

# Integrating with Active Directory Certificate Services (AD CS) Using Jamf Pro

Technical Paper  
Jamf Pro 10.6.0 or Later  
3 December 2020

© copyright 2002-2020 Jamf. All rights reserved.

Jamf has made all efforts to ensure that this guide is accurate.

Jamf  
100 Washington Ave S Suite 1100  
Minneapolis, MN 55401-2155  
(612) 605-6625

Jamf, the Jamf Logo, JAMF SOFTWARE®, and the JAMF SOFTWARE Logo®, are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

Microsoft, Active Directory, Windows, Windows Server, and all references to Microsoft software are either registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries.

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

# Contents

## **4 Introduction**

4 Target Audience

4 What's In This Guide

4 Important Concepts

4 Additional Resources

## **5 Overview**

6 Communication Overview

## **7 Install the Jamf AD CS Connector**

7 Installed Applications

8 Jamf AD CS Connector Certificates

8 Requirements

9 Installing the Jamf AD CS Connector

## **10 Integrate with Active Directory Certificate Services**

10 Requirements

10 Adding AD CS as a PKI Provider in Jamf Pro

11 Viewing and Editing CA Information

12 Viewing AD CS Certificates

## **13 Distribute Certificates Using Configuration Profiles**

13 Requirements

13 Distributing a Certificate Using a Configuration Profile

## **15 Distribute In-House Apps Developed with the Jamf Certificate SDK**

15 Requirements

15 Distributing an In-House App Developed with the Jamf Certificate SDK

## **18 Managed App Configuration Reference for In-House Apps Developed with the Jamf Certificate SDK**

# Introduction

## Target Audience

This guide is designed for IT administrators who want to integrate Jamf Pro with Active Directory Certificate Services (AD CS) to use AD CS as the certificate authority (CA) for distributing certificates to computers and mobile devices.

## What's In This Guide

This guide provides a step-by-step workflow to integrate Jamf Pro with AD CS. Integrating with AD CS allows you to add AD CS as a PKI Provider in Jamf Pro to use as the CA for distributing certificates to devices via configuration profiles.

## Important Concepts

Before using the instructions in this guide, make sure you are familiar with the following Jamf Pro-related concepts:

- Public key infrastructure
- Computer and mobile device configuration profiles
- App distribution

In addition, ensure you are familiar with Managed App Configuration.

## Additional Resources

For more information about the applications, concepts, and processes mentioned in this guide, see the [Jamf Pro Administrator's Guide](#).

For more information about Managed App Configuration, see the following websites:

- <https://www.jamf.com/developers/managed-app-configuration/>
- <https://www.appconfig.org/ios/>

# Overview

Jamf Pro allows you to add Active Directory Certificate Services (AD CS) as a PKI Provider in Jamf Pro. This allows you to use AD CS as the certificate authority (CA) for distributing certificates to computers and mobile devices via configuration profiles.

Adding AD CS as a PKI Provider for certificate distribution involves the following steps:

1. **Install the Jamf AD CS Connector**

The Jamf AD CS Connector is a service that allows Jamf Pro to securely communicate with the AD CS certificate authority server.

