MacOS Agent Deployment with Command Line

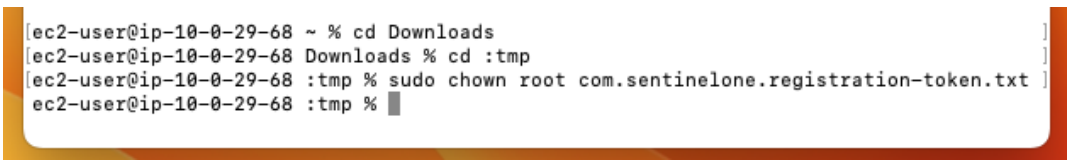
Prerequisites

Ensure the endpoint meets the minimum hardware requirements:

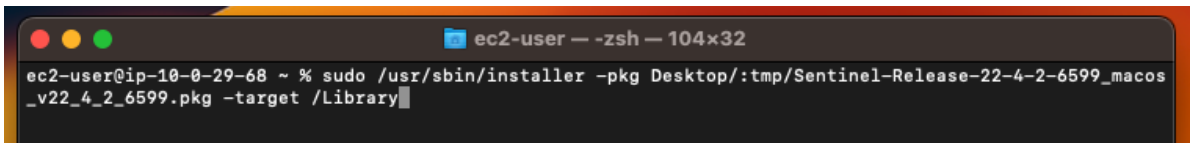
- 1 GHz dual-core CPU or better.
- 1 GB RAM or more, according to the operating system requirements | **2 GB recommended**
- 2 GB free disk space

Instructions

1. Get the site token and the installer package from the dashboard at https://dashboard.skoutsecure.com. Navigate to **Downloads** > **Endpoint Protection**. The site token can be found under Step 3.
2. Save the site token in a plain text file in a folder named **/tmp**, along with the Installer package.
    a. Name the Token file: *com.sentinelone.registration-token*
    b. Change the ownership of the file to root with *sudo chown* root <file name>.



3. Run the installer:
    a. $ sudo /usr/sbin/installer -pkg *<Download path>*/tmp/SentinelInstaller.pkg -target */<Target path>*
        i. **Do not just copy/paste the command, as the download and target paths will be specific to the endpoint.**
        ii. **Example:**

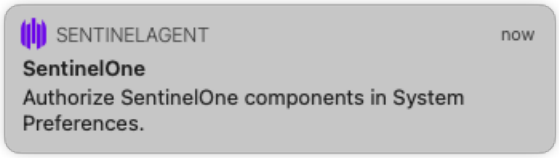


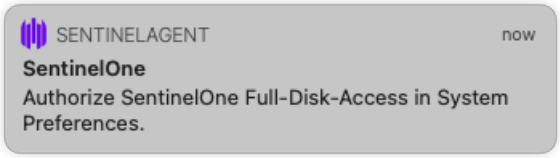
4. Complete the installation.
    a. If the SentinelOne icon shows "**Needs user attention**" or the message "**Authorize SentinelOne components in System Preferences**", follow the steps on the next page.

Authorizing SentinelOne Components in System Preferences

The macOS (10.15 Catalina and later releases) makes sure that applications are installed in a secure way. It limits installation only to applications that are approved by Apple and the user. This change does not let applications access specified paths (such as Documents, Downloads, and Desktop) without user consent.

If the SentinelOne icon shows "**Needs user attention**" or these messages "**Authorize Full-Disk-Access to SentinelOne in System Preferences**", "**Authorize SentinelOne components in System Preferences**". You must approve Full Disk Access for SentinelOne Apps in the System Preferences.

