Configure
Local Administrator Password Solution (LAPS)
in Jamf Pro

Rev 20240105

Contents

Preface

What is Local Administrator Password Solution (LAPS)?
Local Administrator Password Solution (LAPS) was originally a Microsoft solution designed to provide a secure way to manage local administrator account passwords on Windows computers. The LAPS solution automates the process of password generation and storage, ensuring that local administrator passwords are randomized, securely stored, and regularly changed without any manual intervention.

Jamf management framework LAPS allows you to manage the Jamf management account password via the Jamf management framework, which includes the jamf binary.

A Jamf management framework LAPS account can be created during computer enrollment when the Jamf management framework is installed. Jamf management framework LAPS is enabled by default and is always on.

Some advantages of Jamf management framework LAPS include the following:

- Automatic password rotation is enabled.
- Automatic password randomization is enabled.
- You can utilize a pre-existing management account as a LAPS user, without requiring re-enrollment.
- If the management account had cryptographic privileges with a secure token, those privileges are maintained during password rotation.
  NOTE: If the management account password for cryptographically enabled accounts becomes out of sync with the password stored in Jamf Pro, password rotation will fail.

The goal of this guide is to show the results of the macOS administrator accounts created by Jamf Pro with FileVault enabled and rotating the password.

In macOS on APFS volumes, encryption keys are generated either during user creation, setting the first user's password, or during the first login by a user of the Mac computer. This implementation of the encryption keys, when they're generated, and how they're stored are all part of a feature known as Secure Token. Specifically, a secure token is a wrapped version of a key encryption key (KEK) protected by a user's password.

https://support.apple.com/guide/deployment/dep24dbdcf9e/

Jamf References:

https://learn.jamf.com/bundle/technical-paper-laps-current/page/LAPS_Account_Comparison.html

What You'll Need
Learn what hardware, software, and information you'll need to complete the tutorials in this section.

Hardware and Software Requirements for following along with this guide:

- A test Mac computer with macOS 14 or later. This guide will use macOS 14.2.1
- A production Mac computer with macOS 14 or later. This guide will use macOS 14.2.1
- Jamf Pro server with version 11.1.3 or later
- Jamf Pro administrator credentials

Sample account names used in this guide.
Account Name: jamfManage
Jamf Management Account - Created by the Jamf Binary. Configured in Settings > Global > User-initiated enrollment

Account Name: managedAdmin
Managed Administrator Account - Created by the MDM Framework. Configured in Computers > PreStage

Account Name: jappleseed
Local Administrator Account - Configured in the Mac Setup Assistant

Section 1: Side A - Creating a Managed Admin (LAPS Disabled) and a Jamf Management Account (LAPS Enabled)

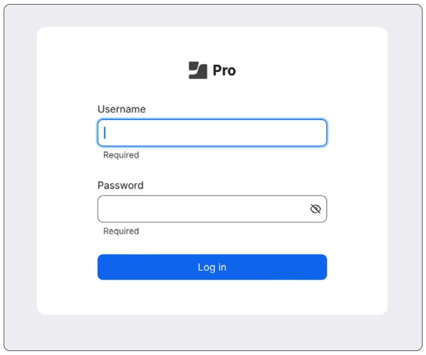
Note: The managed administrator account is created by the MDM Framework

https://support.apple.com/guide/deployment/depca092ad96/

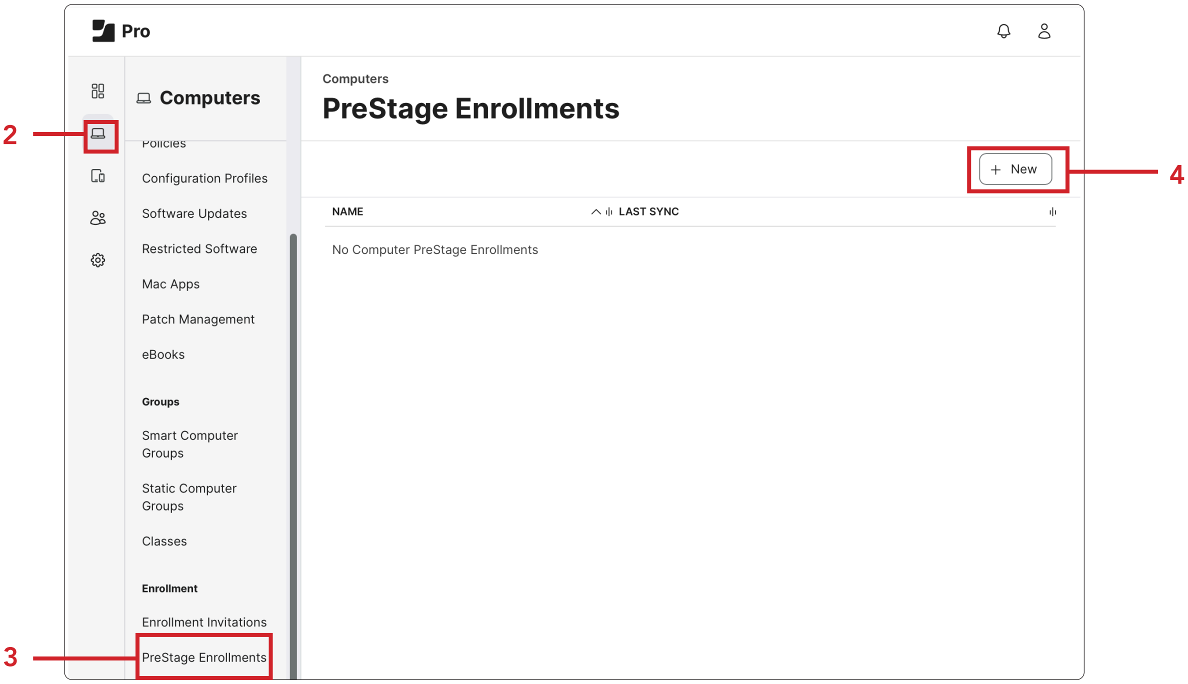
Unlike passwords for regular administrator accounts, passwords for managed administrator accounts can be changed remotely using your MDM solution. However, if the account becomes secure token enabled, the change from MDM updates the login password and not the secure token password.

Create a PreStage

1. On your production Mac computer, log into your Jamf Pro server with administrator privileges

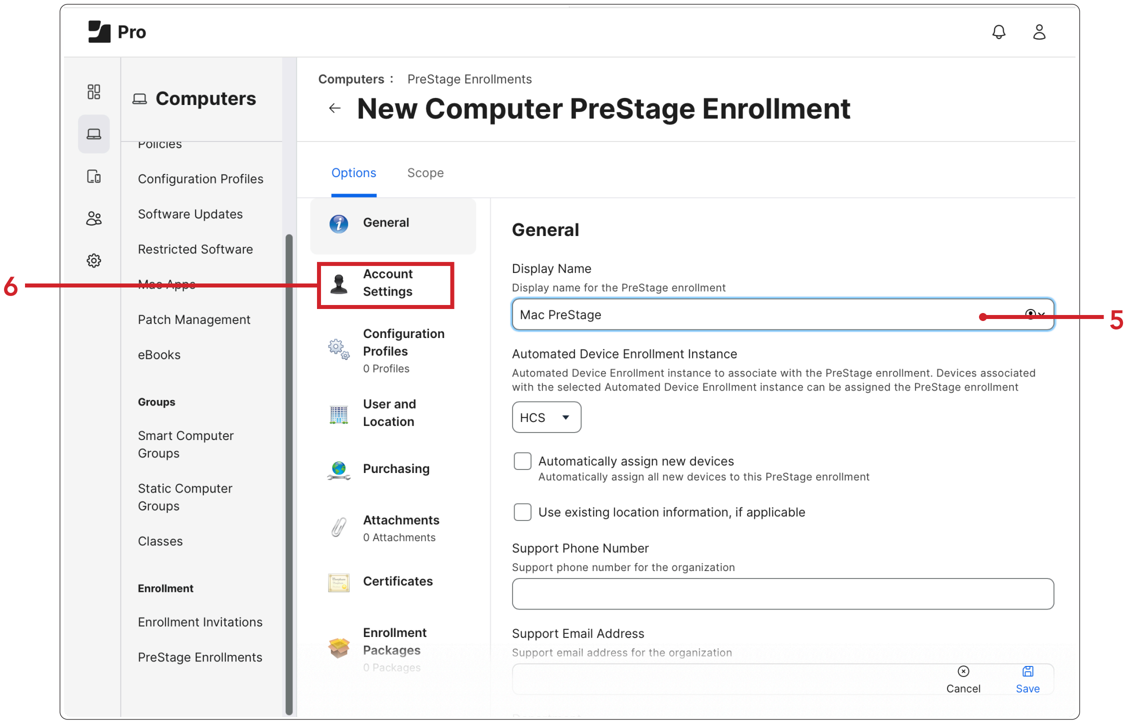


2. Click Computers
3. Click PreStage Enrollments
4. Click New



5. In the Display Name enter: Mac PreStage. The rest of the settings choose at your discretion.

6. Click Account Settings



New Computer PreStage Enrollment

General

Display Name
Display name for the PreStage enrollment
Mac PreStage

Automated Device Enrollment Instance
Automated Device Enrollment instance to associate with the PreStage enrollment. Devices associated with the selected Automated Device Enrollment instance can be assigned the PreStage enrollment
HCS

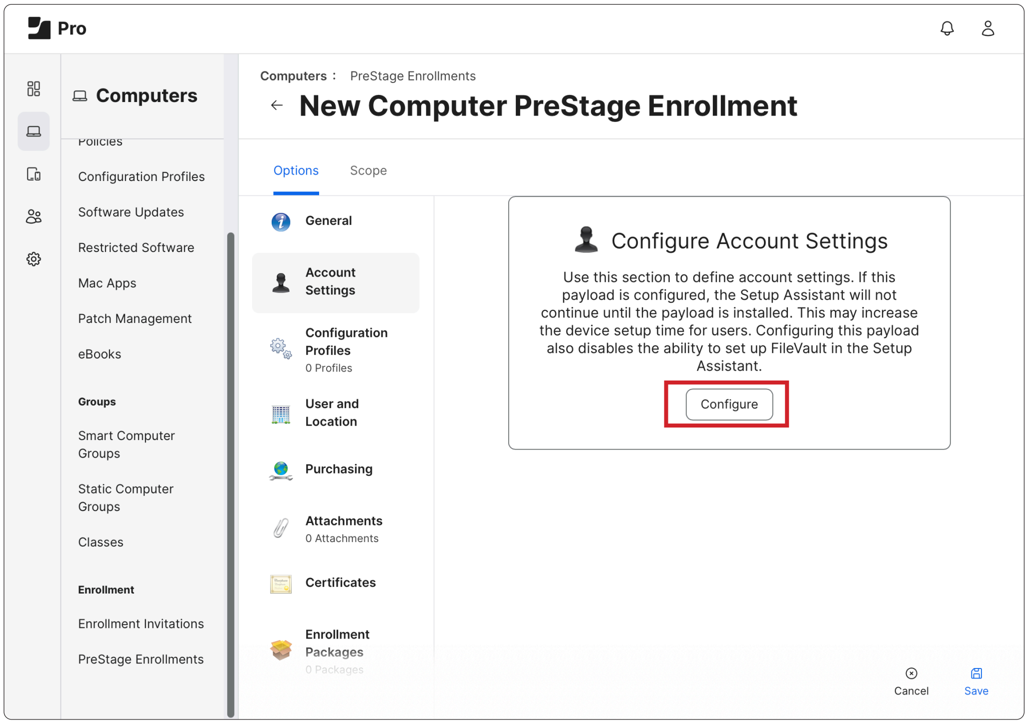
□ Automatically assign new devices
Automatically assign all new devices to this PreStage enrollment

□ Use existing location information, if applicable

Support Phone Number
Support phone number for the organization

Support Email Address
Support email address for the organization

7. Click Configure.

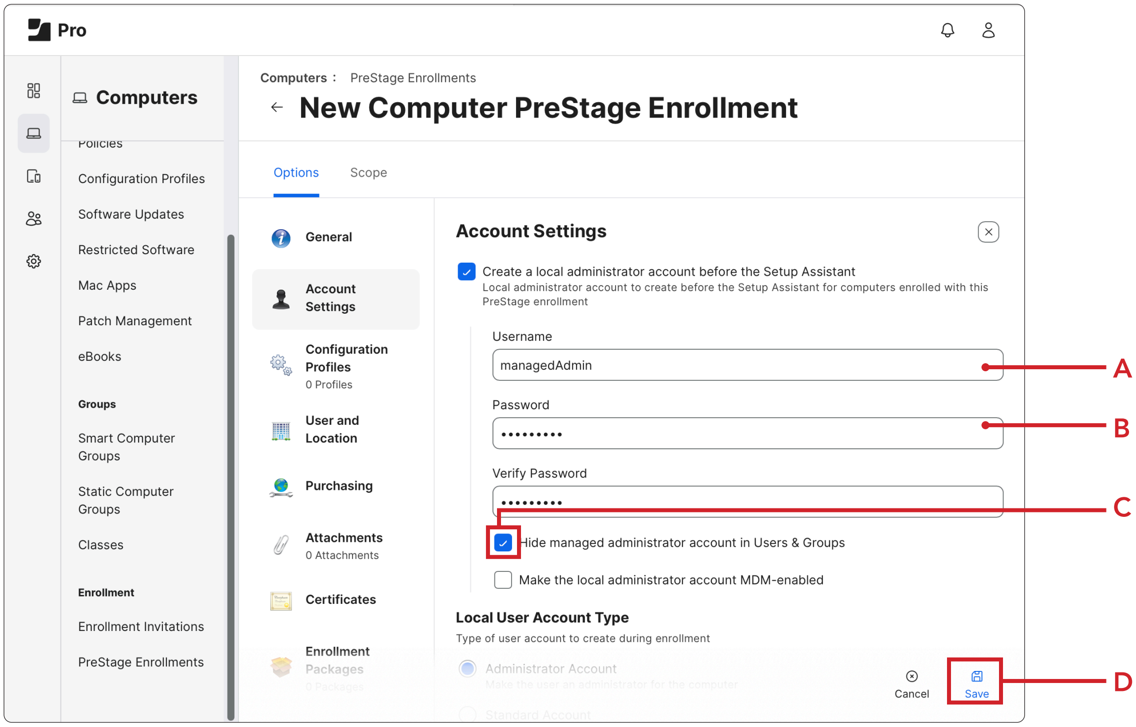


New Computer PreStage Enrollment

Configure Account Settings

Use this section to define account settings. If this payload is configured, the Setup Assistant will not continue until the payload is installed. This may increase the device setup time for users. Configuring this payload also disables the ability to set up FileVault in the Setup Assistant.

8. Select the checkbox for Create a local administrator account before the Setup Assistant
    A. Username: managedAdmin (For the purposes of testing ONLY)
    B. Password: enter a password of your choosing and document for future testing
    C. Select the checkbox for Hide managed administrator account in Users & Groups
        NOTE: Do not Scope any Mac computers as we will be editing the PreStage in a later step.
    D. Click Save



Computers : PreStage Enrollments

New Computer PreStage Enrollment

Account Settings

☑ Create a local administrator account before the Setup Assistant
Local administrator account to create before the Setup Assistant for computers enrolled with this PreStage enrollment

Username: managedAdmin

Password: •••••••••

Verify Password: •••••••••

☑ Hide managed administrator account in Users & Groups

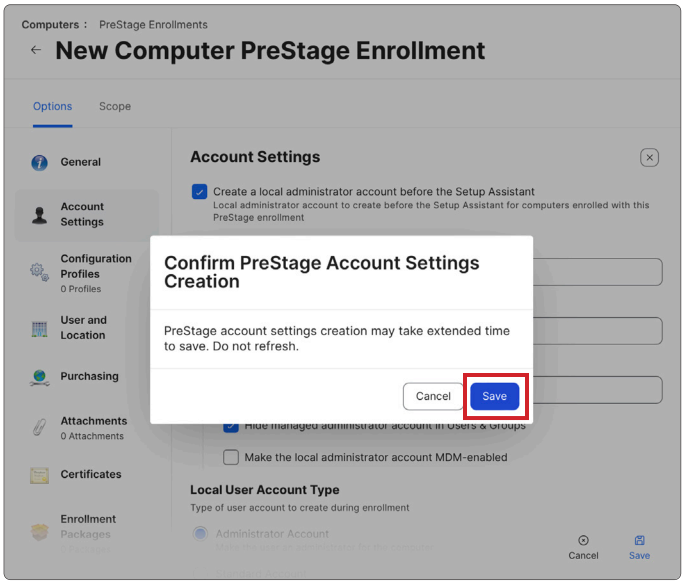
□ Make the local administrator account MDM-enabled

Local User Account Type
Type of user account to create during enrollment

○ Administrator Account
Make the user an administrator for the computer

○ Standard Account

9. Click Save.


Computers : PreStage Enrollments
New Computer PreStage Enrollment
Options
Scope
General
Account Settings
Configuration Profiles
0 Profiles
User and Location
Purchasing
Attachments
0 Attachments
Certificates
Enrollment Packages
Account Settings
Create a local administrator account before the Setup Assistant
Local administrator account to create before the Setup Assistant for computers enrolled with this PreStage enrollment
Hide managed administrator account in Users & Groups
Make the local administrator account MDM-enabled
Local User Account Type
Type of user account to create during enrollment
Administrator Account
Cancel
Save

Confirm PreStage Account Settings Creation

PreStage account settings creation may take extended time to save. Do not refresh.

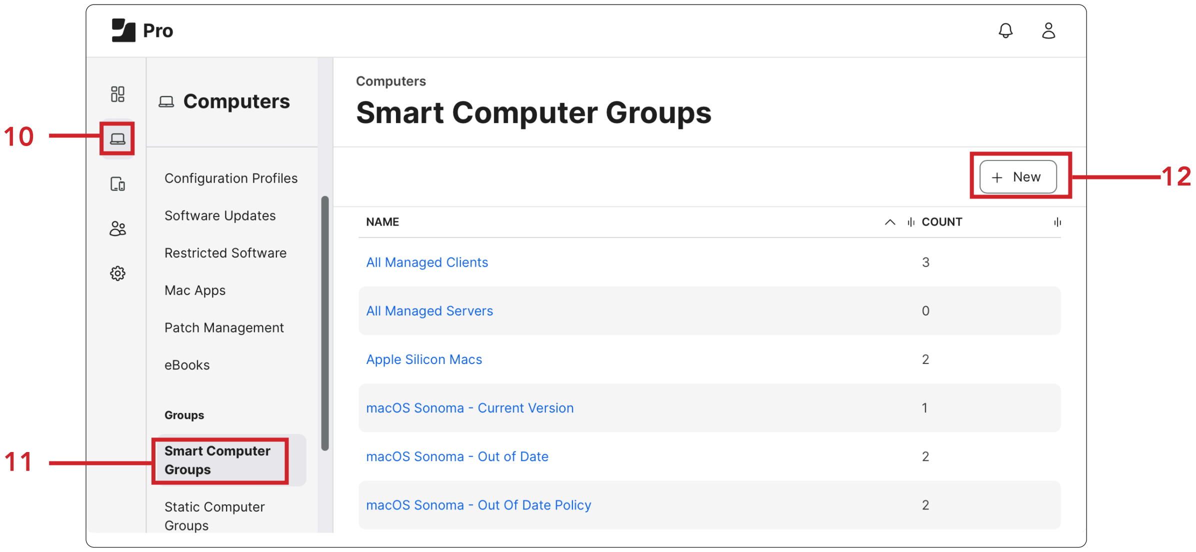
Cancel | Save

Create a Smart Computer Group for computers using the Enrollment Method: PreStage enrollment - Mac PreStage

10. Click Computers.

11. Click Smart Computer Groups.

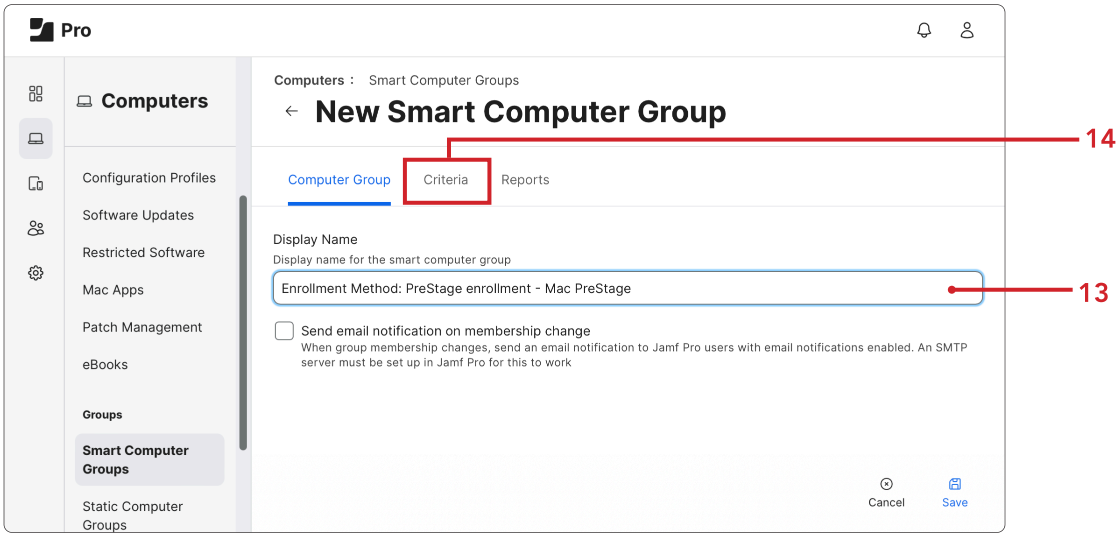
12. Click New.



NAME	COUNT
All Managed Clients	3
All Managed Servers	0
Apple Silicon Macs	2
macOS Sonoma - Current Version	1
macOS Sonoma - Out of Date	2
macOS Sonoma - Out Of Date Policy	2

13. In the Display Name, enter Enrollment Method: PreStage enrollment - Mac PreStage.

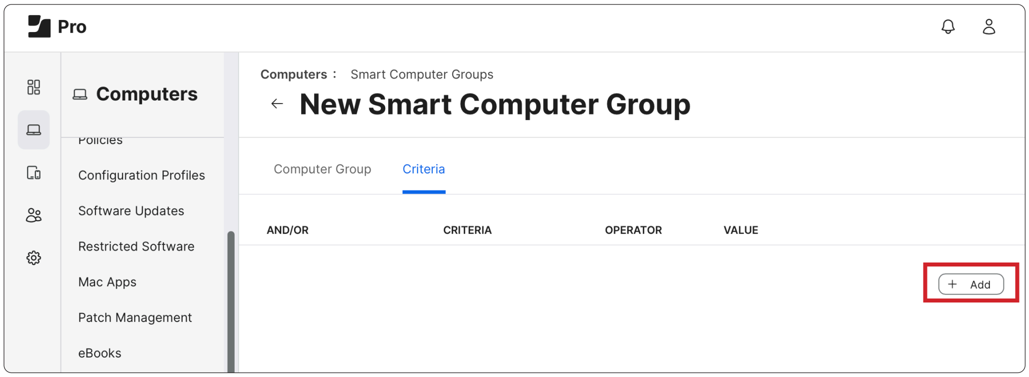
14. Click Criteria.



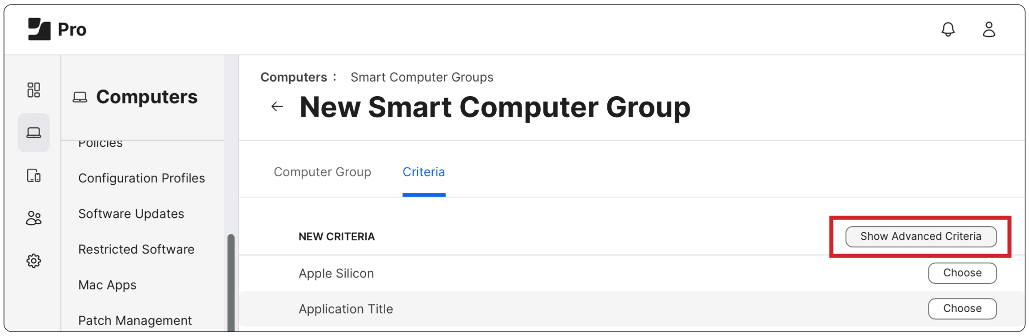
Display Name
Display name for the smart computer group
Enrollment Method: PreStage enrollment - Mac PreStage

□ Send email notification on membership change
When group membership changes, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

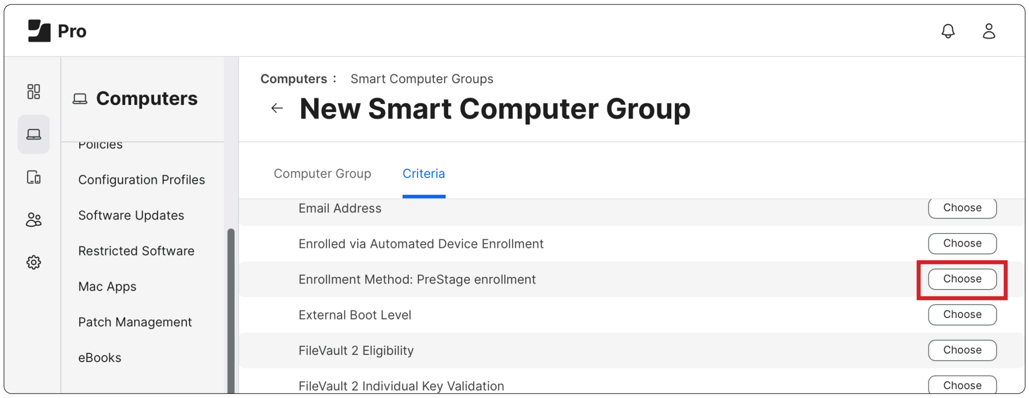
15. Click Add.



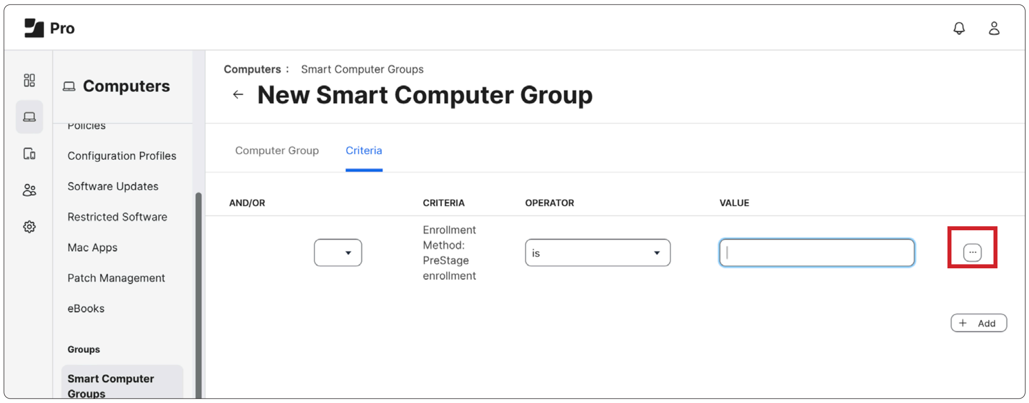
16. Click Show Advanced Criteria.



17. Click Choose next to Enrollment Method: PreStage enrollment.

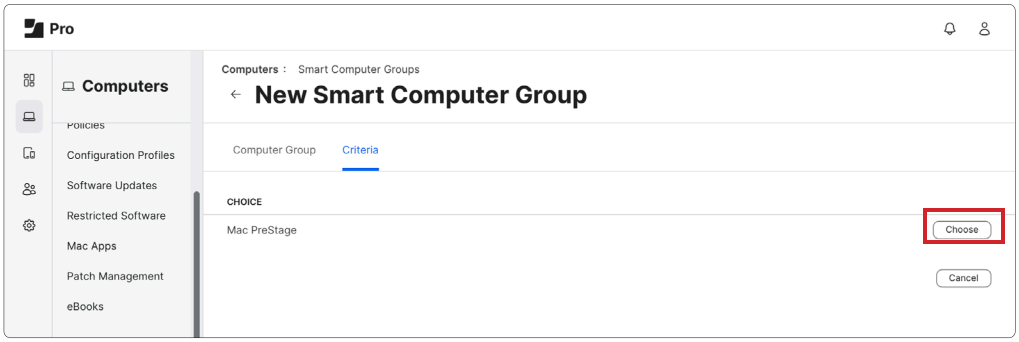


18. Click Browse (•••) to the right of Value.

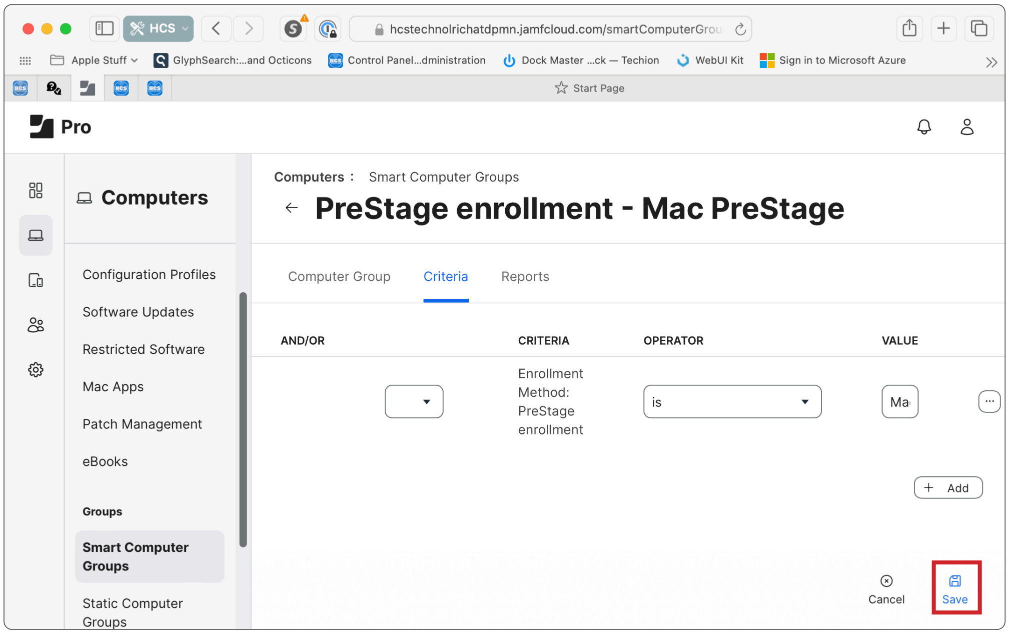


Criteria: Enrollment Method: PreStage enrollment; Operator: is

19. Click Choose for Mac PreStage.



20. Click Save.



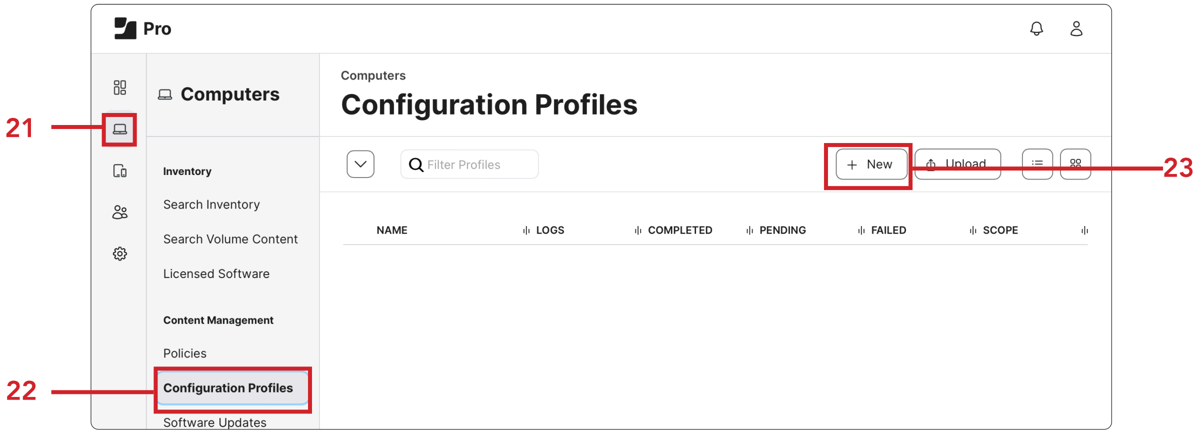
Criteria: Enrollment Method: PreStage enrollment; Operator: is; Value: Ma

Create a Configuration Profile for Computers that enforces FileVault at Setup Assistant

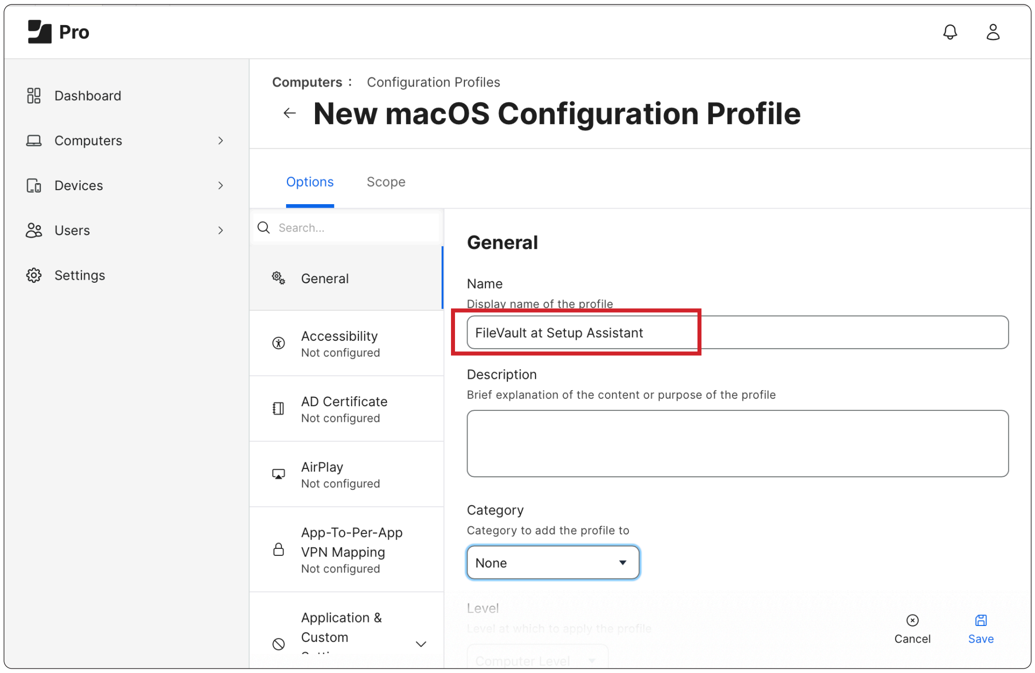
21. Click Computers.

