



Configure Custom USB Drive Restrictions with Notifications



Contents

Preface	3
Section 1: Preparation - Identify Your Approved USB Devices.....	5
Section 2: Jamf Pro - Deploy the HCS Branding Package	8
Section 3: Jamf Pro - Create the Jamf Helper Script.....	15
Section 4: Jamf Pro - Configure Analytic Remediation	17
Section 5: Jamf Protect - Create a Removable Storage Control Set	24
Section 6: Jamf Protect - Create an Analytic Set	28
Section 7: Jamf Protect - Create and Configure the Plan	33
Section 8: Jamf Protect - Configure Email Notifications	35
Section 9: Jamf Protect - Assign Plan to Computers.....	37
Section 10: Test the Configuration.....	42



Preface

What is Removable Media Control?

Removable Media Control is a security feature in Jamf Protect that allows organizations to manage which external storage devices can be connected to their Mac computers. External storage devices include USB flash storage, external hard drives, SD cards, and other removable media.

When Removable Media Control is enabled, administrators can define a list of approved devices based on their hardware vendor and model number. Any device not on the approved list will be blocked from mounting, preventing unauthorized data transfer and reducing the risk of malware infection from untrusted devices.

This guide will walk you through configuring Jamf Pro and Jamf Protect to:

- Create a list of approved USB drives by hardware vendor and model number
- Display a pop-up notification to users when they connect an unapproved device
- Send an email alert to your IT team when an unapproved device is detected

Why Control Removable Media?

External storage devices pose several security risks to organizations:

Data Exfiltration

Users (intentionally or unintentionally) can copy sensitive company data to personal drives

Malware Introduction

Infected USB drives can introduce viruses, ransomware, or other malicious software

Compliance Requirements

Many industries require controls on removable media to meet regulatory standards

Intellectual Property Protection

Prevents unauthorized copying of proprietary information

By implementing Removable Media Control, you maintain visibility and control over what devices can connect to your managed Mac computers while still allowing approved devices that employees need for their work.

Prerequisites

Before beginning this guide, ensure you have the following:

Jamf Pro server

Version 11.23 or later with administrator privileges.

Jamf Protect

With administrator privileges to the macOS Security portal (Jamf Protect web app).

Test Mac computer

Non-production Mac with macOS 26.2 Tahoe or later, enrolled in Jamf Pro with Jamf Protect installed. All testing for this guide was done using macOS 26.2 Tahoe.

SMTP server or email relay

Configured for sending IT team notifications

Working knowledge of the Jamf Pro and macOS Security portal (Jamf Protect web apps)

NOTE:

This guide builds upon the “How to Use Jamf Helper in Jamf Pro” guide. If you are unfamiliar with Jamf Helper (the macOS utility for displaying user notifications), review that guide first to understand how Jamf Helper displays notifications to users. Review the guide here:

<https://hconline.com/support/resources/white-papers/how-to-use-jamf-helper-in-jamf-pro>



Additional Resources

The following resources will help you complete this guide:

- The HCS Branding Package and Script (pre-built): <https://github.hcsonline.com/jpusb>

NOTE: The HCS Branding Package above can be used in Section 2 if you do not want to create your own package.

Guide Structure

This guide is organized so you complete all work in one system before moving to the next:

- Section 1: Preparation on a Mac
- Sections 2-4: Complete all Jamf Pro configuration
- Sections 5-9: Complete all Jamf Protect configuration
- Section 10: Test the configuration



Section 1: Preparation - Identify Your Approved USB Devices

What You'll Need

Hardware and Software

Requirements for following along with this section:

- A Mac computer with macOS 26.2 or later
- USB disks you want to approve

In this section, you will find the Vendor ID for each USB drive you want to allow. These hexadecimal values uniquely identify device types and will be used later when configuring Jamf Protect.

Understanding Device Identification

Jamf Protect identifies removable storage by:

- Vendor ID: A hexadecimal code identifying the manufacturer (e.g., 0x0781 for SanDisk)
- Product ID: A hexadecimal code identifying the product model (e.g., 0x5583 for Extreme Pro)

NOTE: You will use the Vendor ID and Product ID from System Report, not the display names. These are technical identifiers that uniquely identify device types.