2. **Integrate Jamf Pro with AD CS**

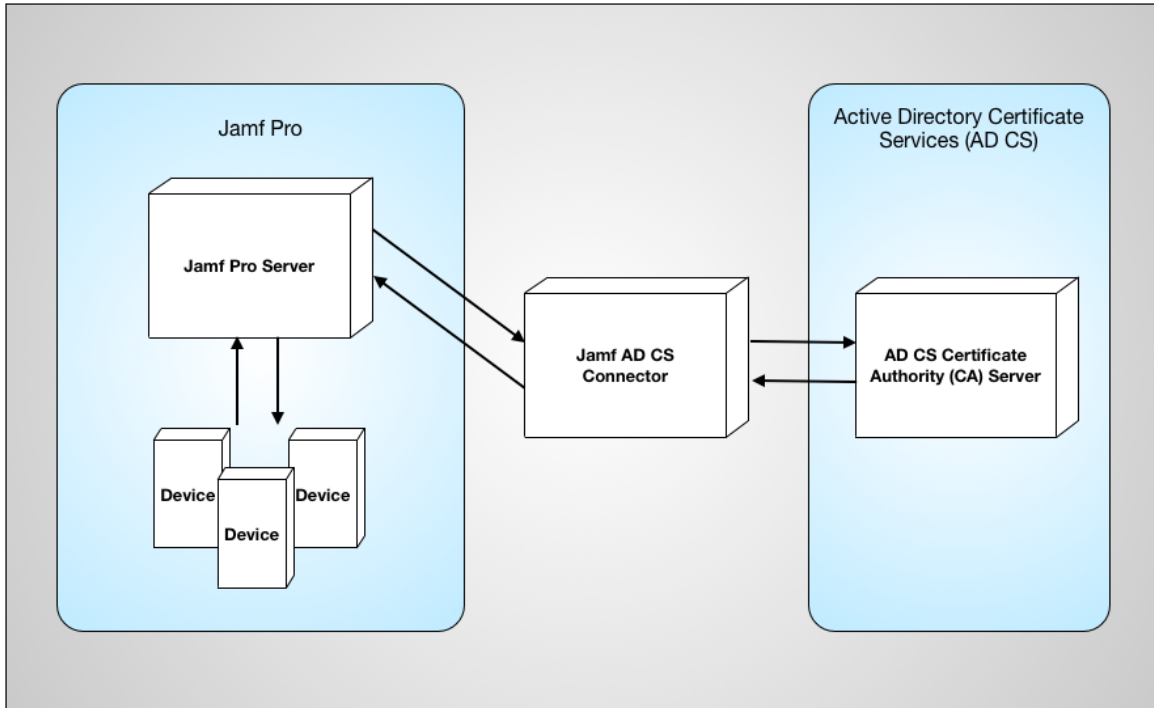
Integrating with AD CS involves configuring settings in Jamf Pro to define the location of the CA server for Jamf Pro. In addition, you can use Jamf Pro to configure settings for the Jamf AD CS Connector to establish secure communication between Jamf Pro and AD CS.

After communication between Jamf Pro and AD CS has been established, you can use the following technologies in Jamf Pro for certificate management:

- **Configuration Profiles**—Jamf Pro allows you to distribute certificates via configuration profiles using AD CS as the CA.
- **In-house Apps**—You can distribute in-house apps developed with the Jamf Certificate SDK to establish identities to support certificate-based authentication to perform Single Sign-On (SSO) or other actions specific to your environment. Jamf Pro allows you to apply a Managed App Configuration to the app during distribution to enable the app to request the necessary certificates.

# Communication Overview

Jamf Pro uses the Jamf AD CS Connector to communicate with AD CS to obtain certificates. The following diagram illustrates how communication is transferred to and from Jamf Pro and AD CS using the Jamf AD CS Connector:



This communication process is started when devices check in with Jamf Pro. If a device requires a certificate (in response to the Jamf Certificate SDK or to a configuration profile), a certificate signing request (CSR) is generated by Jamf Pro and sent to AD CS. AD CS processes the CSR and sends a Request ID back to Jamf Pro. Jamf Pro provides the Request ID to AD CS. When the certificate is ready, AD CS sends it to Jamf Pro and the certificate (.p12) is distributed to the device. All communication between Jamf Pro and AD CS takes place using the Jamf AD CS Connector.

# Install the Jamf AD CS Connector

Before you can integrate Jamf Pro with Active Directory Certificate Service (AD CS), you must install the Jamf AD CS Connector. This service securely transfers all communication between Jamf Pro and AD CS.

When you install the Jamf AD CS Connector, the installer automatically does the following:

- Installs and configures the applications needed to run the Jamf AD CS Connector. For more information, see [Installed Applications](#).
- Installs the Jamf AD CS Connector.
- Generates the certificates required to secure communication with Jamf Pro. For more information, see [Jamf AD CS Connector Certificates](#).

