Enabling Jamf Pro as SCEP Proxy

Technical Paper
Jamf Pro 10.0.0 or Later
31 August 2021

jamf

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

Contents

Introduction

Target Audience

This guide is designed for IT administrators who want to enable Jamf Pro to proxy communication between a SCEP server and computers and mobile devices.

What's in This Guide

This guide provides a step-by-step workflow to enable Jamf Pro as SCEP Proxy. This allows Jamf Pro to communicate with the SCEP server to obtain certificates and install them directly on devices in your environment.

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
- Computer and mobile device enrollment

Additional Resources

For more information about the applications, concepts, and processes mentioned in this guide, see the following documentation:

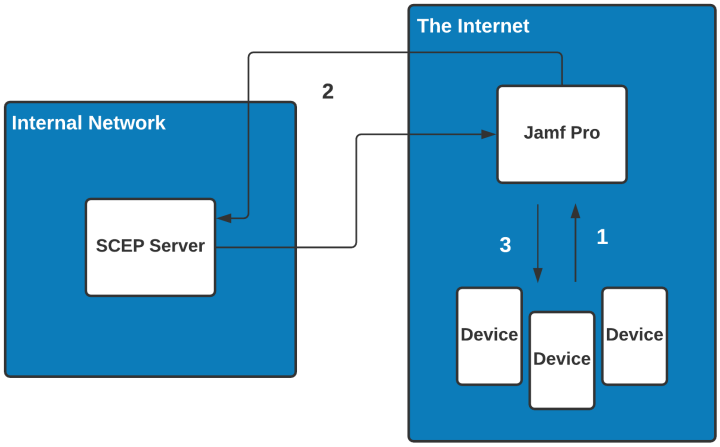
Jamf Pro Administrator's Guide

Overview

Certificates are required for Jamf Pro to communicate with and verify the identity of the computers and mobile devices in your environment. Certificates can also be distributed to allow users to access resources such as VPN or Wi-Fi.

A certificate authority (CA) is a trusted entity that signs and issues the certificates required for certificate-based authentication. Large-scale certificate distribution is simplified by using the Simple Certificate Enrollment Protocol (SCEP) to obtain certificates from the CA and distribute them to the devices in your environment. To issue device certificates, you can use the Jamf Pro built-in CA, integrate with a trusted third-party CA (Symantec), or set up your own external CA that supports SCEP. You can use the PKI Certificates settings in Jamf Pro to set up and manage the certificates in your environment.

When a device that needs a certificate checks in with Jamf Pro, the device communicates with the SCEP server to obtain the certificate. You can enable Jamf Pro to proxy this communication between a SCEP server and the devices in your environment so that devices do not need to access the SCEP server. With Jamf Pro enabled as SCEP Proxy, Jamf Pro communicates directly with the SCEP server to obtain certificates and install them directly on devices. The following diagram explains the communication of Jamf Pro as SCEP Proxy:



1. Computers and mobile devices that need a certificate to access resources such as VPN or Wi-Fi check in with Jamf Pro.
2. Jamf Pro communicates with the SCEP server to obtain the certificate from the SCEP server.
   Note: In a clustered environment, communication is handled by the Jamf Pro web app that receives the request.
3. Jamf Pro installs the certificate directly on the computer or mobile device.

Jamf Pro supports the following certificate properties:

- SHA-512
- SHA-256

- SHA-1
- DES3
- AES

For more information about the network ports that Jamf Pro uses for communication, see the Network Ports Used by Jamf Pro Knowledge Base article.

You can enable Jamf Pro as SCEP Proxy for the following:

- Configuration profiles—Enabling Jamf Pro as SCEP Proxy for configuration profiles allows you to create profiles that contain a certificate that Jamf Pro obtains from the SCEP server and installs on devices. For example, you can distribute a configuration profile that contains a VPN certificate, and Jamf Pro obtains the certificate from the SCEP server and installs it on devices.
- Device enrollment—If your environment uses an external CA that supports SCEP, you can use Jamf Pro to obtain device management certificates from the SCEP server and install them on devices.

Requirements

To enable Jamf Pro as SCEP Proxy, you need the following:

- Jamf Pro (formerly the Jamf Software Server) 10.0.0 or later
- An organizational or third-party CA that supports SCEP
  Note: The CA hosted by Jamf Pro (the "built-in CA") supports SCEP.
- The **Enable certificate-based authentication** setting configured in Jamf Pro (For more information, see Security Settings in the *Jamf Pro Administrator's Guide*.)

Enabling Jamf Pro as SCEP Proxy for Configuration Profiles

Jamf Pro allows you to create configuration profiles with payloads that contain certificates for user access to resources such as VPN or Wi-Fi. Enabling Jamf Pro as SCEP Proxy for a configuration profile allows Jamf Pro to communicate with your SCEP server to install the certificate directly on computers or mobile devices.