Find Your Device's Vendor ID

1. On a Mac, connect the USB drive you want to approve.
2. Click the Apple menu.
3. Select About This Mac.

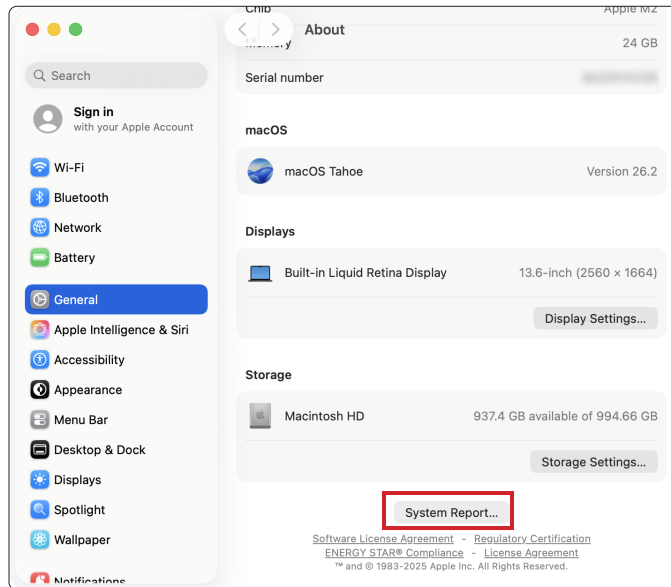


4. Click More Info.

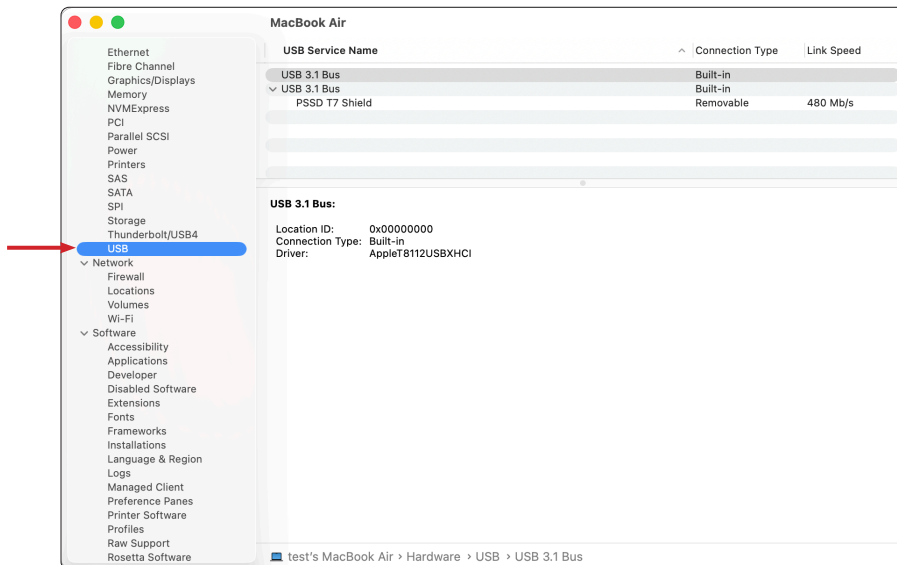




5. Scroll down and click System Report.

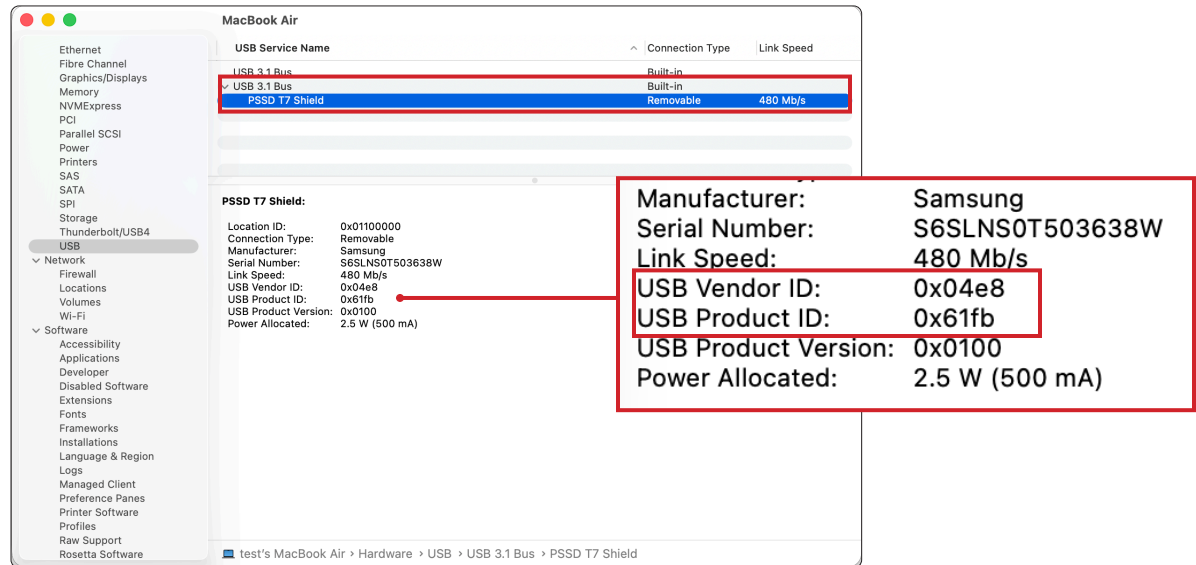


6. In the sidebar, click USB.

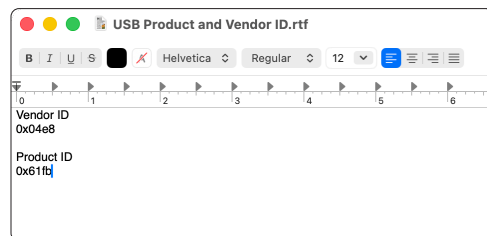




7. Select your device in the USB Device Tree.
8. Locate the Vendor ID field. Confirm the hexadecimal value (e.g., 0x04e8).
9. Locate the Product ID field. Confirm the hexadecimal value (e.g., 0x61fb).



10. Create a TextEdit document.
 11. Enter the following: **Vendor ID**.
 12. Copy the hexadecimal value (e.g., 0x04e8) for USB Vendor ID and paste the value under Vendor ID.
 13. Enter the following: **Product ID**.
 14. Copy the hexadecimal value (e.g., 0x61fb) for USB Product ID and paste the value under Product ID.
- NOTE: The Vendor ID and Product ID are displayed as hexadecimal numbers starting with 0x. Record both values exactly as shown.



15. To add additional USB drives: Leave System Report open, disconnect the current drive, connect the next one, then go to File > Refresh Information.
16. Save the TextEdit Document to the Desktop as **USB Product and Vendor ID**.

This completes this section.



Section 2: Jamf Pro - Deploy the HCS Branding Package

What You'll Need

Hardware and Software

Requirements for following along with this section:

- A Jamf Pro server with version 11.23 or later
- The HCS Branding Package and Script
- Administrator privileges to your Jamf Pro

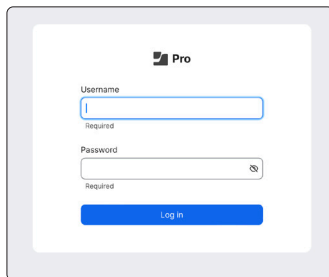
In this section, you will deploy the HCS logo image that will be displayed in the Jamf Helper pop-up notifications. This branding ensures users recognize the notification as coming from an official IT source.

