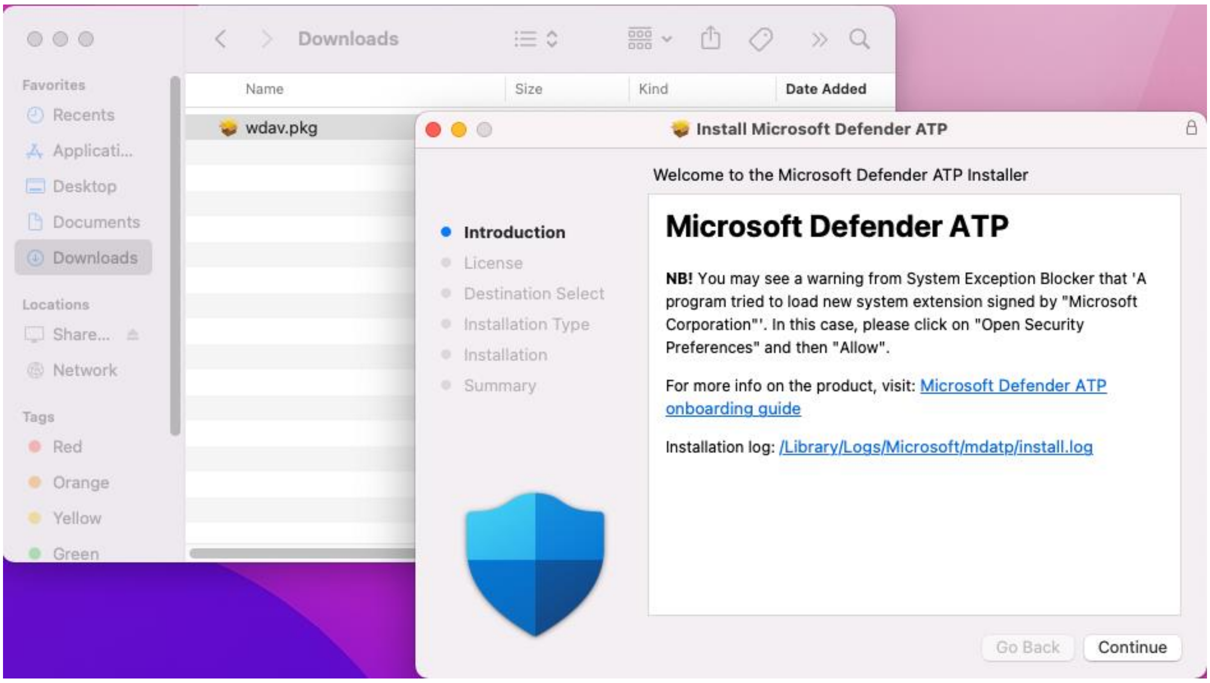
How to Install Microsoft Defender on MAC

To complete this process, you must have admin privileges on the device.

1. Navigate to the downloaded wdav.pkg in Finder and open it.



Welcome to the Microsoft Defender ATP Installer

Microsoft Defender ATP

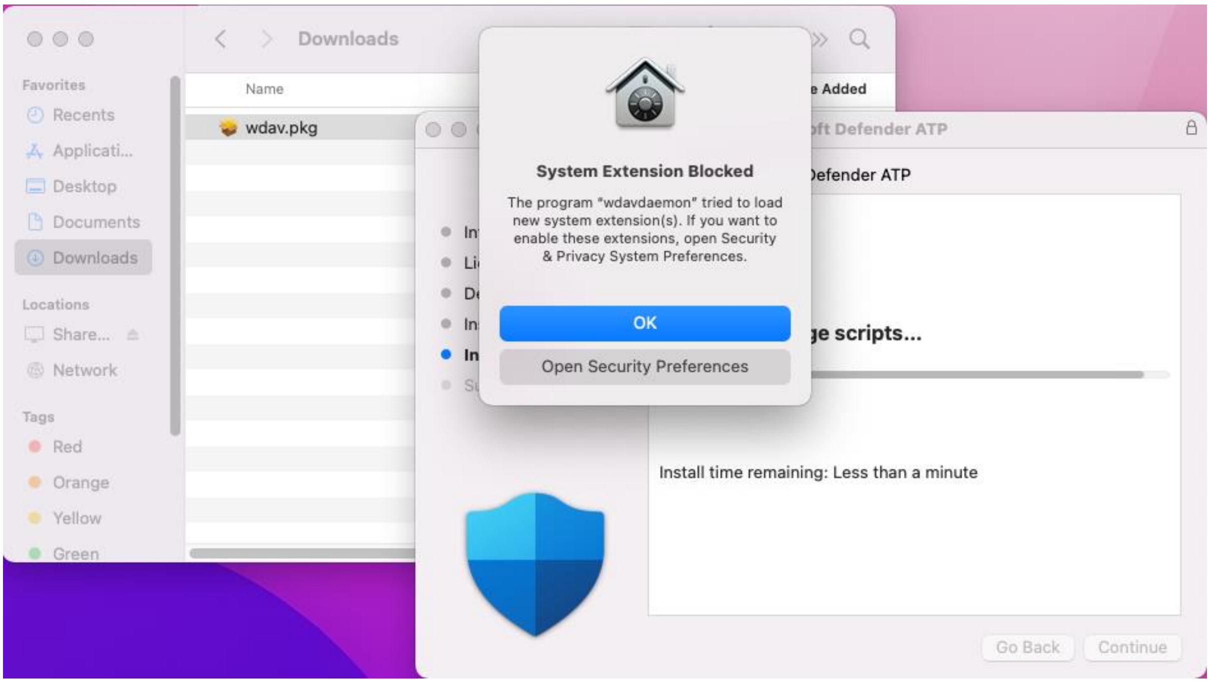
NB! You may see a warning from System Exception Blocker that 'A program tried to load new system extension signed by "Microsoft Corporation"'. In this case, please click on "Open Security Preferences" and then "Allow".