22. Click Configuration Profiles.

23. Click New.



24. In the General Payload, in the Display Name, enter FileVault at Setup Assistant. Optionally select a category.



General

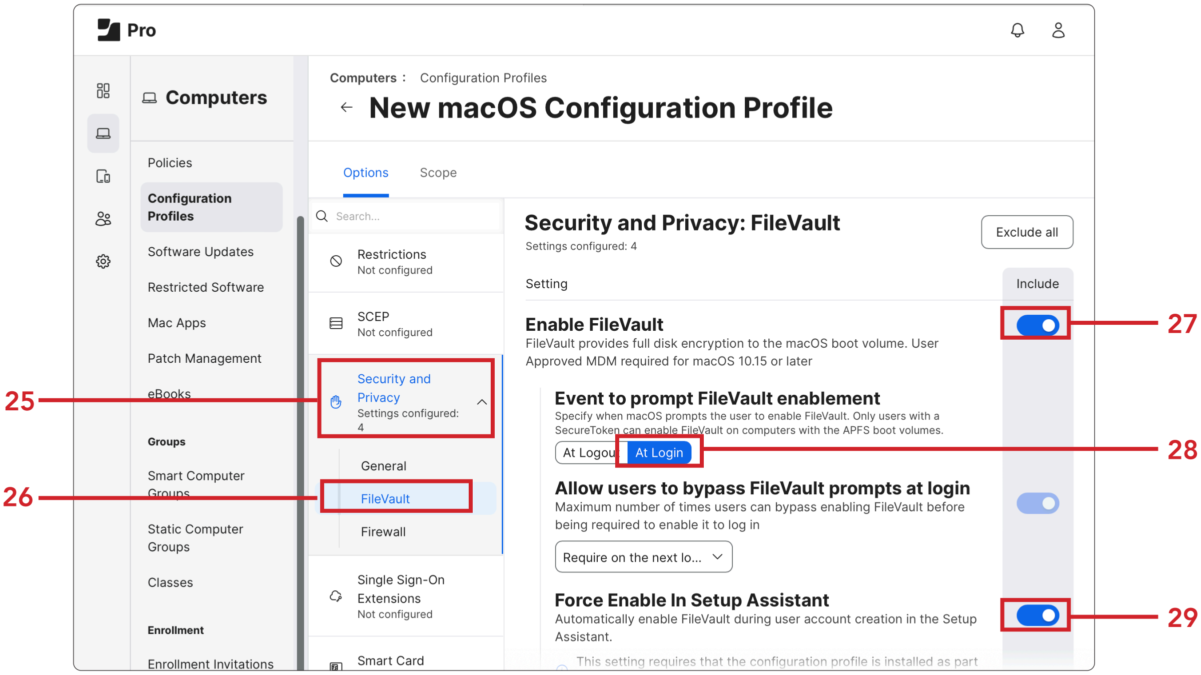
Name
Display name of the profile
FileVault at Setup Assistant

Description
Brief explanation of the content or purpose of the profile

Category
Category to add the profile to
None

Level
Level at which to apply the profile
Computer Level

25. Scroll Down and click Security and Privacy Payload.
26. Click FileVault.
27. Enable FileVault.
28. Enable Event to prompt FileVault enablement set to At Login.
29. Enable Force Enable In Setup Assistant.



Computers : Configuration Profiles

New macOS Configuration Profile

Restrictions
Not configured

SCEP
Not configured

Security and Privacy
Settings configured: 4

General

FileVault

Firewall

Single Sign-On Extensions
Not configured

Smart Card

Security and Privacy: FileVault

Settings configured: 4

Setting

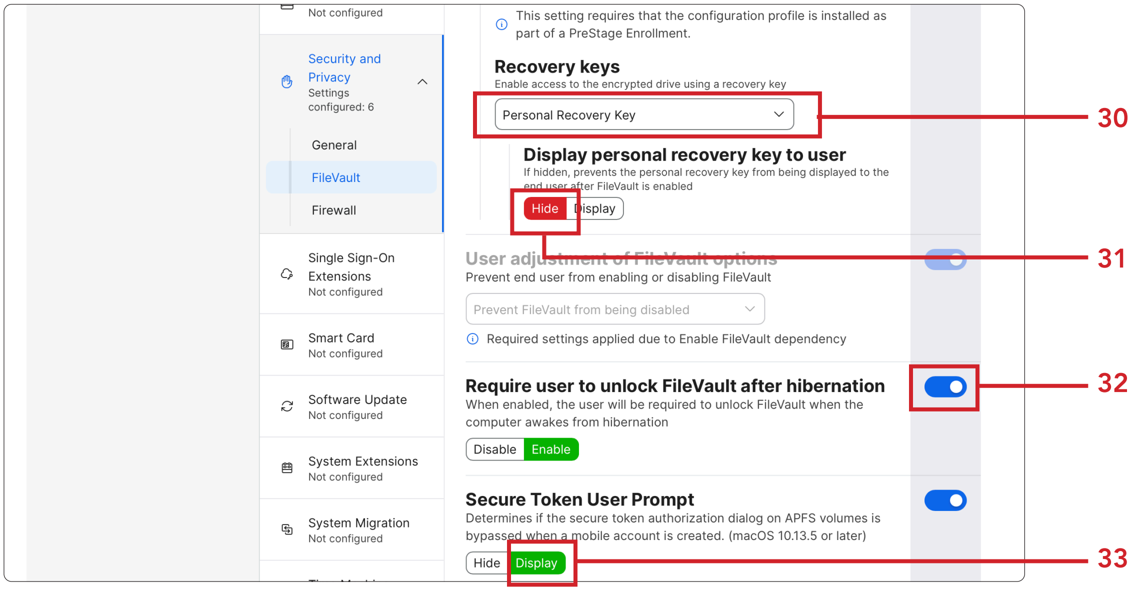
Enable FileVault
FileVault provides full disk encryption to the macOS boot volume. User Approved MDM required for macOS 10.15 or later

Event to prompt FileVault enablement
Specify when macOS prompts the user to enable FileVault. Only users with a SecureToken can enable FileVault on computers with the APFS boot volumes.
At Logout [✓ At Login]

Allow users to bypass FileVault prompts at login
Maximum number of times users can bypass enabling FileVault before being required to enable it to log in
Require on the next lo...

Force Enable In Setup Assistant
Automatically enable FileVault during user account creation in the Setup Assistant.
This setting requires that the configuration profile is installed as part

30. Recovery keys - from the pull-down menu choose Personal Recovery Key.
31. Display personal recovery key to user select Hide.
32. Enable Require user to unlock FileVault after hibernation.
33. Display Secure Token User Prompt.



Not configured

Security and Privacy
Settings configured: 6

General

FileVault

Firewall

Single Sign-On Extensions
Not configured

Smart Card
Not configured

Software Update
Not configured

System Extensions
Not configured

System Migration
Not configured

This setting requires that the configuration profile is installed as part of a PreStage Enrollment.

Recovery keys
Enable access to the encrypted drive using a recovery key
Personal Recovery Key

Display personal recovery key to user
If hidden, prevents the personal recovery key from being displayed to the end user after FileVault is enabled
[✓ Hide] Display

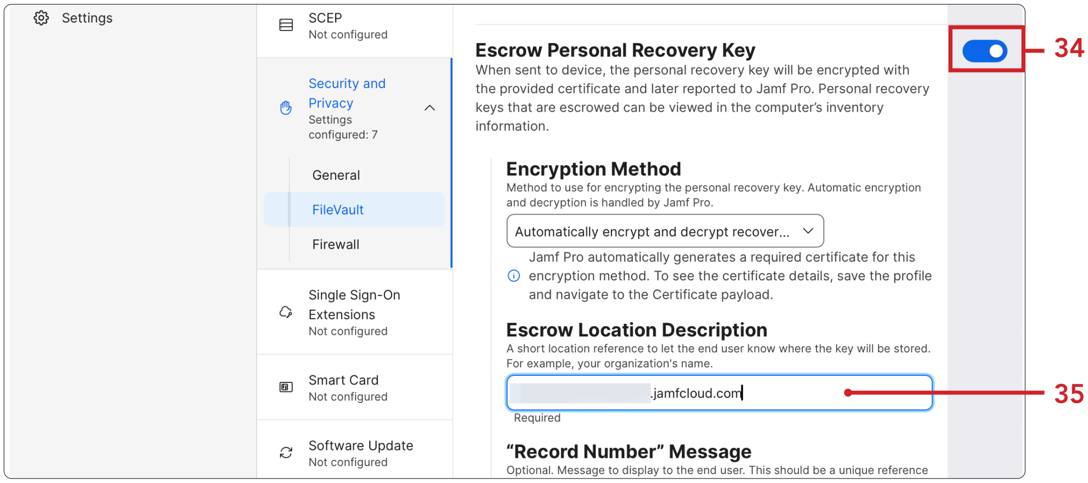
User adjustment of FileVault options
Prevent end user from enabling or disabling FileVault
Prevent FileVault from being disabled
Required settings applied due to Enable FileVault dependency

Require user to unlock FileVault after hibernation
When enabled, the user will be required to unlock FileVault when the computer awakes from hibernation
Disable [✓ Enable]

Secure Token User Prompt
Determines if the secure token authorization dialog on APFS volumes is bypassed when a mobile account is created. (macOS 10.13.5 or later)
Hide [✓ Display]

34. Enable Escrow Personal Recovery Key.

35. Escrow Location Description, enter the URL or a reference to your Jamf Pro server.
I.E. HCS Jamf Pro Server.



Escrow Personal Recovery Key
When sent to device, the personal recovery key will be encrypted with the provided certificate and later reported to Jamf Pro. Personal recovery keys that are escrowed can be viewed in the computer's inventory information.

Encryption Method
Method to use for encrypting the personal recovery key. Automatic encryption and decryption is handled by Jamf Pro.

Automatically encrypt and decrypt recover...

Jamf Pro automatically generates a required certificate for this encryption method. To see the certificate details, save the profile and navigate to the Certificate payload.

Escrow Location Description
A short location reference to let the end user know where the key will be stored. For example, your organization's name.

[redacted].jamfcloud.com

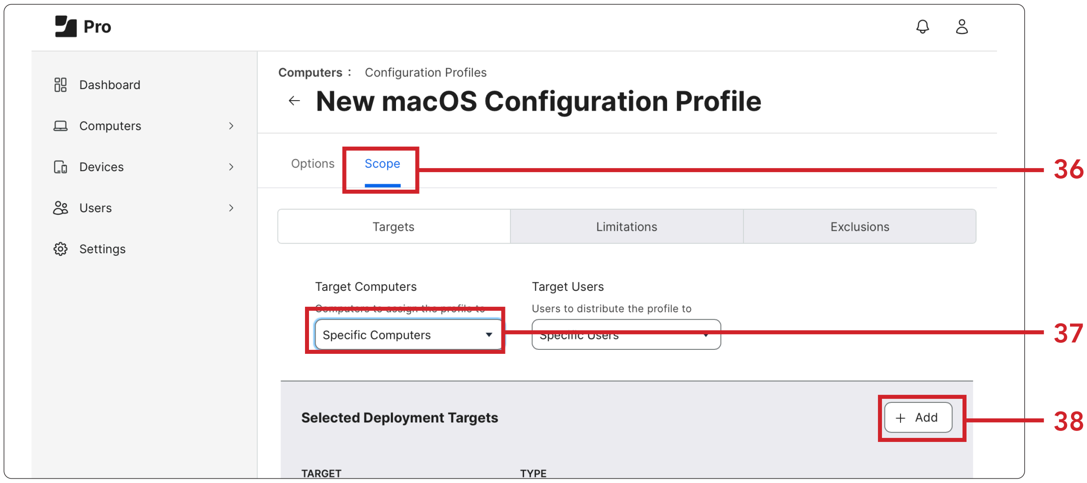
Required

"Record Number" Message
Optional. Message to display to the end user. This should be a unique reference

36. Click Scope.

37. In Target Computers, select Specific Computers.

38. Click the Add button.



New macOS Configuration Profile

Target Computers
Computers to assign the profile to
Specific Computers

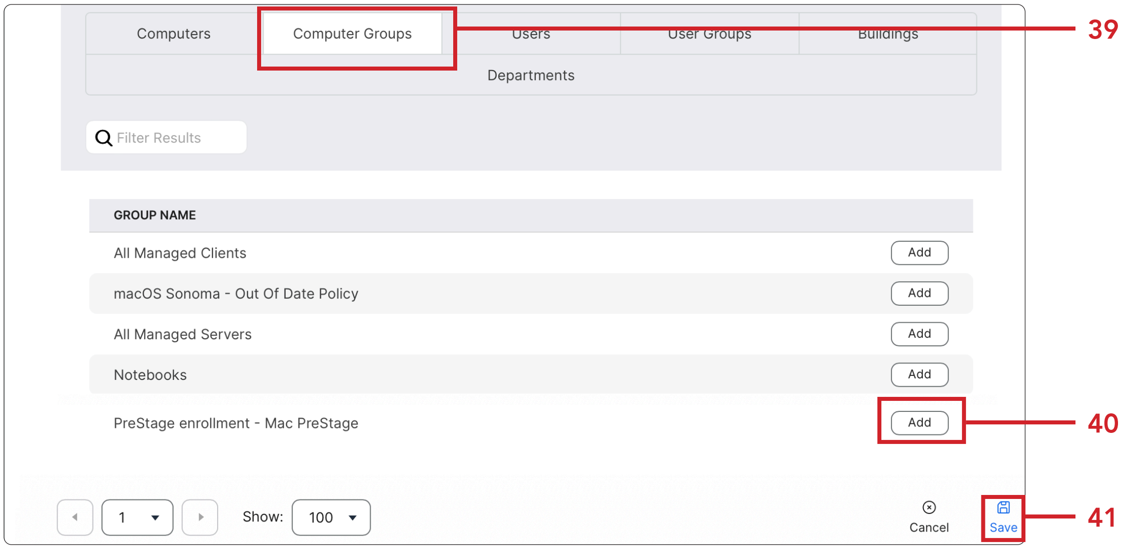
Target Users
Users to distribute the profile to
Specific Users

Selected Deployment Targets

39. Click Computer Groups.

40. Click add next to PreStage enrollment - Mac PreStage.

41. Click Save.



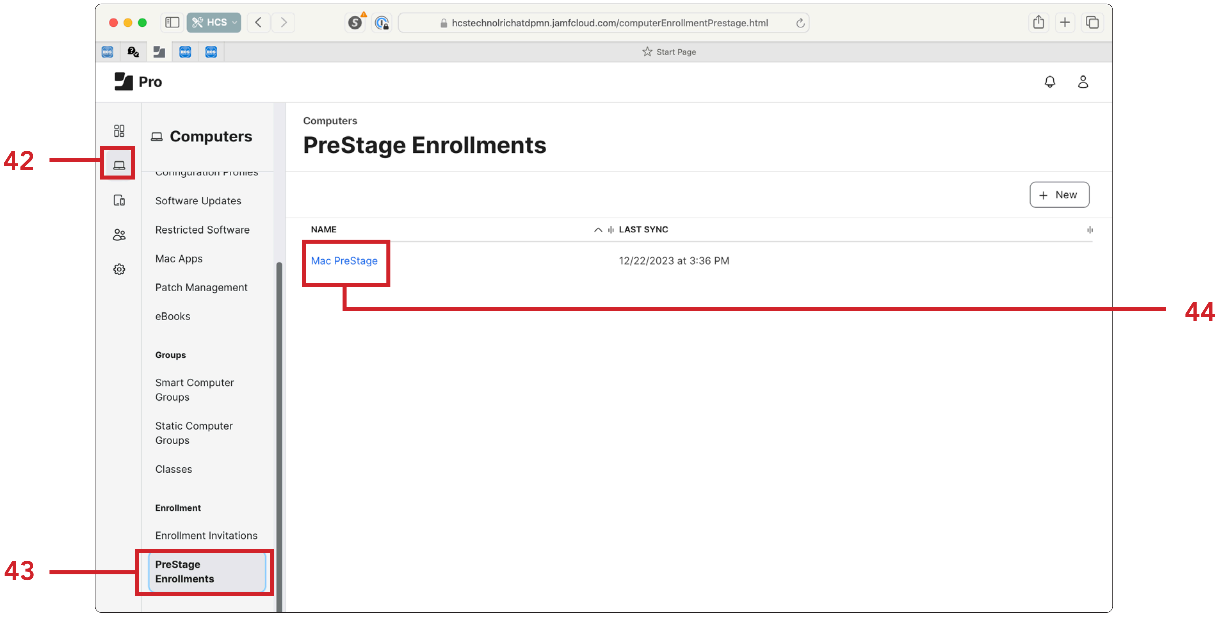
GROUP NAME	
All Managed Clients	Add
macOS Sonoma - Out Of Date Policy	Add
All Managed Servers	Add
Notebooks	Add
PreStage enrollment - Mac PreStage	Add

Edit PreStage

42. Click Computers

43. Click PreStage Enrollments

44. Click Mac PreStage.



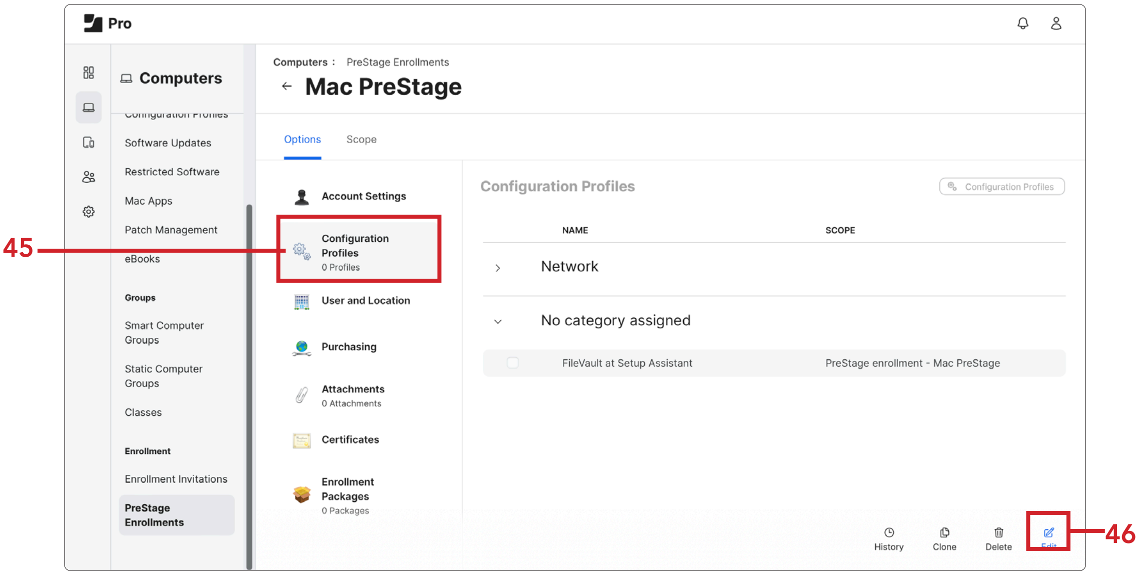
Computers

PreStage Enrollments

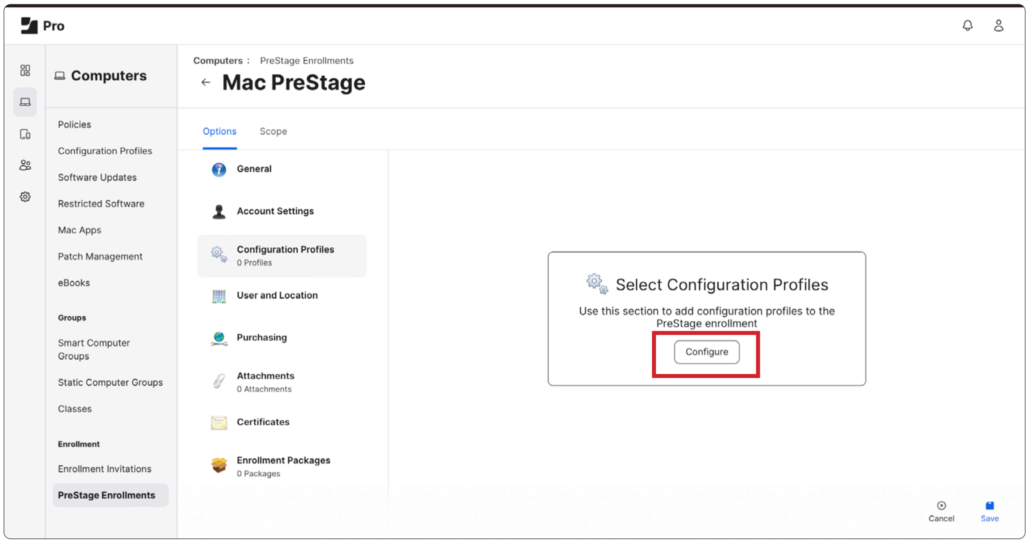
NAME	LAST SYNC
Mac PreStage	12/22/2023 at 3:36 PM

45. Select the Configuration Profiles Payload .

46. Click Edit.



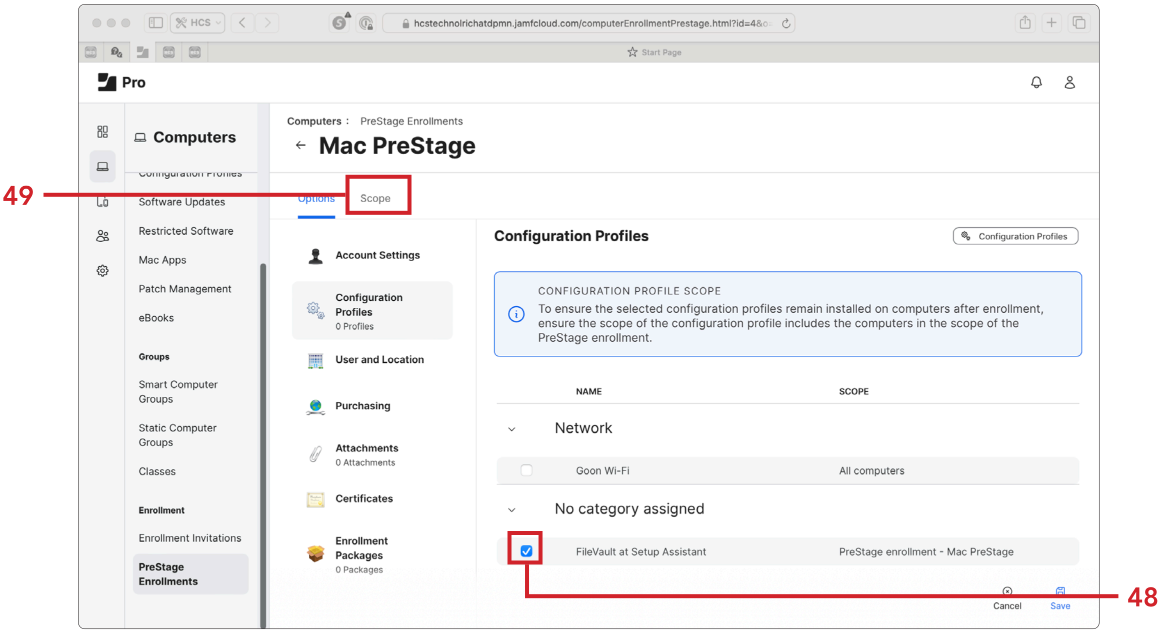
47. Click Configure



Use this section to add configuration profiles to the PreStage enrollment

48. Select the checkbox for FileVault at Setup Assistant

49. Click Scope



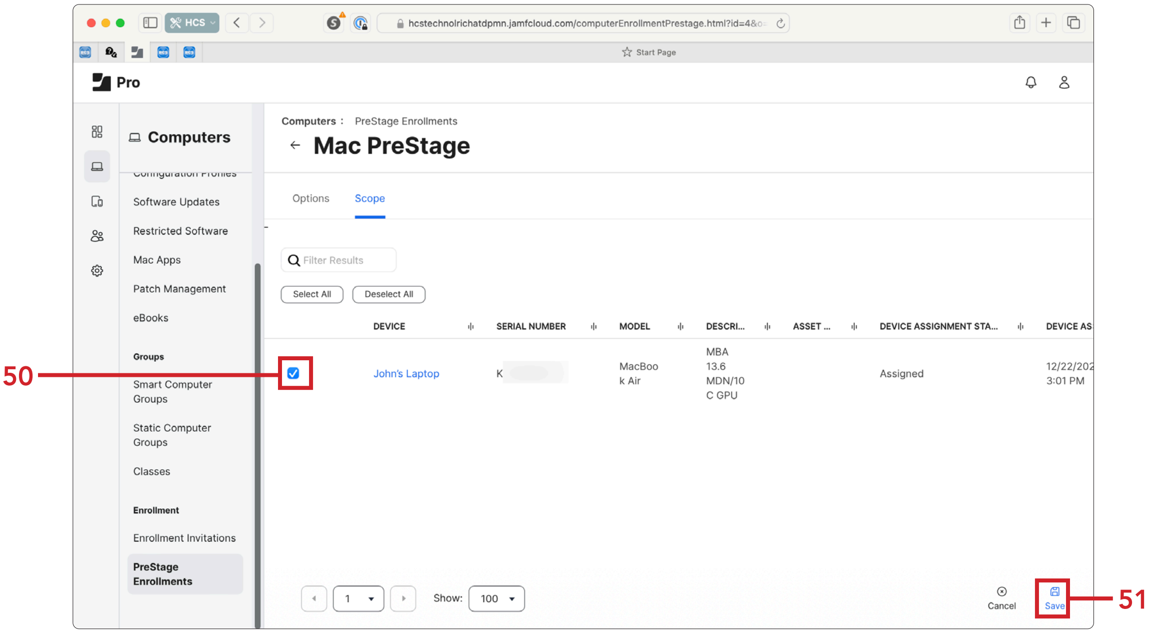
Configuration Profiles

CONFIGURATION PROFILE SCOPE
To ensure the selected configuration profiles remain installed on computers after enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment.

	NAME	SCOPE
Network		
□	Goon Wi-Fi	All computers
No category assigned		
☑	FileVault at Setup Assistant	PreStage enrollment - Mac PreStage

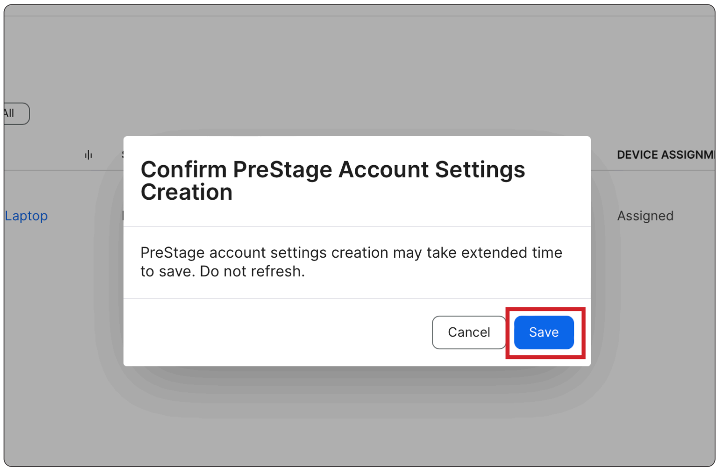
50. Select the checkbox for your test Mac computer.

51. Click Save.



	DEVICE	SERIAL NUMBER	MODEL	DESCRI...	ASSET ...	DEVICE ASSIGNMENT STA...	DEVICE AS
☑	John's Laptop	K[redacted]	MacBook Air	MBA 13.6 MDN/10 C GPU		Assigned	12/22/202 3:01 PM

52. Click Save at the PreStage Account Settings Creation message.



Confirm PreStage Account Settings Creation

PreStage account settings creation may take extended time to save. Do not refresh.

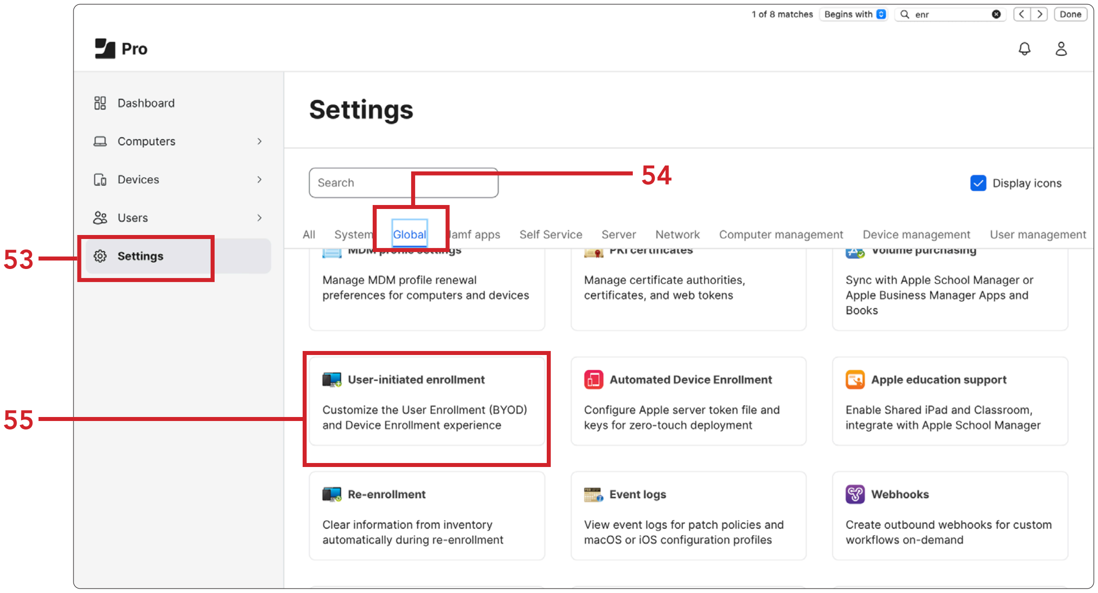
Create a Jamf Management Account

The Jamf Management Account is created by the Jamf binary. When you enroll a Mac computer with Jamf Pro, you must specify a local administrator account called the "management account". However, choosing to create the management account on Mac computers is optional and is only required for some workflows. The management account only needs to be created if you want to log in to a specific Mac computer to perform management tasks

53. Click Settings.

54. Click Global.

55. Click User-initiated enrollment.



MDM profile settings
Manage MDM profile renewal preferences for computers and devices

PKI certificates
Manage certificate authorities, certificates, and web tokens

Volume purchasing
Sync with Apple School Manager or Apple Business Manager Apps and Books

User-initiated enrollment
Customize the User Enrollment (BYOD) and Device Enrollment experience

Automated Device Enrollment
Configure Apple server token file and keys for zero-touch deployment

Apple education support
Enable Shared iPad and Classroom, integrate with Apple School Manager

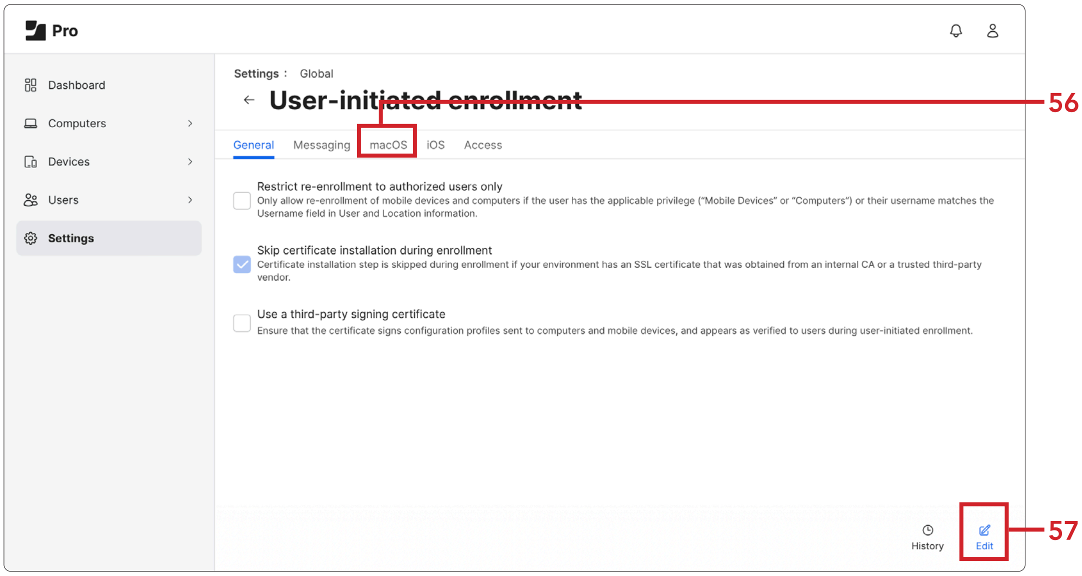
Re-enrollment
Clear information from inventory automatically during re-enrollment

Event logs
View event logs for patch policies and macOS or iOS configuration profiles

Webhooks
Create outbound webhooks for custom workflows on-demand

56. Click macOS.

57. Click Edit.



Settings : Global

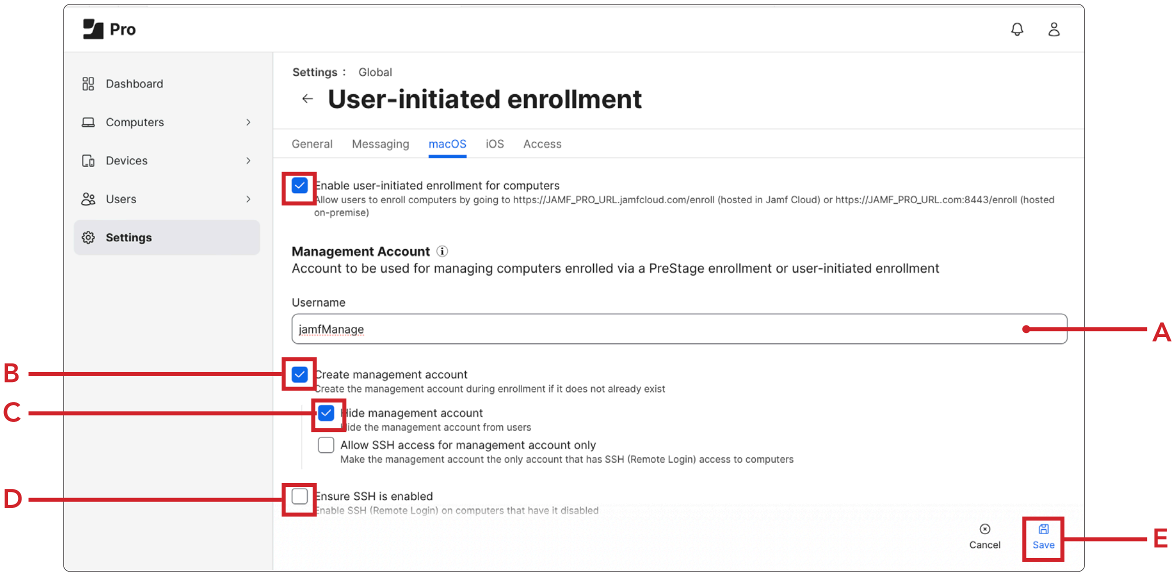
User-initiated enrollment

□ Restrict re-enrollment to authorized users only
Only allow re-enrollment of mobile devices and computers if the user has the applicable privilege ("Mobile Devices" or "Computers") or their username matches the Username field in User and Location information.