Download the Branding Package

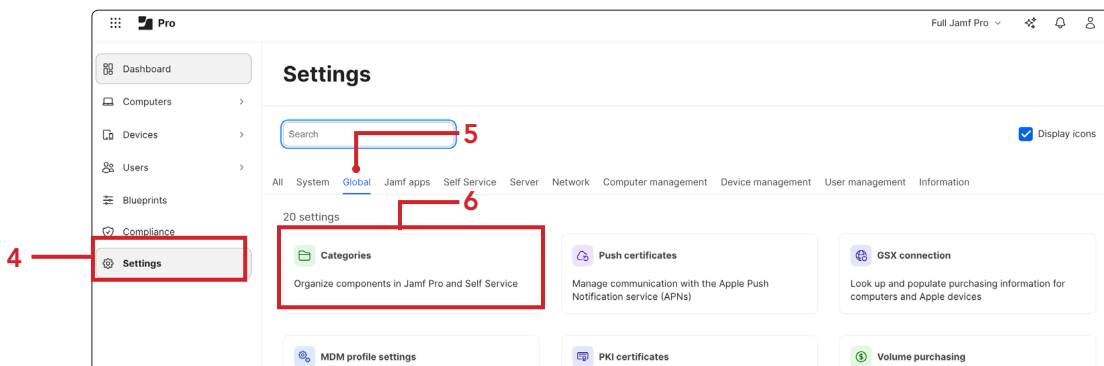
1. Download the the HCS Branding Package and Script from <https://github.hcsonline.com/jpushb>
2. Unzip the downloaded file to extract the HCS-USB-Alert-Branding.pkg.

Create a Category for the Package

3. In a web browser, log in to your Jamf Pro instance with administrator privileges.



4. In Jamf Pro, click Settings (⚙️).
5. Click Global.
6. Click Categories.



7. Click New (+).





8. In the Display Name field, enter: **Branding**.

9. Click Save.

A screenshot of a web application interface for creating a new category. The breadcrumb trail at the top reads 'Settings : Global > Categories'. Below this is a back arrow and the title 'New Category'. The 'Display Name' field, with the subtitle 'Display name for the category', contains the text 'Branding'. A red arrow labeled '8' points to this field. The 'Priority in Self Service' section has a subtitle 'Priority to use for displaying the category within the list of categories in Self Service (e.g. A category with a priority of "1" is displayed before other categories)' and a dropdown menu currently set to '9'. At the bottom right, there are 'Cancel' and 'Save' buttons. A red box highlights the 'Save' button, with a red arrow labeled '9' pointing to it.

10. Click New (+).

A screenshot of the 'Categories' page. The breadcrumb trail is 'Settings : Global'. Below it is a back arrow and the title 'Categories'. At the bottom right, there is a button labeled '+ New'. A red box highlights this button.

11. In the Display Name field, enter: **Security** .

12. Click Save.

A screenshot of the 'New Category' form. The breadcrumb trail is 'Settings : Global > Categories'. Below it is a back arrow and the title 'New Category'. The 'Display Name' field, with the subtitle 'Display name for the category', contains the text 'Security'. A red arrow labeled '11' points to this field. The 'Priority in Self Service' section has a subtitle 'Priority to use for displaying the category within the list of categories in Self Service (e.g. A category with a priority of "1" is displayed before other categories)' and a dropdown menu currently set to '9'. At the bottom right, there are 'Cancel' and 'Save' buttons. A red box highlights the 'Save' button, with a red arrow labeled '12' pointing to it.