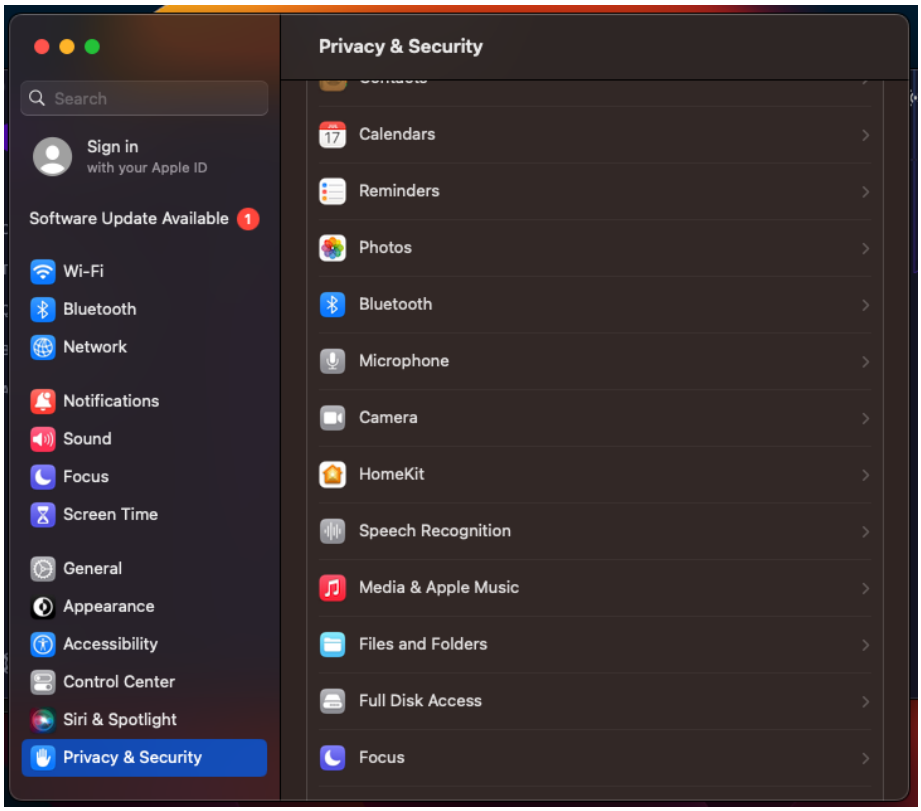




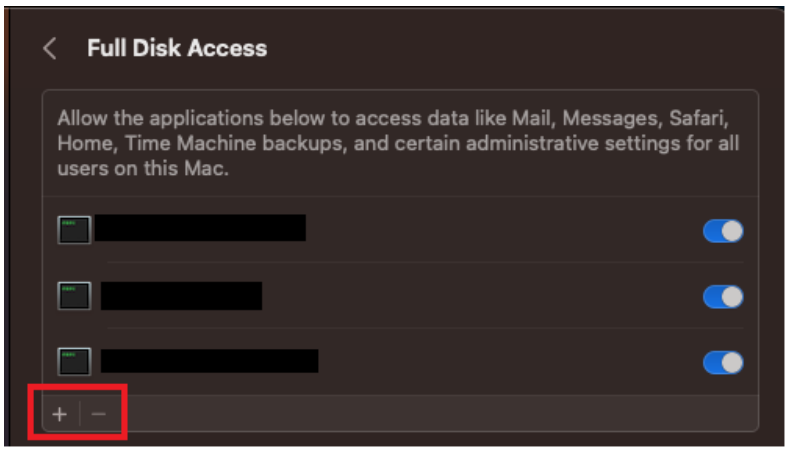
Important: This is done only once on an endpoint. If already done on the endpoint, do not repeat it when the Agent is updated. If you do not complete this prerequisite step, the macOS Agent will not have full visibility to all files from all users.

To authorize Full Disk Access

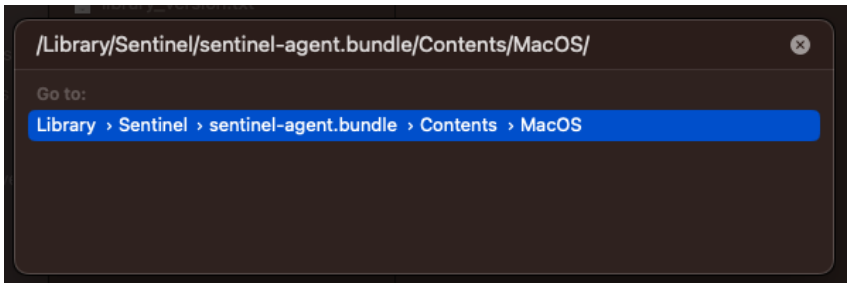
1. Open **System Preferences**. Click **Privacy & Security**, and select the **Full Disk access** tab.