☑ Skip certificate installation during enrollment
Certificate installation step is skipped during enrollment if your environment has an SSL certificate that was obtained from an internal CA or a trusted third-party vendor.

□ Use a third-party signing certificate
Ensure that the certificate signs configuration profiles sent to computers and mobile devices, and appears as verified to users during user-initiated enrollment.

58. Select the checkbox for Enable user-initiated enrollment for computers.
    A. Enter a Username: jamfManage (For the purposes of testing ONLY)
       NOTE: The password will be LAPS Enabled by default
    B. Enable Create management account.
    C. Enable Hide management account.
    D. Disable Ensure SSH is enabled.
    E. Click Save.



Settings : Global

User-initiated enrollment

☑ Enable user-initiated enrollment for computers
Allow users to enroll computers by going to https://JAMF_PRO_URL.jamfcloud.com/enroll (hosted in Jamf Cloud) or https://JAMF_PRO_URL.com:8443/enroll (hosted on-premise)

Management Account
Account to be used for managing computers enrolled via a PreStage enrollment or user-initiated enrollment

Username
jamfManage

☑ Create management account
Create the management account during enrollment if it does not already exist

☑ Hide management account
Hide the management account from users

□ Allow SSH access for management account only
Make the management account the only account that has SSH (Remote Login) access to computers

□ Ensure SSH is enabled
Enable SSH (Remote Login) on computers that have it disabled

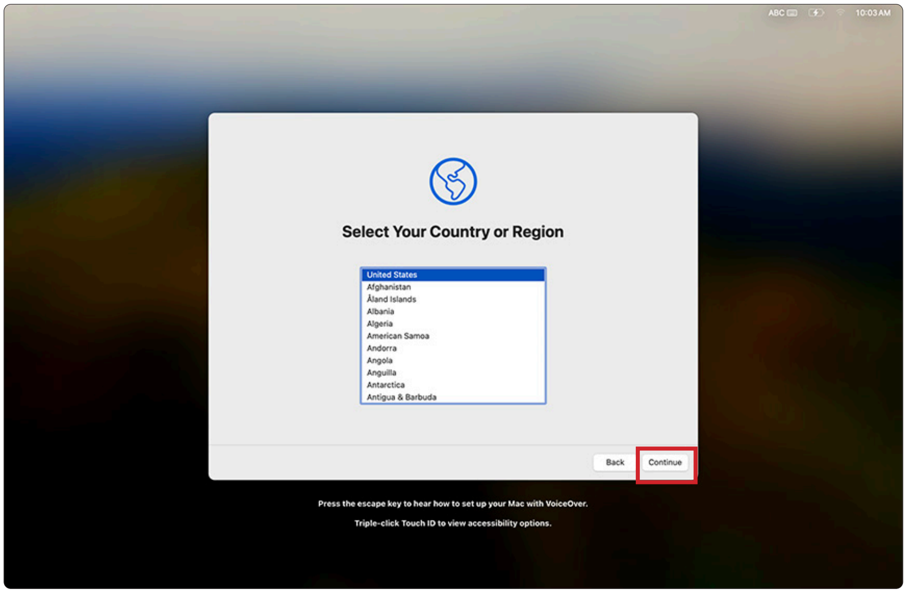
Enroll your Mac computer in Jamf Pro

59. Start your test Mac computer scoped in the PreStage.

60. Click Get Started.

61. Choose Language.

62. Choose Country or Region. Click Continue.



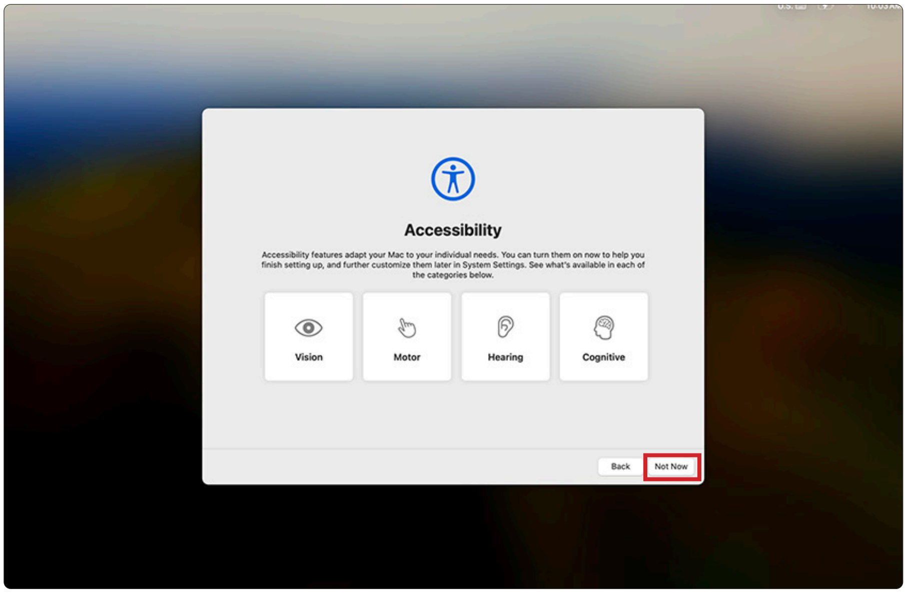
Select Your Country or Region

United States
Afghanistan
Åland Islands
Albania
Algeria
American Samoa
Andorra
Angola
Anguilla
Antarctica
Antigua & Barbuda

Press the escape key to hear how to set up your Mac with VoiceOver.

Triple-click Touch ID to view accessibility options.

63. At the Accessibility screen, select Not Now.

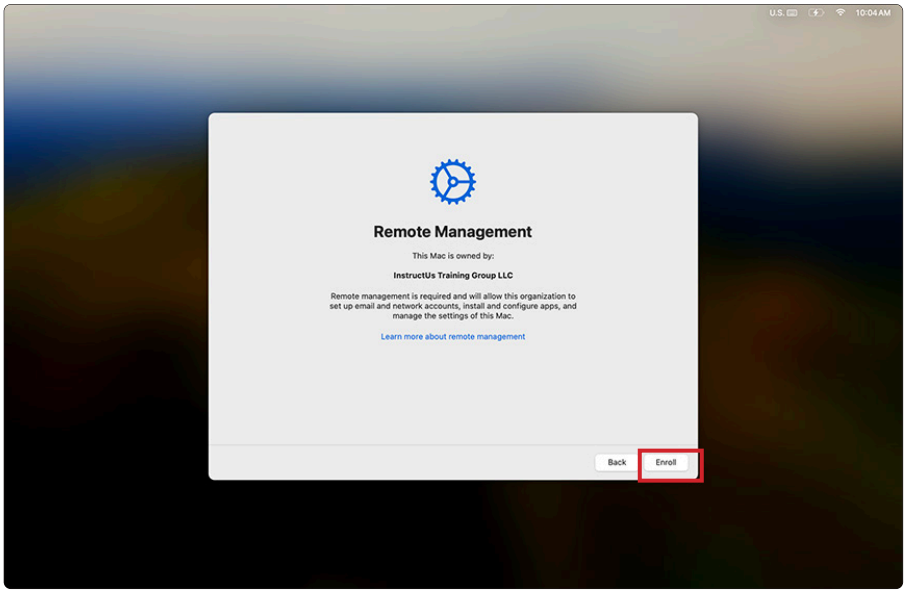


Accessibility

Accessibility features adapt your Mac to your individual needs. You can turn them on now to help you finish setting up, and further customize them later in System Settings. See what's available in each of the categories below.

64. Connect to the appropriate network

65. Confirm Remote Management and Click Enroll.



Remote Management

This Mac is owned by:

InstructUs Training Group LLC

Remote management is required and will allow this organization to set up email and network accounts, install and configure apps, and manage the settings of this Mac.

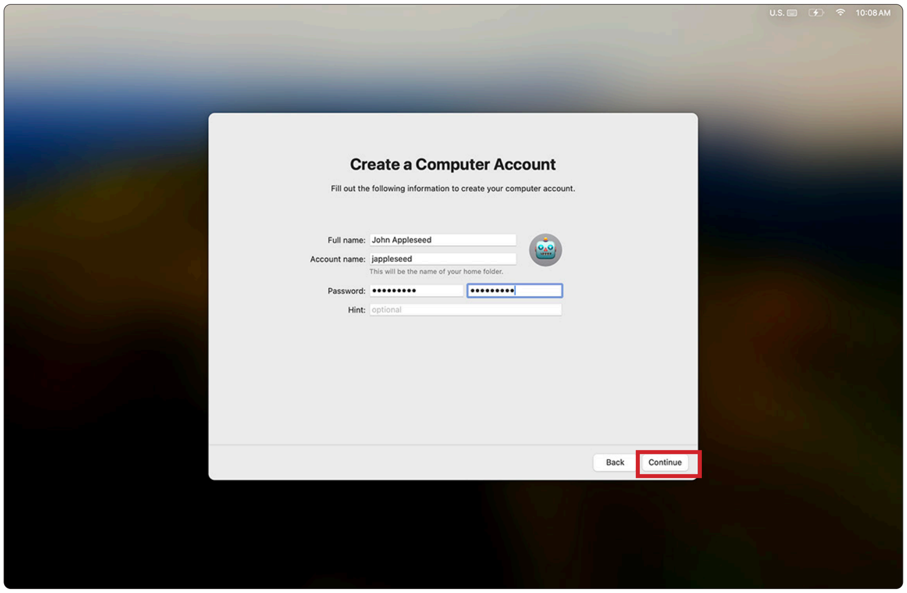
Learn more about remote management

66. At Migration Assistant, at the left-hand corner, click Not Now.

67. For Apple ID, click Setup Later. Click Skip.

68. At the create a computer account screen, Enter a name and password of your choosing. This guide will use John Appleseed for the Full Name and jappleseed for the Account name.

69. Click Continue.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: John Appleseed

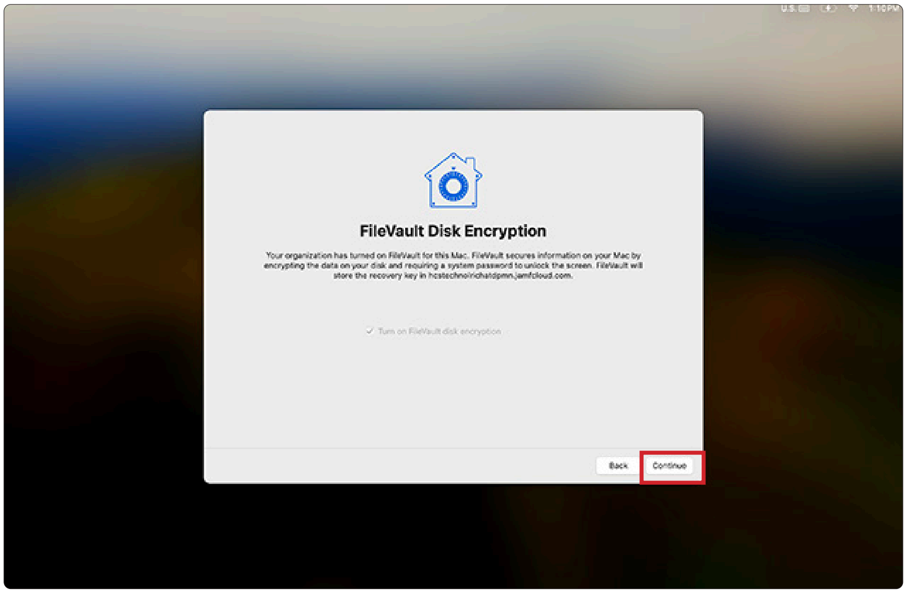
Account name: jappleseed

This will be the name of your home folder.

Password: ••••••••• •••••••••

Hint: optional

70. Confirm FileVault Disk Encryption is enabled and click Continue.



FileVault Disk Encryption

Your organization has turned on FileVault for this Mac. FileVault secures information on your Mac by encrypting the data on your disk and requiring a system password to unlock the screen. FileVault will store the recovery key in hcstechnolrichardpmn.jamfcloud.com.

✓ Turn on FileVault disk encryption

71. Click through and set any additional screens to meet your needs.

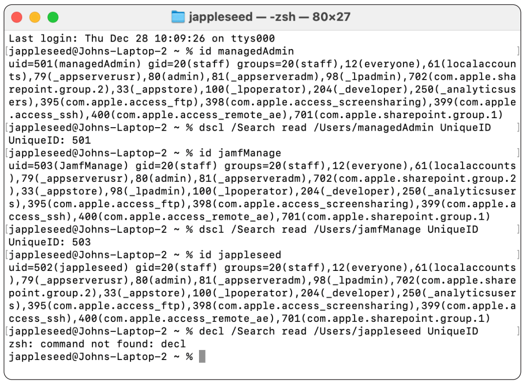
Confirm Managed Admin, Jamf Management Account, and user created during setup assistant

72. Open Terminal. A new shell window opens with your home folder as the working directory

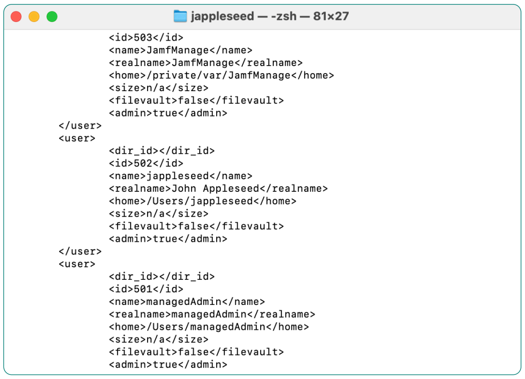
73. Type the following commands and press Return

- `id managedAdmin`
  `dscl /Search read /Users/managedAdmin UniqueID`
- `id jamfManage`
  `dscl /Search read /Users/jamfManage UniqueID`
- `id jappleseed`
  `dscl /Search read /Users/jappleseed UniqueID`

Note: Another option is `sudo jamf listUsers -showAll`



```
Last login: Thu Dec 28 10:09:26 on ttys000
jappleseed@Johns-Laptop-2 ~ % id managedAdmin
uid=501(managedAdmin) gid=20(staff) groups=20(staff),12(everyone),61(localaccoun
ts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),702(com.apple.sha
repoint.group.2),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsus
ers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple
.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % dscl /Search read /Users/managedAdmin UniqueID
UniqueID: 501
jappleseed@Johns-Laptop-2 ~ % id jamfManage
uid=503(JamfManage) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts
),79(_appserverusr),80(admin),81(_appserveradm),702(com.apple.sharepoint.group.2
),33(_appstore),98(_lpadmin),100(_lpoperator),204(_developer),250(_analyticsuser
s),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.a
ccess_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % dscl /Search read /Users/jamfManage UniqueID
UniqueID: 503
jappleseed@Johns-Laptop-2 ~ % id jappleseed
uid=502(jappleseed) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts
),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),702(com.apple.share
point.group.2),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsuser
s),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.a
ccess_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % decl /Search read /Users/jappleseed UniqueID
zsh: command not found: decl
jappleseed@Johns-Laptop-2 ~ % 
```



```
                <id>503</id>
                <name>JamfManage</name>
                <realname>JamfManage</realname>
                <home>/private/var/JamfManage</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
        </user>
        <user>
                <dir_id></dir_id>
                <id>502</id>
                <name>jappleseed</name>
                <realname>John Appleseed</realname>
                <home>/Users/jappleseed</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
        </user>
        <user>
                <dir_id></dir_id>
                <id>501</id>
                <name>managedAdmin</name>
                <realname>managedAdmin</realname>
                <home>/Users/managedAdmin</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
```

Using the command: `sudo jamf listUsers -showAll`

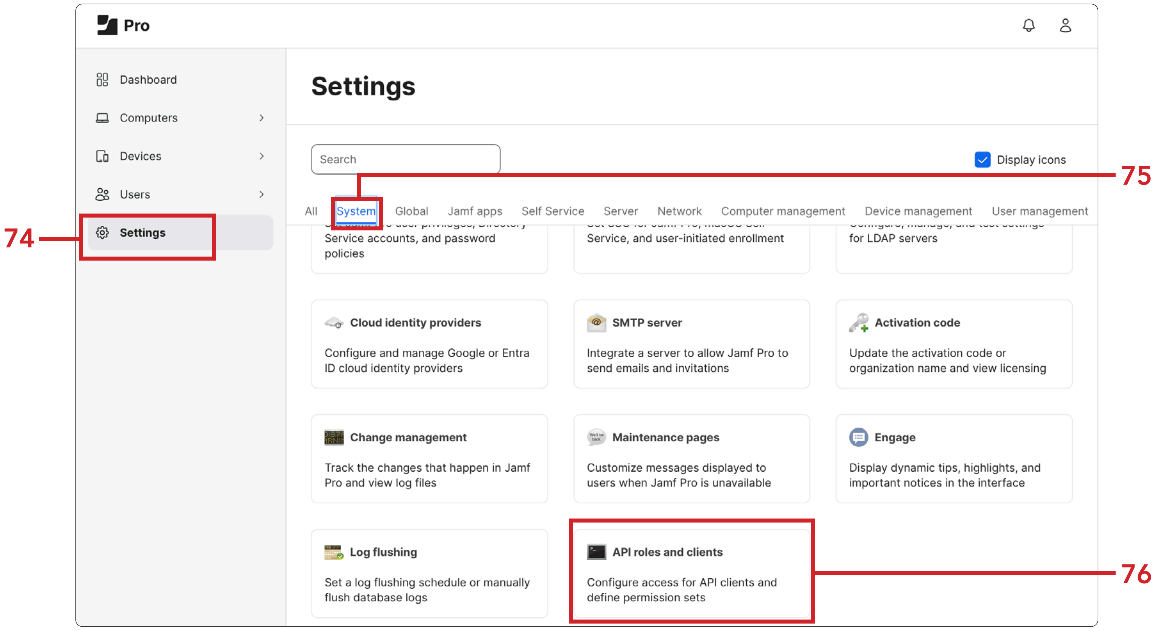
Create a Jamf API Role that has the following minimum permissions

The Jamf API Client ID and Secret are used once to get a token that's then used until it's either expired or renewed. They're not the same as Jamf account username password.

74. Click Settings.

75. Click System.

76. Click API Roles and Clients.



Service accounts, and password policies

Service, and user-initiated enrollment

for LDAP servers

Cloud identity providers
Configure and manage Google or Entra ID cloud identity providers

SMTP server
Integrate a server to allow Jamf Pro to send emails and invitations

Activation code
Update the activation code or organization name and view licensing

Change management
Track the changes that happen in Jamf Pro and view log files

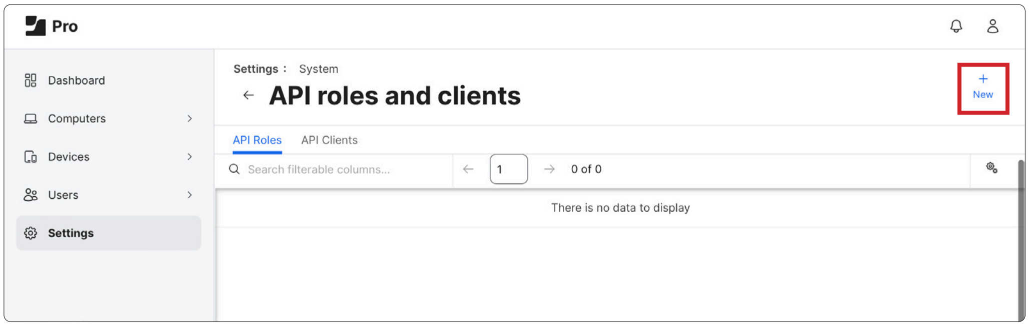
Maintenance pages
Customize messages displayed to users when Jamf Pro is unavailable

Engage
Display dynamic tips, highlights, and important notices in the interface

Log flushing
Set a log flushing schedule or manually flush database logs

API roles and clients
Configure access for API clients and define permission sets

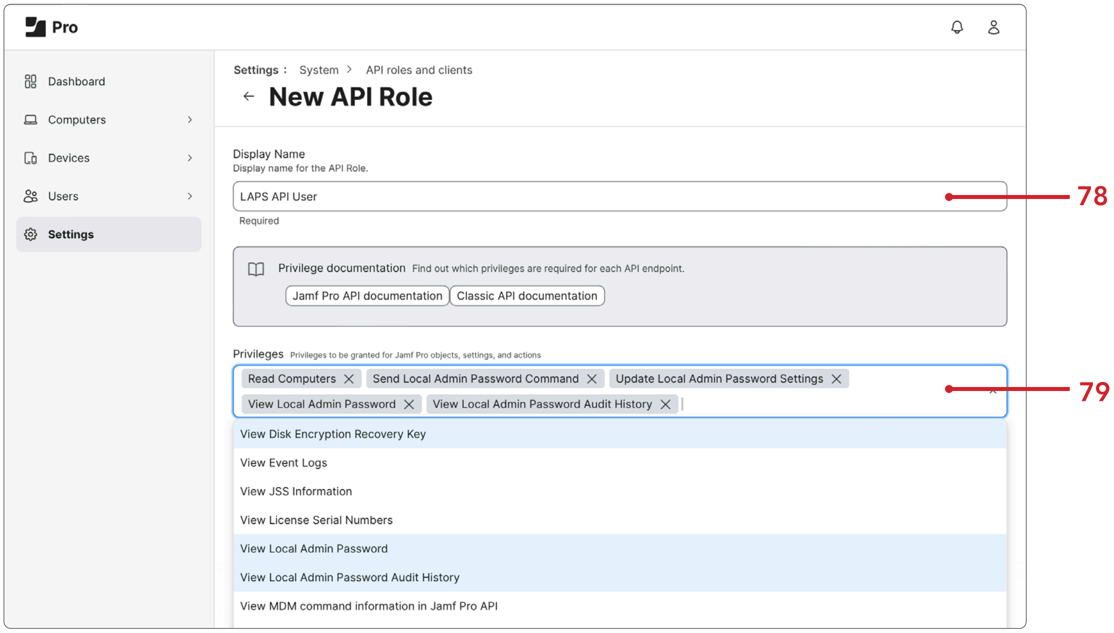
77. Click New.



There is no data to display

78. Enter a Display Name: LAPS API User (For the purposes of testing ONLY)

79. Under Privileges, Select the following privileges:
   - Read Computers
   - Send Local Admin Password Command
   - Update Local Admin Password Settings
   - View Local Admin Password
   - View Local Admin Password Audit History



New API Role

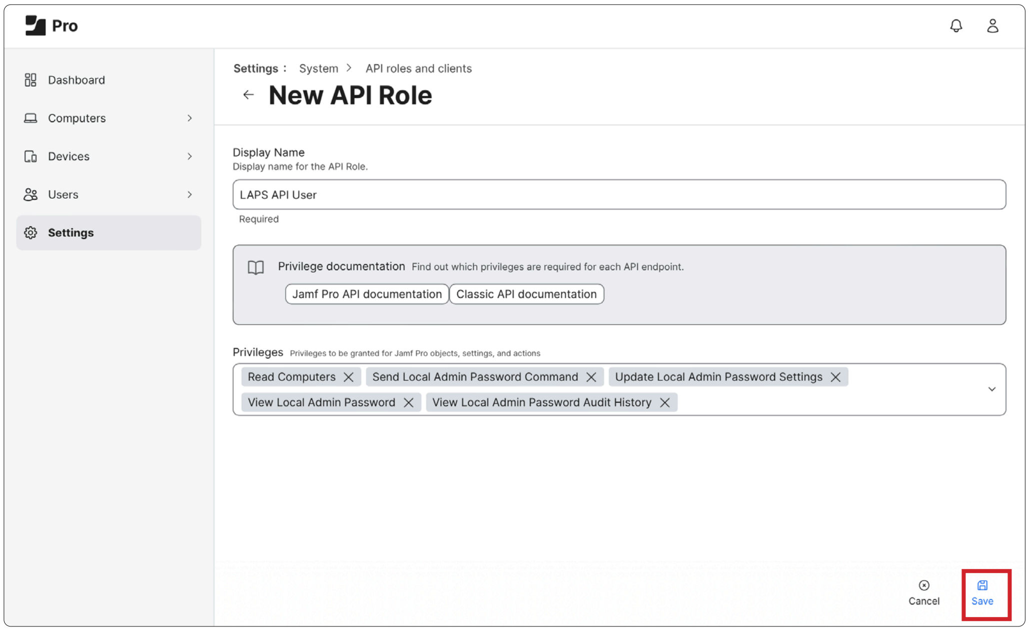
Display Name
Display name for the API Role.
LAPS API User
Required

Privilege documentation Find out which privileges are required for each API endpoint.
Jamf Pro API documentation | Classic API documentation

Privileges Privileges to be granted for Jamf Pro objects, settings, and actions
Read Computers ✕ | Send Local Admin Password Command ✕ | Update Local Admin Password Settings ✕ | View Local Admin Password ✕ | View Local Admin Password Audit History ✕

View Disk Encryption Recovery Key
View Event Logs
View JSS Information
View License Serial Numbers
View Local Admin Password
View Local Admin Password Audit History
View MDM command information in Jamf Pro API

80. Click Save.



New API Role

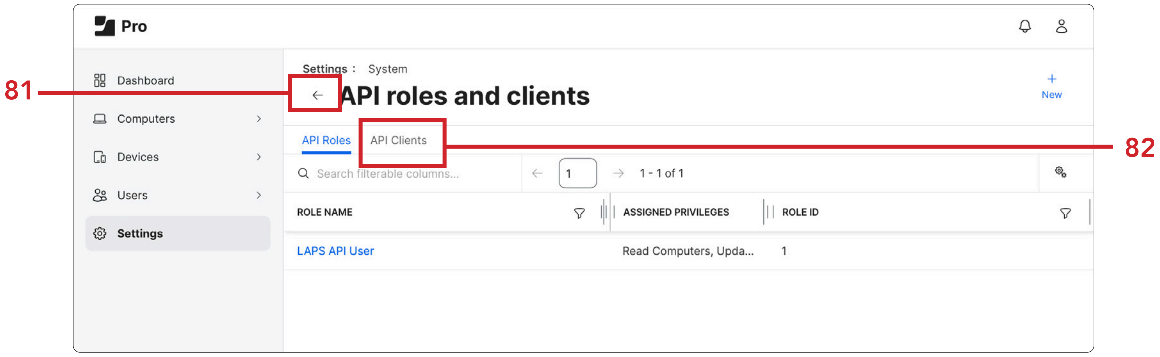
Display Name
Display name for the API Role.
LAPS API User
Required

Privilege documentation Find out which privileges are required for each API endpoint.
Jamf Pro API documentation | Classic API documentation

Privileges Privileges to be granted for Jamf Pro objects, settings, and actions
Read Computers ✕ | Send Local Admin Password Command ✕ | Update Local Admin Password Settings ✕ | View Local Admin Password ✕ | View Local Admin Password Audit History ✕

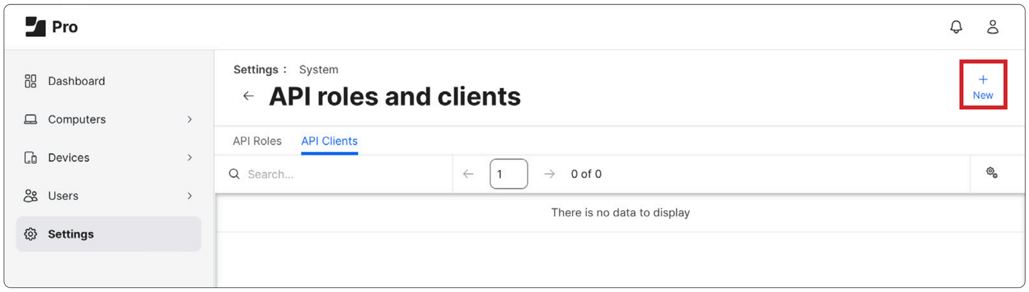
81. Click the Previous arrow.

82. Click API Clients.



ROLE NAME	ASSIGNED PRIVILEGES	ROLE ID
LAPS API User	Read Computers, Upda...	1

83. Click New.



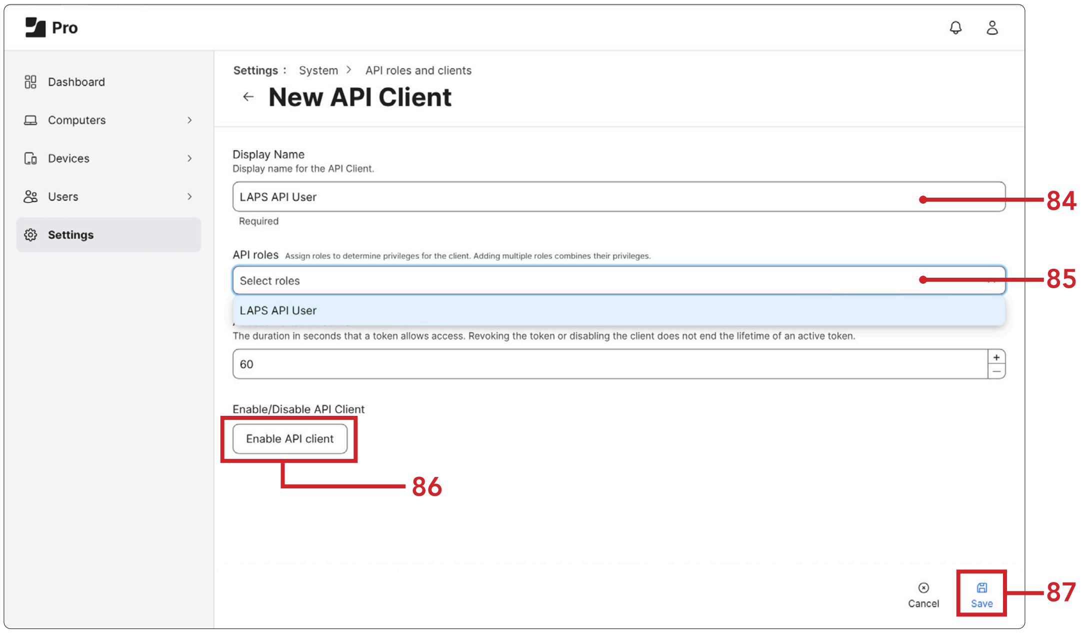
There is no data to display

84. Enter a Display Name: LAPS API User (For the purposes of testing ONLY.)

85. API Role select LAPS API User.

86. Click Enable API Client.

87. Click Save.



Display Name
Display name for the API Client.
LAPS API User
Required

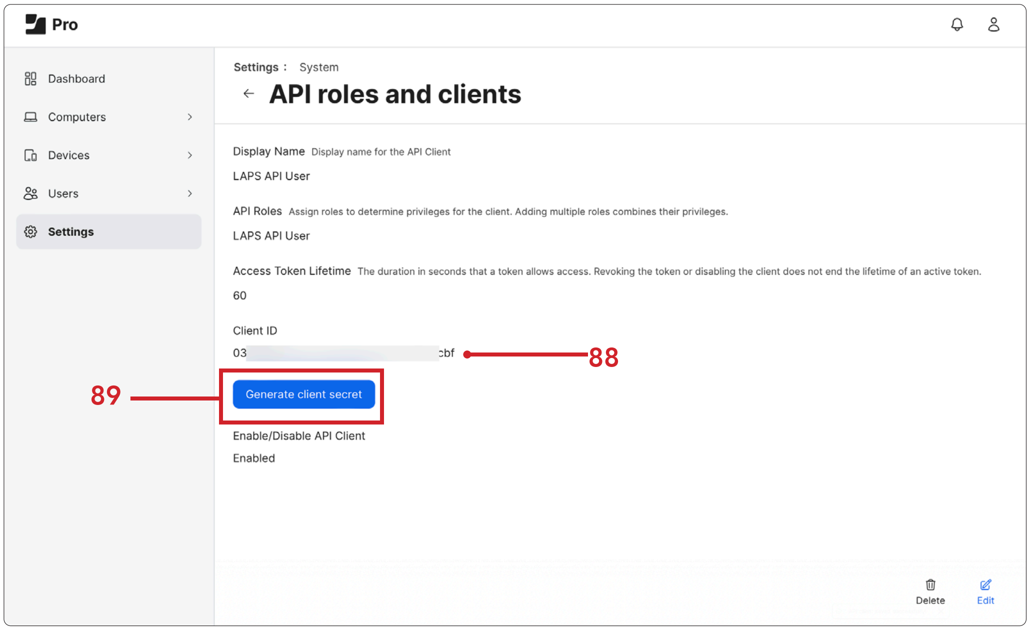
API roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.
Select roles
LAPS API User

The duration in seconds that a token allows access. Revoking the token or disabling the client does not end the lifetime of an active token.
60

Enable/Disable API Client

88. Copy the Client ID for a future step.

89. Click Generate client secret.



Settings : System

API roles and clients

Display Name Display name for the API Client

LAPS API User

API Roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.

LAPS API User

Access Token Lifetime The duration in seconds that a token allows access. Revoking the token or disabling the client does not end the lifetime of an active token.

60

Client ID

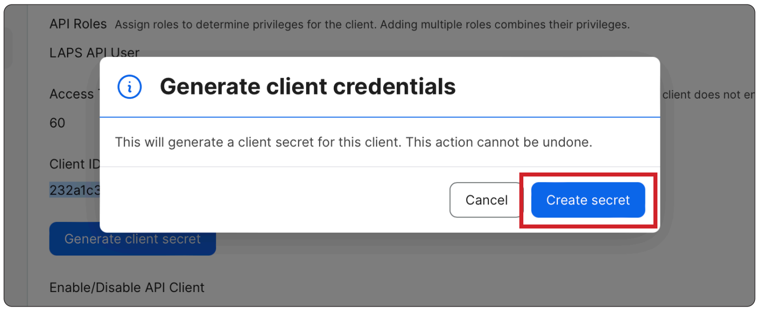
03[redacted]cbf

Generate client secret

Enable/Disable API Client

Enabled

90. Click Create secret.



API Roles Assign roles to determine privileges for the client. Adding multiple roles combines their privileges.