## Installed Applications

When you install the Jamf AD CS Connector, Microsoft Internet Information Services (IIS) for Windows Server is automatically installed. Microsoft IIS is the web application server that runs the Jamf AD CS Connector. A directory named `AD CS Proxy` is installed in the following location:

```
C:\inetpub\wwwroot\adcsproxy
```

For more information about IIS, see the following website:

<https://www.iis.net>

In addition, the following are automatically configured when you install the Jamf AD CS Connector:

- **IIS Client Certificate Mapping Authentication**—IIS is automatically configured to enable communication between Jamf Pro and the Jamf AD CS Connector to take place using IIS Client Certificate Mapping Authentication. For more information about IIS Client Certificate Mapping Authentication, see the [Microsoft Configuration Reference Documentation](#).
- **ASP.NET**—This provides the application framework for the Jamf AD CS Connector and is integrated with the instance of the IIS web application.

# Jamf AD CS Connector Certificates

When you install the Jamf AD CS Connector, the following certificates are automatically generated:

Certificate	Details
<b>Server certificate (.pem or .cer)</b>	<p>This certificate ensures trust between Jamf Pro and the Jamf AD CS Connector. It is a self-signed SSL certificate generated when the Jamf AD CS Connector is installed and allows IIS to validate client certificates.</p> <p>The server certificate is exported to the current working directory with the following filename: <code>adcs-proxy-ca.cer</code></p> <p><b>Note:</b> The server certificate is required when configuring Jamf Pro to communicate with the Jamf AD CS Connector.</p>
<b>Client certificate (.pfx or .p12)</b>	<p>This certificate allows Jamf Pro to authenticate with the Jamf AD CS Connector. The client certificate is generated when the Jamf AD CS Connector is installed and is signed by the server certificate. It is exported in PFX format using a randomly generated password that is output to the shell during the Jamf AD CS Connector installation.</p> <p><b>Note:</b> The client certificate and randomly generated password are required when configuring Jamf Pro to communicate with the Jamf AD CS Connector.</p>

Both certificates are required when configuring Jamf Pro to communicate with the AD CS Proxy Service.

## Requirements

The Jamf AD CS Connector requires a server with the following:

- Windows Server 2016 joined to a domain that has a trust relationship with the domain of the certificate authority  
For more information about joining the server to a domain that has a trust relationship with the domain of the certificate authority, see the following Microsoft documentation:  
[Joining Server Computers to the Domain and Logging On](#)
- .NET Framework 4.5 or later  
For more information about .NET Framework, see the following website:  
<https://www.microsoft.com/net>



## Network Communication

The Jamf AD CS Connector requires the following TCP ports and protocols:

- **DCOM**—The Jamf AD CS Connector uses Microsoft Distributed Component Object Model (DCOM) to communicate with AD CS. You must have the following TCP ports open for this communication:
  - 135
  - 49152-65535

For more information about Microsoft DCOM, see the following website:

[https://docs.microsoft.com/en-us/openspecs/windows\\_protocols/ms-dcom/4a893f3d-bd29-48cd-9f43-d9777a4415b0](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-dcom/4a893f3d-bd29-48cd-9f43-d9777a4415b0)

- **HTTPS**—Jamf Pro initiates HTTPS connections with the Jamf AD CS Connector, typically on TCP port 443. The HTTPS port needs to be opened, inbound, on your network firewall and also on the Windows Firewall running on the server on which the Jamf AD CS Connector is installed.

In addition, since the Jamf AD CS Connector host must be bound to the domain, the ports required by Microsoft to support binding should be open between the Jamf AD CS Connector host and AD domain controller.

For more information, see the [Network Ports Used by Jamf Pro](#) knowledge base article.

## Installing the Jamf AD CS Connector

1. Log in to Jamf Nation and go to the following page:  
<https://www.jamf.com/jamf-nation/my/products>
2. Download the Jamf AD CS Connector to the server on which you plan to install it.
3. Log in to the server as a user with administrator privileges.
4. Double-click the Jamf AD CS Connector to decompress it.
5. Open PowerShell as administrator, and then run the installer by executing a command similar to the following:

```
.\deploy.ps1 -fqdn my.adcs-proxy.url -jamfProDn my.domain.name -cleanInstall
```

This command installs the Jamf AD CS Connector and generates the server and client certificates.

