Malwarebytes | CLOUD

Discovery and Deployment Tool
User Guide

Version 1.0

24 April 2017

Malwarebytes

Notices

Third Party Project Usage

Malwarebytes 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 Malwarebytes software – as well as licenses for each – are available on the following page.

https://www.malwarebytes.com/support/thirdpartynotices/

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. Malwarebytes does 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.

Malwarebytes does 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. Malwarebytes disclaims 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 there to.

Introduction

The *Malwarebytes Discovery and Deployment Tool* is designed to accomplish two tasks. First is to discover all endpoints on your network. Second is to deploy Malwarebytes protection agents onto endpoints which have been identified. The tool may be used by any customer using the *Malwarebytes* cloud platform.

System Requirements

Following are minimum requirements for a computer which will host the *Discovery and Deployment Tool*. Please note that these requirements do not include other functionality that the host is responsible for.

- **Operating Systems/Application Frameworks:**
  - Windows 10 (32/64-bit)
  - Windows 8.1 (32/64-bit)
  - Windows 8 (32/64-bit)
  - Windows 7 (32/64-bit)
  - Windows Vista (32/64-bit)
  - Windows Server 2016
  - Windows Server 2012/2012 R2
  - Windows Small Business Server 2011
  - Windows Server 2008/2008 R2 (32/64-bit)
  - .NET 4.5.2 or 4.6 installed

  PLEASE NOTE: Windows servers using the Server Core Installation process are specifically excluded

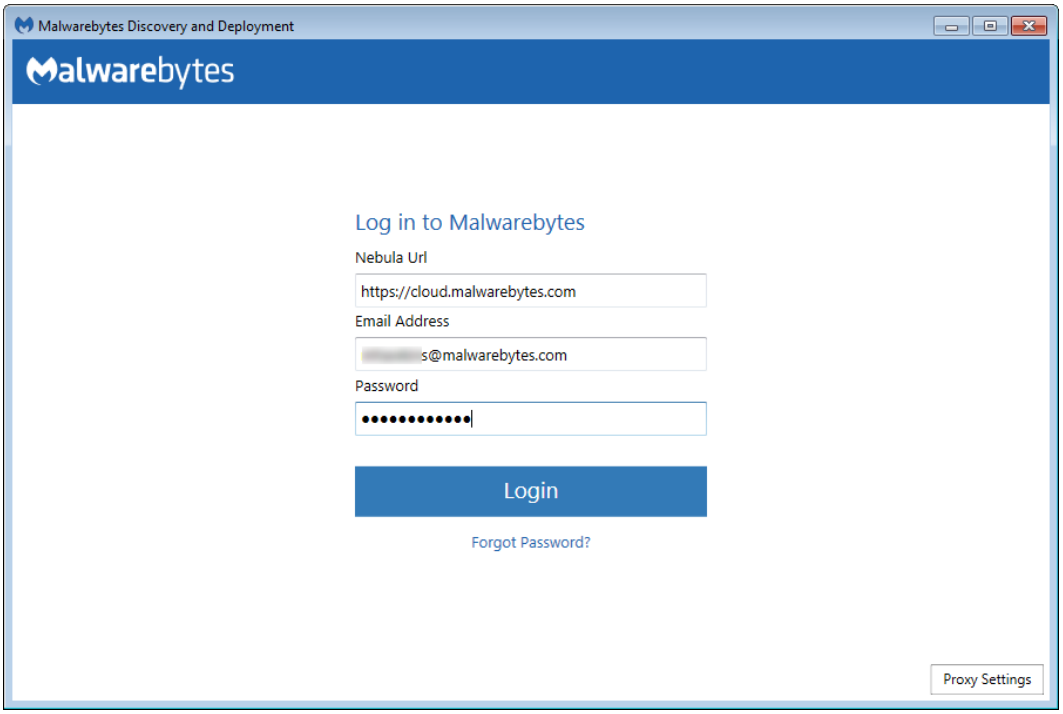
- **CPU:** 800 MHz or faster
- **RAM:** 256 MB (512 MB or more recommended)
- **Free Disk Space:** 20 MB
- **Screen Resolution:** 800x600 or higher
- **Active Internet Connection**

