

MIGRATION GUIDE

Migration Instructions - Malwarebytes for the Cloud

The Discovery and Deployment tool enables the migration of your Malwarebytes Endpoint Security managed endpoints over to Malwarebytes Endpoint Protection.

The migration process transfers the following items from Malwarebytes Endpoint Security to Malwarebytes Endpoint Protection:

- **Endpoint Security Group definitions** – Groups without endpoints are linked to default cloud policies
- **Endpoint Security Policy definitions** – Only policies used by endpoints are migrated
- **Endpoint Security Exclusion definitions**
- **Endpoint Security Scan Schedule definitions** – Only hourly, daily and weekly scan schedules are migrated. Non-recurring/on restart scans are not migrated – you will need to set these up again.
- **Endpoint Agent installation**
- **Endpoint Protection application installation**

Groups and policies

With Endpoint Security, you could assign a policy to an individual endpoint or group. Endpoint Protection only allows assigning a policy to a group.

During the migration process, the Discovery and Deployment tool does the following for you:

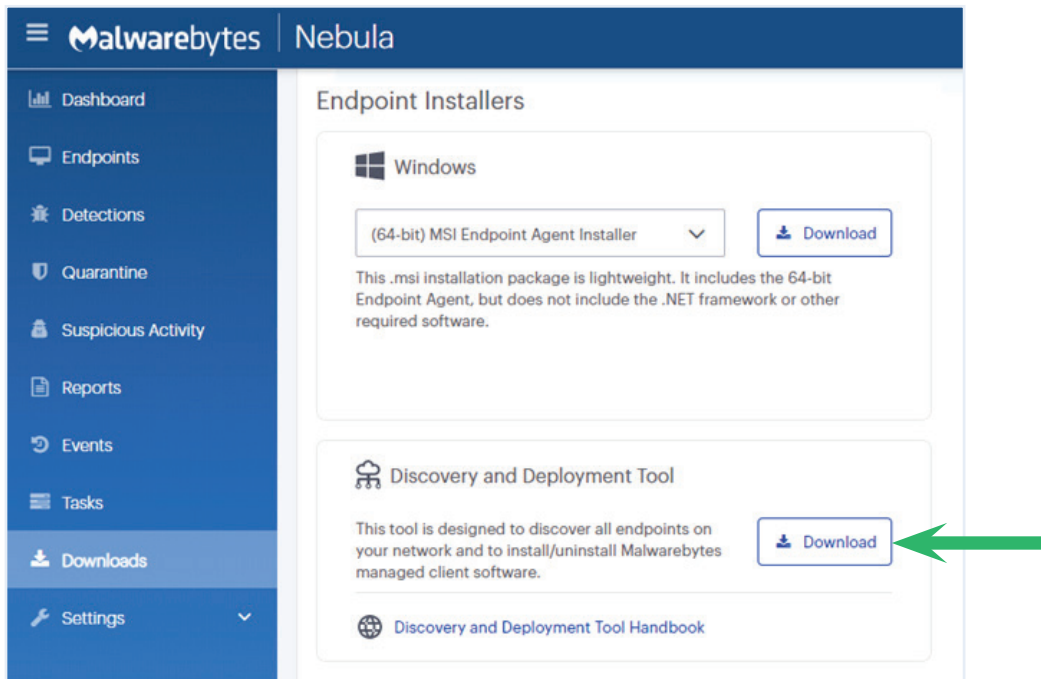
- Looks at endpoints that were migrated with their assigned groups.
- Determines the **most commonly-used policy** for these endpoints.
- Assigns the most commonly-used policy for all affected endpoints.

Be sure to review your policies and groups after migration and fine-tune them as needed.

Download and run the tool

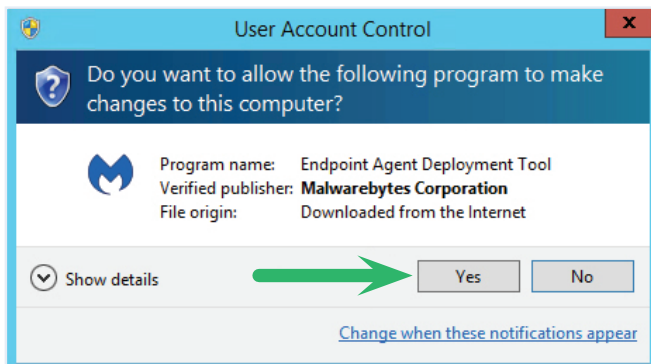
To download the Discovery and Deployment tool, you'll need to login to the Malwarebytes cloud console.