When the Jamf AD CS Connector installation is complete, you can configure settings in Jamf Pro to enable communication between Jamf Pro and the Jamf AD CS Connector.

# Integrate with Active Directory Certificate Services

You can configure the PKI Certificates settings in Jamf Pro to use Active Directory Certificate Services (AD CS) as a PKI Provider.

Adding AD CS as a PKI Provider in Jamf Pro requires you to configure the following settings:

- **AD CS Integration**—These settings define the location of the CA server for Jamf Pro.
- **Jamf AD CS Connection**—These settings enable Jamf Pro to securely communicate with AD CS via the Jamf AD CS Connector.

**Note:** The Jamf AD CS Connector is a service provided by Jamf Pro that must be installed prior to configuring the Jamf AD CS Connection settings in Jamf Pro. For more information, see [Install the Jamf AD CS Connector](#).

After you add AD CS as a PKI Provider in Jamf Pro, you can use the PKI Certificates settings in Jamf Pro to view and edit information about the CA.

In addition, you can use the PKI Certificates settings to view information about the active, expired, or inactive AD CS certificates that have been distributed to devices via configuration profiles.



## Requirements

To integrate with AD CS, you must install the Jamf AD CS Connector. For more information, see [Install the Jamf AD CS Connector](#).

In addition, you need the Jamf AD CS Connector certificates that are generated when you install the Jamf AD CS Connector. For more information, see "Jamf AD CS Connector Certificates" in [Install the Jamf AD CS Connector](#).

## Adding AD CS as a PKI Provider in Jamf Pro

Adding AD CS as a PKI Provider in Jamf Pro requires you to configure the AD CS Integration settings and the Jamf AD CS Connection settings.

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **PKI Certificates** .
5. Click the **Certificate Authority** tab, and then click **Configure New Certificate Authority**.

6. Select **Active Directory Certificate Services (AD CS)** and click **Next**.
7. Configure the AD CS Integration settings:
  - a. Enter the fully qualified domain name of the server that hosts AD CS in the **Fully Qualified Domain Name** field.
  - b. Enter the name of the certificate authority in the **CA Name** field.
8. Configure the Jamf AD CS Connector settings:
  - a. Enter the URL for the location of the Jamf AD CS Connector. If you are using an IP address, contact [Jamf Support](#).
  - b. To upload the server certificate (.pem or .cer), click **Upload** and follow the onscreen instructions. This certificate is generated during the Jamf AD CS Connector installation. For more information, see "Jamf AD CS Connector Certificates" in [Install the Jamf AD CS Connector](#).
  - c. To upload the client certificate (.pfx or .p12), click **Upload** and follow the onscreen instructions. This certificate is generated during the Jamf AD CS Connector installation. For more information, see "Jamf AD CS Connector Certificates" in [Install the Jamf AD CS Connector](#).
9. Click **Save**.
10. Click **Done**.



AD CS is listed as a CA on the Certificate Authorities pane.

When integration with AD CS is complete, you can use Jamf Pro to distribute certificates to devices using configuration profiles with AD CS as the CA. For more information, see [Distribute Certificates Using Configuration Profiles](#).

In addition, if your environment uses in-house apps that have been developed with the Jamf Certificate SDK, you can use Jamf Pro to distribute them. For more information, see [Distribute In-House Apps Developed with the Jamf Certificate SDK](#).

## Viewing and Editing CA Information

After you add AD CS as a PKI Provider in Jamf Pro, you can use the PKI Certificates settings to view and edit information about the CA. For example, you may need to upload a new certificate.



1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **PKI Certificates** .
5. Click **View** for the AD CS certificate in the Managed CA column on the Certificate Authorities pane. The AD CS Integration settings and AD CS Connection Service settings are displayed.
6. Do one of the following:
  - Click **Done** to return to the list of certificates.

- Click **Edit** and make changes as needed. Click **Save**, and then click **Done** to return to the list of certificates.