Program Modes

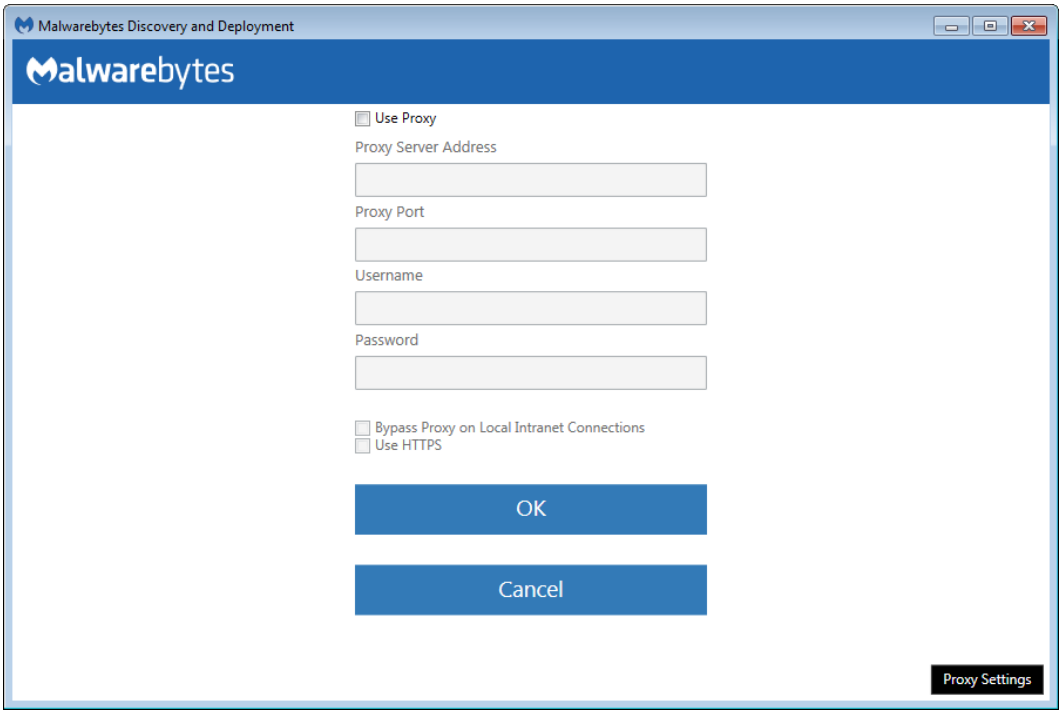
The *Discovery and Deployment Tool* can perform its tasks in both GUI mode and command line mode. Please refer to pages 10-11 for command line operation.

Login

To gain access to the *Malwarebytes* cloud platform, a login is required. This login specifies the identity of your environment, and your identity. A screenshot of the Login screen is shown below. Please note that the URL shown here may be different than what is shown here..



If you are attempting to access the *Malwarebytes* cloud platform from a restrictive network, you may need to use proxy settings to gain access to the Internet. The proxy screen (as shown below) is accessible from the **Proxy Settings** button in the lower right corner of the Login screen. No settings are enabled until the **Use Proxy** checkbox is clicked.



Discovery

Before an agent can be deployed to an endpoint, target endpoints must be identified. The following section provides a brief rundown on how we do that.

Who to Discover

We provide three methods of accomplishing this goal, with discovery results validated by several possible methods. Only one method is required.

- **Method 1 –** Query Active Directory for a list of machines in the domain. If you do not use Active Directory in your company, this is clearly not the best choice.
- **Method 2 –** A Network Scan allows you to provide search criteria for endpoints in your network. You can specify several different criteria, and all will be tested. Criteria includes:
    - IPv4 address
    - IPv4 address range, with minimum and maximum values specified (e.g. 10.10.10.34-10.10.10.106)
    - IPv4 address block, in CIDR format (e.g. 10.10.1.1/16)
    - IPv4 address block, with mask (e.g. 10.1.1.1/255.255.255.0)
    - Hostname
    - FQDN
    - IPv6 address
- **Method 3 –** A text file containing a list of endpoints using criteria as listed for method 2.

How We Discover

For each endpoint we have identified as part of our target group, we determine if they are available for agent installation. Please note that the majority of the tests listed here require ports to be accessible through the firewall. Here's how we do it.