LAPS API User

Access

60

Client ID

232a1c3

Generate client secret

Enable/Disable API Client

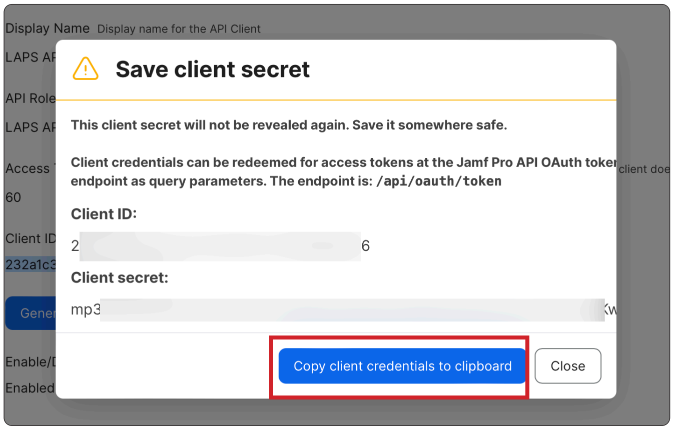
Generate client credentials

This will generate a client secret for this client. This action cannot be undone.

Cancel | Create secret

91. Copy the secret for a future step

92. Click Close



Display Name Display name for the API Client

Save client secret

This client secret will not be revealed again. Save it somewhere safe.

Client credentials can be redeemed for access tokens at the Jamf Pro API OAuth token endpoint as query parameters. The endpoint is: `/api/oauth/token`

Client ID:

2[redacted]6

Client secret:

mp3[redacted]Kw

Copy client credentials to clipboard | Close

Viewing the LAPS Password for the Jamf Management account.

There are two options for viewing the LAPS password:

- Option 1 requires a 3rd party application
- Option 2 requires the Jamf Pro API

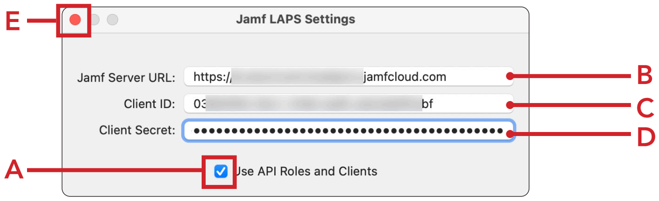
Option 1- Jamf LAPS App

93. On your production Mac computer, download the Jamf LAPS App to review the LAPS Password: https://github.com/jamf/jamf-laps-public/releases/tag/v1.0.1

94. Install Jamf LAPS in /Applications

95. Launch Jamf LAPS

96. In Jamf LAPS Settings, enter the following:
    A. Check Use API Roles and Clients.
    B. Enter your Jamf Server URL.
    C. Enter Client ID: (Saved from previous section).
    D. Enter Client Secret: (Saved from previous section).
    E. Close Jamf LAPS Settings Window.



Jamf LAPS Settings

Jamf Server URL: https://[redacted]jamfcloud.com

Client ID: 03[redacted]bf

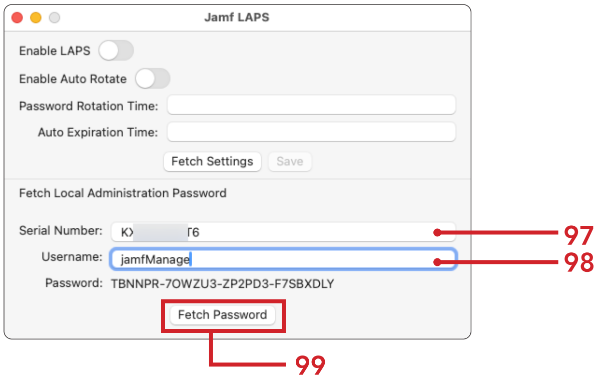
Client Secret: ••

☑ Use API Roles and Clients

97. Enter the Serial Number of your enrolled test Mac computer. You can find the serial number in the Computer Record on the Jamf Pro server.

98. Username: Enter the Jamf Management Account. This guide will use jamfManage.

99. Click Fetch Password.



Jamf LAPS

Enable LAPS ○

Enable Auto Rotate ○

Password Rotation Time:

Auto Expiration Time:

Fetch Local Administration Password

Serial Number: K[redacted]T6

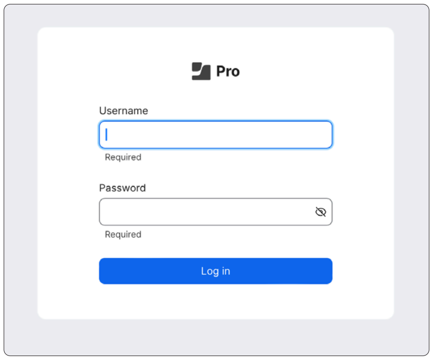
Username: jamfManage

Password: TBNNPR-7OWZU3-ZP2PD3-F7SBXDLY

Option 2
View LAPS Password using the Jamf Pro API

We need to document the client management id of our test Mac computer.

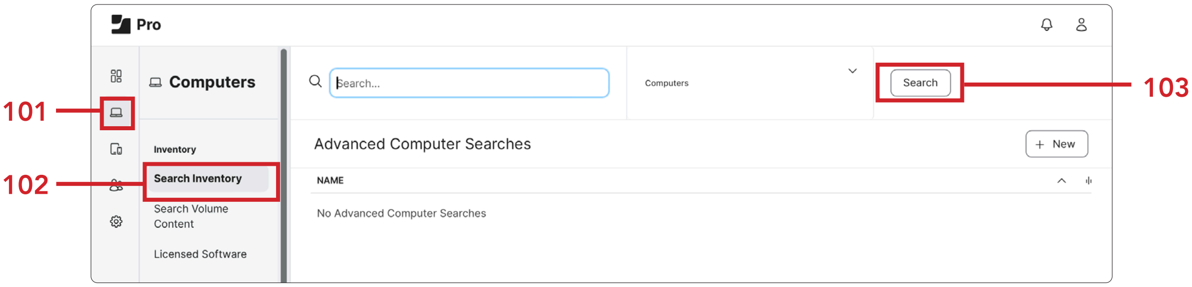
100. On your production Mac computer, log into your Jamf Pro server with proper privileges.



101. Click Computers.

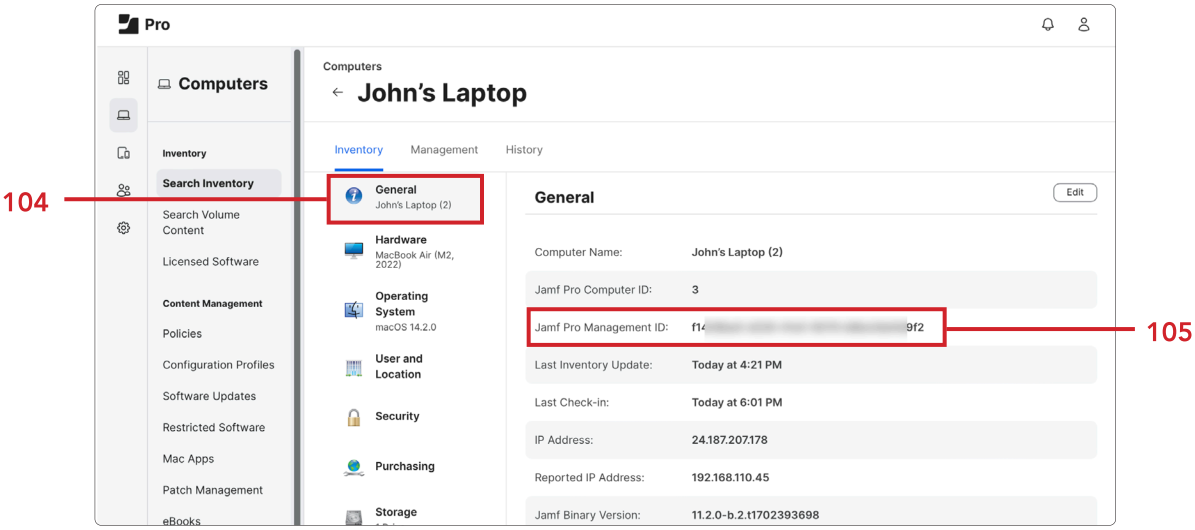
102. Click Search Inventory.

103. Search for your test Mac computer.



104. In the General Category of your Computer Inventory record.

105. Document the the Jamf Pro Management ID (We will need this in a later step.)



Computer Name: John's Laptop (2)

Jamf Pro Computer ID: 3

Jamf Pro Management ID: f14[redacted]9f2

Last Inventory Update: Today at 4:21 PM

Last Check-in: Today at 6:01 PM

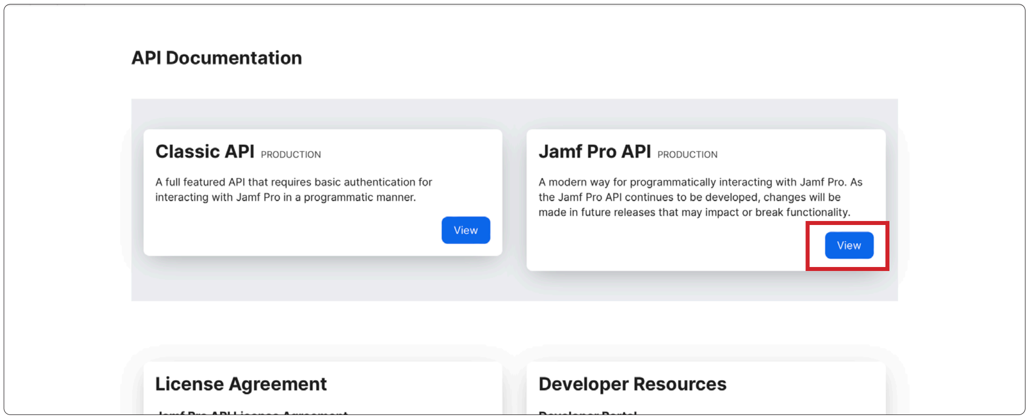
IP Address: 24.187.207.178

Reported IP Address: 192.168.110.45

Jamf Binary Version: 11.2.0-b.2.t1702393698

106. Enter the address of your Jamf Pro server and add /api to the end of the URL.
I.E. https://hcs.jamfcloud.com/api.

107. Click the View button on Jamf Pro API.



API Documentation

Classic API PRODUCTION
A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.
View

Jamf Pro API PRODUCTION
A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.
View

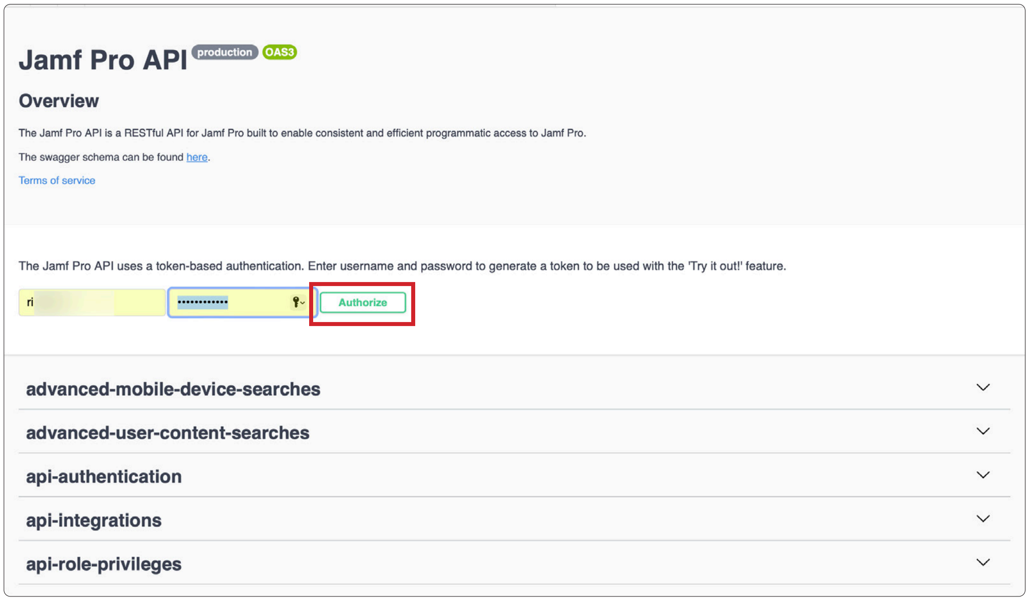
License Agreement
Jamf Pro API License Agreement

Developer Resources
Developer Portal

108. Enter your Jamf Pro credentials. Click Authorize to generate a token.
NOTE: The Jamf API Client ID and Secret cannot be used on this page. Use a Jamf account with these minimal privileges:

- Read Computers
- Send Local Admin Password Command
- Update Local Admin Password Settings
- View Local Admin Password
- View Local Admin Password Audit History

https://learn.jamf.com/bundle/jamf-pro-documentation-current/page/Jamf_Pro_User_Accounts_and_Groups.html



Jamf Pro API production OAS3

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

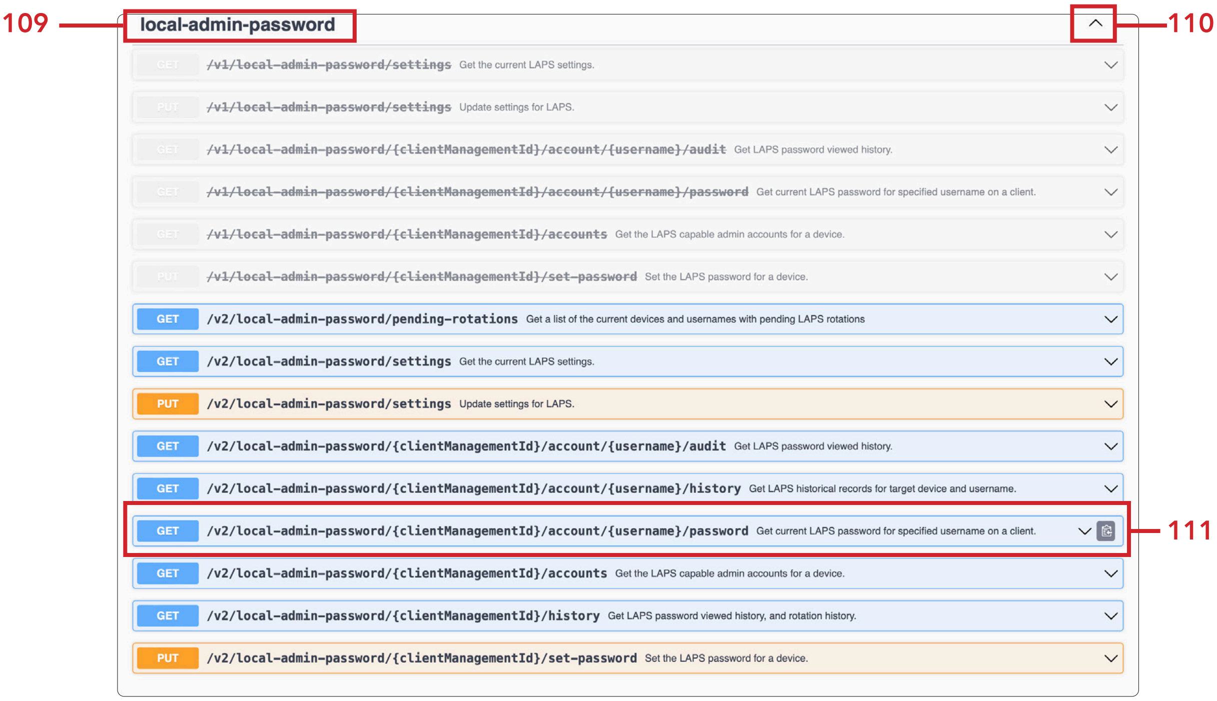
ri | •••••••••••• | Authorize

advanced-mobile-device-searches
advanced-user-content-searches
api-authentication
api-integrations
api-role-privileges

109. Scroll down the list and select local-admin-password.

110. Click Expand (⌄) to see its contents.

111. Click Get for /v2/local-admin-password/{clientManagementId}/account/{username}/password current LAPS password for specified user name on a client



local-admin-password

~~GET /v1/local-admin-password/settings~~ Get the current LAPS settings.

~~PUT /v1/local-admin-password/settings~~ Update settings for LAPS.

~~GET /v1/local-admin-password/{clientManagementId}/account/{username}/audit~~ Get LAPS password viewed history.

~~GET /v1/local-admin-password/{clientManagementId}/account/{username}/password~~ Get current LAPS password for specified username on a client.

~~GET /v1/local-admin-password/{clientManagementId}/accounts~~ Get the LAPS capable admin accounts for a device.

~~PUT /v1/local-admin-password/{clientManagementId}/set-password~~ Set the LAPS password for a device.

GET /v2/local-admin-password/pending-rotations Get a list of the current devices and usernames with pending LAPS rotations

GET /v2/local-admin-password/settings Get the current LAPS settings.

PUT /v2/local-admin-password/settings Update settings for LAPS.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/audit Get LAPS password viewed history.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.

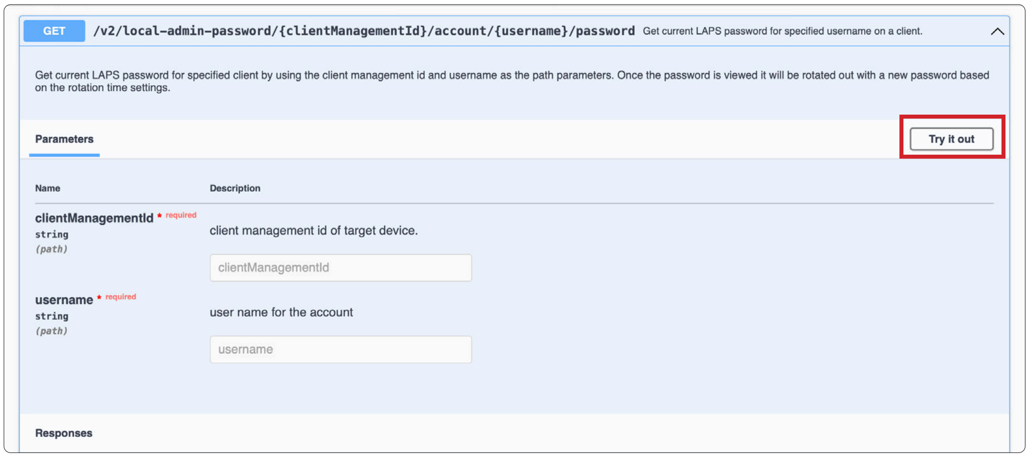
GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

GET /v2/local-admin-password/{clientManagementId}/accounts Get the LAPS capable admin accounts for a device.

GET /v2/local-admin-password/{clientManagementId}/history Get LAPS password viewed history, and rotation history.

PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

112. Click Try it out.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters

Try it out

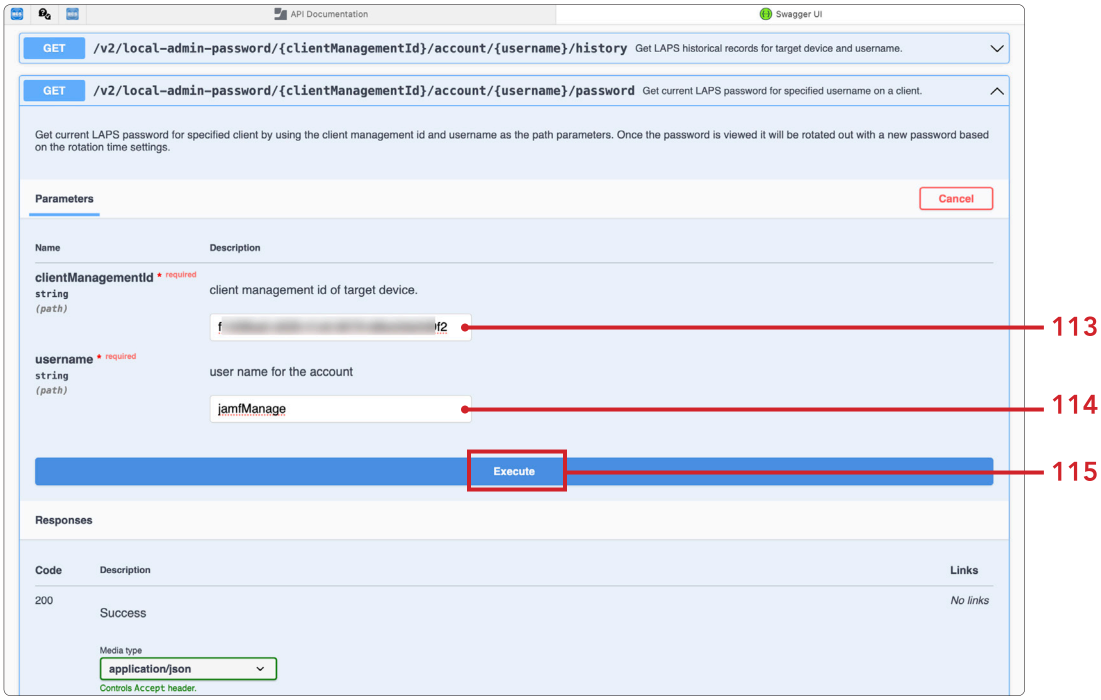
Name	Description
clientManagementId * required string (path)	client management id of target device. clientManagementId
username * required string (path)	user name for the account username

Responses

113. In the clientManagementId field, enter the Jamf Pro Management ID documented from a previous step.

114. In the username field enter jamfManage or your chosen Jamf Management account set in User Initiated enrollment.

115. Click Execute.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.

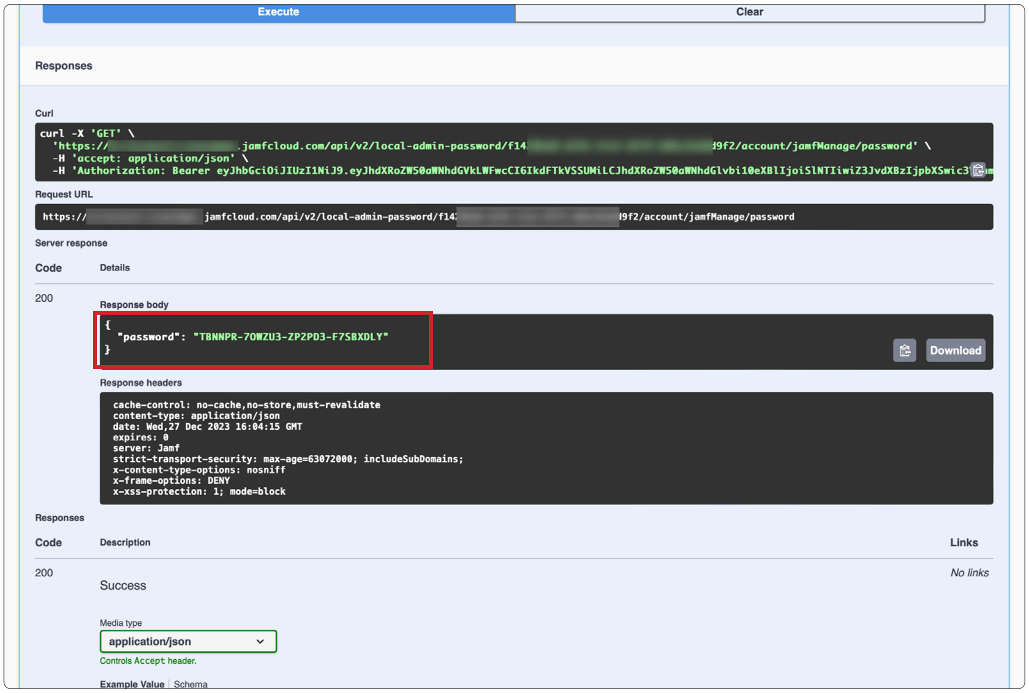
GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Name	Description
clientManagementId * required string *(path)*	client management id of target device. f[redacted]f2
username * required string *(path)*	user name for the account jamfManage

Code	Description	Links
200	Success Media type application/json Controls Accept header.	*No links*

116. Scroll down to confirm your results. You should be able to view the password for jamfManage. NOTE: Once the LAPS password is viewed, the Jamf Pro Server will automatically rotate the LAPS password in 60 minutes. If the Mac computer is offline, the rotation will happen once the Mac computer is online and checks in with the Jamf Pro server.



Responses

Curl

```
curl -X 'GET' \
  'https://[redacted].jamfcloud.com/api/v2/local-admin-password/f14[redacted]d9f2/account/jamfManage/password' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdXRoZW50aWNhdGVkLWFwcCI6IkdFTkVSSUMiLCJhdXRoZW50aWNhdGlvbi10eXBlIjoiSlNTIiwiZ3JvdXBzIjpbXSwic3
```

Request URL

```
https://[redacted]jamfcloud.com/api/v2/local-admin-password/f14[redacted]d9f2/account/jamfManage/password
```

Server response

Code	Details
200	Response body

```
{
  "password": "TBNNPR-7OWZU3-ZP2PD3-F7SBXDLY"
}
```

Response headers

```
 cache-control: no-cache,no-store,must-revalidate
 content-type: application/json
 date: Wed,27 Dec 2023 16:04:15 GMT
 expires: 0
 server: Jamf
 strict-transport-security: max-age=63072000; includeSubDomains;
 x-content-type-options: nosniff
 x-frame-options: DENY
 x-xss-protection: 1; mode=block
```

Responses

Code	Description	Links
200	Success	*No links*

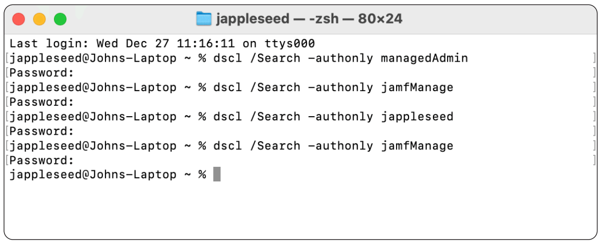
Media type

Confirm password for the Managed Admin, Jamf Management Account, and user created during setup assistant

117. On your test Mac computer, open Terminal.

118. A new shell window opens with your home folder as the working directory

119. Type the following commands and press Return
- `dscl /Search -authonly managedAdmin`
  Enter YOURPRESTAGEPASSWORD.
  NOTE: No response in the terminal means the command was successful.
- `dscl /Search -authonly jamfManage`
  Enter YOURLAPSPASSWORD.
  NOTE: No response in the terminal means the command was successful.
- `dscl /Search -authonly jappleseed`
  Enter YOURPASSWORD.
  NOTE: No response in the terminal means the command was successful.



```
Last login: Wed Dec 27 11:16:11 on ttys000
jappleseed@Johns-Laptop ~ % dscl /Search -authonly managedAdmin
Password:
jappleseed@Johns-Laptop ~ % dscl /Search -authonly jamfManage
Password:
jappleseed@Johns-Laptop ~ % dscl /Search -authonly jappleseed
Password:
jappleseed@Johns-Laptop ~ % dscl /Search -authonly jamfManage
Password:
jappleseed@Johns-Laptop ~ % 
```

120. Check the users for the secure token status (Required to decrypt FileVault and for other macOS task requiring volume ownership).

```
sysadminctl -secureTokenStatus jappleseed
```

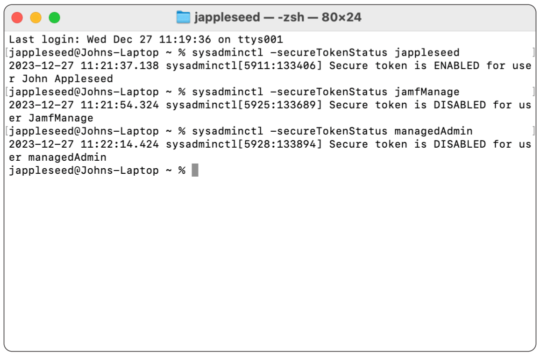
You will get a message letting you know the secure token is enabled for the user jappleseed. NOTE: This user was created during Setup Assistant. Since we logged in, the user has a Secure Token.

```
sysadminctl -secureTokenStatus jamfManage
```

You will get a message letting you know the secure token is disabled for the user jamfManage. NOTE: This user in the Jamf Management account set in User Initiated enrollment. Password is automatically using LAPS. Since we never logged in, the user does not have a Secure Token.

```
sysadminctl -secureTokenStatus managedAdmin
```

You will get a message letting you know the secure token is disabled for the user managedAdmin.
NOTE: This user is the Managed Admin created by MDM. Credentials created in the Jamf PreStage. Since we never logged in, the user does not have a Secure Token.



```
Last login: Wed Dec 27 11:19:36 on ttys001
jappleseed@Johns-Laptop ~ % sysadminctl -secureTokenStatus jappleseed
2023-12-27 11:21:37.138 sysadminctl[5911:133406] Secure token is ENABLED for use
r John Appleseed
jappleseed@Johns-Laptop ~ % sysadminctl -secureTokenStatus jamfManage
2023-12-27 11:21:54.324 sysadminctl[5925:133689] Secure token is DISABLED for us
er JamfManage
jappleseed@Johns-Laptop ~ % sysadminctl -secureTokenStatus managedAdmin
2023-12-27 11:22:14.424 sysadminctl[5928:133894] Secure token is DISABLED for us
er managedAdmin
jappleseed@Johns-Laptop ~ % 
```

121. Logout of the user created during Setup Assistant. This guide was logged in with the user named jappleseed.

122. Login with the Jamf Management Account and the LAPS Password. This guide will use the jamfManage account. - NOTE: Click Other to log in. If you don't see Other, press the escape key on your keyboard. The LAPS password is case sensitive and must include the dashes.

123. Logout of the Jamf Management Account.

124. Login with the user created during Setup Assistant. Assistant. This guide was logged in with the user named jappleseed

125. Check the users for the secure token status (Required to decrypt FileVault and for other macOS task requiring volume ownership.)

```
sysadminctl -secureTokenStatus jappleseed
```

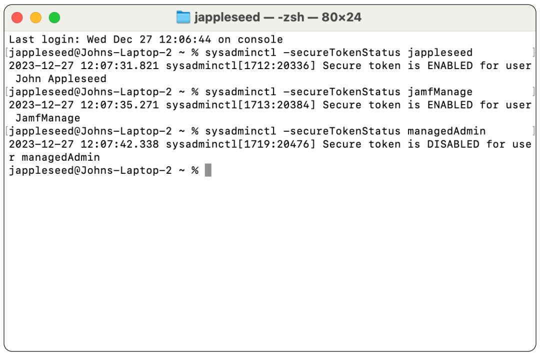
You will get a message letting you know the secure token is enabled for the user jappleseed. NOTE: This user was created during Setup Assistant. Since we logged in, the user has a Secure Token.

```
sysadminctl -secureTokenStatus jamfManage
```

You will get a message letting you know the secure token is enabled for the user jamfManage NOTE: This user is the Jamf Management account set in User Initiated enrollment. Password is automatically using LAPS. Since we logged in, the user has a Secure Token.

```
sysadminctl -secureTokenStatus managedAdmin
```

You will get a message letting you know the secure token is disabled for the user managedAdmin. NOTE: This user is the Managed Admin created by MDM. Credentials created in the Jamf PreStage. Since we never logged in, the user does not have a Secure Token.



```
Last login: Wed Dec 27 12:06:44 on console
[jappleseed@Johns-Laptop-2 ~ % sysadminctl -secureTokenStatus jappleseed        ]
2023-12-27 12:07:31.821 sysadminctl[1712:20336] Secure token is ENABLED for user
 John Appleseed
[jappleseed@Johns-Laptop-2 ~ % sysadminctl -secureTokenStatus jamfManage        ]
2023-12-27 12:07:35.271 sysadminctl[1713:20384] Secure token is ENABLED for user
 JamfManage
[jappleseed@Johns-Laptop-2 ~ % sysadminctl -secureTokenStatus managedAdmin      ]
2023-12-27 12:07:42.338 sysadminctl[1719:20476] Secure token is DISABLED for use
r managedAdmin
jappleseed@Johns-Laptop-2 ~ % 
```

Mac computers with Apple Silicon enables the use of account icons and password fields on the FileVault login screen and support username and password fields at the FileVault login screen. Depending on your settings, you will either select a user at the FileVault login screen or enter a user name and password.

Decrypt FileVault with the Local User Account.

126. Restart your test Mac computer.

127. At the login window, in the Username field, enter jappleseed or your chosen test account.

128. Enter you password to decrypt FileVault and login to your Mac computer.

129. Confirm you were able to log into your Mac computer.

130. Decrypt FileVault with the Jamf Management Account. This guide will use the jamfManage account.

131. Restart your test Mac computer.

132. At the login window, in the Username field, enter jamfManage or your chosen Jamf Management account set in User Initiated enrollment.

133. Enter your password to decrypt FileVault and login to your Mac computer. NOTE this is the LAPS password.

134. Confirm you were able to log into your test Mac computer.

135. Decrypt FileVault with the Managed Admin. This guide will use the managedAdmin account.

136. Restart your test Mac computer.

137. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.

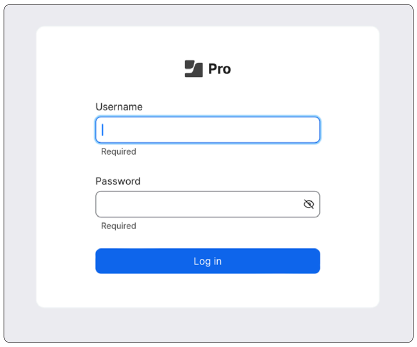
138. Enter you password to decrypt FileVault and login to your Mac computer.

139. Confirm you were NOT able to log into your Mac computer.
NOTE: This should not work since we never logged in with the managedAdmin account. The user does not have a Secure Token and can not decrypt FileVault.

B-Side Deep Track: Use the FileVault escrowed personal recovery key to decrypt a Mac computer

Use Jamf Pro to view the recovery key.

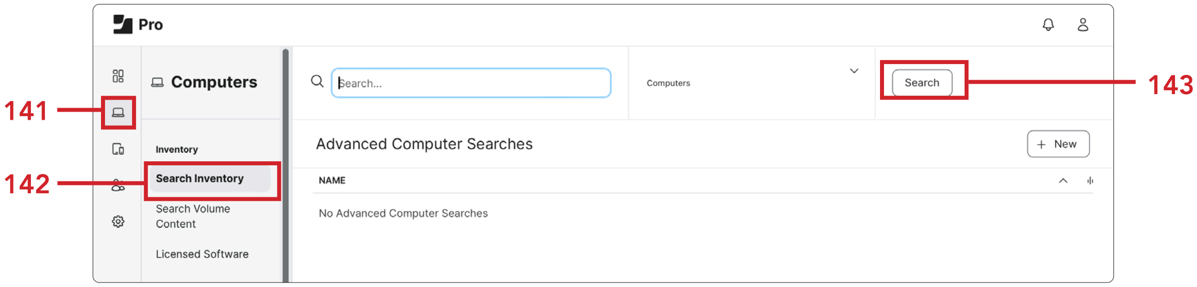
140. On your production Mac computer, log into your Jamf Pro server with administrative credentials.