## Viewing AD CS Certificates

You can view the following information for a certificate issued by AD CS:

- Certificate subject name
- Certificate serial number
- Device name associated with certificate
- Username associated with certificate
- CA Configuration name
- Date/time issued
- Expiration date/time
- Status

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **PKI Certificates** .
5. To view a list of Expiring, Active, Inactive or All certificates, click the number displayed in the corresponding column on the Certificate Authorities pane.  
A list of certificates issued by AD CS is displayed.
6. Click on the certificate subject of the certificate you want to view.  
Information about the certificate is displayed.
7. Click **Done** to return to the list of certificates.

# Distribute Certificates Using Configuration Profiles

After communication between Jamf Pro and Active Directory Certificate Services (AD CS) has been established, you can use Jamf Pro to distribute certificates with AD CS as the certificate authority (CA) to computers and mobile devices in your environment using configuration profiles.

**Note:** Jamf Pro automatically redistributes the certificate via a configuration profile 10 days before the certificate expires.

## Requirements

Before you can distribute certificates using configuration profiles, you must add a PKI Provider to Jamf Pro to use as the CA for certificates. For more information see the following:

- [Integrate with Active Directory Certificate Services](#)
- [PKI Certificates](#) in the *Jamf Pro Administrator's Guide*

In addition, ensure the requirements for distributing configuration profiles are met. See the requirements in the following sections of the *Jamf Pro Administrator's Guide*:

- [Computer Configuration Profiles](#)
- [Mobile Device Configuration Profiles](#)

## Distributing a Certificate Using a Configuration Profile

1. Log in to Jamf Pro.
2. Do one of the following:
  - To create a computer configuration profile, click **Computers** at the top of the page, and then click **Configuration Profiles**.
  - To create a mobile device configuration profile, click **Devices** at the top of the page, and then click **Configuration Profiles**.
3. Click **New**.
4. Use the General payload to configure basic settings, including the level at which to apply the profile and the distribution method.  
Only payloads and settings that apply to the selected level are displayed for the profile.

5. Select the **Certificate** payload and click **Configure**.
6. Enter a display name and then choose an AD CS instance from the **Select Certificate Option** pop-up menu.
7. Use the settings on the pane to specify information about the CA.
8. Click **Save**.

# Distribute In-House Apps Developed with the Jamf Certificate SDK

If your environment uses in-house apps that have been developed with the Jamf Certificate SDK, you can use Jamf Pro to distribute the app to establish identities to support certificate-based authentication. This can enable Single Sign-On (SSO) or other actions specific to your environment. Jamf Pro allows you to apply a Managed App Configuration to the app during distribution to enable the app to request the necessary certificates.

**Note:** In-house apps developed with the Jamf Certificate SDK have only been tested with Active Directory Certificate Services (AD CS) as the certificate authority (CA).

For more information about Managed App Configuration, see the following websites:

- <https://www.jamf.com/developers/managed-app-configuration/>
- <https://www.appconfig.org/ios/>

## Requirements

You must ensure that the in-house app you want to distribute has been developed with the Jamf Certificate SDK.

For more information about the requirements for distributing in-house apps, see [In-House Apps](#) in the *Jamf Pro Administrator's Guide*.

## Distributing an In-House App Developed with the Jamf Certificate SDK

1. Log in to Jamf Pro.
2. Click **Devices** at the top of the page.
3. Click **Mobile Device Apps**.
4. Click **New**.
5. Select **In-house app** and click **Next**.
6. Use the General pane to configure settings for the app, including the distribution method and hosting location.

If you choose "Distribution Points" or "jamfsoftware database" from the **Hosting Location** pop-up menu, be sure to upload the archived app file.

**Note:** Beginning with iOS 10.3, you can require a mobile device to have a tethered network connection to download the app. A tethered network connection requires a computer with macOS 10.12.4 or later, and must be connected to the Internet via Ethernet and have Wi-Fi turned off. Portable computers must be plugged in to a power source because the tethered caching service

prevents computers from going to sleep. Select the **Require tethered network connection for app installation** checkbox. This checkbox is only displayed if "Install Automatically/Prompt Users to Install" is chosen in the **Distribution Method** pop-up menu. App updates will not require tethering; this setting is for initial installations of an app only.