1. Go to cloud.malwarebytes.com.
2. Enter your user credentials.
3. Go to **Endpoints > Add Endpoints**.
4. Click on the **Download** button for **Download Malwarebytes Discovery and Deployment Tool**.

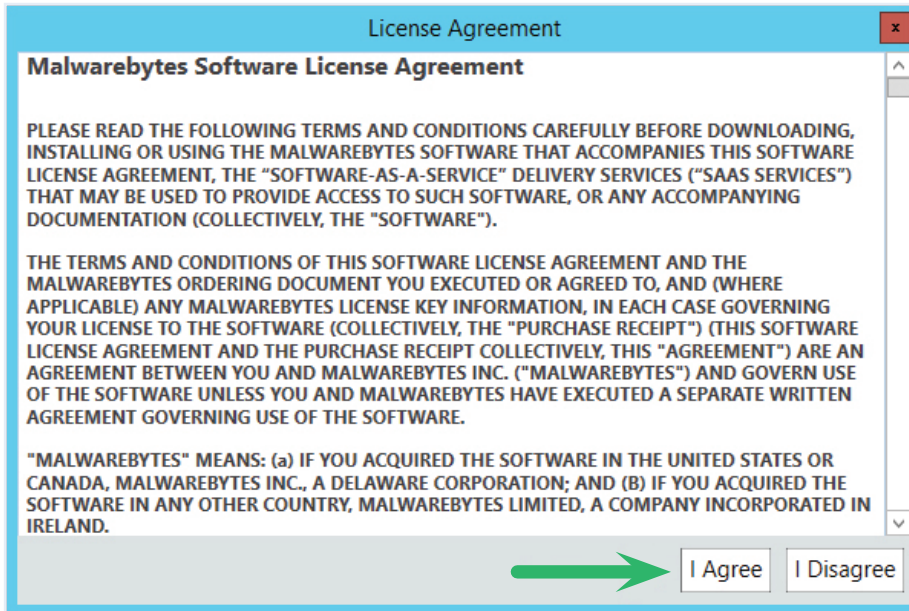


Make sure the tool is running on a Windows computer with external internet access and network visibility to your endpoints.

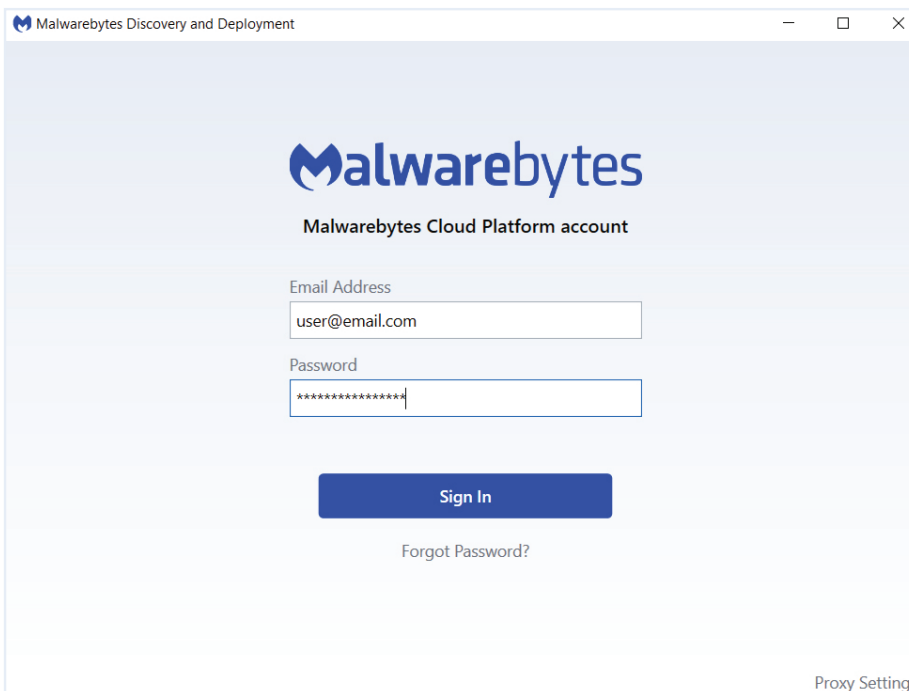
1. Run the downloaded file, EndpointAgentDeploymentTool.exe.
2. The **User Account Control** screen displays. Click **Yes**.