141. Click Computers.

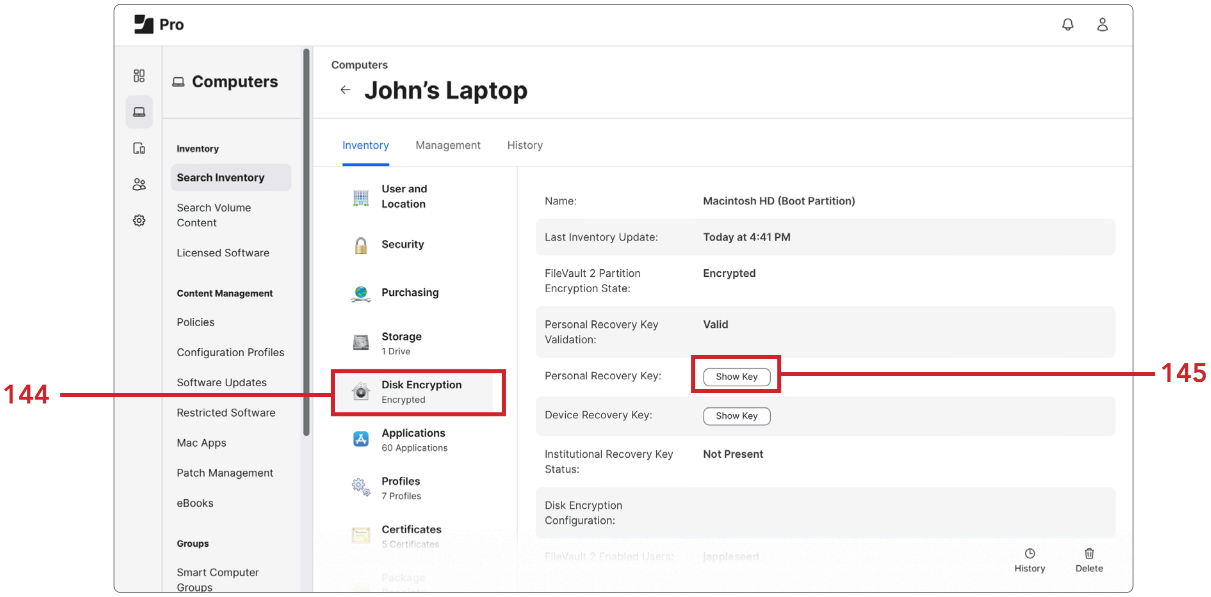
142. Click Search Inventory.

143. Search for your test Mac computer.



144. Click Disk Encryption Category of your Computer Inventory record.

145. Next to Personal Recovery Key: click Show Key.



Name: Macintosh HD (Boot Partition)

Last Inventory Update: Today at 4:41 PM

FileVault 2 Partition Encryption State: Encrypted

Personal Recovery Key Validation: Valid

Personal Recovery Key:

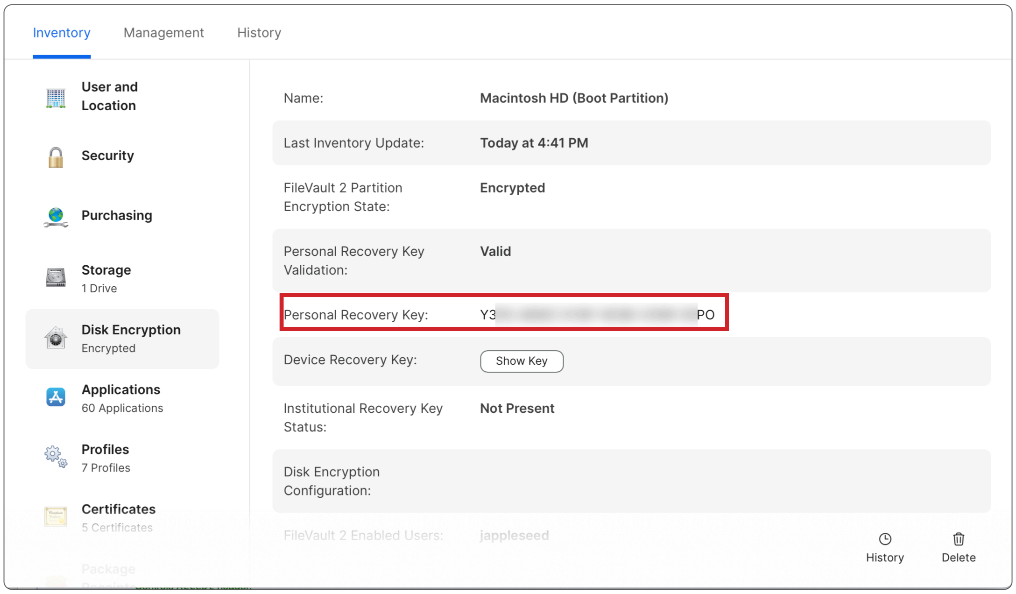
Device Recovery Key:

Institutional Recovery Key Status: Not Present

Disk Encryption Configuration:

FileVault 2 Enabled Users: jappleseed

146. Document the Personal Recovery Key: (We will need this in a later step.)



Name: Macintosh HD (Boot Partition)

Last Inventory Update: Today at 4:41 PM

FileVault 2 Partition Encryption State: Encrypted

Personal Recovery Key Validation: Valid

Personal Recovery Key: Y3[redacted]PO

Device Recovery Key:

Institutional Recovery Key Status: Not Present

Disk Encryption Configuration:

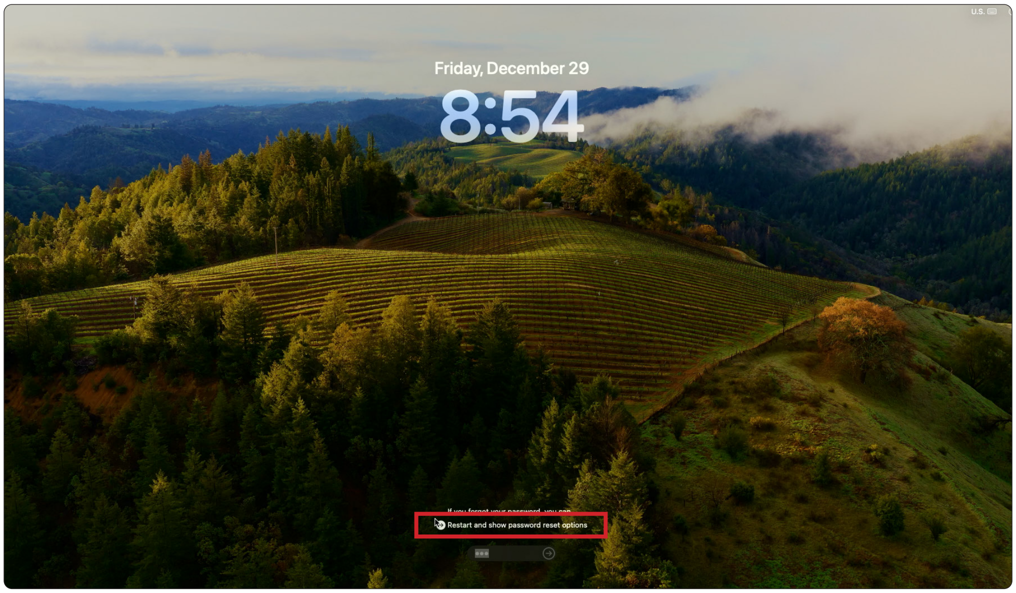
FileVault 2 Enabled Users: jappleseed

Decrypt FileVault with the Personal Recovery Key.

147. Restart your test Mac computer.

148. At the login window, select or input any username and input an incorrect password three times.

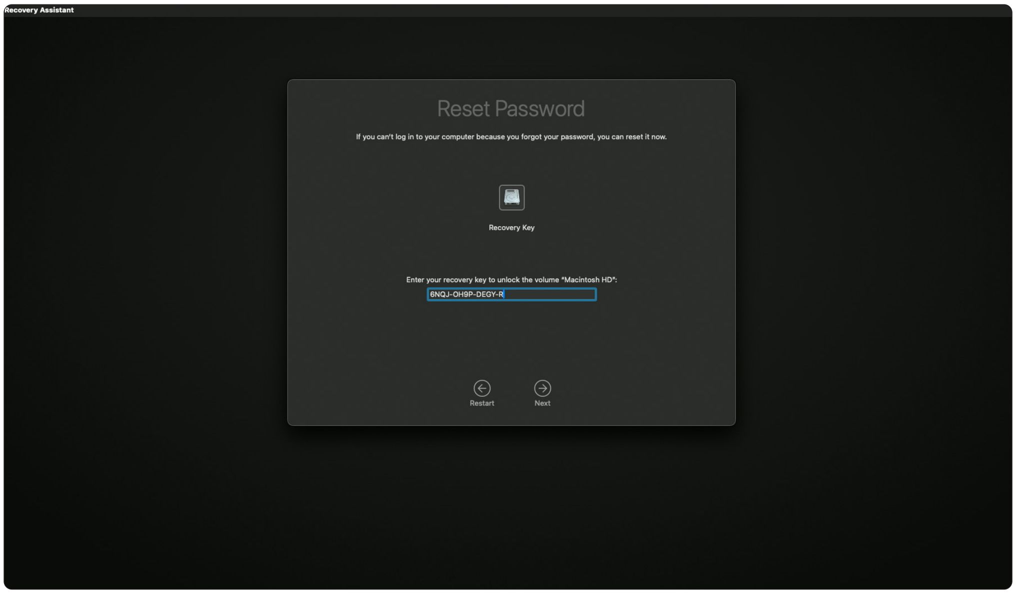
149. Click the arrow to the left of Restart and show password reset options.



If you forget your password, you can

Restart and show password reset options

150. In the Enter your recovery key to unlock volume field, enter the Personal Recovery Key.



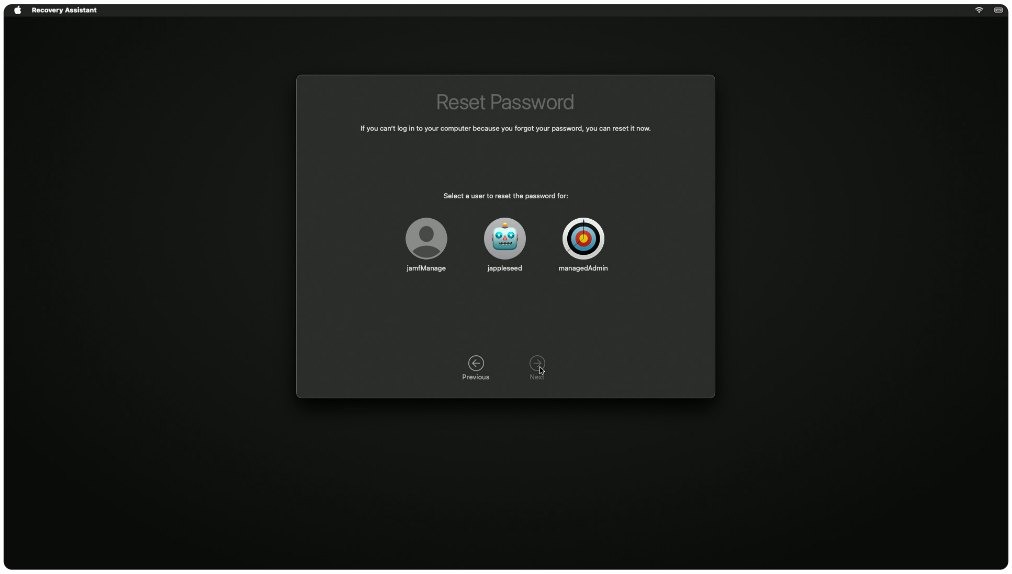
Reset Password

If you can't log in to your computer because you forgot your password, you can reset it now.

Enter your recovery key to unlock the volume "Macintosh HD":

6NQJ-OH9P-DEGY-R

151. Select jappleseed (or the user created in the Setup Assistant.)



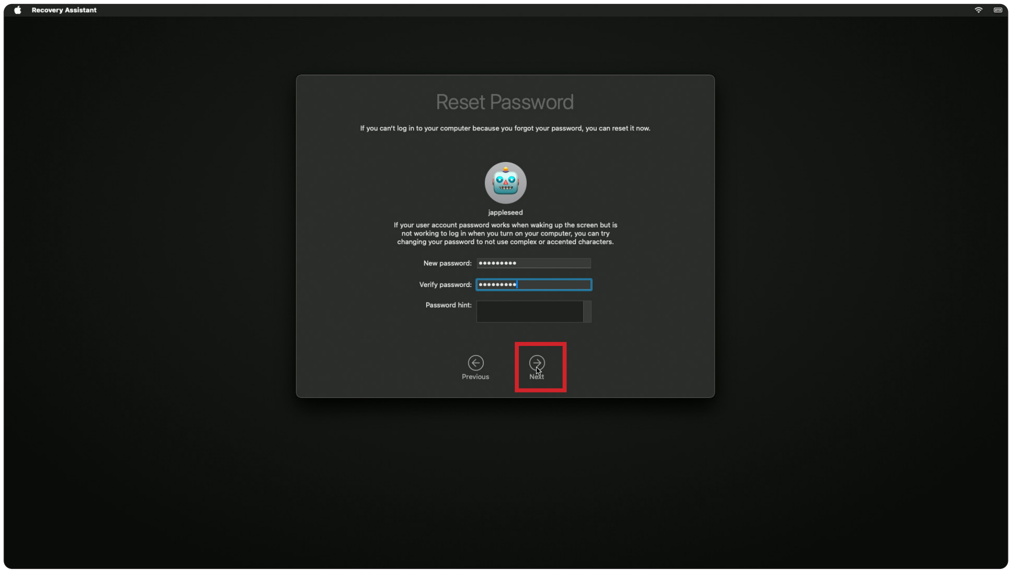
Reset Password

If you can't log in to your computer because you forgot your password, you can reset it now.

Select a user to reset the password for:

152. Enter and verify a new password.

153. Click Next.



Reset Password

If you can't log in to your computer because you forgot your password, you can reset it now.

jappleseed

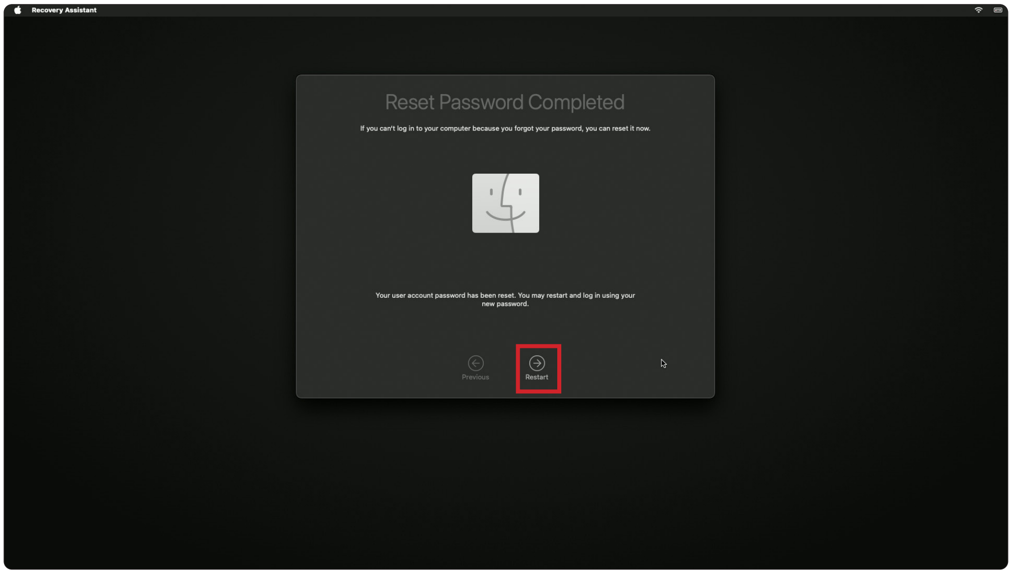
If your user account password works when waking up the screen but is not working to log in when you turn on your computer, you can try changing your password to not use complex or accented characters.

New password: ••••••••••

Verify password: ••••••••••

Password hint:

154. Click Restart.



Reset Password Completed

If you can't log in to your computer because you forgot your password, you can reset it now.

Your user account password has been reset. You may restart and log in using your new password.

Section 2: Side B - Enable LAPS (Local Administrator Password Solution) for the Managed Admin

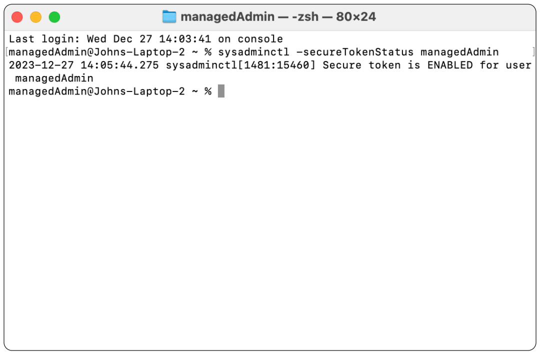
If your test Mac computer was powered down or restarted, you need to log in as a user that can decrypt FileVault before proceeding with the steps in this section.

1. At the login window, select your managed admin account or enter your managed admin in the Username field. The managed admin account is the account that you setup in your Computer PreStage. This guide will use the account named managedAdmin. Enter your password and login to your test Mac computer.

2. Check the users for the secure token status (Required to decrypt FileVault and for other macOS task requiring volume ownership.)

   ```
   sysadminctl -secureTokenStatus managedAdmin
   ```

   You will get a message letting you know the secure token is enabled for the user managedAdmin as we logged in at least once.

   ```
   Last login: Wed Dec 27 14:03:41 on console
   managedAdmin@Johns-Laptop-2 ~ % sysadminctl -secureTokenStatus managedAdmin
   2023-12-27 14:05:44.275 sysadminctl[1481:15460] Secure token is ENABLED for user
    managedAdmin
   managedAdmin@Johns-Laptop-2 ~ %
   ```

Decrypt FileVault with the Managed Admin

3. Restart your test Mac computer.

4. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.

5. Enter you password to decrypt FileVault and login to your Mac computer.

6. Confirm you were able to log into your Mac computer.

Enable LAPS Password for the Managed Admin set in the Computer PreStage.

There are two options for viewing the LAPS password:

- Option 1 requires a 3rd party application
- Option 2 requires the Jamf Pro API.

NOTE: You can edit the passwordRotationTime and autoExpirationTime to your needs if the values below do not work for you.

Option 1: Use the Jamf LAPS application:

7. On your production Mac computer, launch Jamf LAPS. Previously installed in section one of this guide.

8. Enable Laps: Turn on

9. Enable Auto Rotate: Turn on

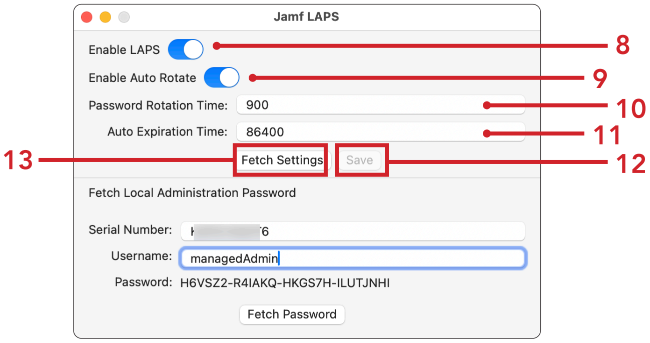
10. Password Rotation Time: Enter 900 (NOTE: Set in seconds which equals 15 minutes.)

11. Auto Expiration Time: Enter 86400 (NOTE: Set in seconds which equals 24 hours.)

12. Click Save

13. Click Fetch Settings (Nothing should Change)

14. LAPS is now enabled for all managed admin accounts. I.E. the managedAdmin account.



Enable LAPS
Enable Auto Rotate
Password Rotation Time: 900
Auto Expiration Time: 86400

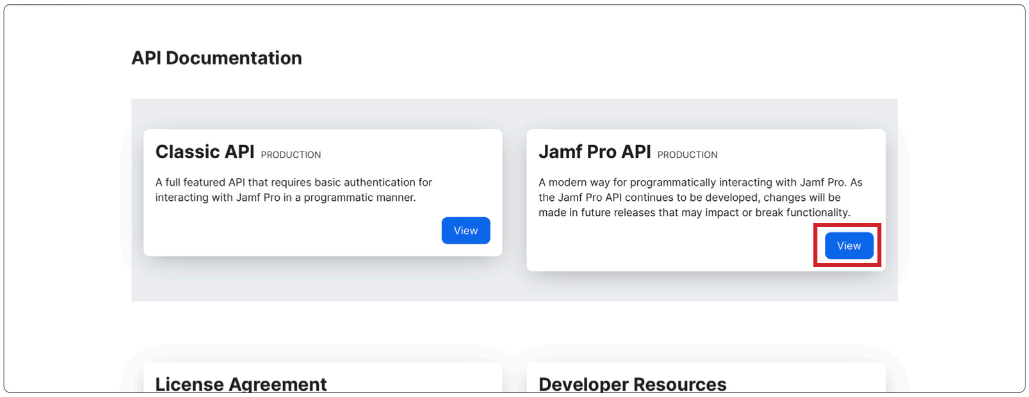
Fetch Local Administration Password

Serial Number: H[redacted]6
Username: managedAdmin
Password: H6VSZ2-R4IAKQ-HKGS7H-ILUTJNHI

Option 2: Use the Jamf Pro API:

15. Enter the address of your Jamf Pro server and add /api to the end of the URL. I.E. https://hcs.jamfcloud.com/api.

16. Click the View button on Jamf Pro API.



API Documentation

Classic API PRODUCTION

A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.

Jamf Pro API PRODUCTION

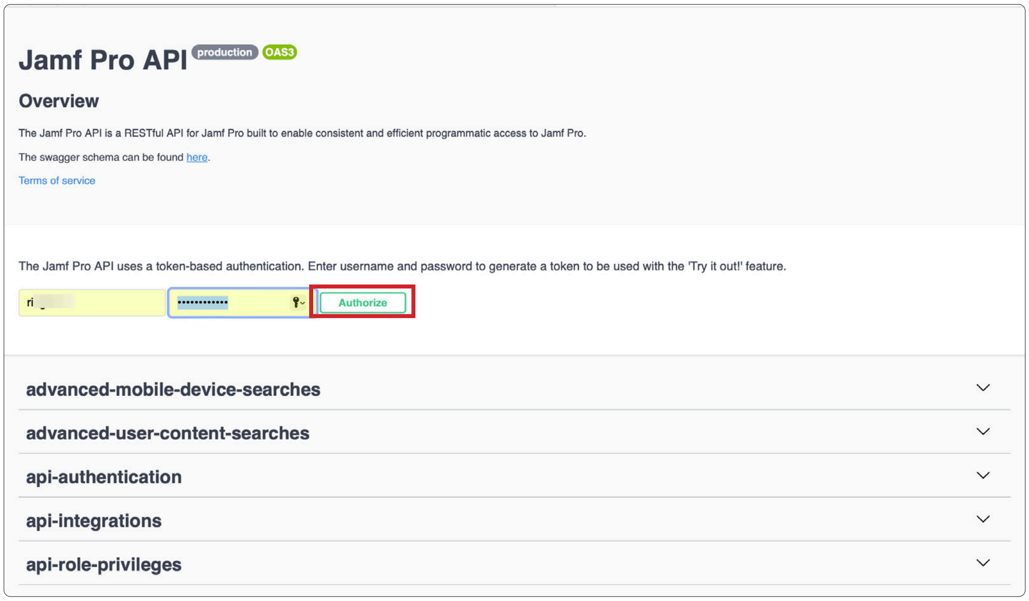
A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.

License Agreement

Developer Resources

17. Enter your Jamf Pro credentials.

18. Click Authorize.



Jamf Pro API

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

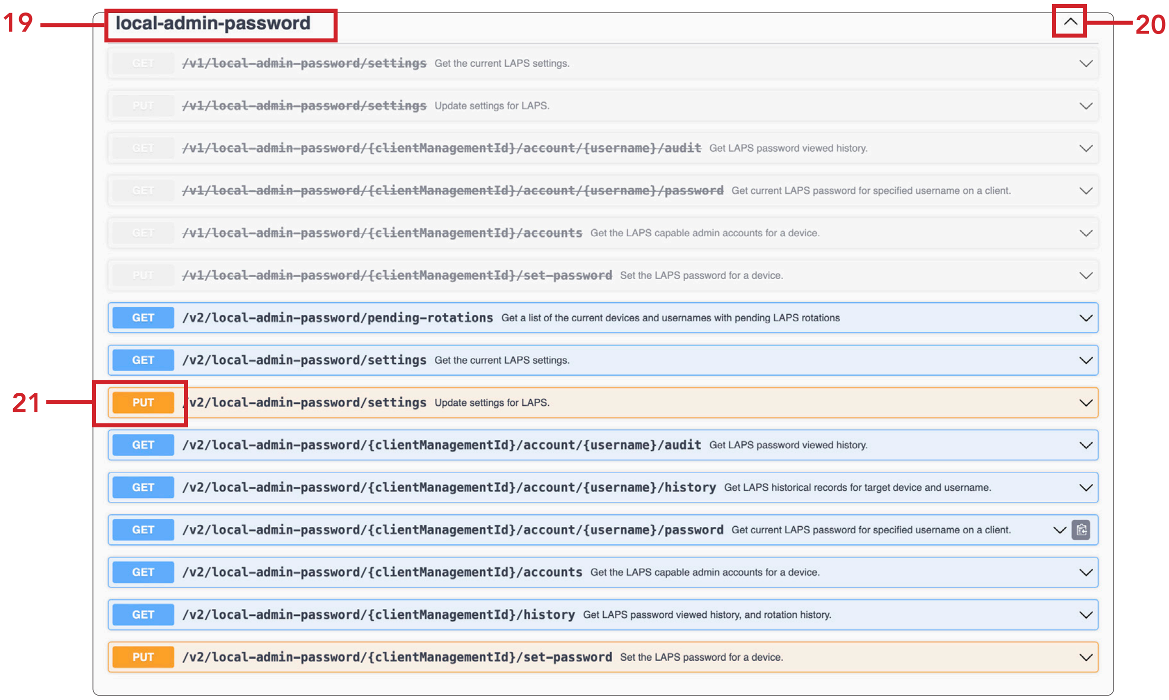
ri [redacted] ••••••••••••

- advanced-mobile-device-searches
- advanced-user-content-searches
- api-authentication
- api-integrations
- api-role-privileges

19. Scroll down the list and select local-admin-password.

20. Click Expand (⌄) to see its contents.

21. Click PUT on v2/local-admin-password/settings.



local-admin-password

GET ~~/v1/local-admin-password/settings~~ Get the current LAPS settings.

PUT ~~/v1/local-admin-password/settings~~ Update settings for LAPS.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/audit~~ Get LAPS password viewed history.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/password~~ Get current LAPS password for specified username on a client.

GET ~~/v1/local-admin-password/{clientManagementId}/accounts~~ Get the LAPS capable admin accounts for a device.

PUT ~~/v1/local-admin-password/{clientManagementId}/set-password~~ Set the LAPS password for a device.

GET /v2/local-admin-password/pending-rotations Get a list of the current devices and usernames with pending LAPS rotations

GET /v2/local-admin-password/settings Get the current LAPS settings.

PUT /v2/local-admin-password/settings Update settings for LAPS.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/audit Get LAPS password viewed history.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.

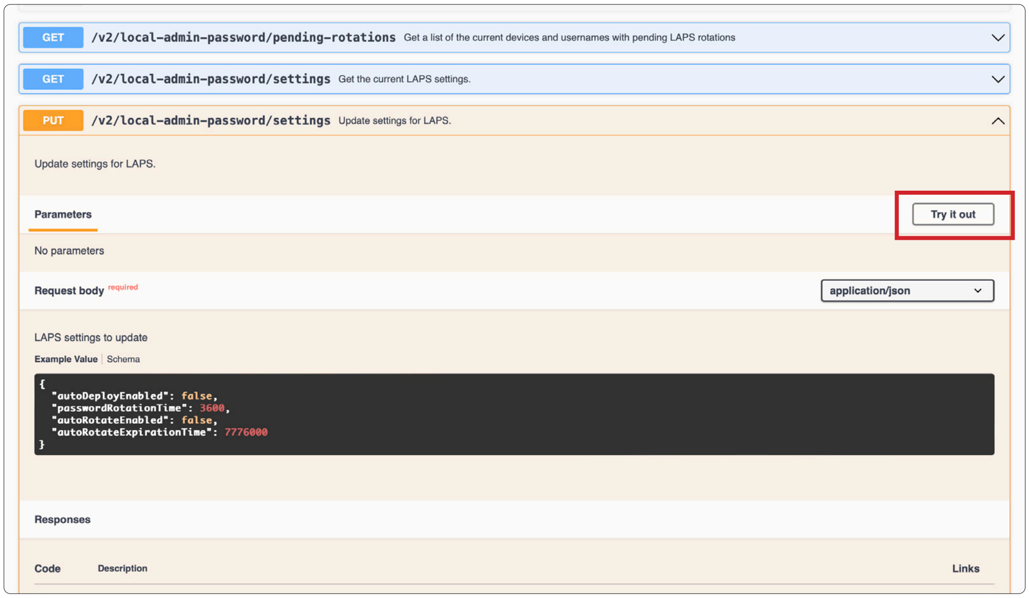
GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

GET /v2/local-admin-password/{clientManagementId}/accounts Get the LAPS capable admin accounts for a device.

GET /v2/local-admin-password/{clientManagementId}/history Get LAPS password viewed history, and rotation history.

PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

22. Click Try it out.



`/v2/local-admin-password/pending-rotations` Get a list of the current devices and usernames with pending LAPS rotations

`/v2/local-admin-password/settings` Get the current LAPS settings.

`/v2/local-admin-password/settings` Update settings for LAPS.

Update settings for LAPS.

Parameters

No parameters

Request body required

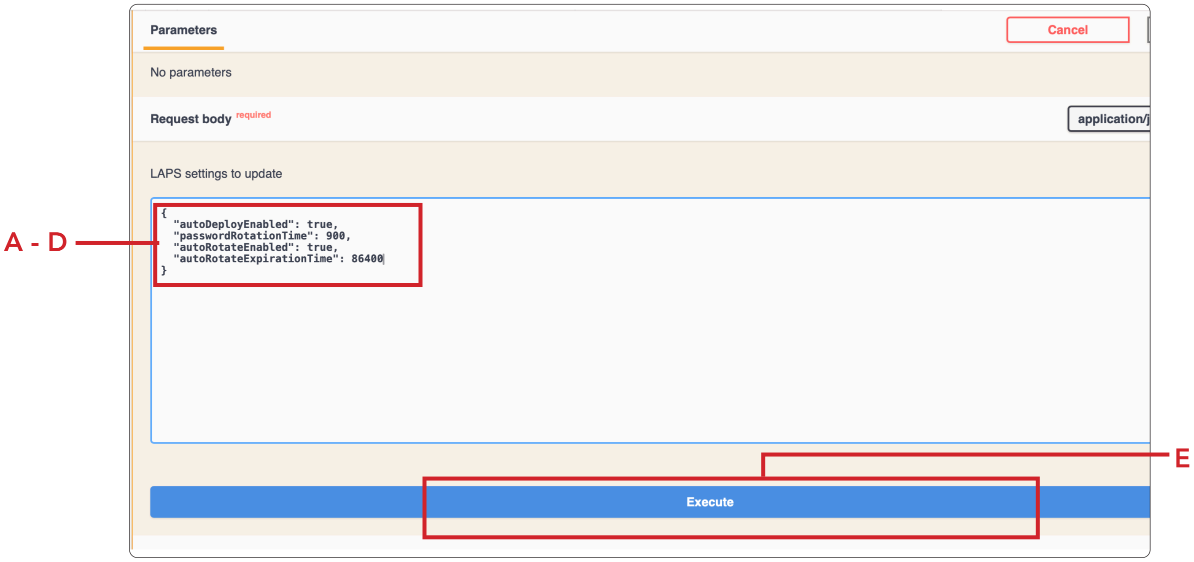
LAPS settings to update

```
{
  "autoDeployEnabled": false,
  "passwordRotationTime": 3600,
  "autoRotateEnabled": false,
  "autoRotateExpirationTime": 7776000
}
```

Responses

Code Description Links

23. In the LAPS settings to update field, Enter the following:
    A. Set autoDeployEnabled to true.
    B. Set passwordRotationTime to 900 (NOTE: Set in seconds which equals 15 minutes).
    C. Set autorotateEnabled to true.
    D. Set autoExpirationTime to 8640 (NOTE: Set in seconds which equals 24 hours).
    E. Click Execute.



Parameters

No parameters

Request body required

LAPS settings to update

```
{
  "autoDeployEnabled": true,
  "passwordRotationTime": 900,
  "autoRotateEnabled": true,
  "autoRotateExpirationTime": 86400
}
```

24. LAPS is now enabled for all managed admin accounts. I.E. the managedAdmin account.

Decrypt FileVault with the Managed Admin

25. Restart your test Mac computer.

26. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.

    Enter your password to decrypt FileVault and login to your Mac computer.
    NOTE: The management account password for cryptographically enabled accounts becomes out of sync with the password stored in Jamf Pro. You will need to use the original password for the Managed Admin set in the Computer PreStage to decrypt FileVault. You will also need to enter the rotated LAPS password for the managed Admin to log into your Mac computer. This means you will need two different logins for the managed admin account on your Mac computer going forward.

Viewing the LAPS Password for the Management Admin account.

There are two options for viewing the LAPS password:

- Option 1 requires a 3rd party application
- Option 2 requires the Jamf Pro API

Option 1: Use Jamf LAPS App

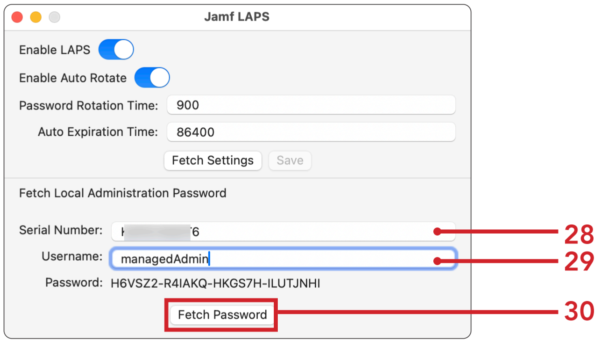
27. On your production Mac computer, launch Jamf LAPS installed in Section 1.