7. Ensure the **Make App Managed when possible** checkbox is selected.
8. Click the **Scope** tab and configure the scope of the app.  
For more information, see [Scope](#) in the *Jamf Pro Administrator's Guide*.
9. (Optional, iOS only) Click the **Self Service** tab and configure the way the app is displayed in Self Service. You can customize the text displayed in the description for the app in Self Service by using Markdown in the **Description** field.  
For information about Markdown, see the following Knowledge Base article:  
[Using Markdown to Format Text](#)  
**Note:** The Self Service tab is only displayed if "Make Available in Self Service" is chosen in the **Distribution Method** pop-up menu.
10. Click the **App Configuration** tab and enter something like the following Managed App Configuration in the **Preferences** field:

```
<dict>
<key>com.jamf.config.jamfpro.invitation</key>
<string>$MOBILEDEVICEAPPINVITE</string>
<key>com.jamf.config.device.udid</key>
<string>$UDID</string>
<key>com.jamf.config.jamfpro.url</key>
<string>https://jamf_pro_server_url/</string>
<key>com.jamf.config.certificate-request.pkiId</key>
<string>PKI_ID</string>
<key>com.jamf.config.certificate-request.template</key>
<string>certificate_template_name</string>
<key>com.jamf.config.certificate-request.subject</key>
<string>certificate_subject</string>
<key>com.jamf.config.certificate-request.sanType</key>
<string>subject_alternative_name_type</string>
<key>com.jamf.config.certificate-request.sanValue</key>
<string>subject_alternative_name_value</string>
<key>com.jamf.config.certificate-request.signature</key>
<string>$JAMF_SIGNATURE_com.jamf.config.certificate-request</string>
</dict>
```



**Note:** You can add your own key-value pairs to the Managed App Configuration to best fit your environment. The key-value pairs that Jamf Pro requires are prefixed with `com.jamf.config`. For more information about the values you need to enter in the key-value pair for the Managed App Configuration, see the [Managed App Configuration Reference for In-House Apps Developed with the Jamf Certificate SDK](#).

11. Click **Save**.

The app is distributed the next time mobile devices in the scope contact Jamf Pro. If users were added as targets to the scope, the app is distributed to the devices those users are assigned to the next time the devices contact Jamf Pro.

# Managed App Configuration Reference for In-House Apps Developed with the Jamf Certificate SDK

Managed App Configuration allows you to configure and customize the in-house apps developed with the Jamf Certificate SDK for your organization. Managed App Configuration is a set of key and value pairs used to configure iOS apps.

The following table explains the key-value pairs that Jamf Pro requires in the Managed App Configuration for in-house apps developed with the Jamf Certificate SDK. All key-value pairs that Jamf Pro requires are represented as a string. The values you must enter in the strings are specific to your organization.

Key-Value Pair	Description
<pre>&lt;key&gt;com.jamf.config. jamfpro.invitation&lt;/key&gt; &lt;string&gt;\$MOBILEDEVICEAPPINVITE&lt;/string&gt;</pre>	<p><b>Jamf Pro Invitation</b></p> <p>The Jamf Pro Invitation is a unique string that is generated by Jamf Pro. The Jamf Pro Invitation ensures that the MDM server the device is managed by matches the server specified in the <code>com.jamf.config.jamfpro.url</code> key-value pair.</p> <p>The value entered for the string must be <code>\$MOBILEDEVICEAPPINVITE</code>.</p>
<pre>&lt;key&gt;com.jamf.config. device.udid&lt;/key&gt; &lt;string&gt;\$UDID&lt;/string&gt;</pre>	<p><b>Device UDID</b></p> <p>The device UDID is the UDID of the device the in-house app is installed on.</p> <p>The value entered for the string must be <code>\$UDID</code>.</p>
<pre>&lt;key&gt;com.jamf.config. jamfpro.url&lt;/key&gt; &lt;string&gt;https://jamf_pro_server_url/&lt;/string&gt;</pre>	<p><b>Jamf Pro URL</b></p> <p>The Jamf Pro URL is the Jamf Pro server instance in which mobile devices are enrolled. Your full Jamf Pro URL must be entered in the string. This includes the correct protocol, fully qualified domain name (FQDN), and port of the server. For example:</p> <pre>&lt;key&gt;com.jamf.config. jamfpro.url&lt;/key&gt; &lt;string&gt;https://jss. instancename.com:8443/&gt;</pre>