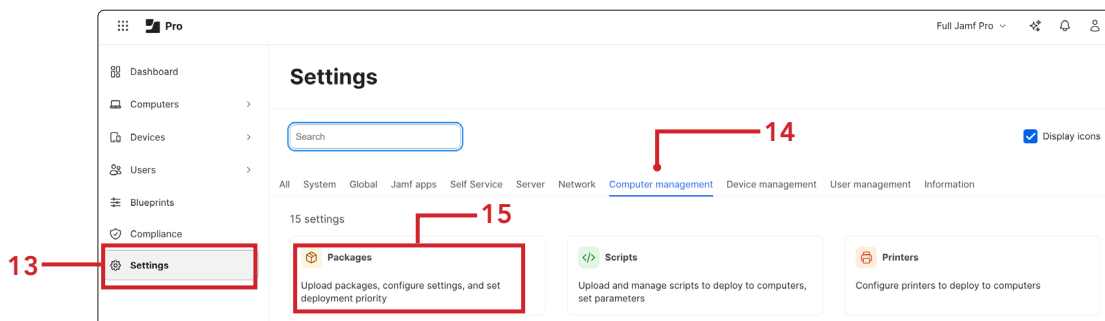


Upload the Branding Package

13. In Jamf Pro, click Settings (⚙️).

14. Click Computer Management

15. Click Packages.



16. Click New (+) to create a new package.

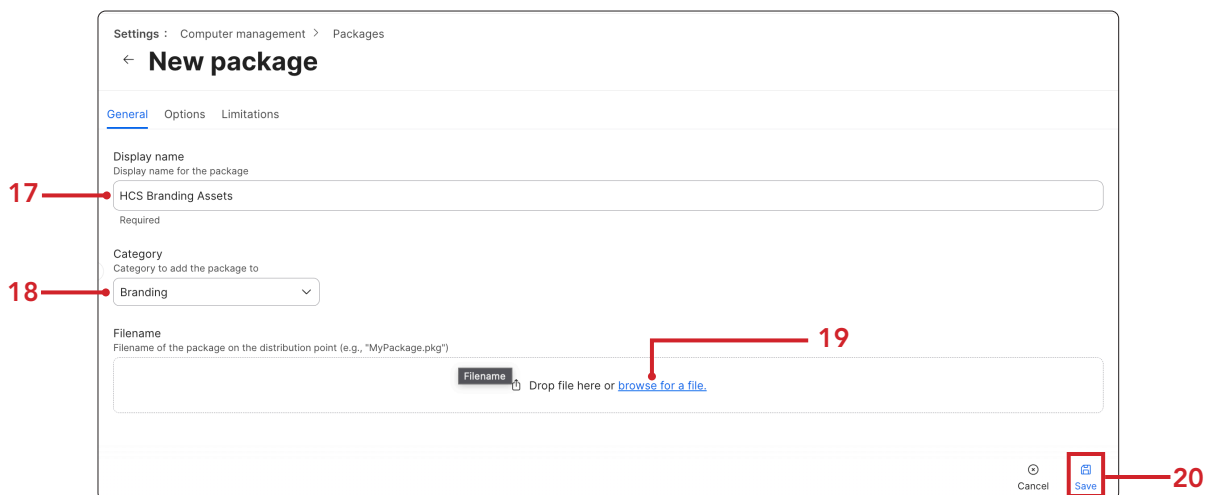


17. In the Display Name field, enter: HCS Branding Assets.

18. Click the Category menu and select Branding.

19. Click browse for a file and upload your package file.

20. Click Save.



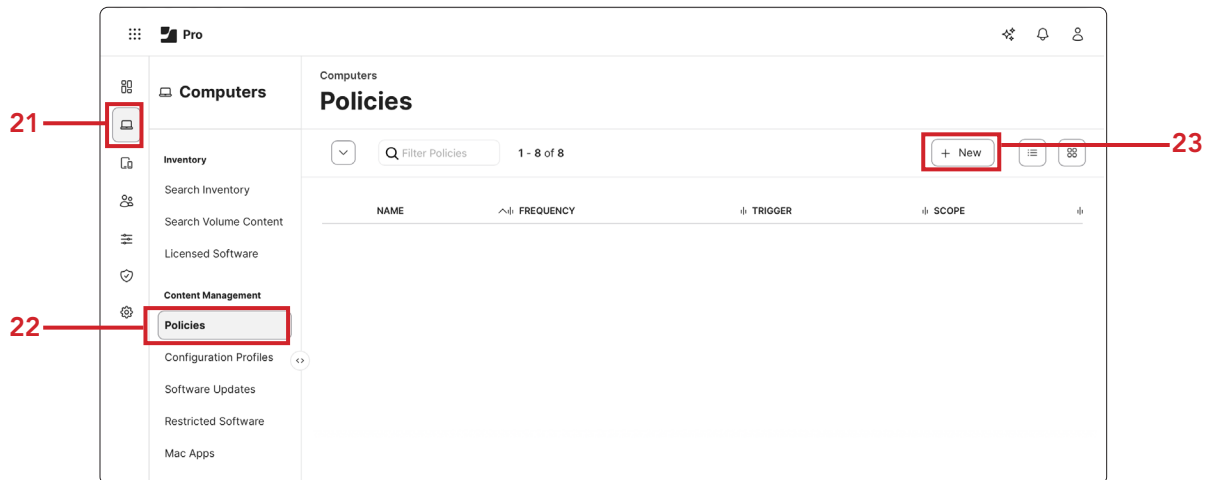


Create a Policy to Deploy the Branding Package

21. In Jamf Pro, click Computers (🖥️) in the sidebar.

22. Click Policies.

23. Click New (+).



24. In the Display Name field, enter: **Deploy HCS Branding Assets**.

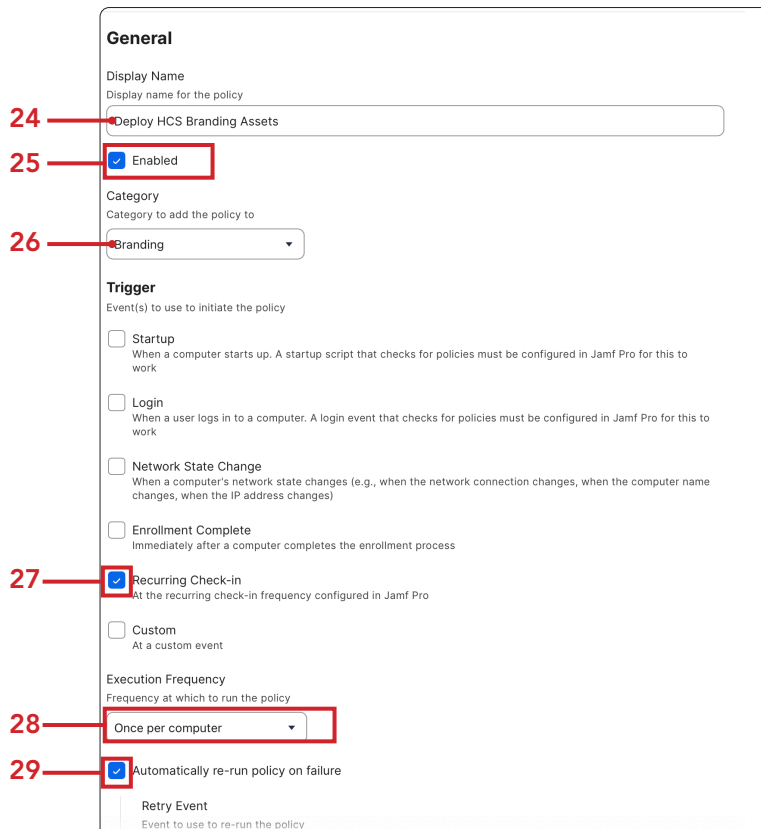
25. Verify Enabled is selected.

26. Select Branding for the Category.

27. Under Trigger, select the checkbox for Recurring Check-in.

28. Click the Execution Frequency menu and select Once per computer.

29. Select the checkbox for Automatically re-run policy on failure.





30. In the left sidebar, click Packages.

31. Click Configure.

30

Computers : Policies

New Policy

Options Scope Self Service User Interaction

General

Packages 0 Packages

Software Updates Not Configured

Scripts 0 Scripts

Printers 0 Printers

Disk Encryption Not Configured

Dock Items 0 Dock Items

Local Accounts 0 Accounts

Management Accounts Not Configured