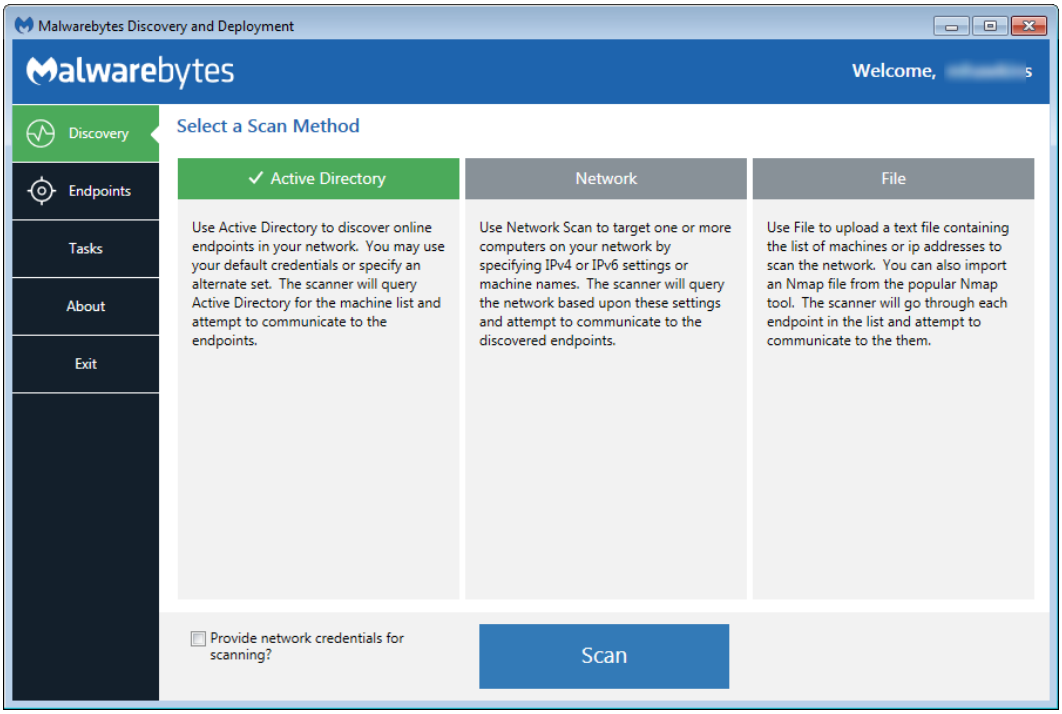
- **Ping –** This is a simple ICMP command which requests the target endpoint to respond. Endpoint configuration or network topology may block pings, so alternative means would be needed to reach those endpoints.
- **DNS –** The IP address or hostname specified in discovery criteria will be searched in the A record of the DNS server used by the host. The Time to Live (TTL) indicates an endpoint which is online or has been online recently.
- **UDP Datagram –** The program will attempt to send a small datagram via UDP to the endpoint, as well as receive a datagram from the endpoint.
- **TCP/IP Probe –** Using the endpoint's IP address, attempts to communicate with several ports associated with critical services (NETBIOS, HTTP, SSH, Telnet, DNS, etc.). While some ports may not respond, it is likely that a machine which is online will respond to some degree. A response to any attempt is considered a success.
- **Nmap –** A powerful multi-purpose open source tool used for network discovery and security auditing. Much information about an endpoint can be found using this tool.

These final tests are used to determine whether an agent has been deployed to the endpoint, checking from the perspective of the endpoint as well as the *Malwarebytes* server.

- **Remote Registry Detector –** Determines whether this service is available to the program, this enabling ability to perform agent installation.
- **WMI Detector –** Determines whether Windows Management Instrumentation (WMI) is accessible to the program for agent installation.
- **Service Controller Detector –** Access to the Service Controller allows the program to get a list of services running on the endpoint.
- **Agent Status Check –** Using endpoint identity information, the program will query the *Malwarebytes* server with that identity information, looking for evidence of a previous agent deployment

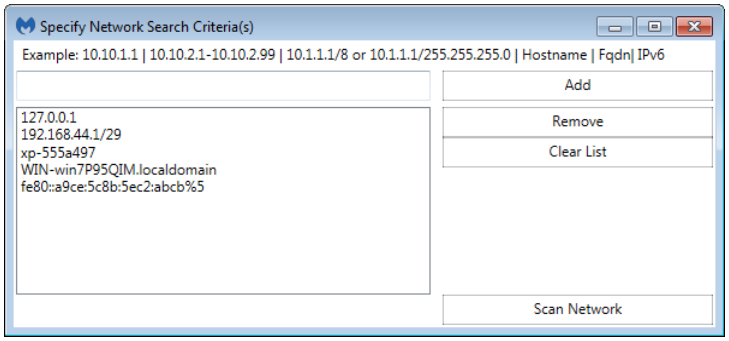
Scan

After specifications have been provided by the user, the *Discovery and Deployment Tool* will go through the list of endpoints which fit criteria, and using the discovery techniques listed above, determine which endpoints are online and which have an endpoint agent already installed. All that is required of the user is a simple press of the **Scan** button. If network credentials are required to scan the network, you may enter them here. The Scan screen looks like this:



Endpoints

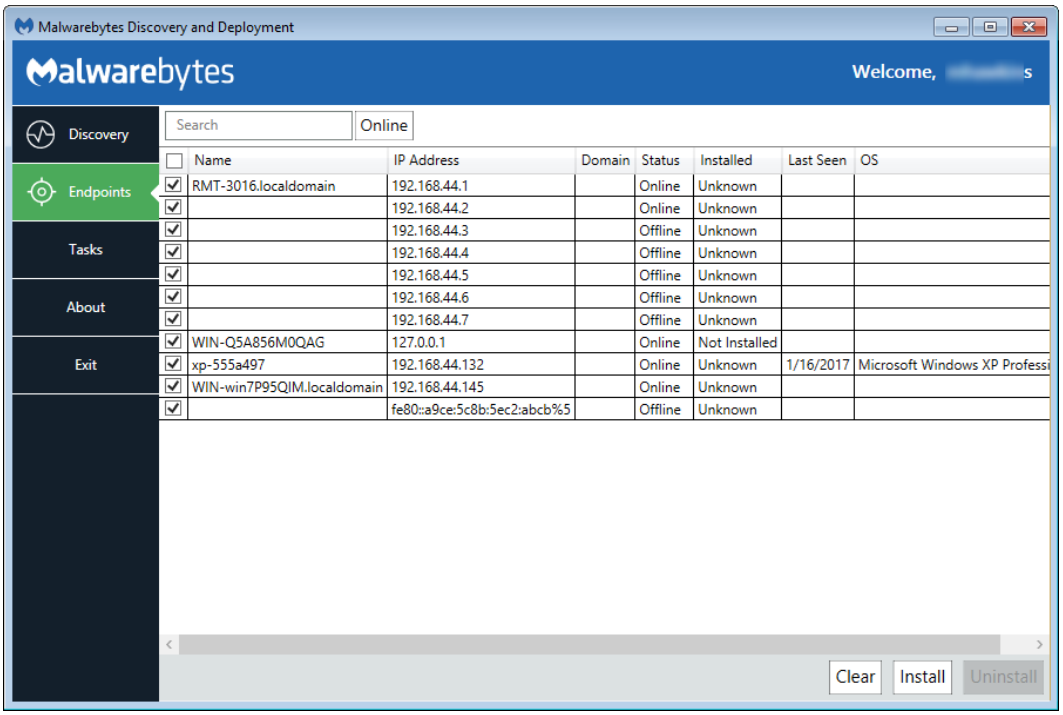
Once a scan has been initiated, this screen will show the results of that scan. Let's use a Network Scan as an example to demonstrate the process.



Here, five endpoint criteria were listed for the desired scan. You may add to this list in the box at the upper left, then clicking the **Add** button. Highlight an entry in the large box and click **Remove** to delete it, and press **Clear List** to remove all criteria.

When satisfied, press **Scan Network** to begin the scan.

As the discovery scan executes, the main program screen will show each endpoint specified and/or within the IP address range specified by the user. Please refer to the following screenshot.

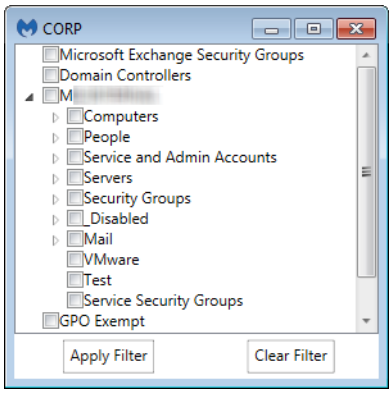


You may click on any field to sort on that field. Click again to reverse the order.

The Search box allows you to search for any endpoint (or group of endpoints) that match criteria which you specify. Please note that the search string will look for matches in both the Name and IP Address fields.