Key-Value Pair	Description
<pre>&lt;key&gt;com.jamf.config. certificate-request.pkiId&lt;/key&gt; &lt;string&gt;PKI_ID&lt;/string&gt;</pre>	<p><b>Certificate Request PKI ID</b></p> <p>The certificate request PKI ID is the ID of an Active Directory Certificate Service (AD CS) instance in Jamf Pro. It is used during certificate generation and is specific to your organization. For example:</p> <pre>&lt;key&gt;com.jamf.config. certificate-request.pkiId&lt; /key&gt; &lt;string&gt;1&lt;/string&gt;</pre>
<pre>&lt;key&gt;com.jamf.config. certificate-request.template&lt;/key&gt; &lt;string&gt;certificate_template_name&lt; /string&gt;</pre>	<p><b>Certificate Request Template Name</b></p> <p>The certificate request template name is the name of the certificate template, usually Machine or User. It is used during certificate generation and is specific to your organization. For example:</p> <pre>&lt;key&gt;com.jamf.config. certificate-request. template&lt;/key&gt; &lt;string&gt;User2&lt;/string&gt;</pre>
<pre>&lt;key&gt;com.jamf.config. certificate-request.subject&lt;/key&gt; &lt;string&gt;certificate_subject&lt;/string&gt;</pre>	<p><b>Certificate Request Subject</b></p> <p>The certificate request subject is the certificate subject that is the representation of a X.500 name (e.g., O=CompanyName, CN=FOO). It is used during certificate generation and is specific to your organization.</p> <p><b>Note:</b> This value can be dynamically supplied by Jamf Pro using variables. For example:</p> <pre>&lt;key&gt;com.jamf.config. certificate-request. template&lt;/key&gt; &lt;string&gt;cn=\$SERIALNUMBER&lt; /string&gt;</pre> <p>For more information about variables in Jamf Pro, see "Payload Variables for Mobile Device Configuration Profiles" in the <i>Jamf Pro Administrator's Guide</i>.</p>

Key-Value Pair	Description
<pre>&lt;key&gt;com.jamf.config. certificate-request.sanType&lt;/key&gt; &lt;string&gt;subject_alternative_name_type&lt; /string&gt;</pre>	<p><b>Certificate Request Subject Alternative Name Type</b></p> <p>The certificate request subject alternative name type is the type of a subject alternative name. It is used during certificate generation and is specific to your organization. For example:</p> <pre>&lt;key&gt;com.jamf.config. certificate-request. sanType&lt;/key&gt; &lt;string&gt;rfc822Name&lt; /string&gt;</pre>
<pre>&lt;key&gt;com.jamf.config. certificate-request.sanValue&lt;/key&gt; &lt;string&gt;subject_alternative_name_value&lt; /string&gt;</pre>	<p><b>Certificate Request Subject Alternative Name Value</b></p> <p>The certificate request subject alternative name value is the value of the subject alternative name. It is used during certificate generation and is specific to your organization.</p> <p><b>Note:</b> This value can be dynamically supplied by Jamf Pro using variables . For example:</p> <pre>&lt;key&gt;com.jamf.config. certificate-request. sanValue&lt;/key&gt; &lt;string&gt;\${EMAIL}&lt;/string&gt;</pre> <p>For more information about variables in Jamf Pro, see "Payload Variables for Mobile Device Configuration Profiles" in the <i>Jamf Pro Administrator's Guide</i>.</p>
<pre>&lt;key&gt;com.jamf.config.certificate- request.signature&lt;/key&gt; &lt;string&gt;\${JAMF_SIGNATURE_com.jamf. config.certificate-request}&lt;/string&gt;</pre>	<p><b>Certificate Request Signature</b></p> <p>Jamf Pro replaces this value with a cryptographic signature of the values related to the certificate request. This signature is verified by the SDK before issuing a certificate to verify that values have not been tampered with.</p> <p>The value entered for the string must be <code>\${JAMF_SIGNATURE_com.jamf.config.certificate-request}</code>.</p>