Configure Packages

Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.

Configure

31

32. Locate the HCS Branding Assets package in the list.

33. Click Add next to HCS Branding Assets.

Computers : Policies

New Policy

Options Scope Self Service User Interaction

General

Packages 0 Packages

Software Updates Not Configured

Scripts 0 Scripts

Packages

NAME CATEGORY

Aftermath.pkg	No category assigned	Add
Comet.pkg	No category assigned	Add
HCS Branding Assets	Branding	Add
JamfConnect.Login.pkg	Jamf Setup Manager	Add



34. Verify Action is set to Install.

Computers : Policies

Deploy HCS Branding Assets

Options Scope Self Service User Interaction

General

Packages
1 Package

Software Updates
Not Configured

Scripts
0 Scripts

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

EPI Password
Not Configured

Packages

Distribution Point
Distribution point to download the package(s) from
Each computer's default distribution point

Deploy HCS Branding Assets

Action
Action to take on computers
Install

Cancel Save

35. Click Scope.

Computers : Policies

Deploy HCS Branding Assets

Options **Scope** Self Service User Interaction

Targets	Limitations	Exclusions
Target Computers Computers to deploy the policy to Specific Computers	Target Users Users to deploy the policy to Specific Users	
Selected Deployment Targets + Add		
TARGET	TYPE	
No Targets		



