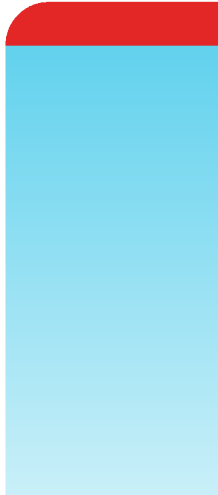


# Jamf Deployment Guide

## FortiClient 7.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



December 07, 2022

FortiClient 7.0 Jamf Deployment Guide

04-700-825779-20221207

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Change log</b>                                 | <b>4</b>  |
| <b>Introduction</b>                               | <b>5</b>  |
| <b>User-initiated enrollment for computers</b>    | <b>6</b>  |
| <b>Enrolling a macOS device in Jamf</b>           | <b>7</b>  |
| <b>Configuration profiles</b>                     | <b>8</b>  |
| <b>Deploying FortiClient using a shell script</b> | <b>11</b> |
| <b>Policy</b>                                     | <b>13</b> |
| <b>Debugging</b>                                  | <b>15</b> |

## Change log

| Date       | Change Description |
|------------|--------------------|
| 2022-12-07 | Initial release.   |
|            |                    |
|            |                    |
|            |                    |
|            |                    |
|            |                    |

# Introduction

This document provides information about deploying FortiClient (macOS) using Jamf mobile device management.

# User-initiated enrollment for computers

This process assumes that a user already has a push certificate configured on the Jamf Pro instance. The administrator can allow users to enroll their own computer by having them log in to an enrollment portal where they follow the onscreen instructions to complete the enrollment process.

## To configure user-initiated enrollment for computers:

1. In Jamf Pro, go to *Settings > Global Management > User-Initiated Enrollment*.
2. Click *Edit*.
3. Use the *General* pane to configure settings as needed for restricting reenrollment, skipping certificate installation or uploading a third party signing certificate to use during enrollment.



Jamf skips the certificate installation step by default.

- 
4. On the *Messaging* pane, do the following to customize the text displayed on devices during the enrollment experience or add languages. Do one of the following:
    - a. To add a language, click *Add*. Select the language from the *Language* popup menu.



English is the default language if the device does not have a preferred language set on it.

- 
- b. To customize the text for a language already listed, click *Edit* next to the language.
5. On the *Platform* tab, select macOS and enable user-initiated enrollment for computers and specify the username and password for the enrollment account.

# Enrolling a macOS device in Jamf

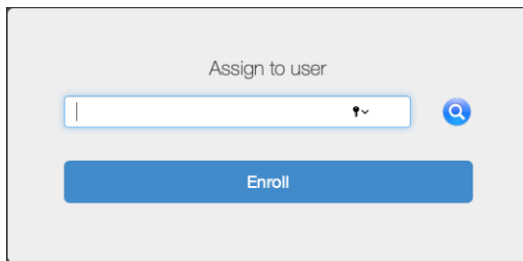
Enrollment is the process of adding computers and mobile devices to Jamf Pro. This establishes a connection between the computers and mobile devices and the Jamf Pro server. User-initiated enrollment allows users to initiate the enrollment process on their own by going to an enrollment URL. The following are examples:

- Hosted in Jamf Cloud: <https://instancename.Jamfcloud.com/enroll>
- Hosted on-premise: <https://jss.instancename.com:8443/enroll>

Once you log in and enroll your end device, the enrollmentProfile.mobileconfig file gets downloaded onto your device. You can open that file with Profile helper, then mobile device management (MDM) profiles are added.

The user must follow the onscreen instructions to install the certificate authority (CA) certificate. After the CA certificate is installed, the user must return to their web browser to install the MDM profile and complete enrollment.

You can click *Enroll* without providing a username.



The Jamf built-in certificate is added to the keychain.

The device has been enrolled and Jamf Pro can manage it.