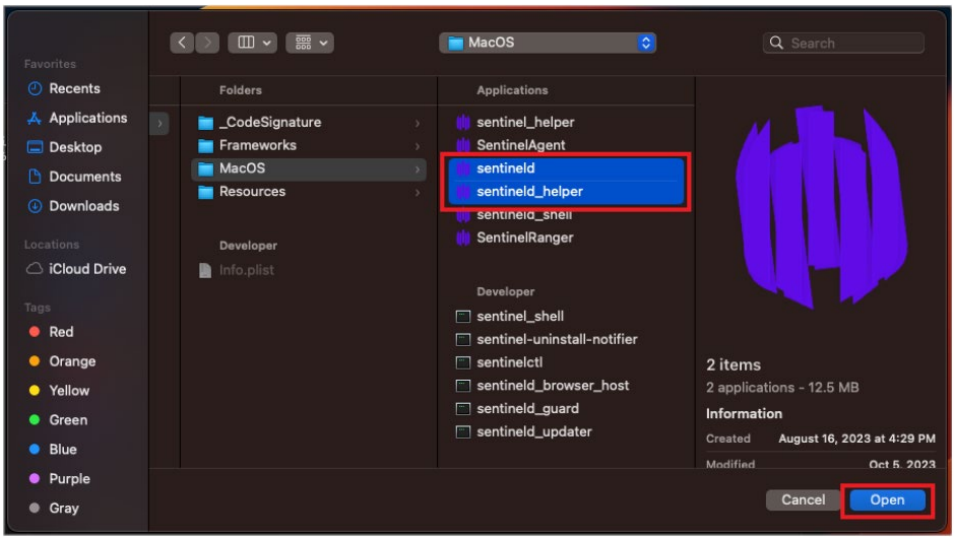
2. Click on the **+** button to make changes. If prompted, enter your password.



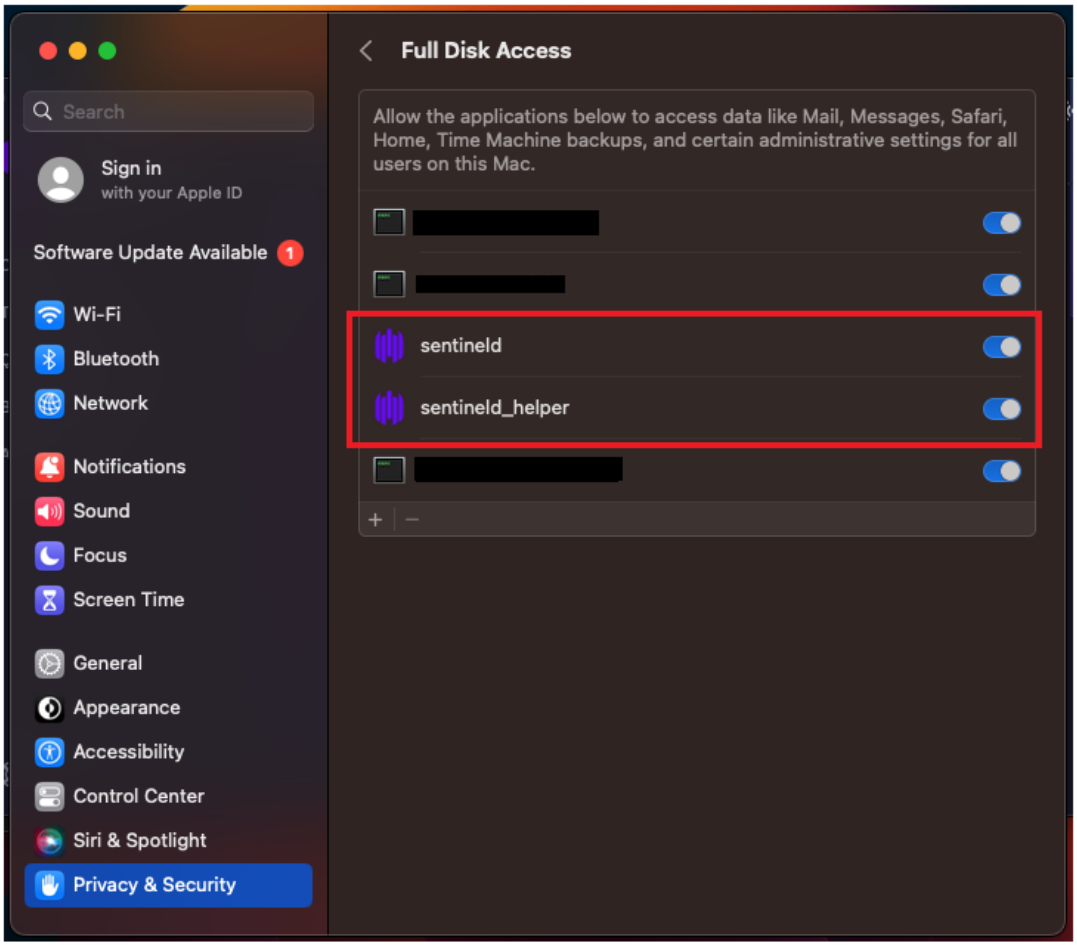
3. Press and hold **Command+Shift+G** at the same time to open the **Go to the folder** menu. Enter the path**: /Library/Sentinel/sentinel-agent.bundle/Contents/MacOS/**



