Netlogon is disabled, any services that depend on it fail to start.

Resolution: Check and start the service on the target endpoint.

ErrorMessage:System.UnauthorizedAccessException: Access to the path '\\xxx.xxx.xxx.xxx\ADMIN$\MBRemoteExec-ppppp-hostname.exe' is denied

The supplied username or password credentials are incorrect.

- For your site, try the username `domain\domainadmin`.
- For non-domain sites, the username `127.0.0.1\ADMINISTRATOR` is necessary. There are prerequisites to using non-domain sites.

ErrorMessage:WMI Technique: Error in Wmi Deploy technique for target: Host name: host.domain; Domain name: domain; . Error: System.Runtime.InteropServices.COMException (0x800706BA): The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)

WMI is used to initiate the installation service, but the service is not available or not responding.

WMI connects to an endpoint, but random ports are used for responses from that endpoint. Therefore, configure your firewalls to properly pass information from the endpoint over those random ports.

For additional information, see Deploy endpoints to Nebula with Microsoft Group Policy.

.

ErrorMessage:Error copying files out to the admin share of: Host name: xxx.xxx.xxx.au; Domain name: xxx.xxx.au; IP Address(es): IP Address: 10.0.0.115, ; : Error: Unknown, 53

This often relates to Windows error message: **System Error 53 Has Occurred. The network path was not found**.

Resolution: Troubleshoot why the network share ADMIN$ cannot be mounted.

Deployment returns "Successful" to the Discovery and Deployment Tool, but the tool does not continue.

Try the following steps:

- Check the logs. If the section following `***** MSI LOGS ****` is empty, MSI has failed to start.
- Manually run **Add/Remove Programs** on the endpoint to check if there is an unfinished installation or uninstallation. If so, complete the installation or uninstallation.
- Check that your Windows directory does not have the following files orphaned from a previous run. If the files exist, delete them and try again.
    - `Setup.MBEndpointAgent.msi`
    - `Setup.MBEndpointAgent.x64.msi`

The Discovery and Deployment Tool cannot connect to cloud.malwarebytes.com when run on Windows Server 2008

By default, Internet access is locked down on Windows Server 2008.

Try the following steps:

- To disable lockdown, see the article Disable Internet Explorer Enhanced Security Configuration (IE ESC) in Windows Server 2008 R2.
- Run the Discovery and Deployment Tool from a different endpoint on your network.

The Discovery and Deployment Tool reports a successful installation, but the endpoint is not showing in Nebula

The `MBEndpointAgent` service continues to run in order to complete the installation. Review the `MBEndpointAgent` log for errors and connectivity issues.

Find log entries at the following locations:

- **Windows Vista and later**: `%systemroot%\documents and settings\administrator\malwarebytes endpoint agent\logs`

Command Line Reference

Commands have the structure:

```
EndpointAgentDeploymentTool -<switch1> <value1> [-<switchn> <valuen>]
```

Example

A silent installation performed on three endpoints, two identified by name and one by IP address. The results of the installation process is saved to a file for later inspection.

```
EndpointAgentDeploymentTool -Action=install -
User=owner@malwarebytes.com -Pwd=MyNebulaPassword -
targetUser=Corp\targetUserName -targetPwd=MyPassword -
Results=c:\files\installresult.txt -
computers=Computer1;Computer2;10.1.1.2;
```

Arguments

The following arguments are available when using command line mode.

-action

Deployment action that the program will perform on the endpoint. Valid values are install and uninstall.

-computers

List of computers used in discovery. While discrete computer names or IP addresses may be specified here, IP address ranges may also be used. Entries should be separated by semicolons (;).

-file

Location of a file which contains endpoint identity information used in discovery. Refer to **Scan Network** section for more details.

-nebulauri

URL of the our server. Default value is https://cloud.threatdown.com.

-proxybypass

Specifies whether the proxy can be bypassed on communications on the local network. Valid answers are **yes/no**, **true/false**, or **1/0**. Only valid if **-proxyuse** is set to {**yes**|**true**|**1**}, and is ignored if **-proxyuse** is {**no**|**false**|**0**}.

-proxypassword

Password associated with **-proxyuser** for internet access through a proxy. Only valid if **-proxyuse** is set to {**yes**|**true**|**1**}, and is ignored if **-proxyuse** is {**no**|**false**|**0**}.

-proxyport

If -proxyuse is set to {yes|true|1}, this is the port number associated with proxy server access to the Internet. It is ignored if -proxyuse is {no|false|0}.

-proxyssl

Specifies whether SSL encryption should be used for Internet access through a proxy. Valid answers are yes/no, true/false, or 1/0. Only valid if -proxyuse is set to {yes|true|1}, and is ignored if -proxyuse is {no|false|0}.

-proxyurl

If -proxyuse is set to {yes|true|1}, this is the FQDN or IP address of the proxy server to be used for Internet access. It is ignored if -proxyuse is {no|false|0}.

-proxyuse

Specifies whether a proxy server is required for connection to the server. Valid answers are yes/no, true/false, or 1/0. If no action is specified, the proxy settings are not applied.

-proxyuser

Username to be used for Internet access through a proxy. Only valid if -proxyuse is set to {yes|true|1}, and is ignored if -proxyuse is {no|false|0}.

-pwd

Password associated with <user>.

-results

A valid file path/name where results of the specified action should be stored. This allows install/uninstall activities to be performed in a silent manner.

-targetpwd

Password associated with <targetuser>.

-targetuser

Username that will be used for agent deployment on endpoints.

-user

User name for login to the server.

-wmionly

If present, only WMI methods will be used for endpoint discovery.