Clicking *Enroll* redirects to a webpage where you can assign the device to a user. For the enrollment to succeed, leave it blank. You can assign the enrolled device to a group on the Jamf side.

For effective functionality, use a physical machine for enrollment. Jamf does not fully support virtual machine enrollment, as they can be inconsistent and cause issues.

# Configuration profiles

When deploying FortiClient (macOS) without Jamf Pro configuration profiles, the endpoint displays the following prompts to the user:

- To grant full disk access to load the following FortiClient processes:
  - FortiClient
  - fmon2
  - fcaptmon
  - fctservctl2
- To grant FortiTray permissions to load and grant network access for following extensions:
  - com.fortinet.forticlient.macos.webfilter
  - com.fortinet.forticlient.macos.vpn.nwextension
  - com.fortinet.forticlient.macos.proxy (only for FortiClient 7.0.6 and above)

Efficient and silent deployment of FortiClient (macOS) requires a Jamf Pro custom configuration profile that allows all the required prompts.

## To configure profiles on Jamf Pro:

1. Log in to Jamf Pro. Go to *Computers > Configuration Profiles*.
2. Download the FortiClient\_<version.build>\_macosx.Jamf.mobileconfig sample configuration profile file:
  - a. Go to [Fortinet Services & Support > Firmware Images](#).
  - b. From the *Select Product* dropdown list, select *FortiClientMac*.
  - c. On the *Download* tab, go to *FortiClientMac > Mac > v7.00 > 7.0*. Select the latest FortiClient version.
  - d. Download the FortiClient\_<version.build>\_macosx.Jamf.mobileconfig sample configuration profile file.
3. Prepare the configuration profile with the EMS zero trust network access (ZTNA) root CA certificate. You can silence the ZTNA certificate prompt by adding the certificate content to the configuration profile between <data> and </data>, or by directly uploading the certificate as a trusted certificate in the Jamf configuration profile after changing the extension types. To add the certificate content to the configuration profile between <data> and </data>, do the following. To directly upload the certificate as a trusted certificate in the Jamf configuration profile after changing the extension types, proceed to step 4:
  - a. On a macOS endpoint where FortiClient is registered to EMS, go to `/Library/Application Support/Fortinet/FortiClient/data/ca_certs/ztna_certs`.
  - b. Copy the certificate content to an accessible location.
  - c. Open the configuration profile file in a text editor, remove `<!-- Add your ZTNA root certificate here -->` and add the certificate content that you copied between <data> and </data>. The following shows an example of the CA certificate payload:

```
</data>
<dict>
<key>PayloadCertificateFileName</key>
<string>EMS_ZTNA_CA.cer</string>
<key>PayloadContent</key>
<data>
<!-- Add your ZTNA root certificate here -->
```



```
</data>
<key>PayloadDescription</key>
<string>Adds a CA root certificate</string>
<key>PayloadDisplayName</key>
<string>EMS ZTNA CA CERTIFICATE</string>
<key>PayloadIdentifier</key>
<string>com.apple.security.root.1255DA5E-C9F1-4FBF-9967-4000DDF1DFC5</string>
<key>PayloadType</key>
<string>com.apple.security.root</string>
<key>PayloadUUID</key>
<string>1255DA5E-C9F1-4FBF-9967-4000DDF1DFC5</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
```

d. Save the modified mobileconfig profile.

4. Click *Upload*, choose *File*, and upload a mobile configuration file available from the Fortinet support page.
5. After uploading an XML mobile configuration file, you must complete some required fields such as team identifiers under system extensions. You must modify the file in the GUI under *System Extensions*. Click *Allow users to approve system extensions*.