Before you can distribute a configuration profile with Jamf Pro as SCEP Proxy for the certificates included in the profile, you must enable Jamf Pro as SCEP Proxy in the PKI Certificate settings. This allows you to use Jamf Pro as SCEP Proxy in the configuration profile that you create.

Note: You must enable Jamf Pro as SCEP Proxy in the configuration profile for each profile created to distribute certificates. For more information about configuration profiles, see Computer Configuration Profiles and Mobile Device Configuration Profiles in the *Jamf Pro Administrator's Guide*.

Configuring the PKI Certificates Settings to Enable Jamf Pro as SCEP Proxy for Configuration Profiles

1. Log in to Jamf Pro.
2. Click **Settings** .
3. Click **Global Management**.
4. Click **PKI Certificates**.
5. Click the **Management Certificate Template** tab, and then click **External CA**.
6. Click **Edit**.
7. Select **Enable Jamf Pro as SCEP Proxy for configuration profiles**.
   Important: If you are using the Jamf Pro built-in CA for device enrollment, ensure that you do not select **Use a SCEP-enabled external CA for computer and mobile device enrollment**. Selecting this option requires you to re-enroll all devices with Jamf Pro.
8. Enter a base URL for the SCEP server.
9. (Optional) Enter the name of the instance in the **Name** field. For Microsoft certificate authorities, "SERVERNAME-MSCEP-RA" is an example.
10. Choose the type of challenge password to use from the **Challenge Type** pop-up menu:
    - If you want all computers and mobile devices to use the same challenge password, choose “Static” and specify a challenge password.
      The challenge password will be used as the pre-shared secret for automatic enrollment.

- (Jamf Pro 10.32.0 or later) If you want to use non-Microsoft CA with a SCEP Dynamic challenge type, you can create a webhook using the event "SCEPChallenge". The receiving web server is sent information about the enrolling device and the configuration profile. This allows the returning message body to be used as the SCEP challenge for that enrollment. For more information, see Webhooks in the Jamf Developer Portal and Webhooks in the *Jamf Pro Administrator's Guide*.
- If you are using a Microsoft CA and you want each computer and mobile device to use a unique challenge password, choose "Dynamic-Microsoft CA".

  When using the "Dynamic-Microsoft CA" challenge type, the **Username** field requires the down-level logon name format. For more information, see the following Microsoft documentation: Using Name Formats.

- If you are using an Entrust CA, choose "Dynamic-Entrust", and then do the following:
  a. Enter the name of your Digital ID Configuration that issues certificates for Entrust in the **Digital ID Configuration Name** field.
  b. Enter the <iggroup> variable defined in your Entrust Digital ID Configuration in the **Group Name** field.
  c. Click **Add** to enter additional RDN variables, and then enter the variable name and value.

11. Click **Save**.

    If you are using an external CA, you need to provide the signing and CA certificates for the external CA after saving. This is done by uploading a signing certificate keystore (.jks or .p12) that contains both certificates to Jamf Pro. For instructions, see "Uploading Signing and CA Certificates for an External CA" on the PKI Certificates page in the *Jamf Pro Administrator's Guide*. If you are using the Jamf Pro built-in CA, no action is necessary after saving.

Creating a Configuration Profile with Jamf Pro as SCEP Proxy

1. Log in to Jamf Pro.
2. Do one of the following:
   - If you are creating a computer configuration profile, click **Computers** at the top of the page, and then click **Configuration Profiles**.
   - If you are creating 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 SCEP payload and click **Configure**.

6. Select **Use the External Certificate Authority settings to enable Jamf Pro as SCEP proxy for this configuration profile**.
   The PKI Certificates settings are applied to the configuration profile.
   Note: You can customize the profile by modifying the Subject and Subject Alternative Name Type settings.
7. Enter the name of the instance in the **Name** field. For Microsoft certificate authorities, "SERVERNAME-MSCEP-RA" is an example.
   If you do not enter a name, "SCEP Proxy" is populated by default in the Name field.
8. If you are using an Entrust CA, do the following:
   a. Enter the name of your Digital ID Configuration that issues certificates for Entrust in the **Digital ID Configuration Name** field.
   b. Enter the <iggroup> variable defined in your Entrust Digital ID Configuration in the **Group Name** field.
   c. Click **Add** to add additional RDN variables, and then enter the variable name and value.
9. Use the rest of the payloads to configure the settings you want to apply including the certificates you want to distribute with the profile.
   Note: It is recommended that you distribute one certificate per configuration profile.
10. Click the **Scope** tab and configure the scope of the profile.
    For more information, see Scope in the *Jamf Pro Administrator's Guide*.
11. (Optional) If you chose to distribute the profile in Self Service, click the Self Service tab to configure Self Service settings for the profile.
    For more information, see Items Available to Users in Jamf Self Service for macOS and Mobile Device Configuration Profiles in the *Jamf Pro Administrator's Guide*.
12. Click **Save**.