4. Select the SentinelOne applications, and click **Open**:
    a. **sentineld.app** and **sentineld_helper.app**

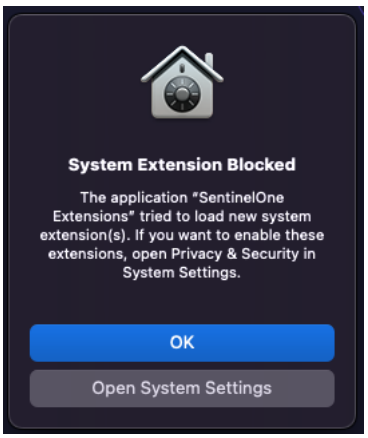


5. The applications will now show up in **Full Disk Access**.

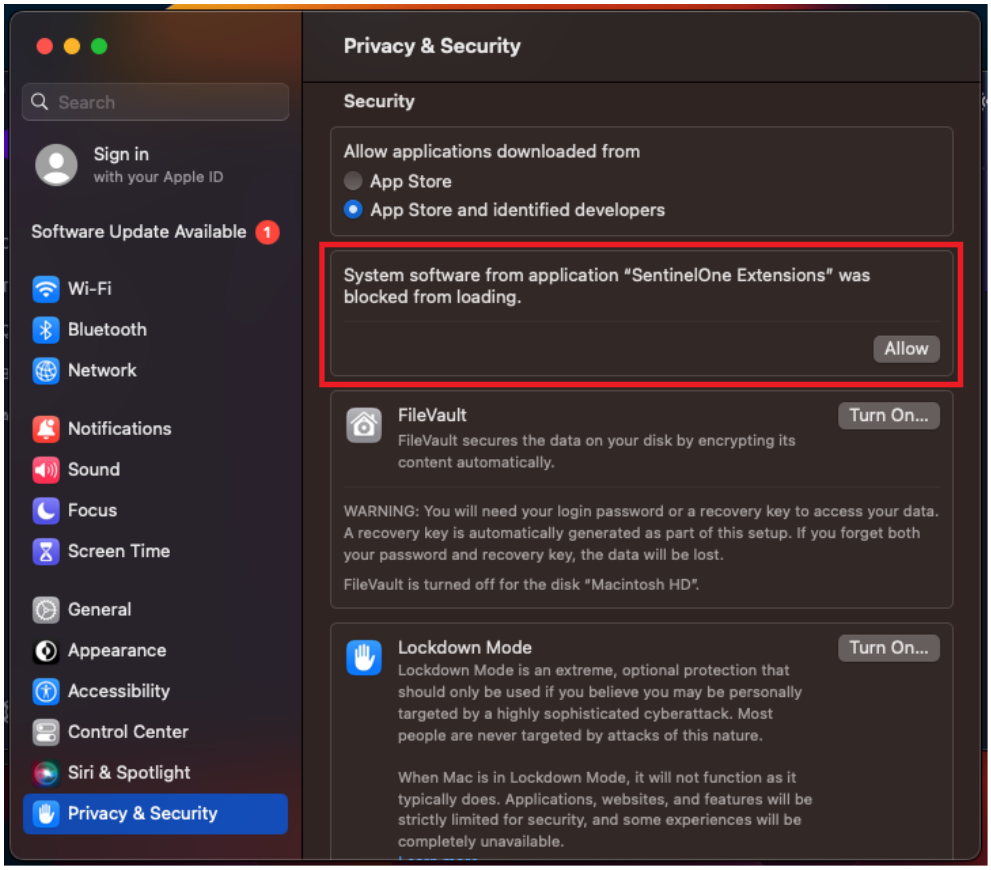


To approve Network Extension

1. If you see the **System Extension Blocked** message, click **Open System Settings**.
    a. Note: If you click **OK**, the window closes. To approve the SentinelOne Network Extension later, open **System Preferences > Privacy & Security >** scroll down to **Security**.



2. At **System software from application "SentinelOne Extensions" was blocked from loading,** click **Allow**.



3. In the window that opens, click **Allow**.

Deployment Via MDM

SentinelOne officially tests the installation and management of the macOS Agent only with Jamf and Workspace ONE. There are separate instructions for Jamf available upon request.

If you use a different Mobile Device Management (MDM) solution, make sure that the MDM solution supports these features:

- Deployment of macOS .pkg.
- Deployment of macOS system configuration profiles.
- Deployment of admin-configured tool/script

Requirements and Documentation

Before you install or upgrade the Agent, see the System Requirements for supported macOS versions and other prerequisites.