Users cannot import system extensions using a mobile configuration file on Jamf Pro and must manually change settings as follows:



- Systems extensions type to allowed system extensions
- Set team identifier to AH4XFXJ7DK
- Add following system extensions to allowed system extensions list and save them:
  - com.fortinet.forticlient.macos.vpn.nwextension
  - com.fortinet.forticlient.macos.webfilter
  - com.fortinet.forticlient.macos.proxy (only for FortiClient 7.0.6 and above)

6. Go to *Content Filter*. Configure the required fields: *Filter Name*, *Identifier*, *Filter Order (inspector)*, *Socket Filter Bundle Identifier*, and *Socket Filter Designated Requirement*.

Computers : Configuration Profiles
< Configuration Profile for FortiClient

Options
Scope
Show in Jamf Pro Dashboard

General
VPN
1 payload configured
Privacy Preferences Policy Control
1 payload configured
System Extensions
1 payload configured
Content Filter
Settings configured: 4

Unknown Keys
Jamf Pro cannot recognize one or more settings in this payload and display them in the interface. To avoid potential issues with Jamf Pro upgrades, review the key-value pairs in the profile and decide if they are correct and needed in your environment. Download the profile and store a copy of the original file in a preferred location. Edit the .mobileconfig file as required and upload the modified profile to Jamf Pro. Alternatively, if your environment does not need the unknown keys, use the interface to remove them. To keep your changes, save the profile. Note that during the configuration profiles redesign, the PayloadEnabled key is marked as unknown by default. You can safely remove it from the .mobileconfig file because it is not required in a profile definition.

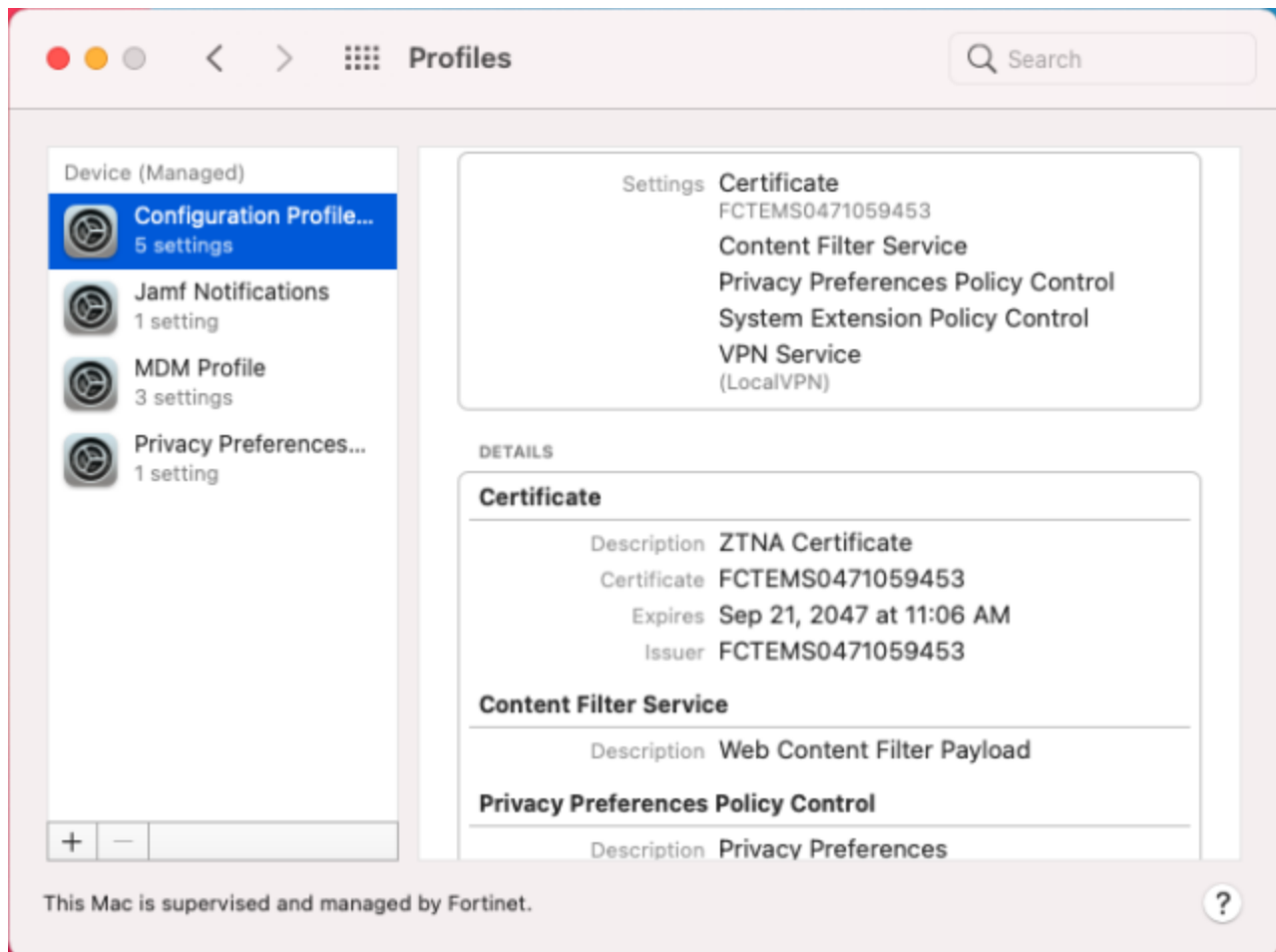
Content Filter
Settings configured: 4
Filter Name
Display name of the filter in the app and on the device
Fortinet Content Filter
Identifier
Identifier for the filter plug-in
com.fortinet.forticlient.macos
Filter Order
Specify the order in which traffic is filtered. Filters with a grade of firewall see network traffic before filters with a grade of inspector.
Inspector
Socket Filter
Socket Filter Bundle Identifier
Bundle identifier of the socket filter provider system extension
com.fortinet.forticlient.macos.webfilter
Socket Filter Designated Requirement
Designated requirement of the socket filter provider system extension
Identifier "com.fortinet.forticlient.macos.webfilter" and anchor apple generic and certificate "[field:1.2.840.113635.100.6.2.6]" exists "/" and certificate leaf[field:1.2.840.113635.100.6.113]" exists "/" and certificate leaf[subject.OU] = AH4XFXJ7DK