36. Click the Target Computers dropdown and scope to your needs. This guide will scope to All Computers.

37. Click Save. The branding package will now deploy to computers when they enroll or check in with Jamf Pro.

36

Computers : Policies

← **Deploy HCS Branding Assets**

Options Scope Self Service User Interaction

Targets Limitations Exclusions

Target Computers
Computers to deploy the policy to

All Computers

Target Users
Users to deploy the policy to

Specific Users

Selected Deployment Targets

+ Add

TARGET	TYPE	
test's MacBook Air	Computer	Remove

Cancel Save

37

This completes this section.



Section 3: Jamf Pro - Create the Jamf Helper Script

What You'll Need

Hardware and Software

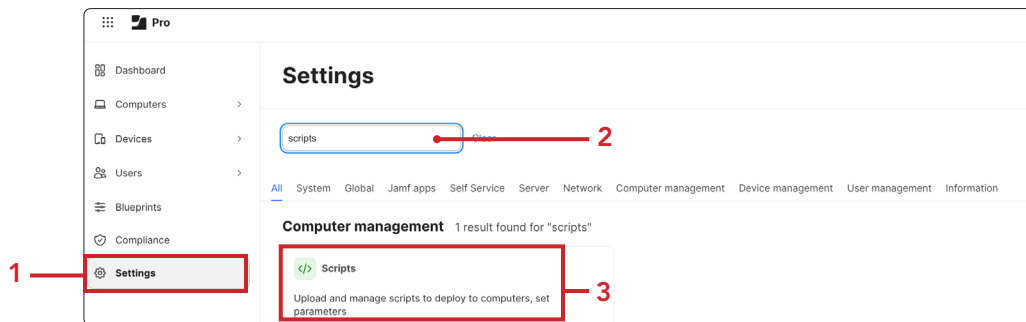
Requirements for following along with this section:

- A Jamf Pro server with version 11.23 or later with administrator privileges
- The HCS Branding Package and Script deployed from Section 2
<https://github.com.hcsonline.com/jpusb>

In this section, you will copy an existing script that displays a pop-up notification to users when they connect an unapproved USB drive. The notification uses Jamf Helper to display the message to the user with the HCS branding.

Add the Script to Jamf Pro

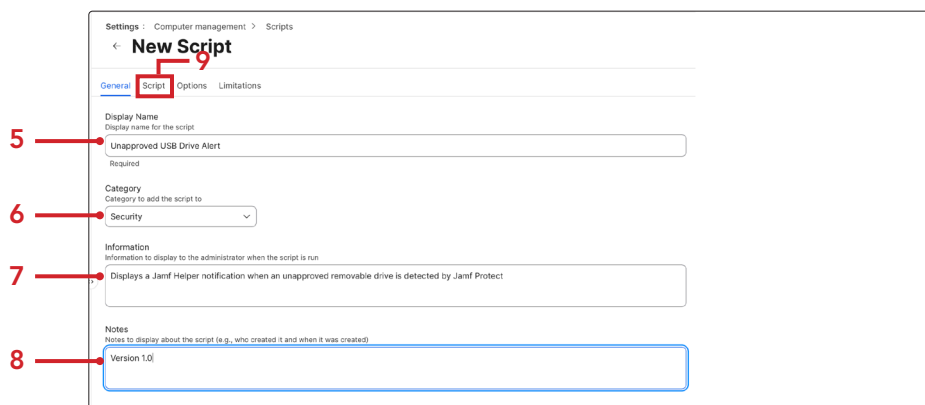
1. In Jamf Pro, click Settings (⚙️).
2. Enter scripts in the search field.
3. Click Scripts.



4. Click New (+).

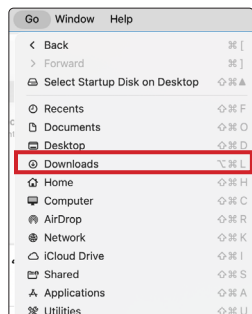


5. In the Display Name field, enter: **Unapproved USB Drive Alert**.
6. Click the Category menu and select Security.
7. In the Information field, enter: **Displays a Jamf Helper notification when an unapproved removable drive is detected by Jamf Protect.**
8. In the Notes field, enter: **Version 1.0.**
9. Click Script.