Further Considerations

If you want to disable Jamf Pro as SCEP Proxy for configuration profiles in the PKI Certificates settings, you must first disable Jamf Pro as SCEP Proxy for any configuration profiles that have the option enabled.

Enabling Jamf Pro as SCEP Proxy for Enrollment

If your environment uses an external CA that supports SCEP, you can use Jamf Pro to obtain management certificates from the SCEP server and install them directly on computers and mobile devices during enrollment with Jamf Pro. The certificates establish a connection between the devices and the Jamf Pro server allowing you to perform inventory, configuration, security management, and distribution tasks on the devices. For more information about enrollment, see Computer Enrollment Methods and Mobile Device Enrollment Methods in the *Jamf Pro Administrator's Guide*.

Important: Changing from Jamf Pro's built-in CA to an external CA requires you to re-enroll all devices with Jamf Pro.

Configuring the PKI Certificates Settings to Enable Jamf Pro as SCEP Proxy for Enrollment

1. Log in to Jamf Pro.
2. Click **Settings** .
3. Click **Global Management**.
4. Click **PKI Certificates**.
5. Click the **Management Certificate Template** tab, and then click **External CA**.
6. Click **Edit**.
7. Select **Use a SCEP-enabled external CA for computer and mobile device enrollment**.
   Note: This setting is already selected if your environment is configured to use an external CA. If you switch from the built-in CA to an external CA, you need to re-enroll all devices with Jamf Pro after saving the changes.
8. Select **Use Jamf Pro as SCEP Proxy for computer and mobile device enrollment**.
   Note: If your environment is configured to use Jamf Pro as SCEP Proxy for mobile device enrollment prior to Jamf Pro 10.0.0 via the Jamf API, all management certificates will now be distributed to both computers and mobile devices with Jamf Pro as SCEP Proxy once these settings are saved.
9. Enter a base URL for the SCEP server.
10. (Optional) Enter the name of the instance in the **Name** field. For Microsoft certificate authorities, "SERVERNAME-MSCEP-RA" is an example.
11. Choose the type of challenge password to use from the **Challenge Type** pop-up menu:
    - If you want all computers and mobile devices to use the same challenge password, choose “Static” and specify a challenge password.
      The challenge password will be used as the pre-shared secret for automatic enrollment.

- If you are using a non-Microsoft CA and you want each computer and mobile device to use a unique challenge password, choose “Dynamic”.
  The Dynamic challenge type requires use of the Jamf API and membership in the Jamf Developer Program. The Dynamic challenge uses the "Fingerprint" or "Thumbprint" to authenticate the user instead of a username and password. The Thumbprint hash value for the **Fingerprint** field in Jamf Pro can be found on the profile you receive. Before selecting this option, contact your Jamf account representative to learn more about the Jamf Developer Program and the additional steps you need to take to use this option.
- If you are using a Microsoft CA and you want each computer and mobile device to use a unique challenge password, choose “Dynamic-Microsoft CA”. When using the “Dynamic-Microsoft CA” challenge type, the **Username** field requires the down-level logon name format. For more information, see the following Microsoft documentation: Using Name Formats.

  Note: If you choose the “Dynamic” or “Dynamic-Microsoft CA” challenge type, you must use user-initiated enrollment to enroll computers and mobile devices so that a unique challenge password is used for each device. For more information, see User-Initiated Enrollment for Computers and User-Initiated Enrollment for Mobile Devices in the *Jamf Pro Administrator's Guide* .

- If you are using an Entrust CA, choose "Dynamic-Entrust".
  a. Enter the name of your Digital ID Configuration that issues certificates for Entrust in the **Digital ID Configuration Name** field.
  b. Enter the <iggroup> variable defined in your Entrust Digital ID Configuration in the **Group Name** field.
  c. Click **Add** to enter additional RDN variables, and then enter the variable name and value.
  Important: "JAMF Device Certificate" must be entered in the **Group Name** field. If you have defined "JAMF Device Certificate" as a value in an RDN variable name in your Entrust Digital ID Configuration, click **Add** to enter the variable name and "JAMF Device Certificate" value.

12. Click **Save**.

After saving, you need to provide the signing and CA certificates for the external CA. This is done by uploading a signing certificate keystore (.jks or .p12) that contains both certificates to Jamf Pro. For instructions, see "Uploading Signing and CA Certificates for an External CA" in the PKI Certificates section of the *Jamf Pro Administrator's Guide*.

After the PKI Certificates settings are saved, you can use Jamf Pro as SCEP Proxy to install management certificates directly on devices during enrollment with Jamf Pro.