7. If you did not add the certificate content to the configuration profile in step 4, directly upload the certificate as a trusted certificate in the Jamf configuration profile after changing the extension types:
  - a. Go to *Options > Certificate*.
  - b. Upload the ZTNA root CA certificate.
  - c. Enable *Allow export from keychain*.
  - d. Click *Save*.



You can follow either method to silence the certificate prompts during FortiClient deployment. Configuring the certificate using both methods does not affect the FortiClient deployment and only one ZTNA root CA certificate is present in the keychain.

8. On the *Scope* tab, select the target computers where you want to assign this configured profile.
9. To verify if the endpoint gets proper profiles, go to *System Preferences > Profiles*. Ensure that all required extensions are allowed.



# Deploying FortiClient using a shell script

After adding a profile, you must create a policy to deploy FortiClient. With Jamf Pro, you can deploy FortiClient to macOS devices that have any user accounts (administrator and non-administrator user accounts) without requiring user interaction. You can deploy FortiClient in the following way:

For this procedure, all macOS devices should meet the following prerequisites:

- Running macOS Catalina (version 10.15) or a later version
- Managed by Jamf Pro
- Shell scripts begin with `#!/` and are in a valid location, such as `#!/bin/sh` or `#!/usr/bin/env zsh`.
- Command line interpreters for the applicable shells are installed.