LAPS

28. Enter the Serial Number of the enrolled Mac computer.

29. Username: Enter the Managed Admin Account. This guide will use the managedAdmin account.

30. Click Fetch Password



Jamf LAPS

Enable LAPS ●
Enable Auto Rotate ●
Password Rotation Time: 900
Auto Expiration Time: 86400

Fetch Local Administration Password

Serial Number: [redacted]
Username: managedAdmin
Password: H6VSZ2-R4IAKQ-HKGS7H-ILUTJNHI

Option 2: View LAPS Password using the Jamf Pro API

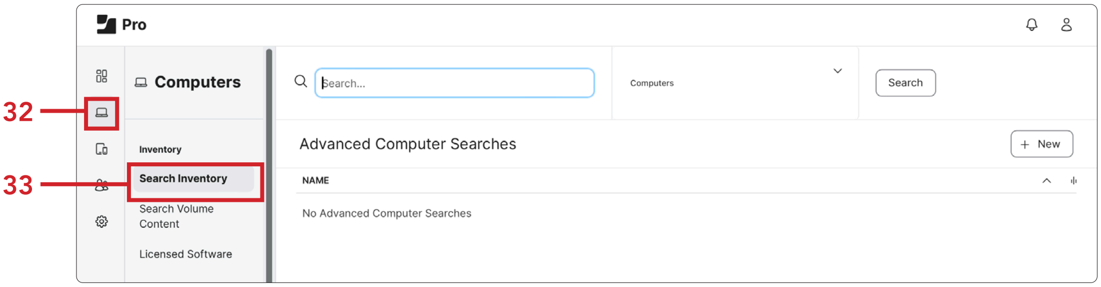
We need to document the client management id of our test Mac computer.

31. Log into your Jamf Pro server with administrative privileges.

32. Click Computers.

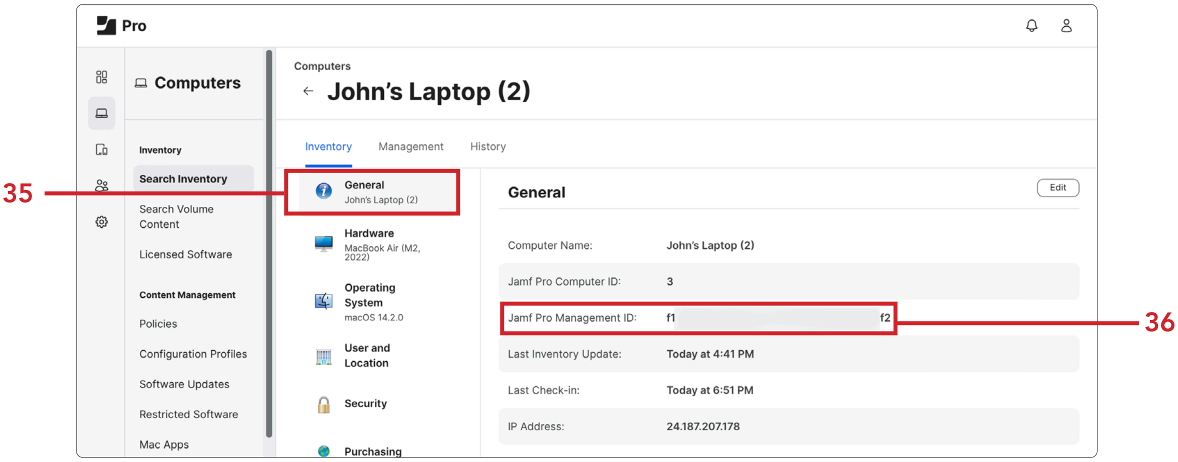
33. Click Search Inventory.

34. Search for your test Mac computer.



35. In the General Category of your Computer Inventory record.

36. Document the the Jamf Pro Management ID (We will need this in a later step.)



Computer Name: John's Laptop (2)

Jamf Pro Computer ID: 3

Jamf Pro Management ID: f1 [redacted] f2

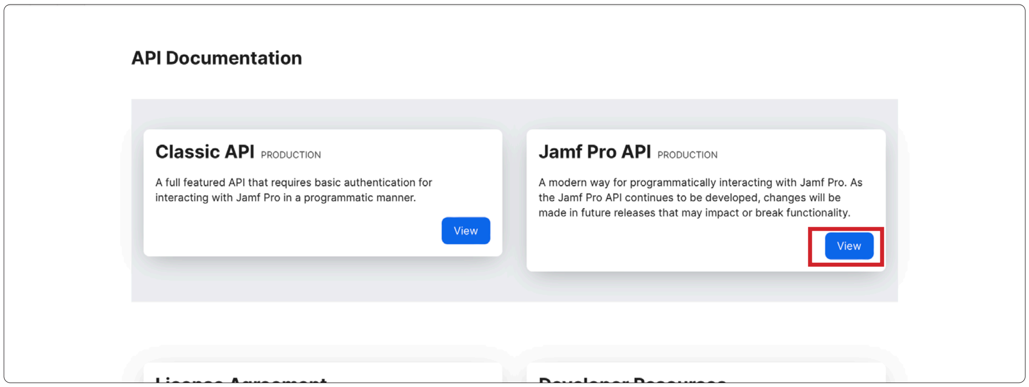
Last Inventory Update: Today at 4:41 PM

Last Check-in: Today at 6:51 PM

IP Address: 24.187.207.178

37. Enter the address of your Jamf Pro server and add /api to the end of the URL.
I.E. https://hcs.jamfcloud.com/api.

38. Click View for Jamf Pro API.

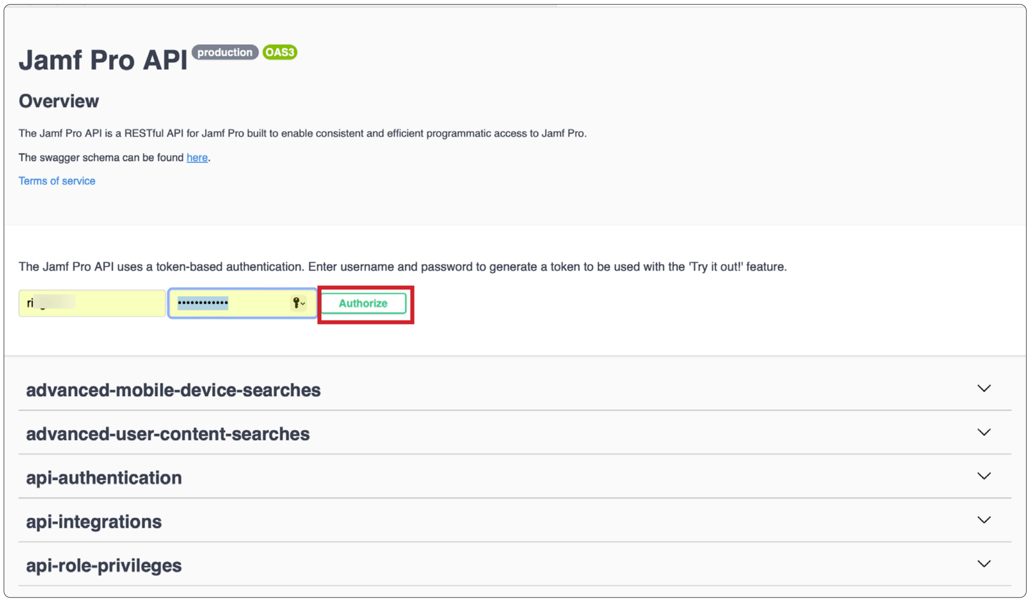


A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.

A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.

39. Enter your Jamf Pro credentials.

40. Click Authorize to generate a token.



Jamf Pro API production OAS3

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

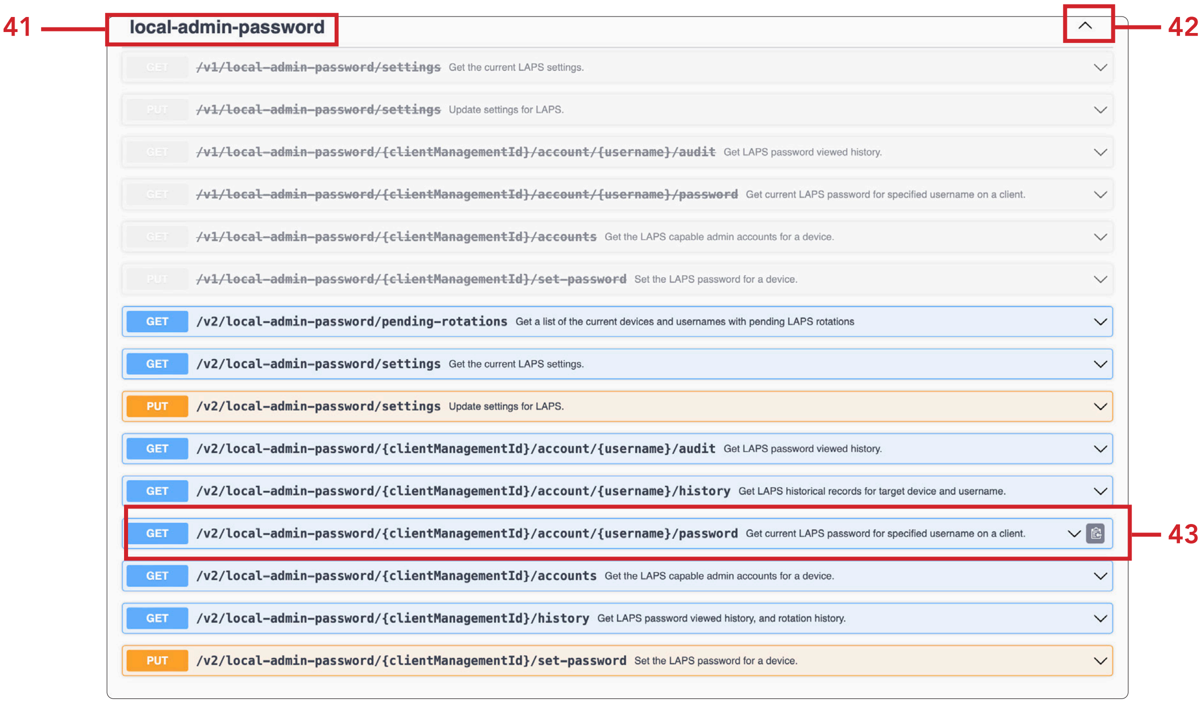
ri [redacted] | •••••••••••• | Authorize

- advanced-mobile-device-searches
- advanced-user-content-searches
- api-authentication
- api-integrations
- api-role-privileges

41. Scroll down the list and select local-admin-password.

42. Click Expand (⌄) to see its contents.

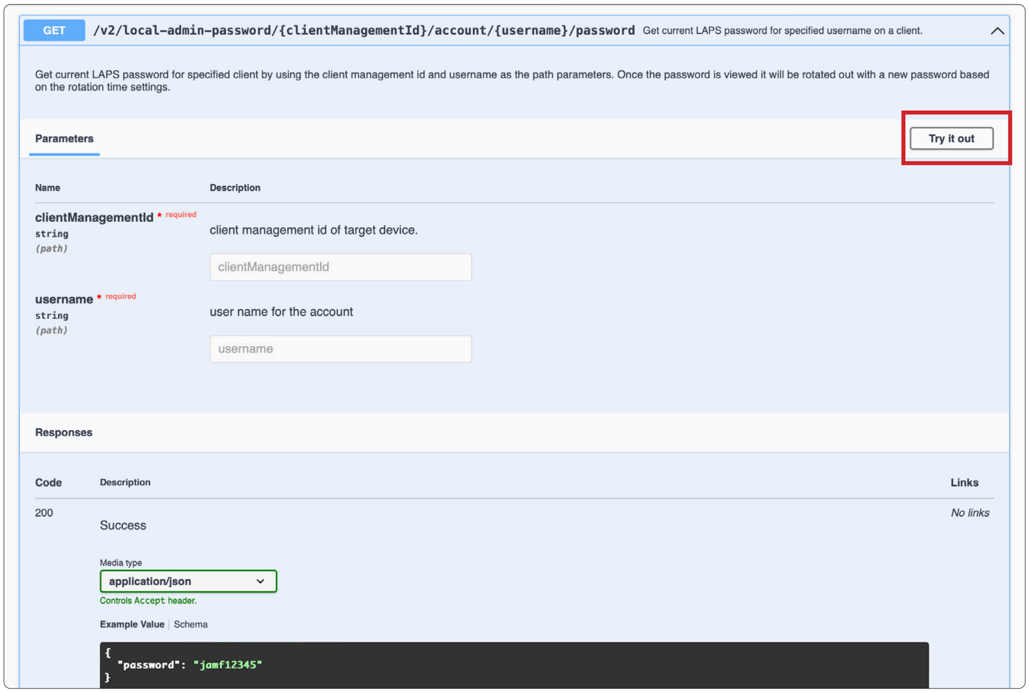
43. Click Get for /v2/local-admin-password/{clientManagementId}/account/{username}/password current LAPS password for specified user name on a client



local-admin-password

- GET ~~/v1/local-admin-password/settings~~ Get the current LAPS settings.
- PUT ~~/v1/local-admin-password/settings~~ Update settings for LAPS.
- GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/audit~~ Get LAPS password viewed history.
- GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/password~~ Get current LAPS password for specified username on a client.
- GET ~~/v1/local-admin-password/{clientManagementId}/accounts~~ Get the LAPS capable admin accounts for a device.
- PUT ~~/v1/local-admin-password/{clientManagementId}/set-password~~ Set the LAPS password for a device.
- GET /v2/local-admin-password/pending-rotations Get a list of the current devices and usernames with pending LAPS rotations
- GET /v2/local-admin-password/settings Get the current LAPS settings.
- PUT /v2/local-admin-password/settings Update settings for LAPS.
- GET /v2/local-admin-password/{clientManagementId}/account/{username}/audit Get LAPS password viewed history.
- GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.
- GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.
- GET /v2/local-admin-password/{clientManagementId}/accounts Get the LAPS capable admin accounts for a device.
- GET /v2/local-admin-password/{clientManagementId}/history Get LAPS password viewed history, and rotation history.
- PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

44. Click Try it out.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters

Try it out

Name	Description
clientManagementId * required string *(path)*	client management id of target device. clientManagementId
username * required string *(path)*	user name for the account username

Responses

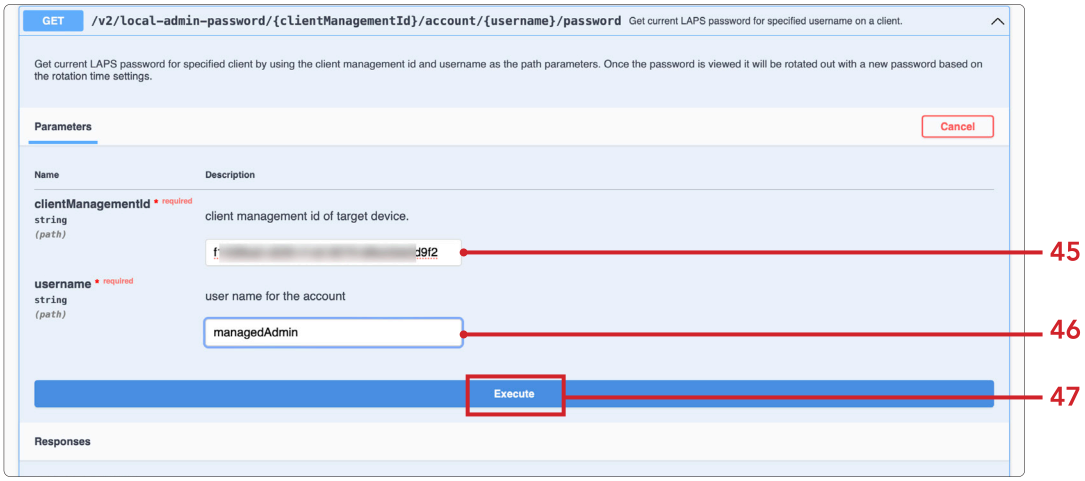
Code	Description	Links
200	Success Media type application/json Controls Accept header. Example Value | Schema	*No links*

```
{
  "password": "jamf12345"
}
```

45. In the clientManagementId enter the Jamf Pro Management ID documented from a previous step.

46. In the username enter managedAdmin or your chosen Management Admin account set in the Computer PreStage.

47. Click Execute.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters

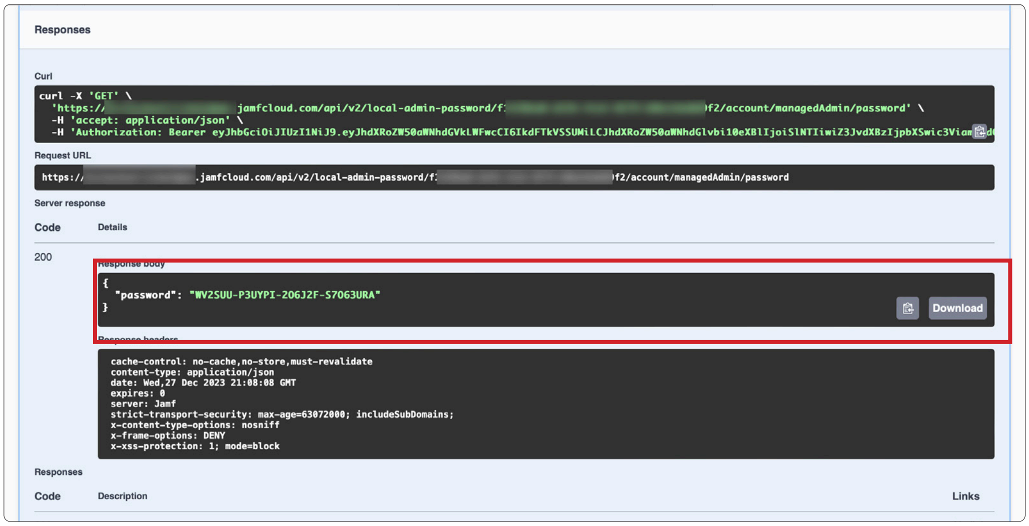
Cancel

Name	Description
clientManagementId * required string *(path)*	client management id of target device. f[redacted]d9f2
username * required string *(path)*	user name for the account managedAdmin

Execute

Responses

48. Scroll down to retrieve the password.



Responses

Curl

```
curl -X 'GET' \
  'https://[redacted]jamfcloud.com/api/v2/local-admin-password/f[redacted]f2/account/managedAdmin/password' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdXRoZW50aWNhdGVkLWFwcCI6IkdFTkVSSUMiLCJhdXRoZW50aWNhdGlvbi10eXBlIjoiSlNTIiwiZ3JvdXBzIjpbXSwic3Viamd
```

Request URL

```
https://[redacted].jamfcloud.com/api/v2/local-admin-password/f[redacted]f2/account/managedAdmin/password
```

Server response

Code	Details
200	Response body

```
{
  "password": "WV2SUU-P3UYPI-206J2F-S7063URA"
}
```

Response headers

```
cache-control: no-cache,no-store,must-revalidate
content-type: application/json
date: Wed,27 Dec 2023 21:08:08 GMT
expires: 0
server: Jamf
strict-transport-security: max-age=63072000; includeSubDomains;
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

Responses

Code	Description	Links

49. Go back to your test Mac computer and log in with the managedAdmin account credentials. Confirm you were able to log into your Mac computer.

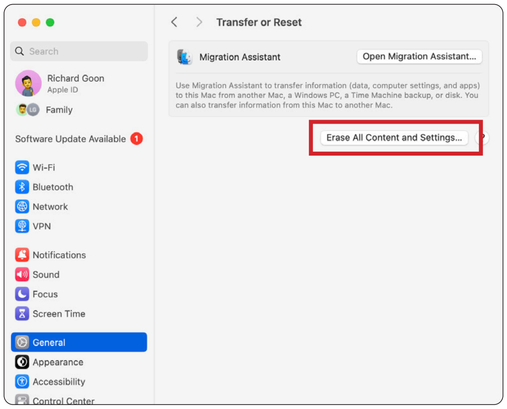
    NOTE: Once the LAPS password is viewed, the Jamf Pro Server will automatically rotate the LAPS password in the time you scheduled in a previous step. If the Mac Computer is offline, the rotation will happen once the Mac computer is online and checks in with the Jamf Pro server.

Section 3: 45 RPM Version - LAPS Enabled for the Managed Admin - Mac computers enrolling with Automated Device Enrollment (ADE)

This section assumes that you followed the previous sections and enabled LAPS (Local Administrator Password Solution).

1. On your test Mac computer, Go to System Settings > General > Transfer or Reset.

2. Click Erase All Contents and Settings.



Use Migration Assistant to transfer information (data, computer settings, and apps) to this Mac from another Mac, a Windows PC, a Time Machine backup, or disk. You can also transfer information from this Mac to another Mac.

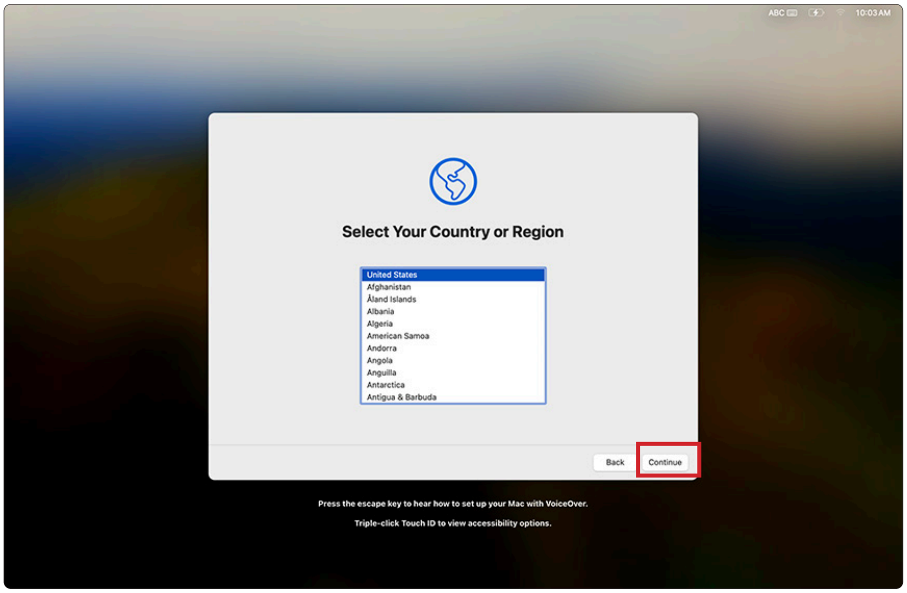
3. Connect to a network and activate your Mac computer.

4. Start the test Mac computer scoped in the PreStage.

5. Click Get Started.

6. Choose Language.

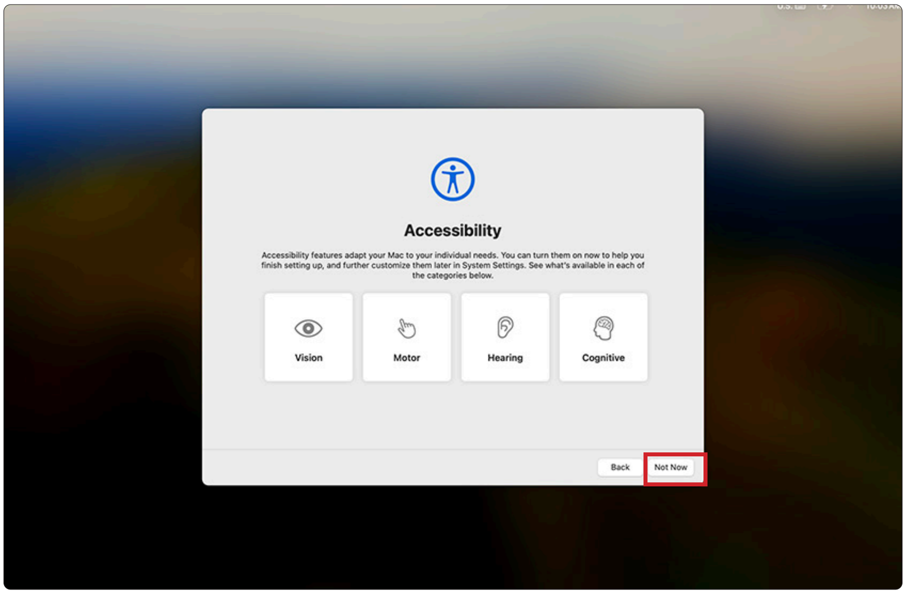
7. Choose Country or Region. Click Continue.



Press the escape key to hear how to set up your Mac with VoiceOver.

Triple-click Touch ID to view accessibility options.

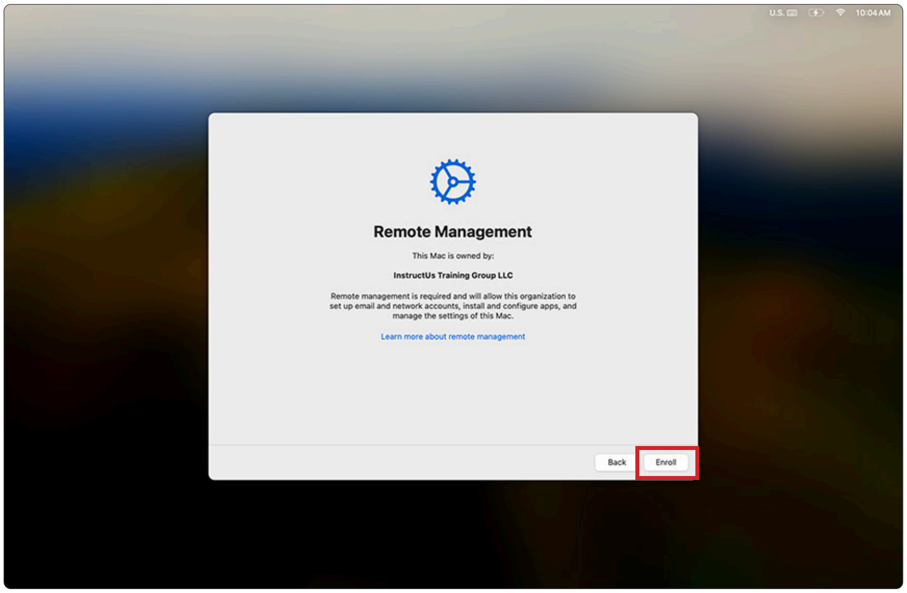
8. At the Accessibility screen, select Not Now.



Accessibility features adapt your Mac to your individual needs. You can turn them on now to help you finish setting up, and further customize them later in System Settings. See what's available in each of the categories below.

9. Connect to the appropriate network

10. Confirm Remote Management and Click Enroll.



This Mac is owned by:

InstructUs Training Group LLC

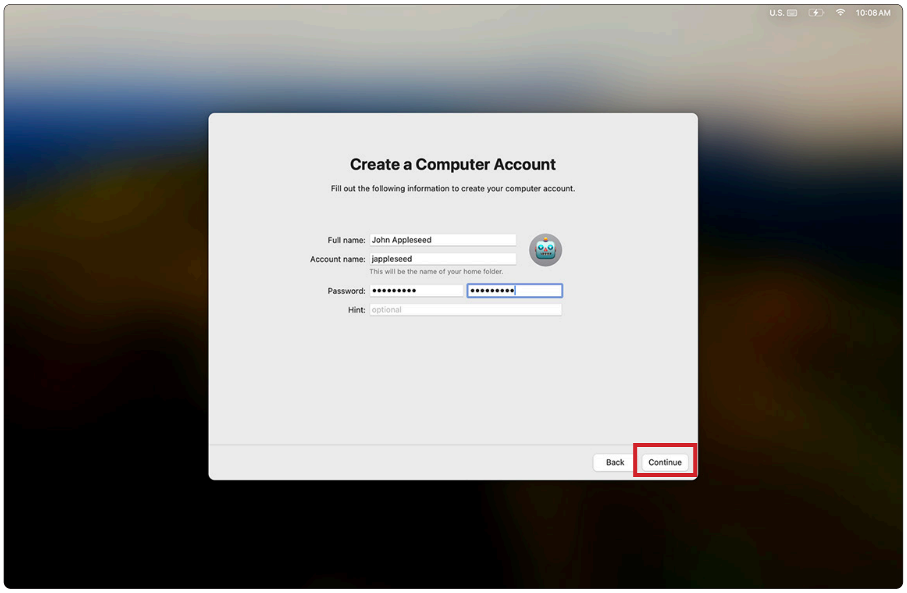
Remote management is required and will allow this organization to set up email and network accounts, install and configure apps, and manage the settings of this Mac.

11. At Migration Assistant, at the left-hand corner, click Not Now.

12. For Apple ID, click Setup Later. Click Skip.

13. At the create a computer account screen, Enter a name and password of your choosing. This guide will use John Appleseed for the Full Name and jappleseed for the Account name

14. Click Continue.



Create a Computer Account

Fill out the following information to create your computer account.

Full name: John Appleseed

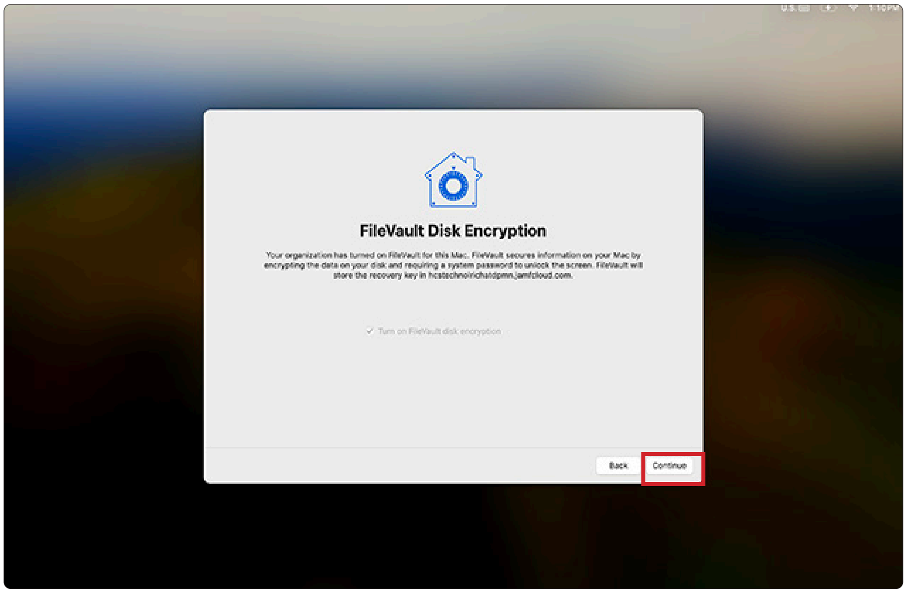
Account name: jappleseed

This will be the name of your home folder.

Password: ••••••••• •••••••••

Hint: optional

15. Confirm FileVault Disk Encryption is enabled and click Continue.



FileVault Disk Encryption

Your organization has turned on FileVault for this Mac. FileVault secures information on your Mac by encrypting the data on your disk and requiring a system password to unlock the screen. FileVault will store the recovery key in hcstechnolrichardpmn.jamfcloud.com.

✓ Turn on FileVault disk encryption

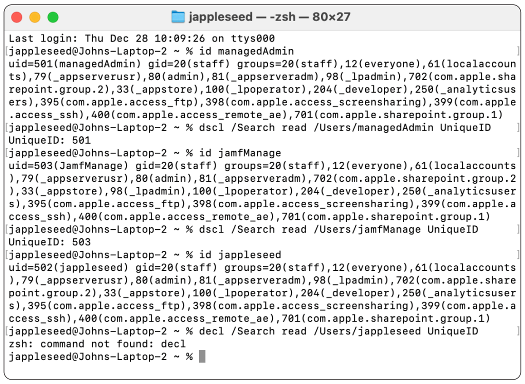
16. Click through and set the screens to meet you needs

Confirm Managed Admin, Jamf Management Account, and user created during setup assistant

17. On the test Mac computer, open Terminal. A new shell window opens with your home folder as the working directory

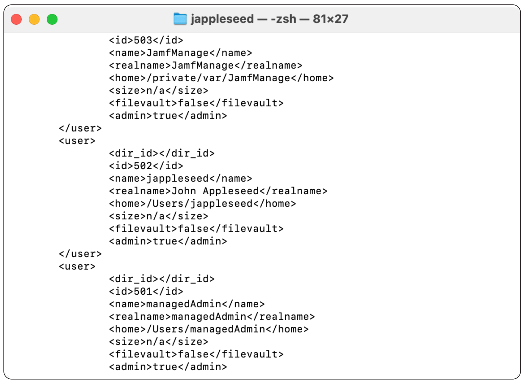
18. Type the following commands and press Return

- `id managedAdmin`
  `dscl /Search read /Users/managedAdmin UniqueID`
- `id jamfManage`
  `dscl /Search read /Users/jamfManage UniqueID`
- `id jappleseed`
  `decl /Search read /Users/jappleseed UniqueID`



```
Last login: Thu Dec 28 10:09:26 on ttys000
jappleseed@Johns-Laptop-2 ~ % id managedAdmin
uid=501(managedAdmin) gid=20(staff) groups=20(staff),12(everyone),61(localaccoun
ts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),702(com.apple.sha
repoint.group.2),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsus
ers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple
.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % dscl /Search read /Users/managedAdmin UniqueID
UniqueID: 501
jappleseed@Johns-Laptop-2 ~ % id jamfManage
uid=503(JamfManage) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts
),79(_appserverusr),80(admin),81(_appserveradm),702(com.apple.sharepoint.group.2
),33(_appstore),98(_lpadmin),100(_lpoperator),204(_developer),250(_analyticsuser
s),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.a
ccess_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % dscl /Search read /Users/jamfManage UniqueID
UniqueID: 503
jappleseed@Johns-Laptop-2 ~ % id jappleseed
uid=502(jappleseed) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts
),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),702(com.apple.share
point.group.2),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsuser
s),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.a
ccess_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
jappleseed@Johns-Laptop-2 ~ % decl /Search read /Users/jappleseed UniqueID
zsh: command not found: decl
jappleseed@Johns-Laptop-2 ~ %
```

Note: Another option is `sudo jamf listUsers -showAll`
(Scroll to the bottom)