The pulldown next to the Search box allows filtering of discovery results, so that only endpoints which match the specified discovery status will be displayed. Allowable status includes *All*, *Online*, *Offline*, *Probing*, and *Queued for Probing*. Please note that while scanning is extremely fast, probing takes much more time. Probing is responsible for detection of endpoint status, agent installation status and operating system. The tool will probe as many endpoints as possible based on the resources required, and upon completion, will probe the next endpoint in the queue.

A second filter which can be applied in a domain environment is the **AD Filter**. Clicking the AD Filter buttons superimposes the filter window (shown below) over the program interface.



This tree is a hierarchical view of your Active Directory layout, broken down by Organizational Unit (OU). A typical OU structure is shown here. We do not presume how your OU structure is defined, therefore all OU's are shown here.

If you filter based on the Computers OU, any child OU's are also selected by default. You can drill down and deselect any entries which are not to be included in the filter specifications.

Once you have completed OU selection, click **Apply Filter** to effect a change on your Endpoints screen. The AD Filter button on the Endpoints screen will turn black while a filter is used.

The Results filter and the AD Filter can be used at the same time.

Status is the status of each endpoint. Installed indicates whether a Malwarebytes agent has been installed. If Status is *online* and Installed is *unknown*, that may indicate an endpoint which can be reached but software detection cannot be performed. It is also possible that missing or incorrect credentials were specified by the user. Ports 135, 137, and 445 are required for software probing.

Finally, the Refresh button restarts the discovery process. There are no results saved from the previous discovery process. The Cancel button terminates the discovery process. In a large network environment, this may take a few moments.

Let's briefly shift gears and discuss an Active Directory Scan. Everything that has been said so far also applies to an AD scan, though there are a few differences. The program will query Active Directory for a list of endpoints in the domain, then display results of that query. The endpoint Name will show the full FQDN for the machine, and Domain will be populated by the Active Directory domain name. By clicking the AD Filters button, you can specify which Organizational Units (OUs) to focus on.

Preparing for Deployment

Now that we can see the state of our endpoints, we can use *remote deployment* to install agents on these endpoints. Select all (or specific) machines and click the **Install** button to begin deployment.

Please note: 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. Please read the following article for further information:

https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows-vista

Here are a few hints which will give you the best results.

- Administrator credentials are required to perform the remote deployment. A domain account will suffice if the target endpoint is part of the domain and the domain account used is part of the local administrators group.
- Access on port 137 must be enabled on the target endpoint.
- The installer will not attempt to overwrite a previously existing program version on the endpoint. You are permitted to uninstall the program on that endpoint.
- Endpoints whose Status is *Offline* or whose Installed state is *Unknown* may still be able to have software deployed via a push install. Status will be reported whether deployment is successful or not.

Finally, the *Discovery and Deployment Tool* must connect with Malwarebytes infrastructure servers to download the most current MSI install package and the account token which will be used as a unique identifier when software package updates are available.

The next two sections describe technical information related to deployment, but user interactions are limited to selecting the machine and clicking the **Install** button. This is simply to let you know what we're doing and how we're doing it!

Deployment with Malwarebytes Methods

We use a Windows construct called *Named Pipes* to communicate with the endpoint. 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.

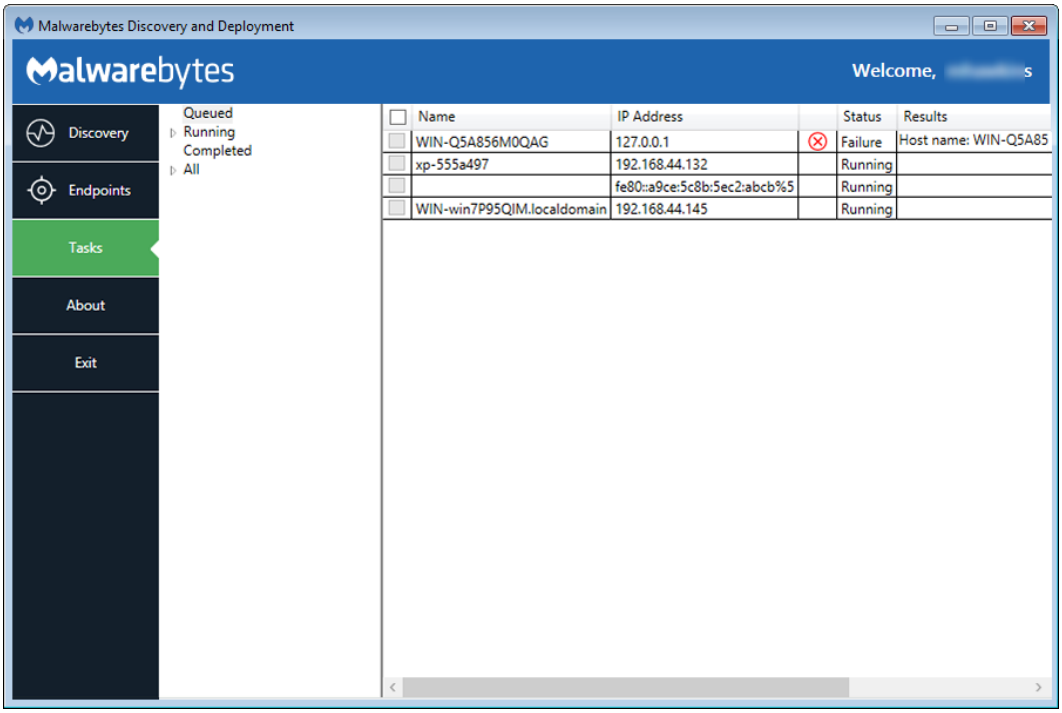
Deployment with Windows Methods (WMI)