## To modify the script file:

1. On a test macOS device, download the FortiClient deployment shell script .sh file:
  - a. From [Fortinet Service & Support](#), go to *Firmware Images*.
  - b. From the *Select Product* dropdown list, select *FortiClientMac*.
  - c. On the *Download* tab, go to *Mac > v7.00 > 7.0*.
  - d. Select the latest shell scripts.
2. In a terminal, open the downloaded script file.
3. Do one of the following:
  - a. If using on-premise EMS, modify the `weburl` value to your FortiClient download link from EMS. For example, you would change the value from `weburl=<"FortiClient download URL from EMS">` to `weburl="https://your_EMS_FQDN:10443/installers/Default/FCT_MAC_7.0.7_GA/FortiClient_7.0.7.dmg"`, if the download link is `https://your_EMS_FQDN:10443/installers/Default/FCT_MAC_7.0.7_GA/FortiClient_7.0.7.dmg`.
  - b. If using FortiClient Cloud, download the FortiClient installer from FortiClient Cloud. Extract the .zip file. Copy the .dmg file to a local web server that endpoints can reach and that you own. Modify the `weburl` value to your local web server URL.
4. Modify the `FortiClient_Installerversion` value in the script file based on your FortiClient installer version. For example, change the value from `FortiClient_Installerversion=<Your FortiClient Installer version>` to `FortiClient_Installerversion="7060245"` if the FortiClient version is 7.0.7.0245. Enter the version number without periods.
5. Modify the values `av`, `af`, `sb`, `sra`, `sso`, `vs`, `wf`, and `ztna` values to 1 or 0 based on the enabled features in the FortiClient installer. For example, change the value from `av=<Feature enabled or disabled>` to `av="1"` to enable malware protection. Otherwise, set `av="0"` to disable malware protection on the FortiClient installer. By default, all values for `av`, `af`, `sb`, `sra`, `sso`, `vs`, `wf`, and `ztna` are set to "1" based on the default installer with all features enabled.
6. If desired, modify the script file based on your requirements. The shell script mainly performs the following tasks:
  - Uninstalling older FortiClient versions if present and installing a new version
  - Downloading the FortiClient deployment package from the EMS server. The managed macOS device must be able to access the download link to download the package.
  - Installing FortiClient on a fresh macOS device.
  - Skipping FortiClient uninstallation if trying to install same FortiClient version
  - Upgrading free VPN-only FortiClient to full FortiClient

- Upgrading to same or different version of FortiClient with different security features enabled that are unavailable on existing FortiClient

## 7. Save the file.

### To add the script to Jamf Pro using the script editor:

1. In Jamf Pro, go to *Settings > Computer Management > Scripts*.
2. Click *New*.
3. In the *General* pane, configure the script's basic settings, including the display name and category.
4. On the *Script* tab, enter the script contents in the editor. You can use the tab settings to configure syntax highlighting and theme colors in the script editor.
5. On the *Options* tab, configure additional settings for the script, including the priority.
6. (Optional) On the *Limitations* tab, configure operating system requirements for the script.
7. Click *Save*.