```
                <id>503</id>
                <name>JamfManage</name>
                <realname>JamfManage</realname>
                <home>/private/var/JamfManage</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
        </user>
        <user>
                <dir_id></dir_id>
                <id>502</id>
                <name>jappleseed</name>
                <realname>John Appleseed</realname>
                <home>/Users/jappleseed</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
        </user>
        <user>
                <dir_id></dir_id>
                <id>501</id>
                <name>managedAdmin</name>
                <realname>managedAdmin</realname>
                <home>/Users/managedAdmin</home>
                <size>n/a</size>
                <filevault>false</filevault>
                <admin>true</admin>
```

View the LAPS Password for the Management Admin account.

There are two options for viewing the LAPS password:

- Option 1 requires a 3rd party application
- Option 2 requires the Jamf Pro API.

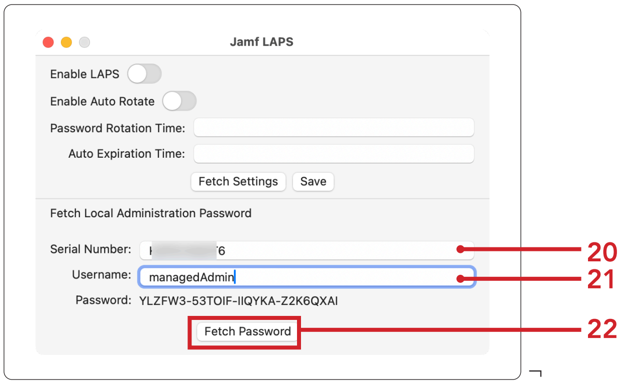
Option 1: Use Jamf LAPS App

19. On your production Mac computer, launch Jamf LAPS. Previously installed in section one of this guide.

20. Enter the Serial Number of the enrolled Mac computer.

21. Username: Enter managedAdmin.

22. Click Fetch Password. NOTE: Copy the LAPS password to a text document for later use in this guide.



Jamf LAPS

Enable LAPS

Enable Auto Rotate

Password Rotation Time:

Auto Expiration Time:

Fetch Settings | Save

Fetch Local Administration Password

Serial Number: [redacted]

Username: managedAdmin

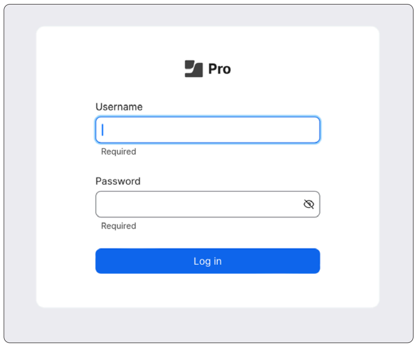
Password: YLZFW3-53TOIF-IIQYKA-Z2K6QXAI

Fetch Password

Option 2: View LAPS Password using the Jamf Pro API

We need to document the client management id of our test Mac computer.

23. On your production Mac computer, log into your Jamf Pro server with proper privileges.



Pro

Username:

Required

Password:

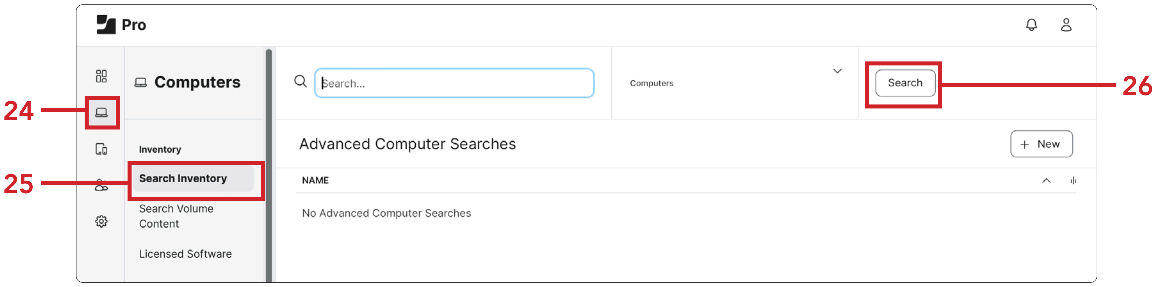
Required

Log in

24. Click Computers.

25. Click Search Inventory.

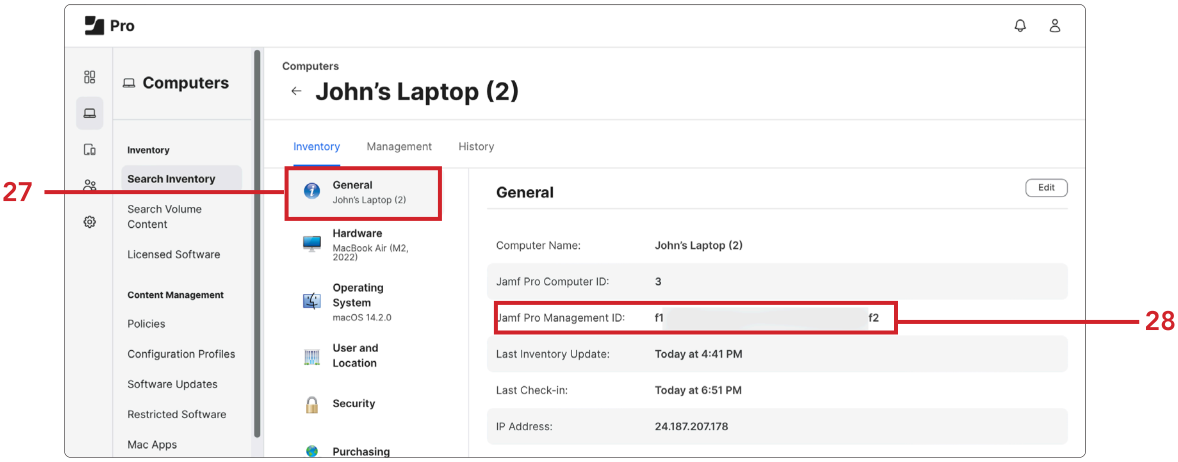
26. Search for your test Mac computer.



No Advanced Computer Searches

27. Click General Category of your Computer Inventory record.

28. Document the Jamf Pro Management ID (We will need this in a later step)



Computer Name: John's Laptop (2)

Jamf Pro Computer ID: 3

Jamf Pro Management ID: f1[redacted]f2

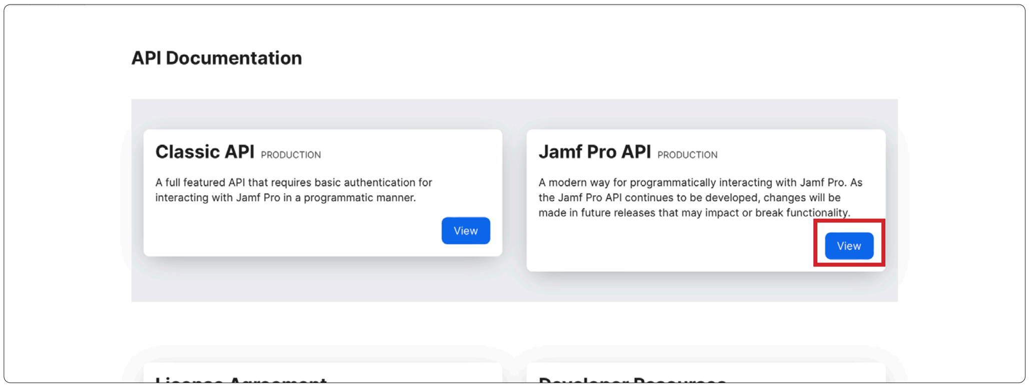
Last Inventory Update: Today at 4:41 PM

Last Check-in: Today at 6:51 PM

IP Address: 24.187.207.178

29. Enter the address of your Jamf Pro server and add /api to the end of the URL. I.E. https://hcs.jamfcloud.com/api.

30. Click View for Jamf Pro API.

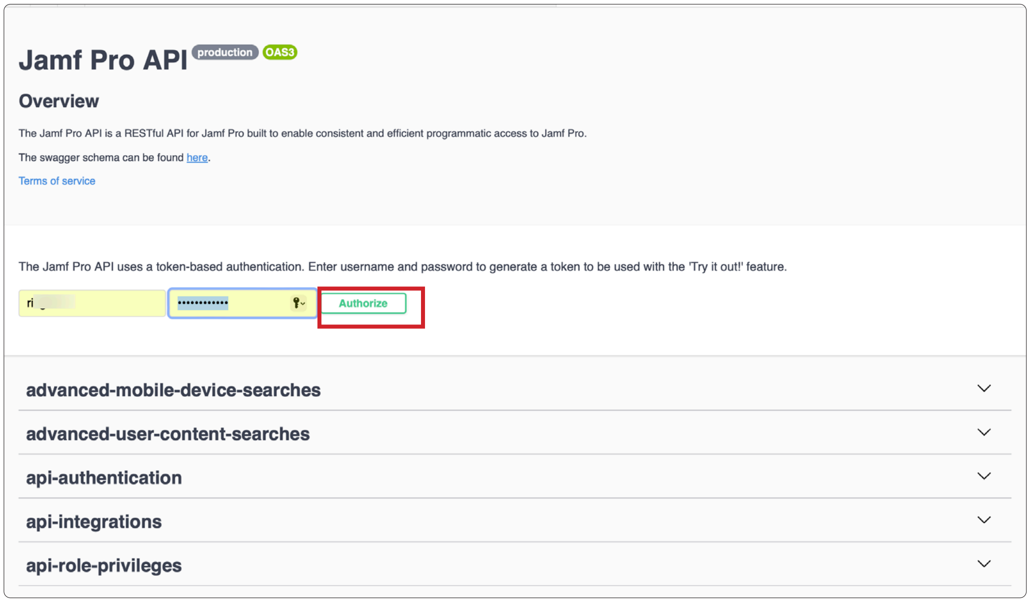


A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.

A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.

31. Enter your Jamf Pro credentials.

32. Click Authorize to generate a token. NOTE: This guide will use a Jamf Pro administrator account.



Jamf Pro API

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

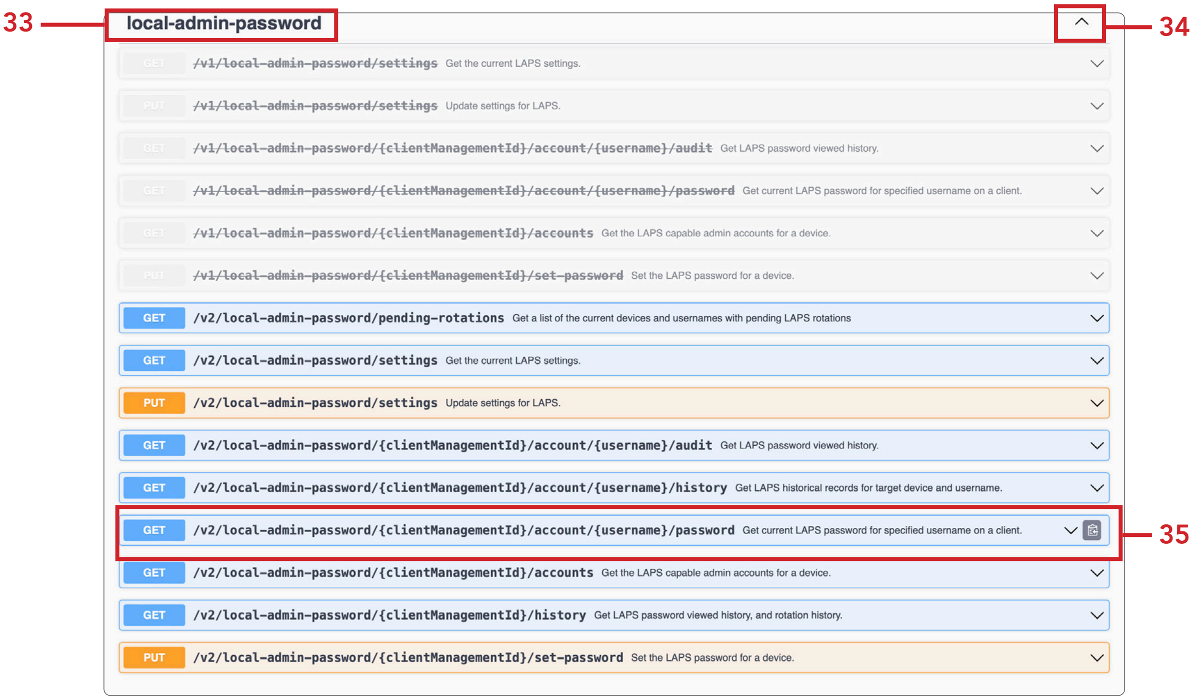
ri [redacted] | •••••••••••• | Authorize

- advanced-mobile-device-searches
- advanced-user-content-searches
- api-authentication
- api-integrations
- api-role-privileges

33. Scroll down the list and select local-admin-password.

34. Click Expand (⌄) to see its contents.

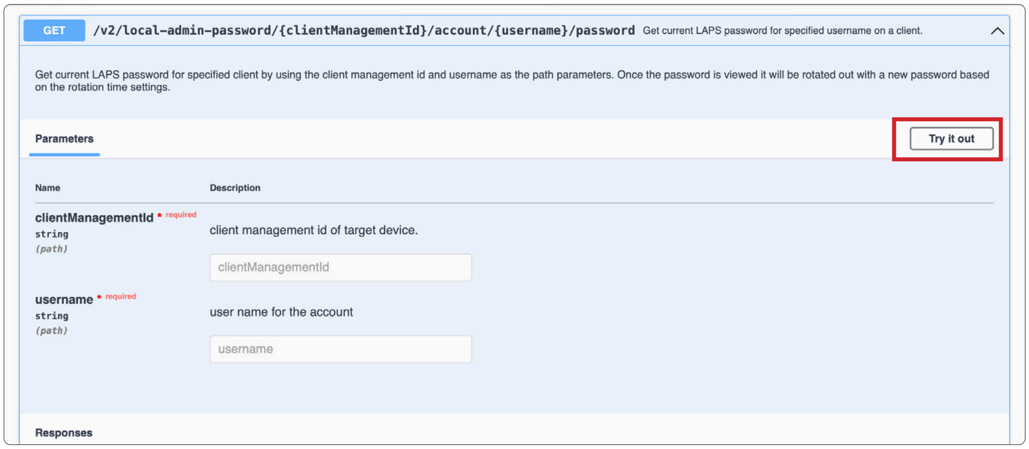
35. Click Get for /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified user name on a client



local-admin-password

GET	~~/v1/local-admin-password/settings~~	Get the current LAPS settings.
PUT	~~/v1/local-admin-password/settings~~	Update settings for LAPS.
GET	~~/v1/local-admin-password/{clientManagementId}/account/{username}/audit~~	Get LAPS password viewed history.
GET	~~/v1/local-admin-password/{clientManagementId}/account/{username}/password~~	Get current LAPS password for specified username on a client.
GET	~~/v1/local-admin-password/{clientManagementId}/accounts~~	Get the LAPS capable admin accounts for a device.
PUT	~~/v1/local-admin-password/{clientManagementId}/set-password~~	Set the LAPS password for a device.
GET	/v2/local-admin-password/pending-rotations	Get a list of the current devices and usernames with pending LAPS rotations
GET	/v2/local-admin-password/settings	Get the current LAPS settings.
PUT	/v2/local-admin-password/settings	Update settings for LAPS.
GET	/v2/local-admin-password/{clientManagementId}/account/{username}/audit	Get LAPS password viewed history.
GET	/v2/local-admin-password/{clientManagementId}/account/{username}/history	Get LAPS historical records for target device and username.
GET	/v2/local-admin-password/{clientManagementId}/account/{username}/password	Get current LAPS password for specified username on a client.
GET	/v2/local-admin-password/{clientManagementId}/accounts	Get the LAPS capable admin accounts for a device.
GET	/v2/local-admin-password/{clientManagementId}/history	Get LAPS password viewed history, and rotation history.
PUT	/v2/local-admin-password/{clientManagementId}/set-password	Set the LAPS password for a device.

36. Click Try it out.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters | Try it out

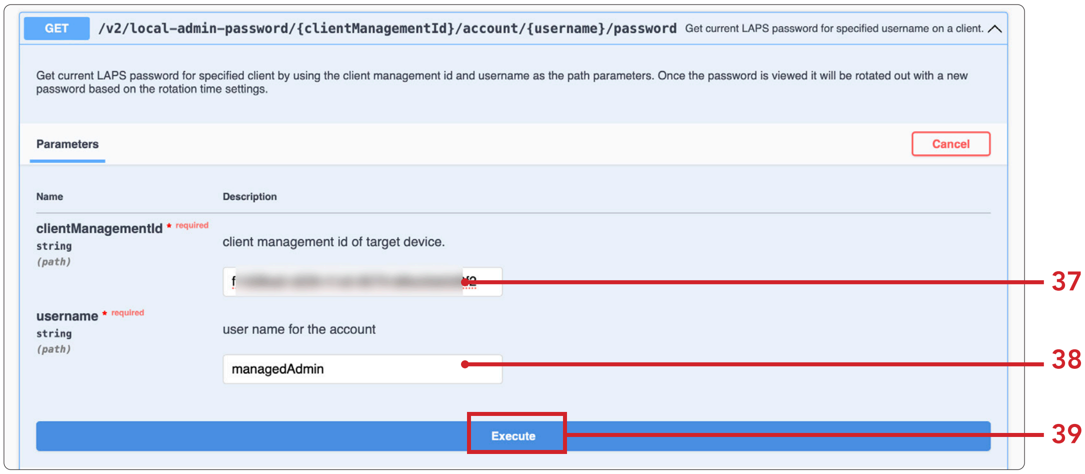
Name	Description
clientManagementId * required string *(path)*	client management id of target device. clientManagementId
username * required string *(path)*	user name for the account username

Responses

37. In the clientManagementId field, enter the Jamf Pro Management ID documented from a previous step.

38. In the username field, enter managedAdmin or your chosen Management Admin account set in Computer PreStage.

39. Click Execute.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

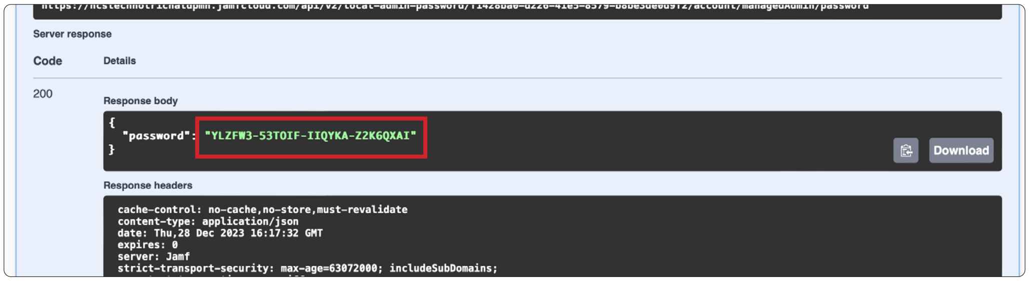
Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters | Cancel

Name	Description
clientManagementId * required string *(path)*	client management id of target device. f[redacted]f2
username * required string *(path)*	user name for the account managedAdmin

Execute

40. Copy the LAPS password to a text document for later use in this guide.



```
https://hcstechnolrichatupmn.jamfcloud.com/api/v2/local-admin-password/f1428ba0-d226-41e5-8579-b8be3de0d9f2/account/managedAdmin/password
```

Server response

Code	Details
200	Response body

```
{
  "password": "YLZFW3-53TOIF-IIQYKA-Z2K6QXAI"
}
```

Response headers

```
cache-control: no-cache,no-store,must-revalidate
content-type: application/json
date: Thu,28 Dec 2023 16:17:32 GMT
expires: 0
server: Jamf
strict-transport-security: max-age=63072000; includeSubDomains;
```

Generate a secure token for the managedAdmin account

41. Logout of the user created during Setup Assistant. This guide is using the jappleseed account.

42. Login with the managedAdmin account or your chosen Management Admin account set in Computer PreStage and the LAPS Password.
    NOTE: Click Other to log in. If you don't see Other, press the escape key on your keyboard. The LAPS password is case sensitive and must include the dashes.

43. Click through and set the screens to meet you needs.

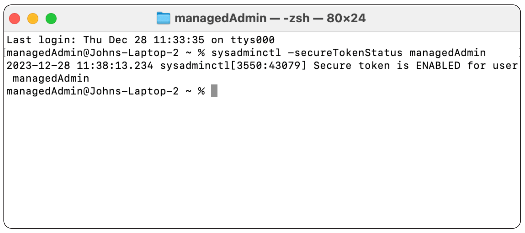
Check the users for the secure token status for the managedAdmin account. (Required to decrypt FileVault and for other macOS tasks requiring volume ownership)

44. On your test Mac computer, open Terminal. A new shell window opens with your home folder as the working directory.

45. Enter the following command and press Return.

    ```
    sysadminctl -secureTokenStatus managedAdmin
    ```

    You will get a message letting you know the secure token is enabled for the user managedAdmin.
    NOTE: The Managed Admin was created by MDM. Since we logged in with the managedAdmin account, the user now has a Secure Token.

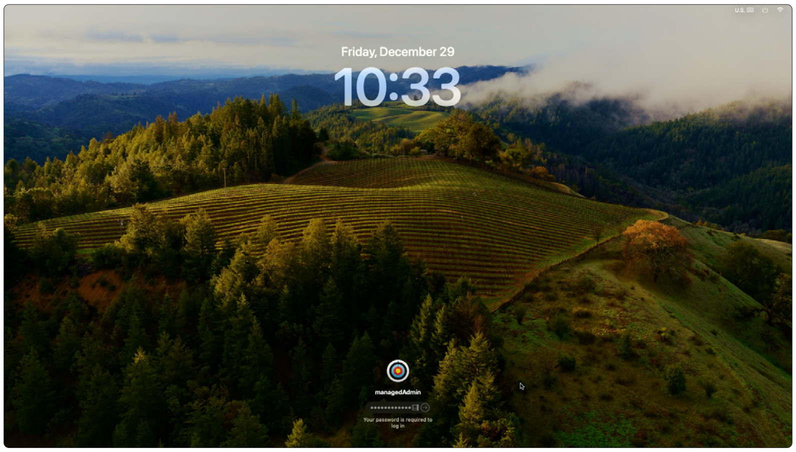


```
Last login: Thu Dec 28 11:33:35 on ttys000
managedAdmin@Johns-Laptop-2 ~ % sysadminctl -secureTokenStatus managedAdmin
2023-12-28 11:38:13.234 sysadminctl[3550:43079] Secure token is ENABLED for user
 managedAdmin
managedAdmin@Johns-Laptop-2 ~ %
```

Decrypt FileVault with the Managed Admin:

Depending on when you viewed the Managed Admin's LAPS Password, it may have been rotated and you will need to get the updated LAPS Password. If the Mac computer is offline, the rotation will happen once the Mac computer is online and checks in with the Jamf Pro server. The management account password for cryptographically enabled accounts will be out of sync with the password stored in Jamf Pro. You will need to use the original LAPS password for the Managed Admin to decrypt FileVault. You will also need to enter the rotated LAPS password for the managed Admin to log into your Mac computer. This means you will need two different logins for the managed admin account on your Mac computer going forward.

46. Restart your test Mac computer.
47. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.
48. Enter the first LAPS password documented in the previous step to decrypt FileVault.



Friday, December 29

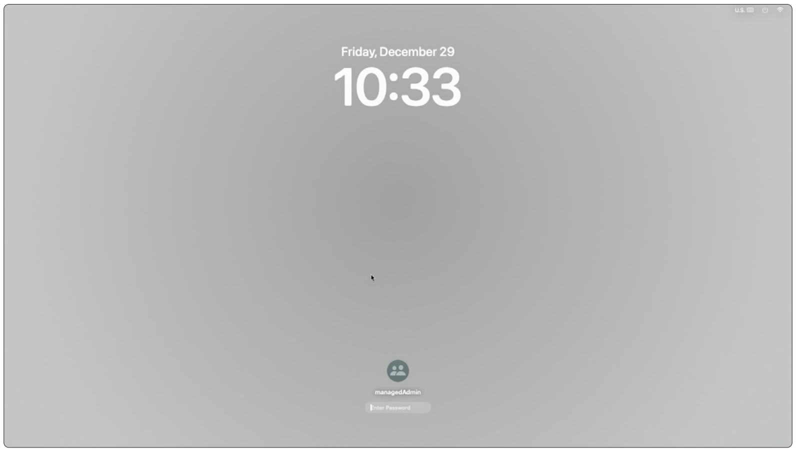
10:33

managedAdmin

Your password is required to log in

Enter the old LAPS password

49. Login to your Mac computer with the new LAPS password.



Friday, December 29

10:33

managedAdmin

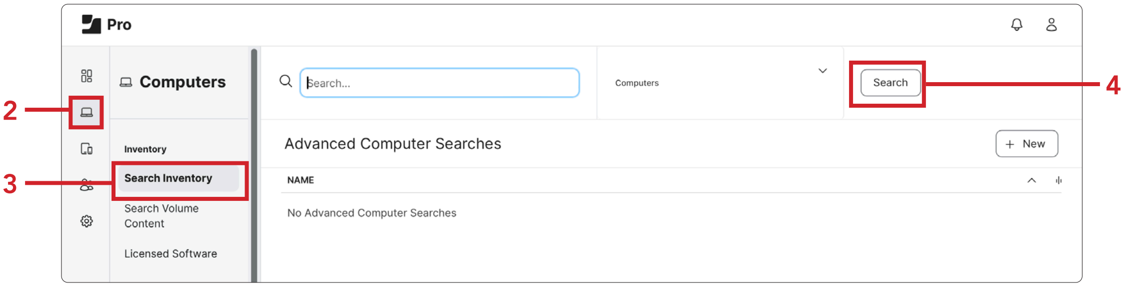
Enter Password

Enter the new LAPS password

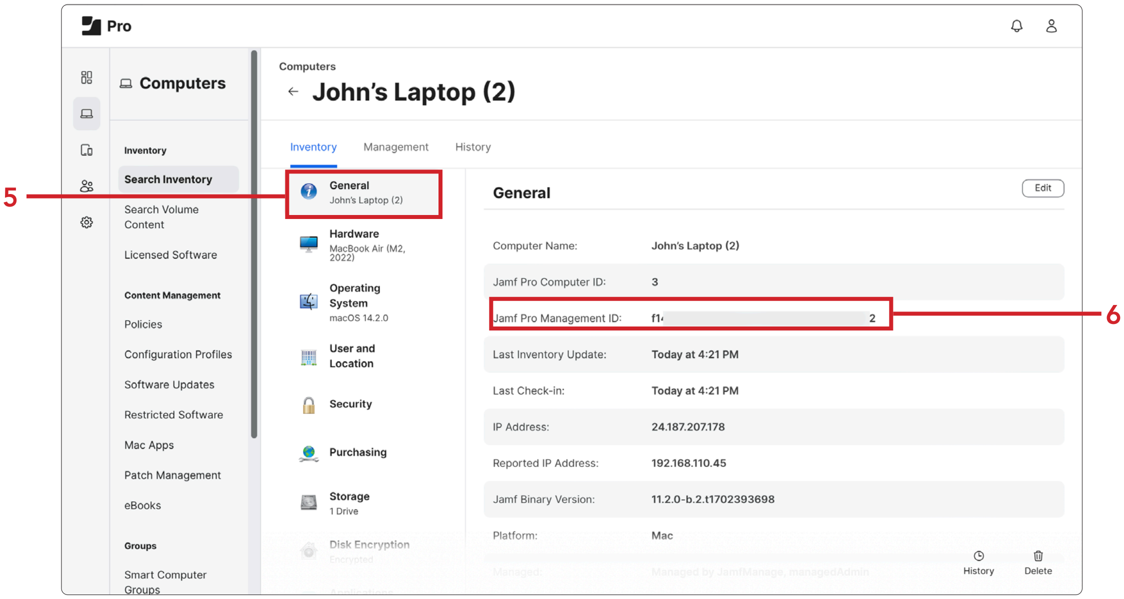
Section 4: 78 RPM Bonus Track - Set a temporary LAPS Password for the Managed Admin and Jamf Management Account

On your production Mac computer, document the client management id of your test Mac computer.

1. Log into your Jamf Pro server with administrative privileges.
2. Click Computers.
3. Click Search Inventory.
4. Search for your test Mac computer.



5. Click General Category of your Computer Inventory record.
6. Document the Jamf Pro Management ID (We will need this in a later step.)



Computer Name: John's Laptop (2)

Jamf Pro Computer ID: 3

Jamf Pro Management ID: f1[redacted]2

Last Inventory Update: Today at 4:21 PM

Last Check-in: Today at 4:21 PM

IP Address: 24.187.207.178

Reported IP Address: 192.168.110.45

Jamf Binary Version: 11.2.0-b.2.t1702393698

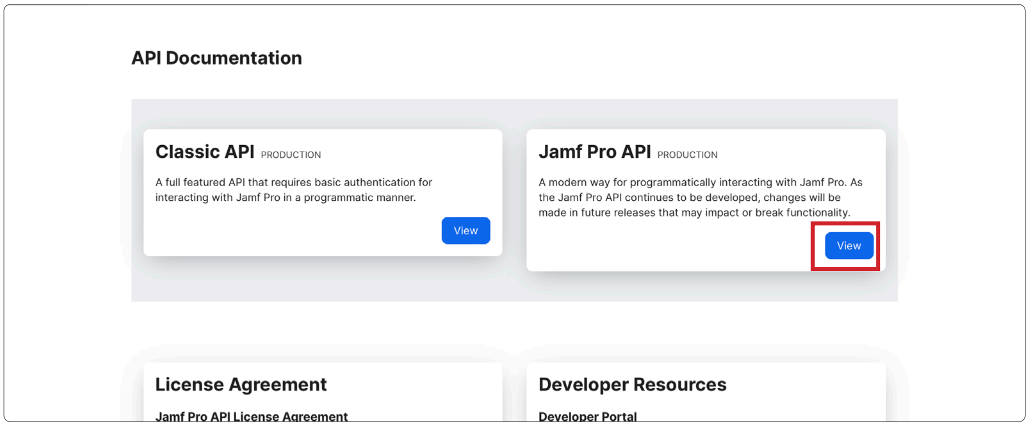
Platform: Mac

Managed: Managed by JamfManage, managedAdmin

Use the Jamf Pro API:

7. Enter the address of your Jamf Pro server and add /api to the end of the URL. I.E. https://hcs.jamfcloud.com/api.

8. Click the View button on Jamf Pro API.



API Documentation

Classic API PRODUCTION

A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.

Jamf Pro API PRODUCTION

A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.

License Agreement

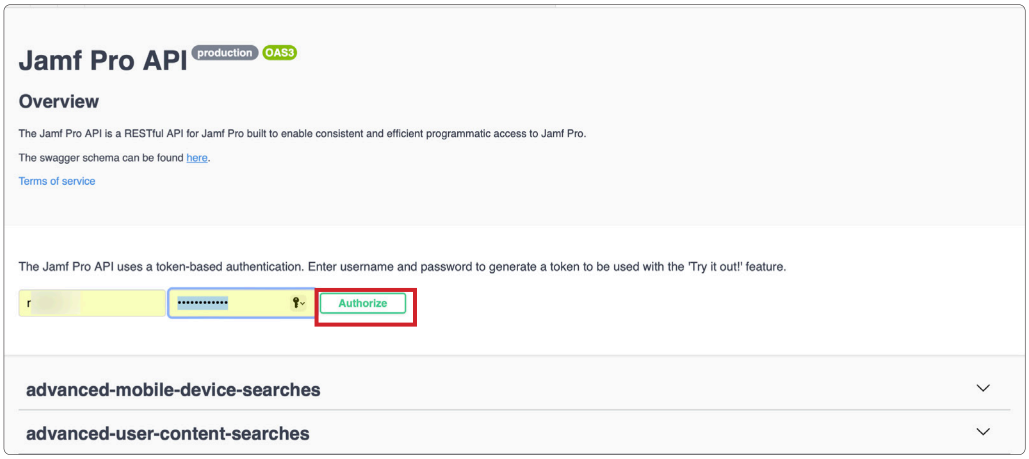
Jamf Pro API License Agreement

Developer Resources

Developer Portal

9. Enter your Jamf Pro credentials.

10. Click Authorize.



Jamf Pro API production OAS3

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

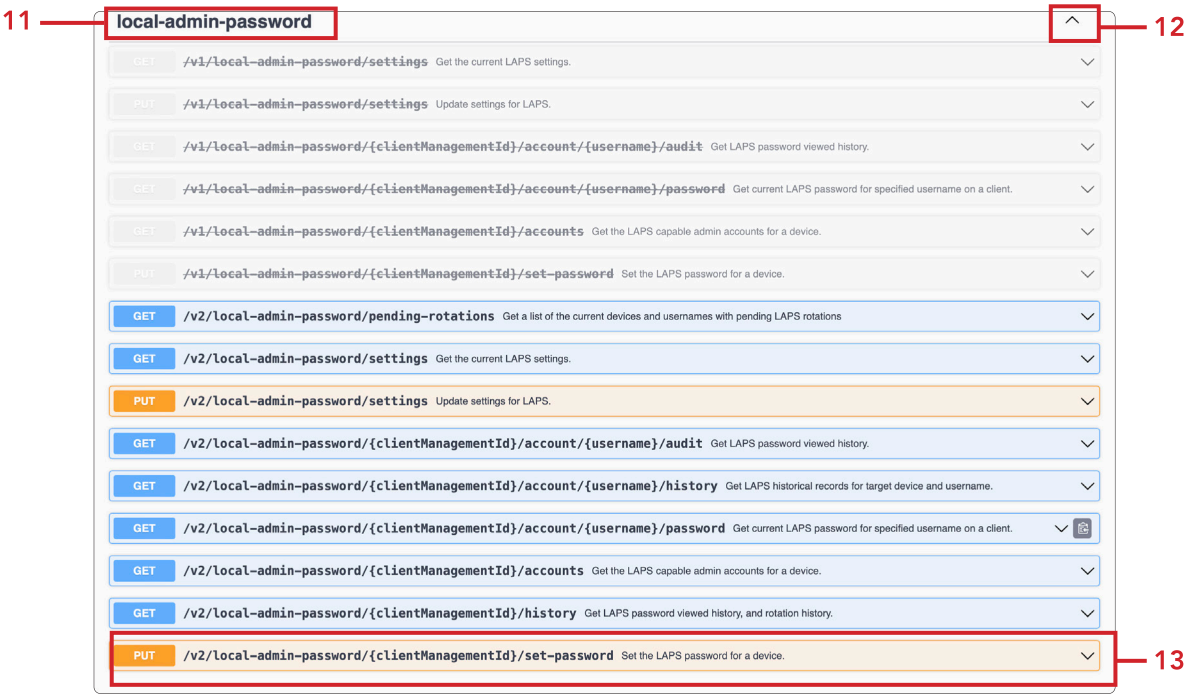
The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

Authorize
advanced-mobile-device-searches
advanced-user-content-searches

11. Scroll down the list and select local-admin-password.

12. Click Expand to see its contents.

13. Click PUT on v2/local-admin-password/{clientManagementId}/set-password.



local-admin-password

GET ~~/v1/local-admin-password/settings~~ Get the current LAPS settings.

PUT ~~/v1/local-admin-password/settings~~ Update settings for LAPS.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/audit~~ Get LAPS password viewed history.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/password~~ Get current LAPS password for specified username on a client.

GET ~~/v1/local-admin-password/{clientManagementId}/accounts~~ Get the LAPS capable admin accounts for a device.

PUT ~~/v1/local-admin-password/{clientManagementId}/set-password~~ Set the LAPS password for a device.

GET /v2/local-admin-password/pending-rotations Get a list of the current devices and usernames with pending LAPS rotations

GET /v2/local-admin-password/settings Get the current LAPS settings.

PUT /v2/local-admin-password/settings Update settings for LAPS.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/audit Get LAPS password viewed history.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.

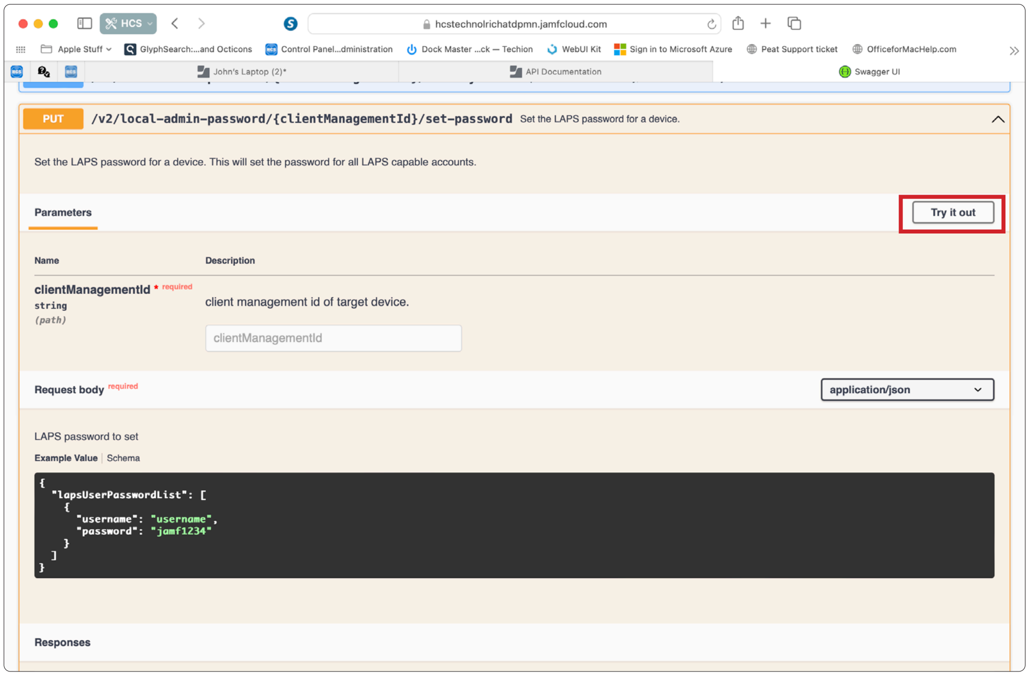
GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

GET /v2/local-admin-password/{clientManagementId}/accounts Get the LAPS capable admin accounts for a device.

GET /v2/local-admin-password/{clientManagementId}/history Get LAPS password viewed history, and rotation history.

PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

14. Click Try it out.


HCS
hcstechnolrichatdpmn.jamfcloud.com
Apple Stuff
GlyphSearch:...and Octicons
Control Panel...dministration
Dock Master ...ck — Techion
WebUI Kit
Sign in to Microsoft Azure
Peat Support ticket
OfficeforMacHelp.com
John's Laptop (2)*
API Documentation
Swagger UI

PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

Set the LAPS password for a device. This will set the password for all LAPS capable accounts.

Parameters

Try it out

Name	Description
clientManagementId * required string *(path)*	client management id of target device. clientManagementId

Request body required

application/json

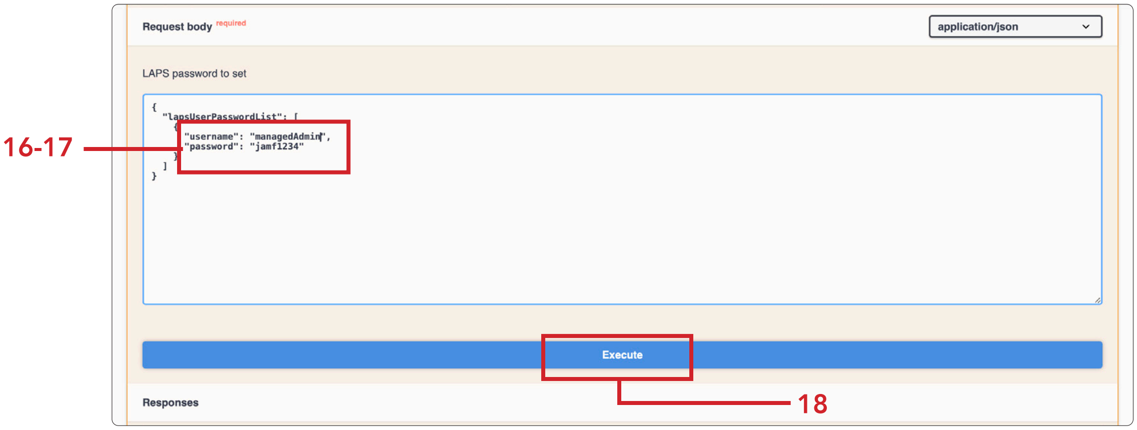
LAPS password to set

Example Value | Schema