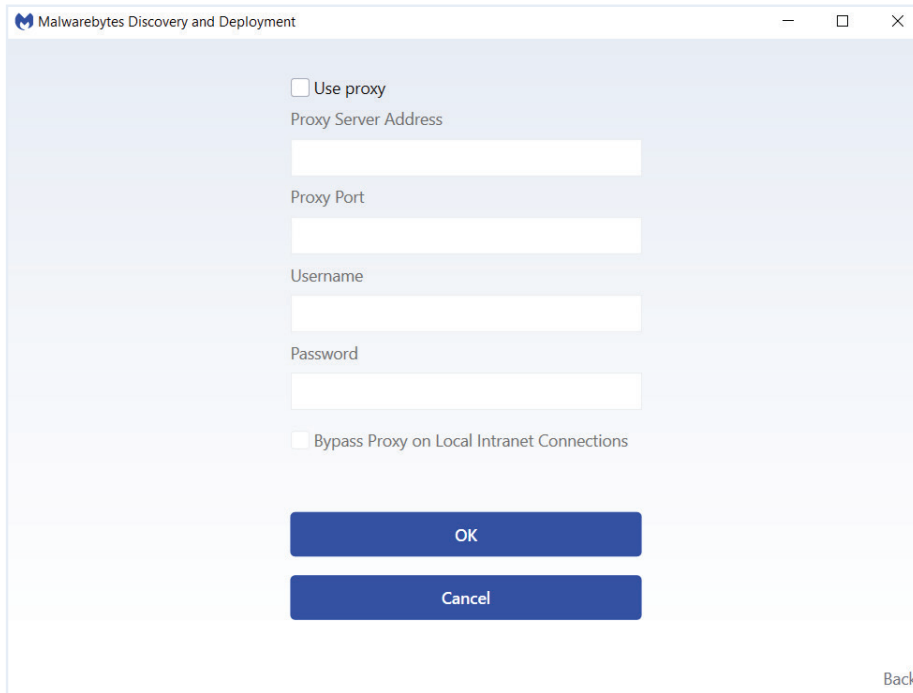
3. The **Malwarebytes Software License Agreement** displays. Click **I Agree**.



4. Enter your Malwarebytes Cloud user credentials.



5. **Optional:** Configure proxy settings.
- Click the **Proxy Settings** link.
 - Check **Use Proxy**.
 - Enter your proxy information and click **OK**.



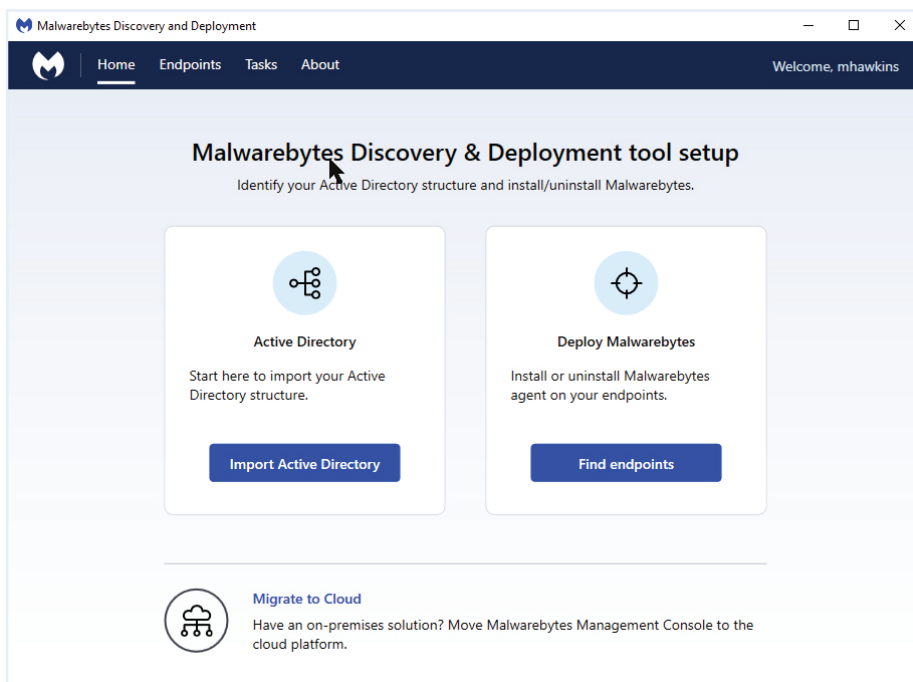
The screenshot shows a dialog box titled "Malwarebytes Discovery and Deployment". It contains the following elements:

- Use proxy
- Proxy Server Address: [text input field]
- Proxy Port: [text input field]
- Username: [text input field]
- Password: [text input field]
- Bypass Proxy on Local Intranet Connections
- OK button
- Cancel button
- Back link at the bottom right.



Note: Any proxy specifications entered here are propagated to endpoints deployed by the tool.

You're now logged into the Discovery and Deployment tool!



The screenshot shows the main dashboard of the Malwarebytes Discovery & Deployment tool. It features a navigation bar with "Home", "Endpoints", "Tasks", and "About" links, and a user greeting "Welcome, mhawkins". The main content area is titled "Malwarebytes Discovery & Deployment tool setup" and includes the instruction "Identify your Active Directory structure and install/uninstall Malwarebytes." Below this are two primary action cards:

- Active Directory:** "Start here to import your Active Directory structure." with an "Import Active Directory" button.
- Deploy Malwarebytes:** "Install or uninstall Malwarebytes agent on your endpoints." with a "Find endpoints" button.

At the bottom, there is a "Migrate to Cloud" section with a cloud icon and the text: "Have an on-premises solution? Move Malwarebytes Management Console to the cloud platform."

6. Click on **Migrate to Cloud**.



7. Enter the following information:

- **Server Name** – the name of your server. The default SQL Express database name is pre-filled. If your hostname is different, change it here.
- **Authentication** – Choose the type of authentication used to connect to your database. If SQL Server authentication is used, you need to supply a username and password.

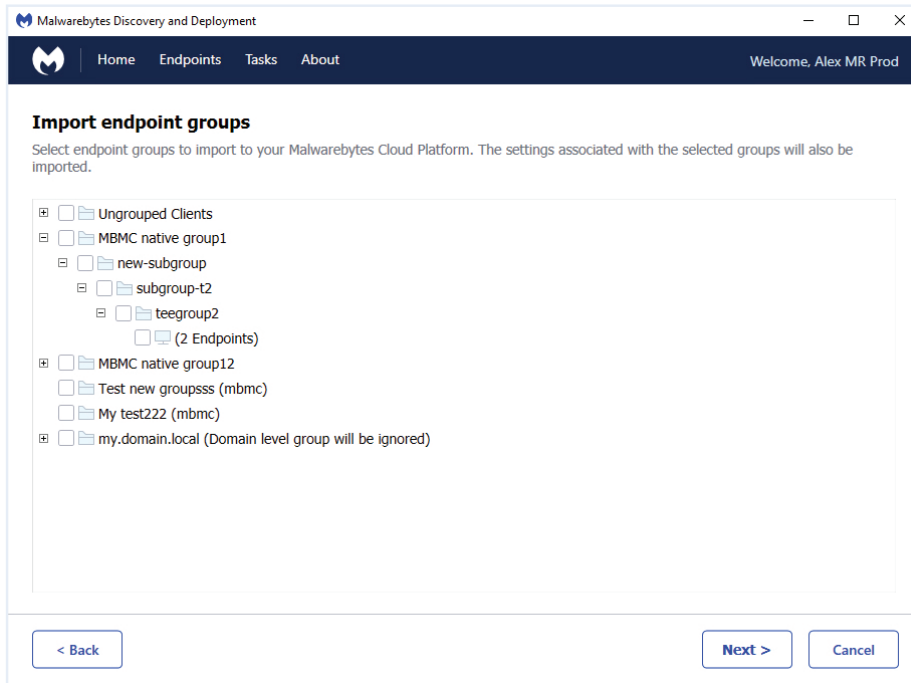
A screenshot of a web application window titled "Malwarebytes Discovery and Deployment". The window has a dark blue header with a logo, navigation links for "Home", "Endpoints", "Tasks", and "About", and a user greeting "Welcome, Alex MR Prod". The main content area is titled "Start Migration" and contains the following elements:

- A sub-header "Start Migration" and a prompt: "Connect to your SQL server to start the migration."
- A "Server Name" label and a text input field containing ".sqlexpress".
- An "Authentication" section with two radio buttons: "Use Windows authentication" (selected) and "Use SQL Server authentication".
- A light blue shaded box titled "Enter your SQL Server credentials" containing "Username" and "Password" labels and corresponding text input fields.
- A "Database" label and a dropdown menu.
- A "Test Connection" button with a refresh icon.
- At the bottom, there are three buttons: "< Back", "Next >" (disabled), and "Cancel".