For more info on the product, visit: Microsoft Defender ATP onboarding guide

Installation log: /Library/Logs/Microsoft/mdatp/install.log

2. Select **Continue**, agree with the License terms, and enter the password when prompted.

3. At the end of the installation process, you'll be prompted to approve the system extensions used by the product. Select **Open Security Preferences**.

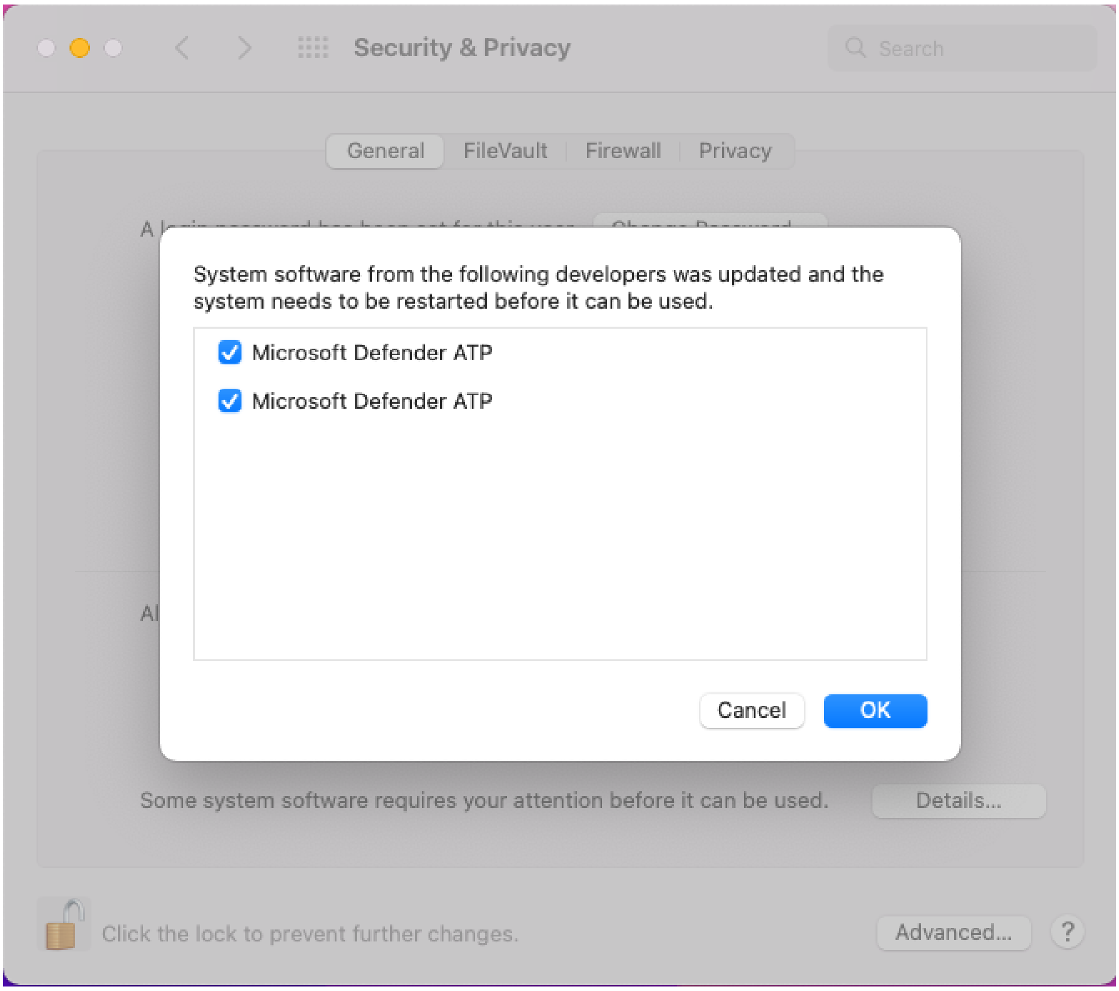


System Extension Blocked

The program "wdavdaemon" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

Install time remaining: Less than a minute

4. From the **Security & Privacy** window, select **Allow**.



System software from the following developers was updated and the system needs to be restarted before it can be used.