Settings : Computer Management > Scripts

← FCT Installation script

General **Script** Options Limitations

Mode: Default Theme: Default

```

1  #!/bin/bash
2
3  weburl="https://Your Ems IP:10443/installers/Default/707/FortiClient_7.0.7.dmg" # Replace with your own URL path
4
5  FortiClient_InstallerVersion="7070245" #Enter your FortiClient installer version
6
7  # Please modify below values based on the new FCT installer feature set created on the EMS, and please don't modify other part of the script.
8
9  av="1" # Enter 0 when Malware feature is disabled in the FortiClient installer
10 af="1" # Enter 0 when Application Firewall feature is disabled in the FortiClient installer
11 sb="0" # Enter 0 when Advanced Persistent Threat (APT) components feature is disabled in the FortiClient installer
12 sra="1" # Enter 0 when Secure Access Architecture Components feature is disabled in the FortiClient installer
13 sso="0" # Enter 0 when Single Sign-On Mobility Agent feature is disabled in the FortiClient installer
14 vs="1" # Enter 0 when vulnerability Scan feature is disabled in the FortiClient installer
15 wf="1" # Enter 0 when Web Filtering feature is disabled in the FortiClient installer
16
17 # FortiClient 6.4 does not have ZTNA feature, and FCT 7.0 or higher version will always install ZTNA feature because of the mantis 0825169.
18
19 # ztna="1" # You should keep this value as "1" until the mantis 0825169 get fixed.
20
21
22 tmpdir="/tmp/Installer"
23 MOUNT_POINT="$tmpdir/mount"
24
25 appname="FortiClient" # The name of our App deployment script (also used for Octory monitor)
26
27 logandmetadir="/Library/Logs/MDM/$appname"
28 log="$logandmetadir/$appname.log"

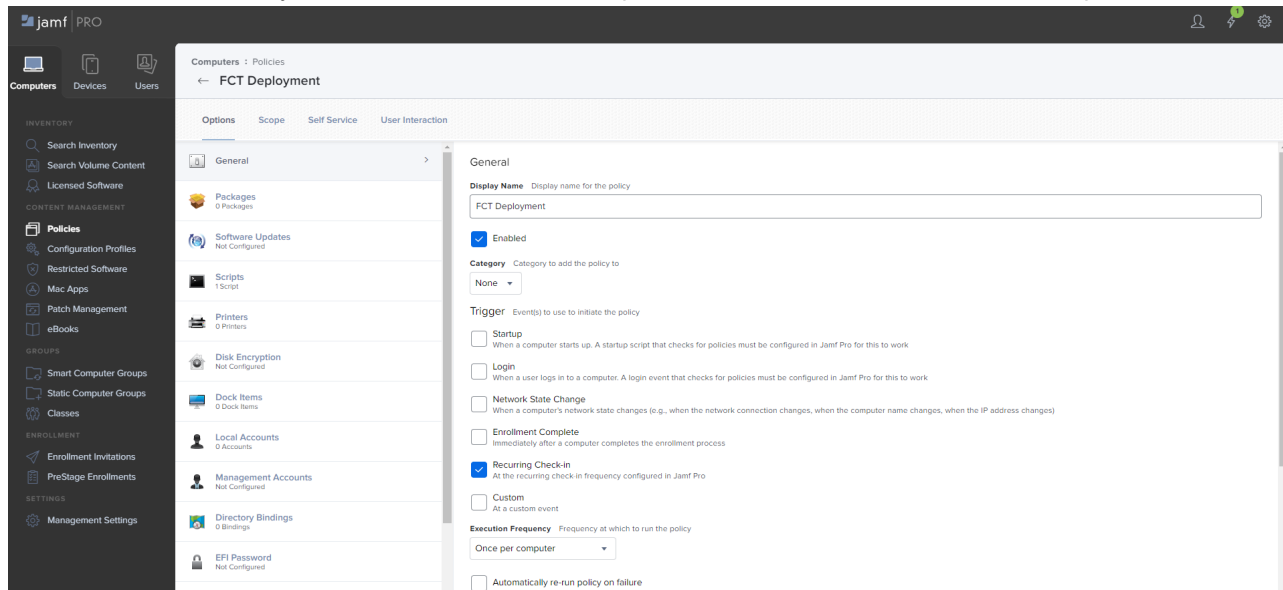
```

# Policy

Policies allow you to remotely automate common management tasks on managed computers. Using a policy, you can run scripts, manage accounts, and distribute software. When you create a policy, you specify the tasks that you want to automate, how often it runs (execution frequency), when the policy runs (trigger), and the users and computers for which it runs (scope). You can also make policies available in Self Service for users to run on their computers as needed.

## To configure a policy:

1. In Jamf Pro, go to *Computers > Policies*.
2. Click *New*.
3. Under *General*, configure the policy's basic settings, including the trigger and execution frequency.
4. Configure the desired tasks.
5. Under *Scripts*, select *configure*, and add the script that you created for FortiClient installation.
6. On the *Scope* tab, configure the policy scope.
7. (Optional) On the *Self Service* tab, make the policy available in Self Service.
8. Click *Save*. Jamf Pro may take some time to run the script on devices, based on the Jamf Pro computer ID.