8. Click **Test Connection** to verify you can connect to the database. If you have multiple database instances on the specified hostname, choose the correct instance from the list provided.

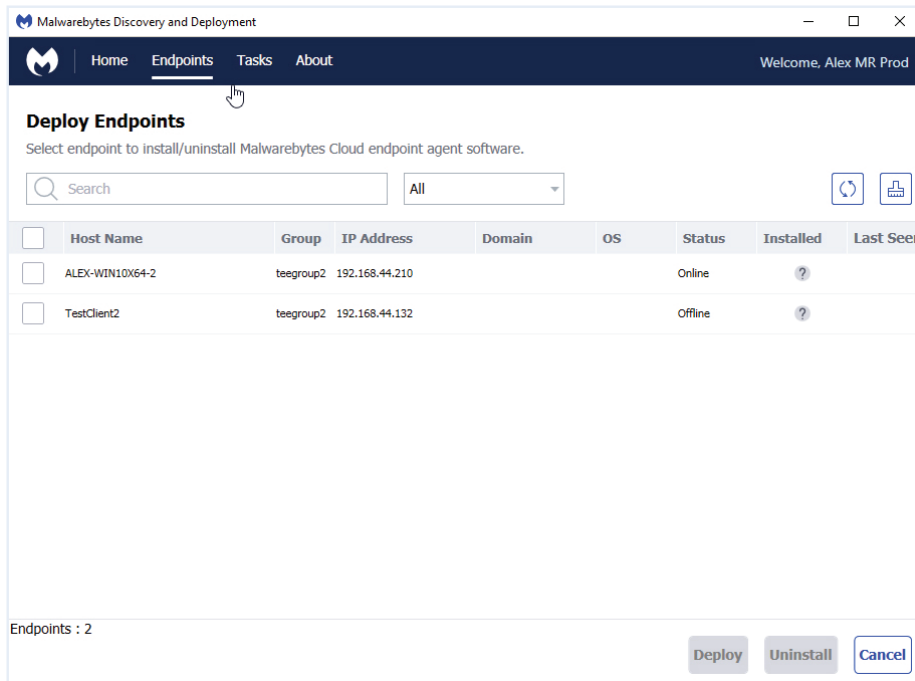
9. Click **Next**.

10. Check the groups you want to migrate from Endpoint Security over to Endpoint Protection.



11. Click **Next**. The migration progress is displayed on the screen, and a migration report displays after selected groups have been migrated.
12. Click **Next** to view the migration report that shows your policy migration results. Exclusions that have been migrated to the cloud will also be displayed.
13. Verify the migrated settings and click **Next**. Migrated scan schedules are now displayed. The migration phase is complete.
14. Log in to the Malwarebytes Cloud Console and check the results of the migration.

15. Click **Next** to start the agent deployment.



16. Check endpoints and click **Deploy**. Enter the admin username and password as required.

17. Once deployment is under way, use the **Tasks** tab to monitor deployment progress.



The **Tasks** tab is divided into two sections. The left side of the **Tasks** screen shows a quick status of the 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.

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.

To eliminate redundant software, the endpoint deployment process uninstalls any Malwarebytes products that are no longer needed with Endpoint Protection.

It removes the following applications from each endpoint:

- Managed Malwarebytes Endpoint Security client
- Unmanaged Malwarebytes Anti-Malware
- Unmanaged Malwarebytes Anti-Exploit
- Unmanaged Malwarebytes Anti-Ransomware

Congratulations! You are now migrated to Malwarebytes Endpoint Protection!



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



Note: If you haven't created any policies or groups in Malwarebytes Endpoint Security, don't worry. You can easily install Malwarebytes Endpoint Protection by following the instructions in our handy [Get Started video](#).



malwarebytes.com/business



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.

Copyright © 2020, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.