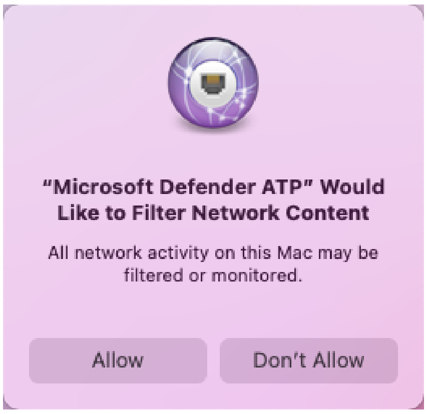
☑ Microsoft Defender ATP

☑ Microsoft Defender ATP

Some system software requires your attention before it can be used.

Click the lock to prevent further changes.

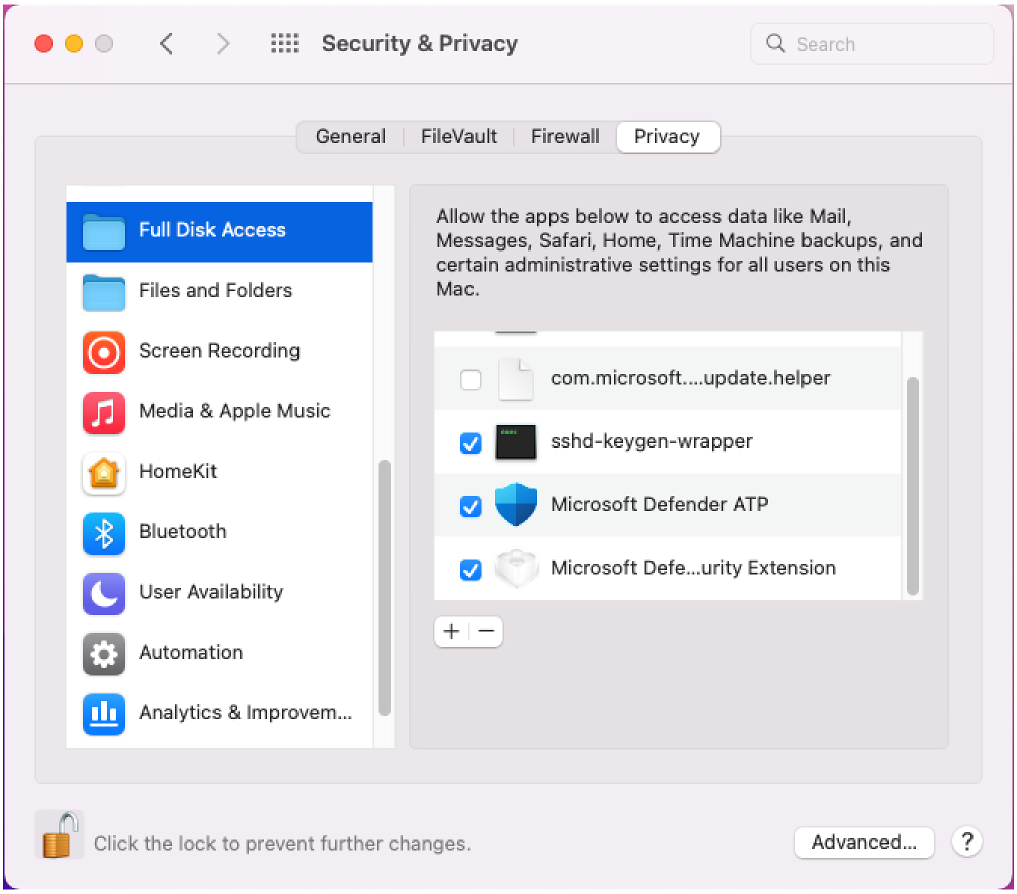
5. Repeat steps 3 & 4 for all system extensions distributed with Microsoft Defender for Endpoint on Mac.
6. As part of the Endpoint Detection and Response capabilities, Microsoft Defender for Endpoint on Mac inspects socket traffic and reports this information to the Microsoft 365 Defender portal. When prompted to grant Microsoft Defender for Endpoint permissions to filter network traffic, select **Allow**.