```
{
  "lapsUserPasswordList": [
    {
      "username": "username",
      "password": "jamf1234"
    }
  ]
}
```

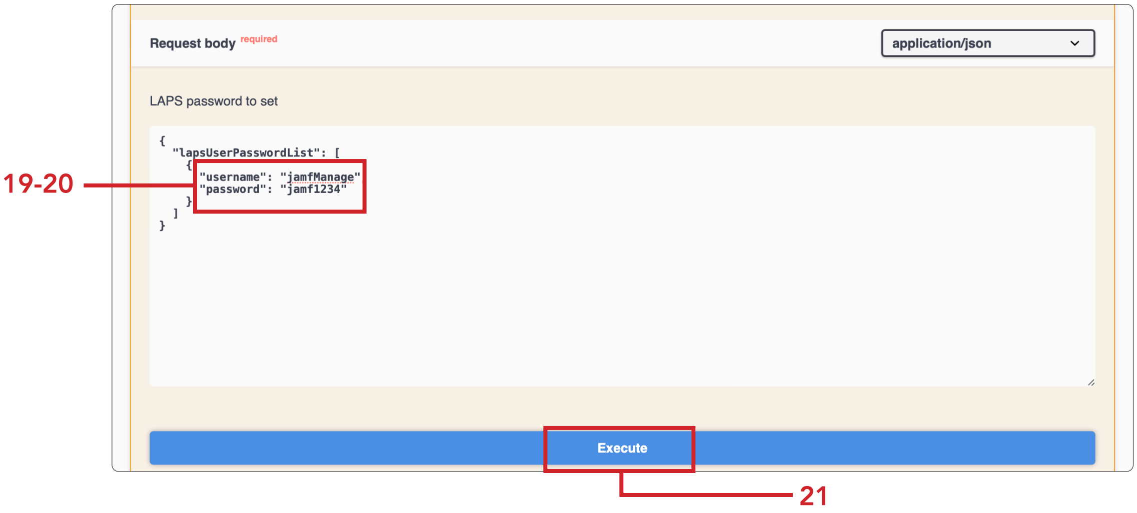
Responses

15. In the client management id of the target device field, Enter the Jamf Pro Management ID documented from a previous step.
16. In the LAPS password to set field, change username to managedAdmin.
17. In the LAPS password to set field, change password to jamf1234.
18. Click Execute.



```
{
  "lapsUserPasswordList": [
    {
      "username": "managedAdmin",
      "password": "jamf1234"
    }
  ]
}
```

19. In the LAPS password to set field, change username to jamfManage.
20. In the LAPS password to set field, change password to jamf1234.
21. Click Execute.

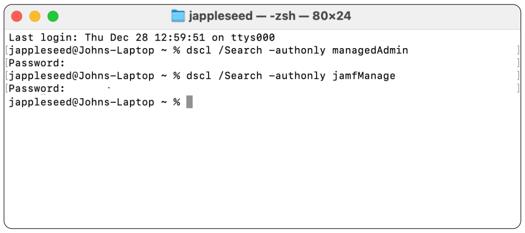


```
{
  "lapsUserPasswordList": [
    {
      "username": "jamfManage"
      "password": "jamf1234"
    }
  ]
}
```

Confirm password for the managedAdmin and jamfManage accounts:

22. On the test Mac computer, Open Terminal. A new shell window opens with your home folder as the working directory.

23. Type the following commands and press Return:
    - `dscl /Search -authonly managedAdmin`
      Enter `jamf1234` (set in the previous step)
      NOTE: No response in the terminal means the command was successful
    - `dscl /Search -authonly jamfManage`
      Enter `jamf1234` (set in the previous step)
      NOTE: No response in the terminal means the command was successful



jappleseed — -zsh — 80×24

```
Last login: Thu Dec 28 12:59:51 on ttys000
jappleseed@Johns-Laptop ~ % dscl /Search -authonly managedAdmin
Password:
jappleseed@Johns-Laptop ~ % dscl /Search -authonly jamfManage
Password:
jappleseed@Johns-Laptop ~ %
```

View the LAPS Password for the Management Admin account.

There are two options for viewing the LAPS password:

- Option 1 requires a 3rd party application.
- Option 2 requires the Jamf Pro API.

Option 1: Use Jamf LAPS App

24. On your production Mac computer, launch Jamf LAPS installed in Section 1.

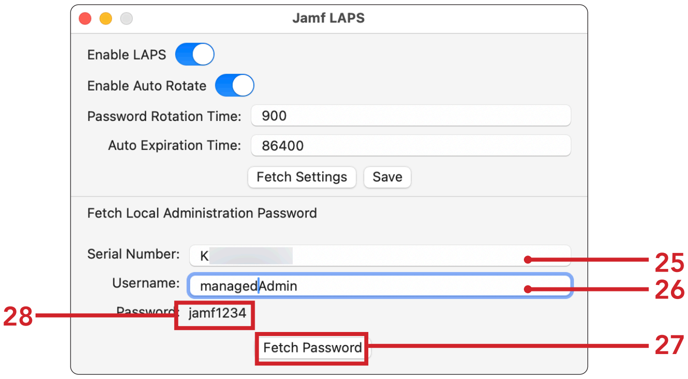
LAPS

25. Enter the Serial Number of the enrolled Mac computer.

26. Username: Enter the Managed Admin Account.

27. Click Fetch Password.

28. Confirm jamf1234.



Jamf LAPS

Enable LAPS: on
Enable Auto Rotate: on
Password Rotation Time: 900
Auto Expiration Time: 86400

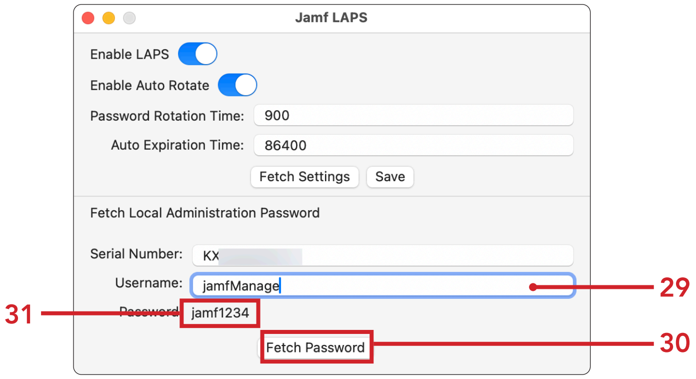
Fetch Local Administration Password

Serial Number: K[redacted]
Username: managedAdmin
Password: jamf1234

29. Username: Enter the Jamf Management Account.

30. Click Fetch Password.

31. Confirm jamf1234.



Jamf LAPS

Enable LAPS: on

Enable Auto Rotate: on

Password Rotation Time: 900

Auto Expiration Time: 86400

Fetch Local Administration Password

Serial Number: KX[redacted]

Username: jamfManage

Password: jamf1234

Option 2 View LAPS password using the Jamf Pro API

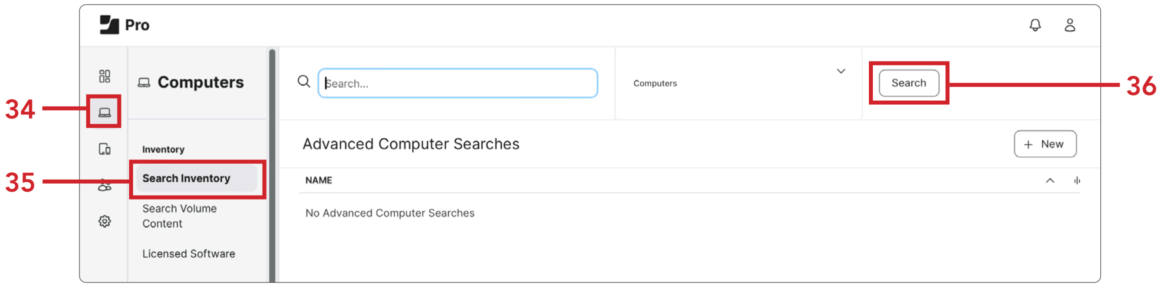
32. We need to document the client management id of our test Mac computer.

33. On your production Mac computer, log into your Jamf Pro server with proper privileges.

34. Click Computers.

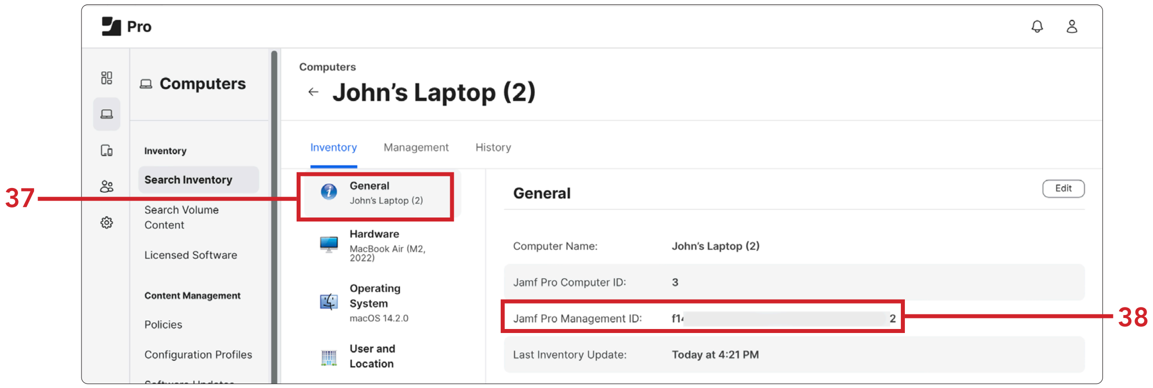
35. Click Search Inventory.

36. Search for your test Mac computer.



37. Click General Category of your Computer Inventory record.

38. Document the Jamf Pro Management ID (We will need this in a later step.)



Computer Name: John's Laptop (2)

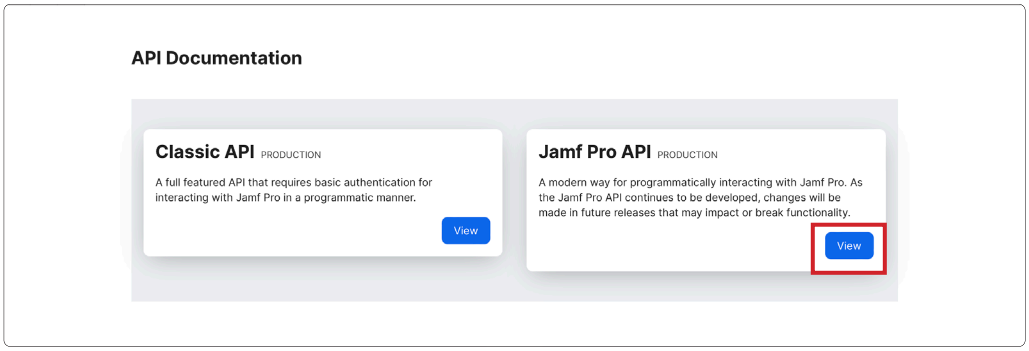
Jamf Pro Computer ID: 3

Jamf Pro Management ID: f1[redacted]2

Last Inventory Update: Today at 4:21 PM

39. Enter the address of your Jamf Pro server and add /api to the end of the URL. I.E. https://hcs.jamfcloud.com/api.

40. Click the View button on Jamf Pro API.



API Documentation

Classic API PRODUCTION

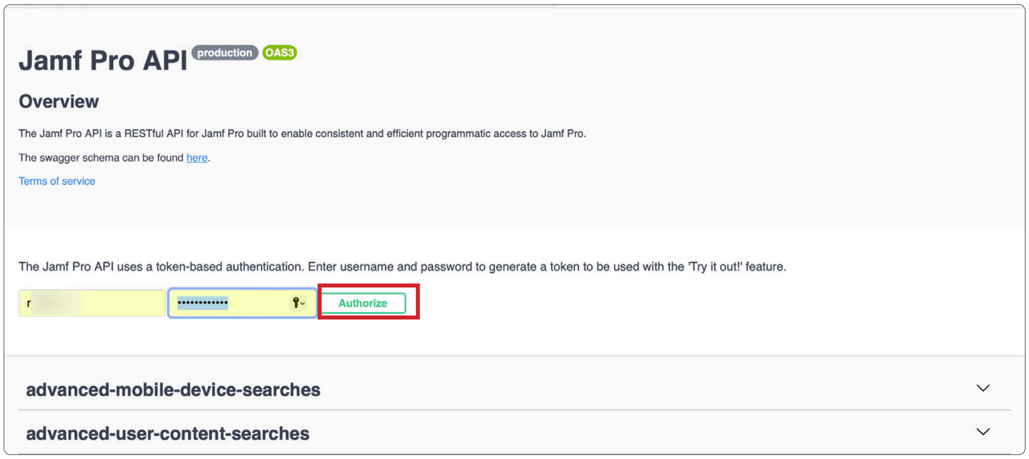
A full featured API that requires basic authentication for interacting with Jamf Pro in a programmatic manner.

Jamf Pro API PRODUCTION

A modern way for programmatically interacting with Jamf Pro. As the Jamf Pro API continues to be developed, changes will be made in future releases that may impact or break functionality.

41. Enter your Jamf Pro credentials.

42. Click Authorize to generate a token. NOTE: This guide will use a Jamf Pro administrator account.



Jamf Pro API production OAS3

Overview

The Jamf Pro API is a RESTful API for Jamf Pro built to enable consistent and efficient programmatic access to Jamf Pro.

The swagger schema can be found here.

Terms of service

The Jamf Pro API uses a token-based authentication. Enter username and password to generate a token to be used with the 'Try it out!' feature.

r[redacted] ••••••••••••

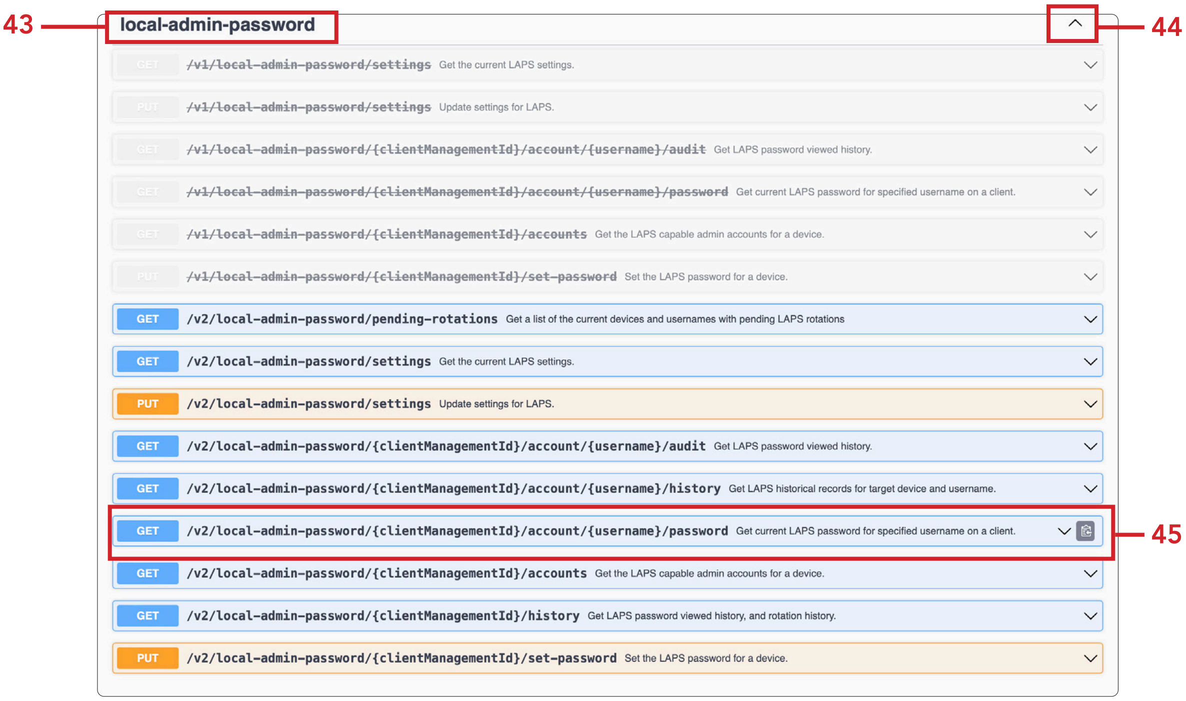
advanced-mobile-device-searches

advanced-user-content-searches

43. Scroll down the list and select local-admin-password.

44. Click Expand the list to see its contents.

45. Click Get for /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified user name on a client.



local-admin-password

GET ~~/v1/local-admin-password/settings~~ Get the current LAPS settings.

PUT ~~/v1/local-admin-password/settings~~ Update settings for LAPS.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/audit~~ Get LAPS password viewed history.

GET ~~/v1/local-admin-password/{clientManagementId}/account/{username}/password~~ Get current LAPS password for specified username on a client.

GET ~~/v1/local-admin-password/{clientManagementId}/accounts~~ Get the LAPS capable admin accounts for a device.

PUT ~~/v1/local-admin-password/{clientManagementId}/set-password~~ Set the LAPS password for a device.

GET /v2/local-admin-password/pending-rotations Get a list of the current devices and usernames with pending LAPS rotations

GET /v2/local-admin-password/settings Get the current LAPS settings.

PUT /v2/local-admin-password/settings Update settings for LAPS.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/audit Get LAPS password viewed history.

GET /v2/local-admin-password/{clientManagementId}/account/{username}/history Get LAPS historical records for target device and username.

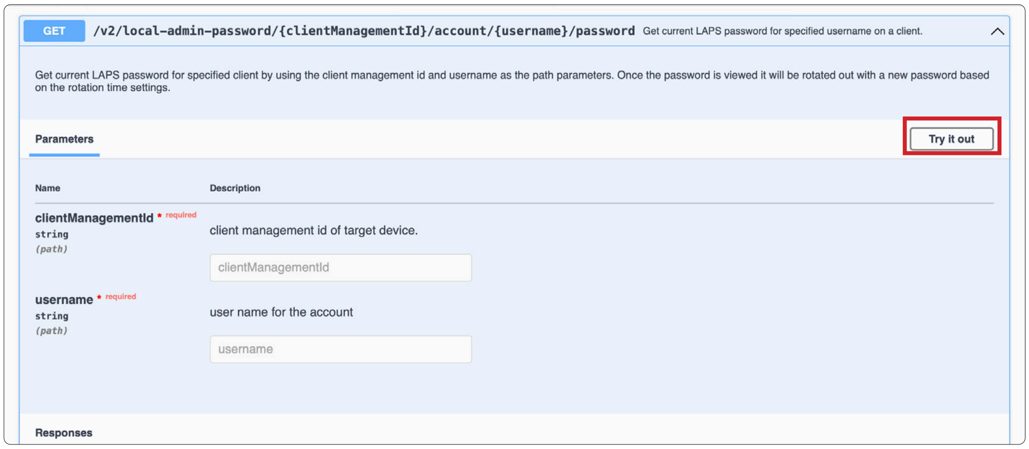
GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

GET /v2/local-admin-password/{clientManagementId}/accounts Get the LAPS capable admin accounts for a device.

GET /v2/local-admin-password/{clientManagementId}/history Get LAPS password viewed history, and rotation history.

PUT /v2/local-admin-password/{clientManagementId}/set-password Set the LAPS password for a device.

46. Click Try it out.



GET /v2/local-admin-password/{clientManagementId}/account/{username}/password Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Parameters

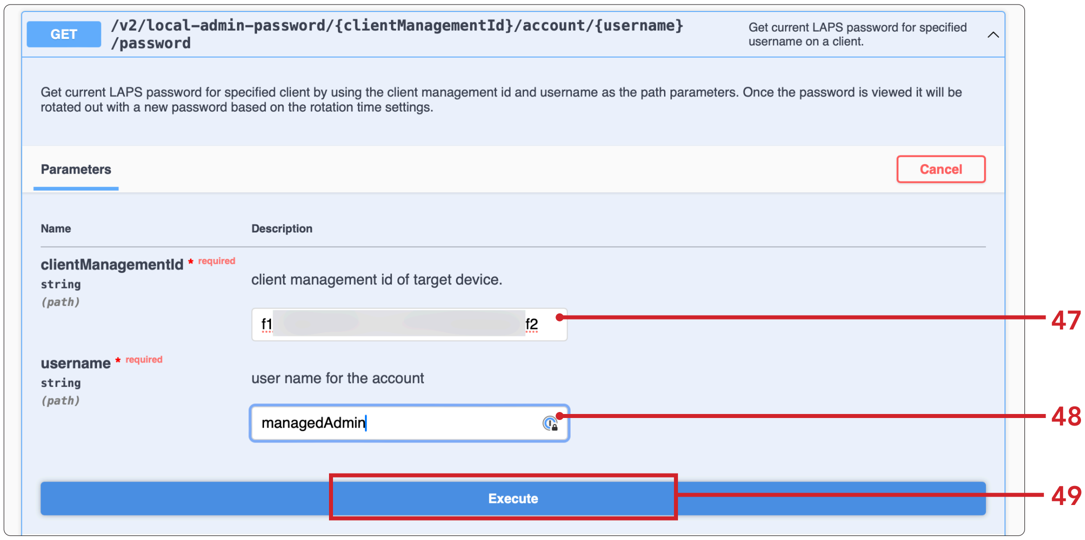
Name	Description
clientManagementId * required string *(path)*	client management id of target device. clientManagementId
username * required string *(path)*	user name for the account username

Responses

47. In the clientManagementId field, enter the Jamf Pro Management ID documented from a previous step

48. In the username field, enter managedAdmin or your chosen Management Admin account set in Computer PreStage

49. Click Execute.



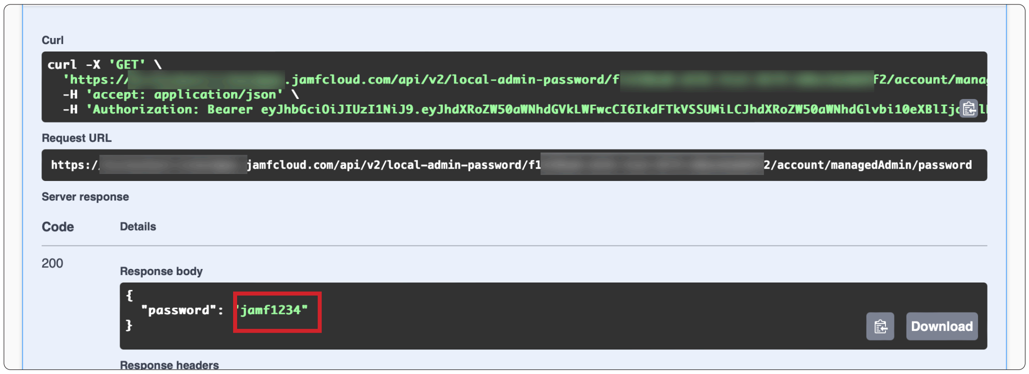
GET `/v2/local-admin-password/{clientManagementId}/account/{username}/password`

Get current LAPS password for specified username on a client.

Get current LAPS password for specified client by using the client management id and username as the path parameters. Once the password is viewed it will be rotated out with a new password based on the rotation time settings.

Name	Description
clientManagementId * required string (path)	client management id of target device. f1[redacted]f2
username * required string (path)	user name for the account managedAdmin

50. Confirm jamf1234.



Curl

```
curl -X 'GET' \
  'https://[redacted].jamfcloud.com/api/v2/local-admin-password/f[redacted]f2/account/mana
  -H 'accept: application/json' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdXRoZW50aWNhdGVkLWFwcCI6IkdFTkVSSUMiLCJhdXRoZW50aWNhdGlvbi10eXBlIjc
```

Request URL

```
https:/[redacted]jamfcloud.com/api/v2/local-admin-password/f1[redacted]2/account/managedAdmin/password
```

Server response

Code	Details
200	Response body

```
{
  "password": "jamf1234"
}
```

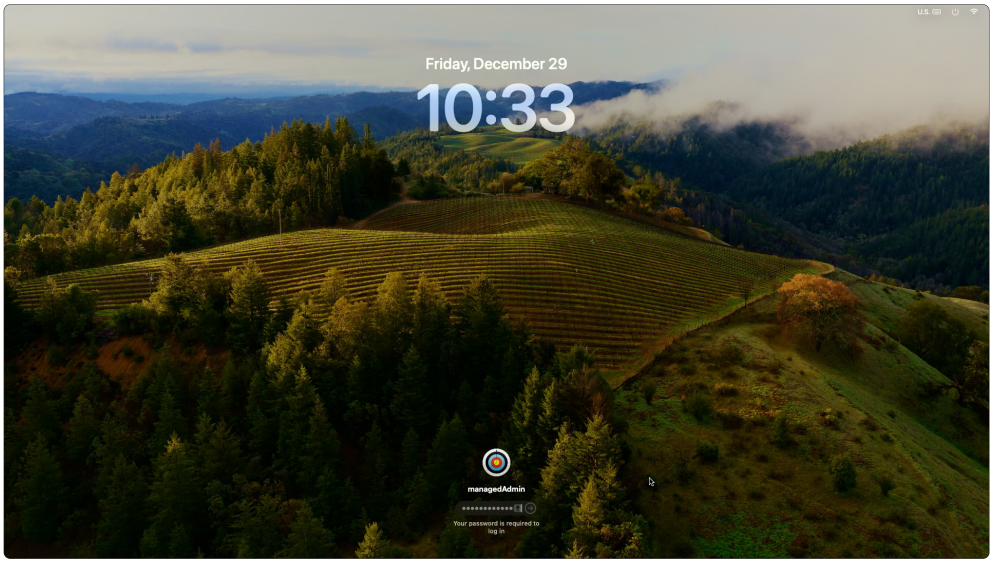
51. Repeat these steps for the Jamf Management Account. I.E. the jamfManage account.

Decrypt FileVault with the Managed Admin

52. Restart the Mac computer.

53. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.

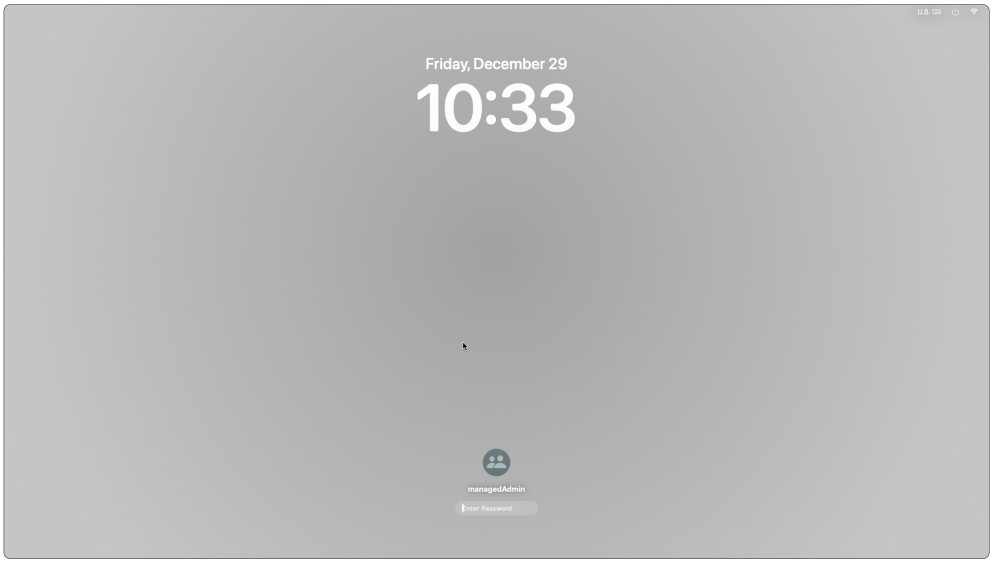
54. Enter the LAPS password to decrypt FileVault and login to your Mac computer.



Your password is required to log in

55. At the login window, in the Username field, enter managedAdmin or your chosen Management account set in the Computer PreStage.

56. Enter the password jamf1234 (Set in a previous step.)



Decrypt FileVault with the Jamf Management Account

57. Restart the test Mac computer.

58. At the login window, in the Username field, enter jamfManage set in User Initiated enrollment

59. Enter the password jamf1234 (Set in a previous step)

NOTE: Depending on when you viewed the Managed Admin's LAPS Password, it may have been rotated and you will need to get the updated LAPS Password.

If the Mac computer is offline, the rotation will happen once the Mac computer is online and checks in with the Jamf Pro server.

The management account password for cryptographically enabled accounts will be out of sync with the password stored in Jamf Pro.

You will need to use the original LAPS password for the Managed Admin to decrypt FileVault.

You will also need to enter the set LAPS password for the managed Admin to log into your Mac computer. NOTE: This guide used jamf1234 as the set password for the managedAdmin account.

Continued Success of your Apple and Jamf solution requires having the right training, support and resources available when you need them.

Training

Apple Device Support
https://it-training.apple.com/tutorials/apt-support

Apple Deployment and Management
https://it-training.apple.com/tutorials/apt-deployment

Jamf 100 Course
https://www.jamf.com/training/online-training/100/

Jamf 170 Course
https://www.jamf.com/training/online-training/170/

Jamf Training Catalog
https://trainingcatalog.jamf.com