Malwarebytes Nebula

QUICK START GUIDE

Welcome to Malwarebytes Endpoint Protection!

Endpoint Protection is built on the Nebula cloud platform where you centrally manage your endpoints to protect your organization.

You're just steps away from advanced protection, detection, remediation, and centralized management.

This quick start guide walks you through the following steps:

- **Step 1:** Access your Nebula console
- **Step 2:** System and network requirements
- **Step 3:** Install the Malwarebytes Endpoint Agent
- **Step 4:** Review the Default policy
- **Step 5:** Customize your profile

Step 1: Access your Nebula console

The first step in setting up your security environment is to log in to your Nebula console and familiarize yourself with the console navigation. Also, you learn how to add users to help manage your console. By the end of Step 1, you'll have:

- Logged into your Nebula console
- Explored the navigation pane
- Added console users

Log into your Nebula console

1. Locate your verification email.
2. In the email, click the **Verify** button.
3. Your web browser opens to the Create your account page. Complete the required fields and click **Submit**.
4. The Nebula console login page displays. Enter your email address and password to login.

For more information, click here.

Exploring the navigation pane

The left side of the screen is where you navigate to different pages in Nebula. Take a moment to familiarize yourself with your Nebula console.

- Endpoints
- Detections
- Quarantine
- Reports
- Events
- Tasks

Add console users

To add additional users to your Nebula console, follow these steps:

1. In the navigation pane, click **Settings** > **Users**.
2. Click **New**.
3. Enter the invitee's email address and choose their user role and group access. For more information on user roles and group access, click here.
4. Click **Invite**.

Step 2: System and network requirements

After you've added users and explored your console, verify your endpoints meet Malwarebytes system requirements and allow network access for Malwarebytes services. By the end of Step 2, you'll have:

- Verified system requirements
- Verified network access

Verify system requirements

You can deploy the Malwarebytes Endpoint Agent to your Windows, Mac, and Linux devices. Before deploying the agent, click here to verify your endpoints meet the minimum requirements.

Verify network access

If your company's Internet access is protected by a firewall or you have other limitations, you'll need to allow access to port 443 for all of the Malwarebytes services listed here.

Step 3: Install the Malwarebytes Endpoint Agent

It's time to deploy the agent to your endpoints. You can deploy manually, remotely, or by using our Discovery and Deployment Tool. By the end of Step 3, you'll have deployed using one of the following methods:

- Manual installation
- Remote installation
- Discovery and Deployment Tool

Manual installation

This method requires you to install the agent at the endpoint device.
To install the Endpoint Agent, follow these steps:

1. Go to the device you want to install on.
2. Log in to Malwarebytes Nebula using your administrator credentials.
3. In the left-side pane, click **Downloads**.
4. Click to download the files that match your device's operating system.
5. Run the setup file.
6. Follow the steps provided in the installation process.

Remote installation

You can remotely install the agent using a third-party installer, by emailing the download link, or by setting up a Linux repository. See the instructions for your environment's devices:

- Windows
- Mac
- Linux

Discovery and Deployment Tool

This free tool identifies Windows endpoints on your network by Active Directory or IP address, then distributes the agent to those endpoints. To download the Discovery and Deployment Tool:

1. In the left-side pane, click **Downloads**.
2. In the Discovery and Deployment Tool section, click **Download**.
3. Use the tool to identify endpoints in your network and deploy the agent.

For detailed instructions, click here.

Step 4: Review the Default policy

Your deployed endpoints now appear on the Endpoints page of the Nebula console. New endpoints are automatically assigned to the Default Group. Your Default Group is automatically assigned to your Default policy. Review the Default policy and make any changes to meet your protection preferences. By the end of Step 4, you'll have:

- Reviewed Endpoint Interface options
- Reviewed General policy options
- Reviewed Settings policy options

Review Endpoint Interface options

The Endpoint Interface options identify the notifications sent to the endpoint agent and the action the user can take based on the notification.

1. In the left-side pane, click **Settings** > **Policies**.
2. Click the **Default** policy.
3. Locate the **Endpoint Interface** options and make any needed changes. For more information, click here.
4. Click **Save**.

Review General policy options

The General tab determines how the endpoint agent handles system reboots, protection updates, and events to report to Nebula.

1. In the left-side pane, click **Settings** > **Policies**.
2. Click the **Default** policy.
3. Select either **Windows**, **Mac**, or **Linux** tabs.
4. Select the **General** tab and make any needed changes. For more information, click here.
5. Click **Save**.

Review Settings policy options

The Settings tab is where you define your scanning and Real-Time Protection configurations.

1. In the left-side pane, click **Settings** > **Policies**.
2. Click the **Default** policy.
3. Select either **Windows**, **Mac**, or **Linux** tabs.
4. Select the **Settings** tab and make any needed changes. For more information, click here.
5. Click **Save**.

Step 5: Customize your profile

Now that your environment is protected by Malwarebytes Endpoint Protection, let's customize your profile. By the end of Step 5, you'll have:

- Customized notifications settings
- Viewed your license information

Customize notifications settings

Notifications help you monitor your organization's threat protection, detection, and response. Choose the notification types you want Malwarebytes Nebula to send you.

1. Click your display name at the top-right of the screen > **Profile**.
2. Click the **Notifications** tab.
3. Check the boxes for notifications you want to receive.
4. Click **Save Changes**.

For more detailed instructions, click here.

View your license information

The License Information tab displays your license key, active subscriptions, number of deployed devices, and your subscription expiration date. To view license information:

1. Click your display name at the top-right of the screen > **Profile**.
2. Click the **License Information** tab to find your subscription information and license key.

For more information, click here.

Congratulations! Malwarebytes Endpoint Protection is now up and running.

We recommend you:

- Enroll in Malwarebytes Academy for online product training.
- Visit the Malwarebytes Support site for additional information on Malwarebytes Nebula.
- Watch the Let's get started with Malwarebytes Nebula video.

If you have any questions, contact your Malwarebytes Account Manager.

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.