"Microsoft Defender ATP" Would Like to Filter Network Content

All network activity on this Mac may be filtered or monitored.

7. Open **System Preferences** > **Security & Privacy** and navigate to the **Privacy** tab. Grant **Full Disk Access** permission to **Microsoft Defender** and **Microsoft Defenders Endpoint Security Extension**.



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

- □ com.microsoft....update.helper
- ☑ sshd-keygen-wrapper
- ☑ Microsoft Defender ATP
- ☑ Microsoft Defe...urity Extension

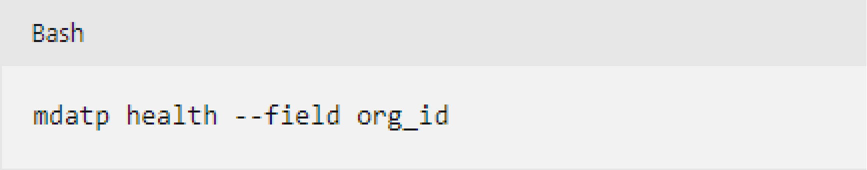
Click the lock to prevent further changes.

Client configuration

1. Copy wdav.pkg and MicrosoftDefenderATPOnboardingMacOs.sh to the device where you deploy Microsoft Defender for Endpoint on macOS.

   The client device isn't associated with org_id. Note that the *org_id* attribute is blank.

   BashCopy
   mdatp health --field org_id

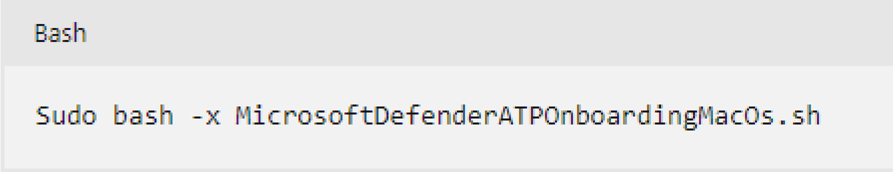
   

   Bash

   ```
   mdatp health --field org_id
   ```

2. Run the Bash script to install the configuration file:

   BashCopy
   Sudo bash -x MicrosoftDefenderATPOnboardingMacOs.sh

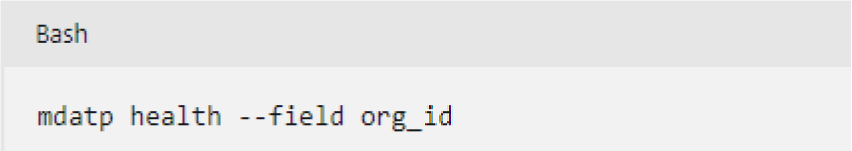
   

   Bash

   ```
   Sudo bash -x MicrosoftDefenderATPOnboardingMacOs.sh
   ```

3. Verify that the device is now associated with your organization and reports a valid org ID:

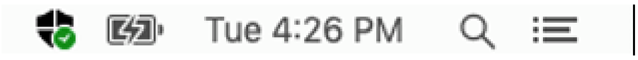
   BashCopy
   mdatp health --field org_id

   Bash

   ```
   mdatp health --field org_id
   ```

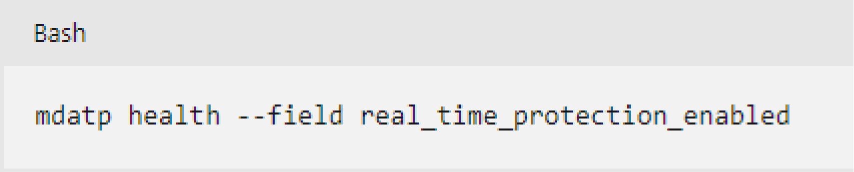
   After installation, you'll see the Microsoft Defender icon in the macOS status bar in the top-right corner.