The recurring check-in frequency is the interval at which the computer checks in with Jamf Pro for available policies. By default, the recurring check-in frequency is set to every 15 minutes. You can manually configure a different interval.

## To manually configure recurring check-in:

1. Go to *Settings*.
2. Under *Computer Management-Management Framework*, click *Check-In*.
3. Click *Edit*.
4. Configure the recurring check-in frequency using the popup menu.

5. Click **Save**. Each computer checks in at the specified interval, starting at the time that you apply the setting to the computer. Check-in times vary across computers.



You can monitor statuses related to policies in the Jamf Pro dashboard.

---

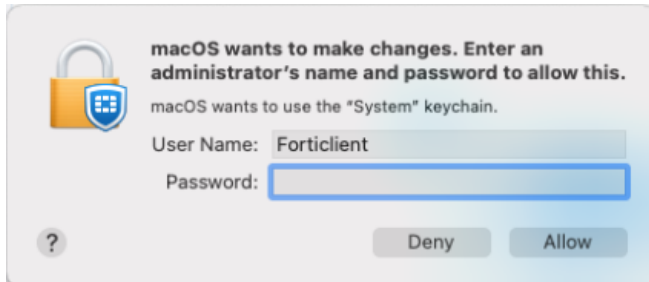
# Debugging

## To check deployment status and logs on endpoints:

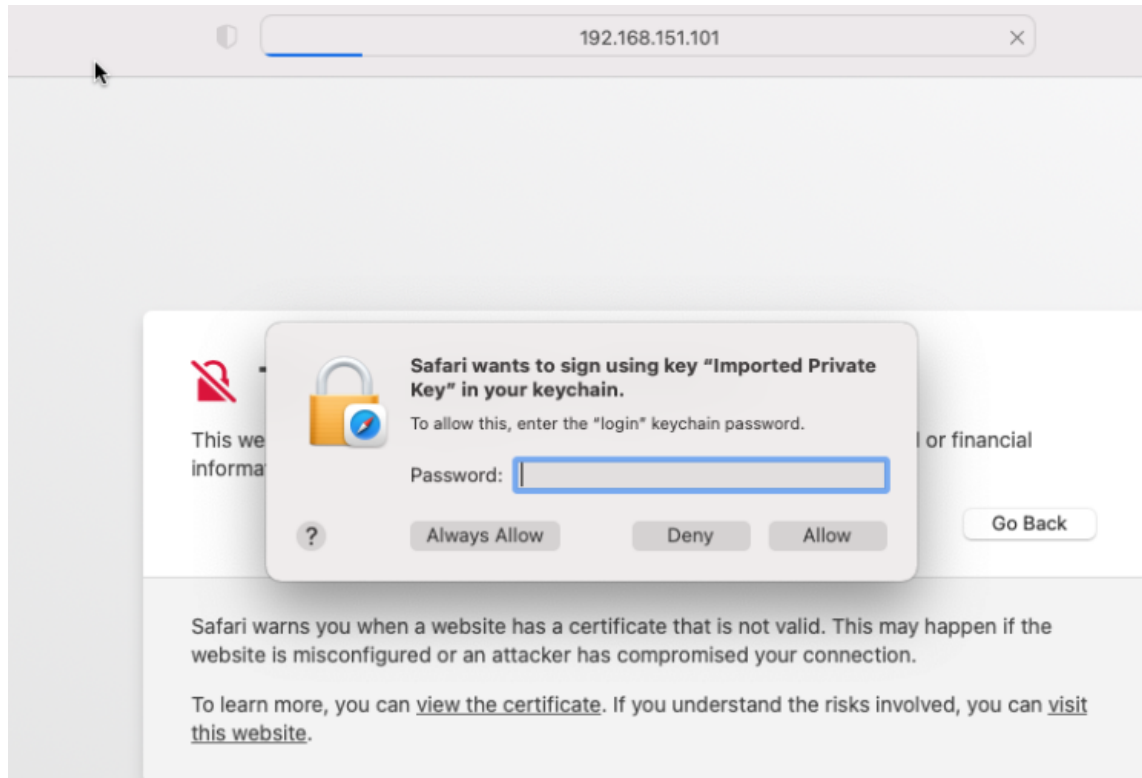
1. In the console application, go to log reports.
2. Look for the Jamf.log and Forticlient.log files. You can see logs related to FortiClient deployment and installation.