Windows Management Instrumentation (WMI) is another method we use. It is typically used when our primary method is unsuccessful. WMI Deployment uses the **ADMIN$** share. Endpoint port 135 must be available through the firewall. Local admin credentials are required.

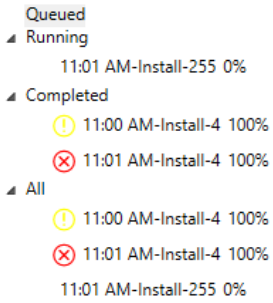
Please note: You should not use the Discovery and Deployment Tool to deploy agents to endpoints outside of your local network. This includes those which connect to the network using a VPN connection. The ports which are opened for the deployment process would remain open after deployment is complete, creating a security risk on that endpoint.

Tasks

Once we have selected endpoints to install a Malwarebytes agent on, we can use the Tasks tab to look at status and progress of the agent deployment. A screenshot is shown here to illustrate this tab in use.



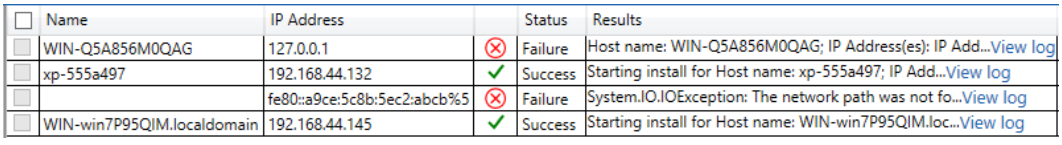
This tab is divided into two sections. The left section is a quick status of install/uninstall activity that has occurred or is currently in process. The view shown here indicates there are results in the *Running* and *All* categories, but neither are expanded to show results. You will also notice no indicator next to *Completed*. It looks like an error but it's not. Once remaining scans complete, status will be updated appropriately.



Looking at this *Status* example, you can see that an install began at 11:00am and met with mixed results (exclamation mark denotes at least one failure). Another 4-point endpoint install began at 11:01am. The red X inside the circle indicates that all four installations failed.

Finally, a third installation began at 11:01am. This installation was for 255 machines, and completion status is shown at 0%. Completion status would increment to 100% with final status showing a green checkmark (complete success), exclamation mark (one or more failures), or red X inside a circle (complete failure).