How to Allow Full Disk Access

1. To grant consent, open **System Preferences** > **Security & Privacy** > **Privacy** > **Full Disk Access**. Click the lock icon to make changes (bottom of the dialog box). Select Microsoft Defender for Endpoint.
2. Run an AV detection test to verify that the device is properly onboarded and reporting to the service. Perform the following steps on the newly onboarded device:
    1. Ensure that real-time protection is enabled (denoted by a result of 1 from running the following command):

       BashCopy
       mdatp health --field real_time_protection_enabled


Bash

```
mdatp health --field real_time_protection_enabled
```

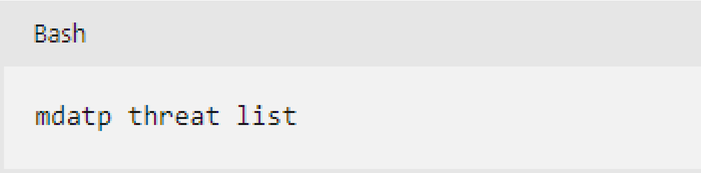
Open a Terminal window. Copy and execute the following command:
BashCopy
curl -o ~/Downloads/eicar.com.txt
https://www.eicar.org/download/eicar.com.txt

Bash

```
curl -o ~/Downloads/eicar.com.txt https://www.eicar.org/download/eicar.com.txt
```

The file should have been quarantined by Defender for Endpoint on Mac. Use the following command to list all the detected threats:

BashCopy
mdatp threat list


Bash

```
mdatp threat list
```

3. Run an EDR detection test to verify that the device is properly onboarded and reporting to the service. Perform the following steps on the newly onboarded device:
    1. In your browser such as Microsoft Edge for Mac or Safari.
    2. Download MDATP MacOS DIY.zip from https://aka.ms/mdatpmacosdiy and extract.

       You may be prompted:

       Do you want to allow downloads on "mdatpclientanalyzer.blob.core.windows.net"?
       You can change which websites can download files in Websites Preferences.

4. Click **Allow**.
5. Open **Downloads**.
6. You should see **MDATP MacOS DIY**.

📌 Tip

If you double-click, you will get the following message:

"MDATP MacOS DIY" cannot be opened because the developer cannot be verifier.
macOS cannot verify that this app is free from malware.
[Move to Trash] [Cancel]

7. Click **Cancel**.
8. Right-click **MDATP MacOS DIY**, and then click **Open**.

   The system should display the following message:

   macOS cannot verify the developer of MDATP MacOS DIY. Are you sure you want to open it?
   By opening this app, you will be overriding system security which can expose your computer and personal information to malware that may harm your Mac or compromise your privacy.

9. Click **Open**.

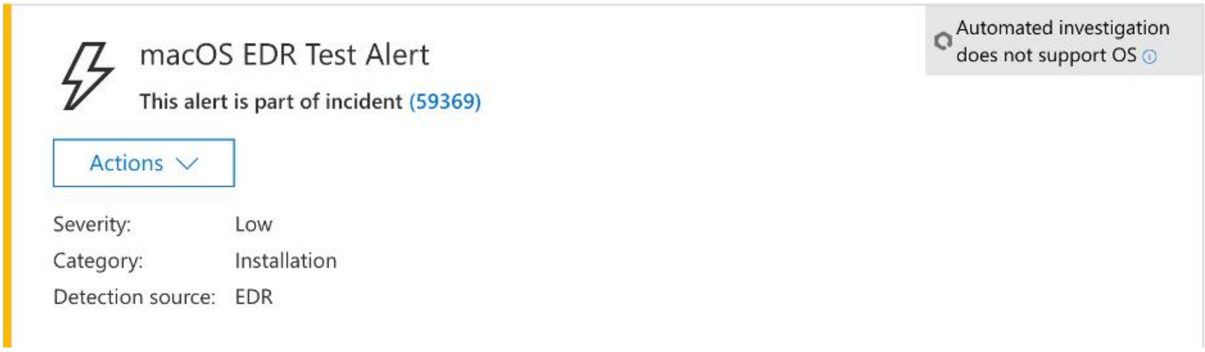
   The system should display the following message:

   Microsoft Defender for Endpoint - macOS EDR DIY test file
   Corresponding alert will be available in the MDATP portal.

10. Click **Open**.

    In a few minutes an alert named "macOS EDR Test Alert" should be raised.

11. Go to Microsoft 365 Defender portal (https://security.microsoft.com/).
12. Go to the Alert Queue.



macOS EDR Test Alert
This alert is part of incident (59369)

Severity: Low
Category: Installation
Detection source: EDR

Look at the alert details and the device timeline and perform the regular investigation steps.