Note the following:

- Manually uninstalling FortiClient using the FortiClientUninstaller tool removes the VPN virtual adapter and stored zero trust network access (ZTNA) certificates on the endpoint. As a result, reinstalling FortiClient displays the FortiTray VPN and system keychain modification prompts. In this case, push and distribute the MDM configuration profile again before reinstalling FortiClient to fully silence the prompts.
- When connecting to VPN with client certificates, the system prompts the user for keychain access credentials to access and read the stored certificate. The user can decide to allow or deny access. Selecting *Always Allow* silences future prompts when FortiTray accesses the certificate.

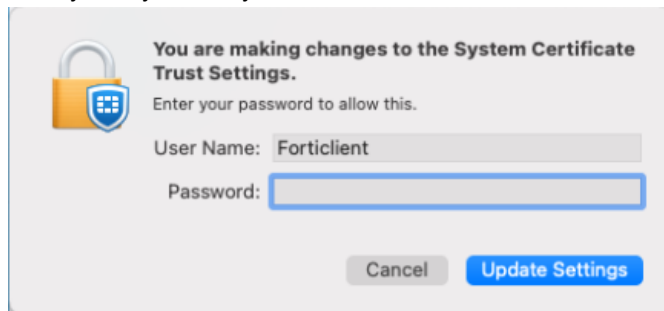


- When FortiClient acts as a ZTNA client, the system is expected to display prompts to ask for user credentials to access the ZTNA client certificate stored in the login keychain.

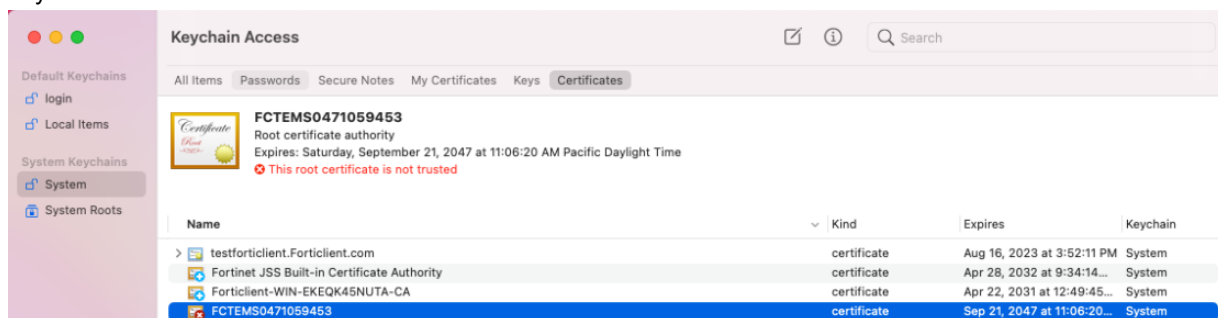


The ZTNA feature does not work if you click *Allow*. Select *Always Allow*.

- Revoking the endpoint client certificate from EMS results in the system prompting for administrator credentials to modify the system keychain.



- If you revoke the ZTNA root CA Certificate, the system prompts for administrator credentials to modify the system keychain.







[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.