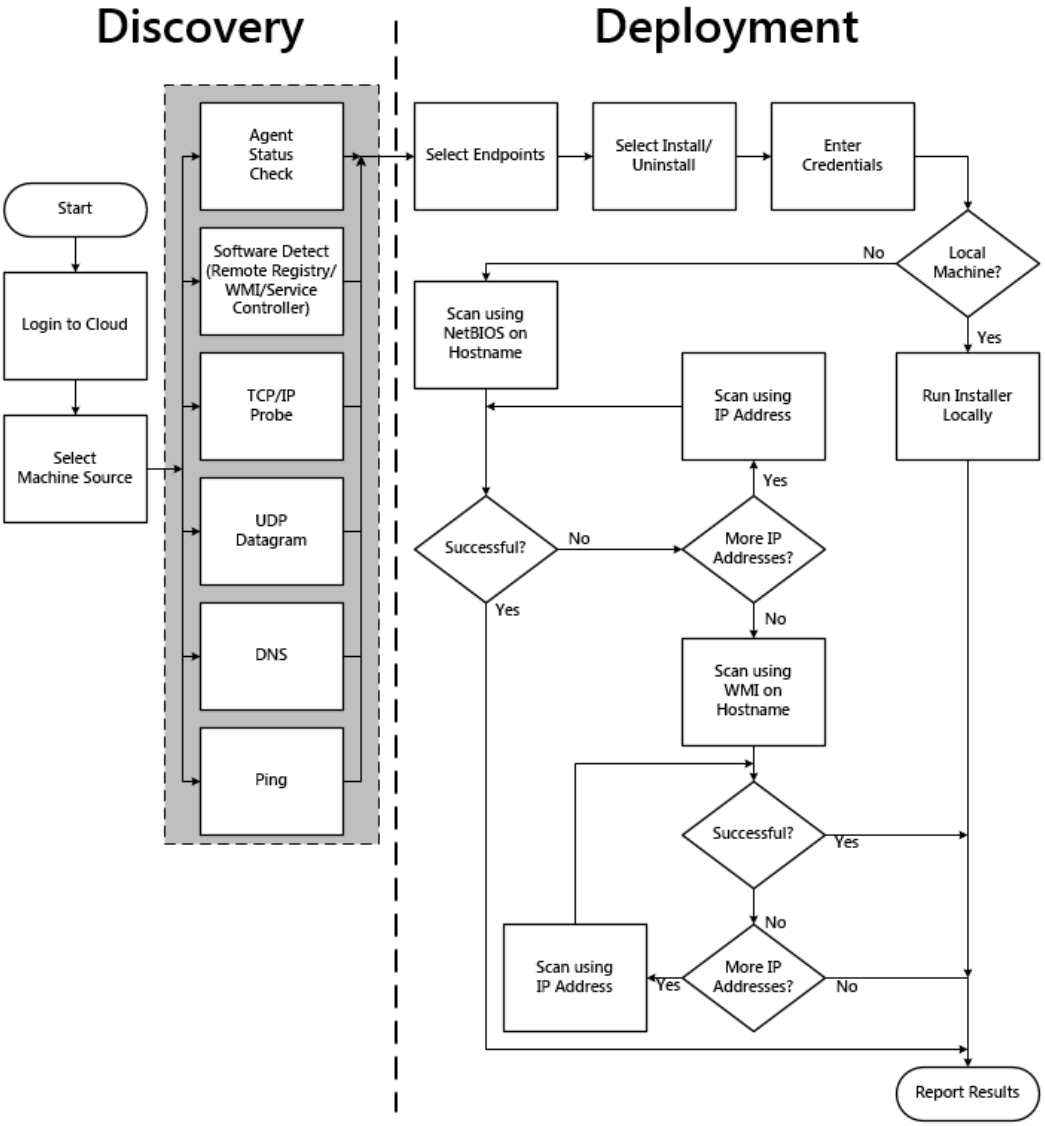
The screenshot below shows installation results for these same four endpoints. *Status* is shown with both words and symbols, and *Results* shows relevant information as well as a link to view logs. Only an excerpt of the screen is shown here because the screen required expansion to show *Results* detail, and that action would have caused display of the full screen to become illegible here.



Please note that when several endpoints are selected for installation, you may also see *Status* shown as Queued. Resources are required for each installation, and when requirements exceed availability, installation will be Queued until resources are available.

Additional Information

The following graphic shows the logic flow of the Discovery and Deployment Tool. The program is divided into two sections which work seamlessly to provide the desired functionality.



Command Line Reference

The *Discovery and Deployment tool* can be used via its GUI interface as well as a command line mode. All commands take the form:

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

Use of the tool is best illustrated by an example, which follows. This is all one line, but is broken up here for easier reading.

```
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;
```

Here, a silent installation was performed on three endpoints, two identified by name and one by IP address. The results of the installation process was saved to a file for later inspection. When using the command line mode, the following arguments may be used. They are listed here in alphabetical order.

-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. Please refer to page 3 ("*Who to Discover*") for a list of specifications which this information can take.

-nebulauri

URL of the *Malwarebytes* server. Default value is **https://cloud.malwarebytes.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 *Malwarebytes* server. Valid answers are **yes/no**, **true/false**, or **1/0**.

-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 *Malwarebytes* server.

-wmionly

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