Full Disk Access Policy

Grant Full Disk Access to these SentinelOne components:

- **com.sentinelone.sentineld**
  - **Identifier:** com.sentinelone.sentineld
  - **Identifier Type:** Bundle ID
  - **Code Requirements:**

```
anchor apple generic and identifier "com.sentinelone.sentineld" and
(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and
certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and
certificate leaf[subject.OU] = "4AYE5J54KN")
```

- **com.sentinelone.sentineld-helper**
  - **Identifier:** com.sentinelone.sentineld-helper
  - **Identifier Type:** Bundle ID
  - **Code Requirements:**

```
anchor apple generic and identifier "com.sentinelone.sentineld-helper"
and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and
certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and
certificate leaf[subject.OU] = "4AYE5J54KN")
```

- For Agents 21.7 and later, grant Full Disk Access to **com.sentinelone.sentineld-shell**.
    - **Identifier:** com.sentinelone.sentineld-shell
    - **Identifier Type:** Bundle ID
    - **Code Requirements:**

```
anchor apple generic and identifier "com.sentinelone.sentineld-shell"
and (certificate leaf[field.1.2.840.113635.100.6.1.9] or certificate
1[field.1.2.840.113635.100.6.2.6] and certificate
leaf[field.1.2.840.113635.100.6.1.13] and certificate leaf[subject.OU] =
"4AYE5J54KN")
```

Network Monitoring Extension Policy

The SentinelOne Agent Network Extension is used for Deep Visibility™ IP networks events, Firewall Control, and Network Quarantine capabilities.

Grant access to this policy for Firewall Control and Network Quarantine capabilities and for Deep Visibility™ network event features:

- **Display Name**: SentinelOne Network Monitoring Extension
- **System Extension Types**: Allowed System Extensions
- **Team Identifier**:4AYE5J54KN
- **Allowed System Extensions:** com.sentinelone.network-monitoring

Creating a Network Monitoring Extension Profile

Use the Network Monitoring Extension profile to pre-authorize the installation of the Network Extension.

The instructions here describe the steps in JAMF. Use a similar procedure in other MDM tools.

To create a New Configuration Profile

1. Download the Network Monitoring Extension mobileconfig file.
2. Click **Computers** > **Configuration Profiles**.
3. Click **+ New**.
4. In the sidebar on the left click **System Extensions**
5. Create a new Allowed Team ID's and System Extensions profile:
    - **Display Name**: SentinelOne Network Monitoring Extension
    - **System Extension Types**: Allowed System Extensions
    - **Team Identifier**:4AYE5J54KN

- **Allowed System Extensions:** com.sentinelone.network-monitoring

6. Optional: Create a Removable System Extension to pre-authorize the removal of the system extension when the Agent is uninstalled.

Note

- Supported on macOS Monterey and later.
- If you use the removable System Extension, use the SentinelOne Removable System Extension moblieconfig file.

- **Display Name**: SentinelOne Removable Network Monitoring Extension
- **System Extension Types**: Removable System Extensions
- **Team Identifier**:4AYE5J54KN
- **Removable System Extensions:** com.sentinelone.network-monitoring

7. Click Save.
8. Click **Scope**.
9. Select **Targets** and set the devices to receive the configuration profile.
10. Click **Save**.

Network Filter Validation Policy

Use the Network Filter Validation policy to pre-authorize the usage of the SentinelOne Network Filter by the Network Monitoring Extension.

Grant access to this policy for Firewall Control and Deep Visibility™ network events features:

- **Filter Type:** Plugin
- **Plugin bundle identifier:** com.sentinelone.extensions-wrapper
- **Filter data provider bundle identifier:** com.sentinelone.network-monitoring
- **Filter data provider designated requirement:**

```
anchor apple generic and identifier "com.sentinelone.network-monitoring" and
(certificate leaf[field.1.2.840.113635.100.6.1.9] or certificate
1[field.1.2.840.113635.100.6.2.6] and certificate
leaf[field.1.2.840.113635.100.6.1.13] and certificate leaf[subject.OU] =
"4AYE5J54KN")
```

- **Filter sockets:** true

Creating a Network Filter Validation Profile

Use the Network Filter Validation profile to pre-authorize the usage of the SentinelOne Network Filter by the Network Monitoring Extension.

The instructions here describe the steps in JAMF. Use a similar procedure in other MDM tools.

To Upload a New Configuration Profile:

1. Download the Network Filter Validation mobileconfig file.
2. Click **Computers** > **Configuration Profiles**.
3. Click **Upload**.
4. Click **Choose File**.
5. Select the **Network Filter Validation** mobileconfig file you downloaded, and click **Upload**.

   Alternatively, copy this text and save it as a mobileconfig file.