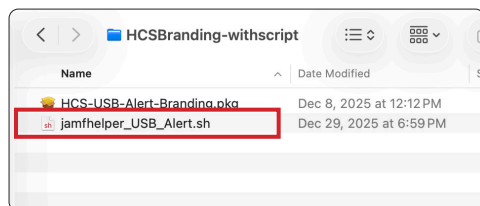




10. In the Finder, go to the Go menu and select Downloads.



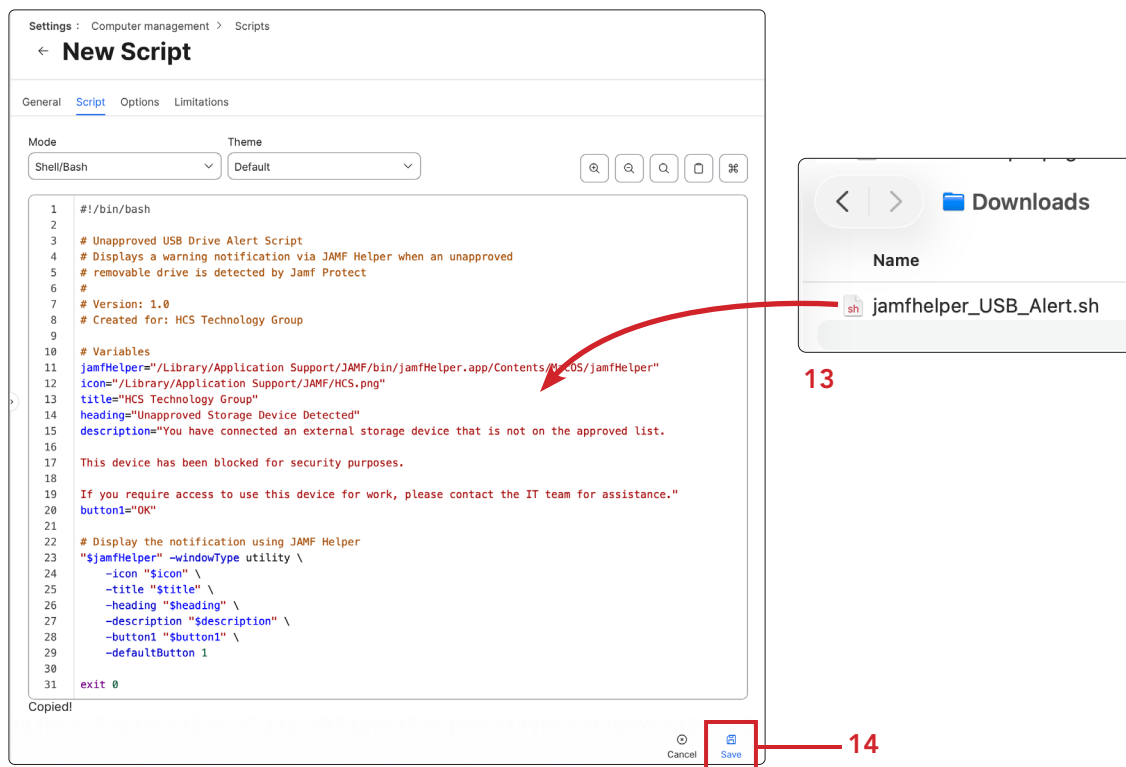
11. Locate the script, jamfhelper_USB_Alert.sh inside the folder, HCSBranding-withscript.



12. Go back to your Jamf Pro.

13. Drag and drop jamfhelper_USB_Alert.sh into the script field:

14. Click Save.



This completes this section.



Section 4: Jamf Pro - Configure Analytic Remediation

What You'll Need

Hardware and Software

Requirements for following along with this section:

- A Jamf Pro server with version 11.23 or later
- Administrator privileges to your Jamf Pro console
- The Unapproved USB Drive Alert script from Section 3

In this section, you will create an Extension Attribute, Smart Computer Group, and Remediation Policy that allow Jamf Protect to trigger the Jamf Helper notification.

Understanding the Identifier

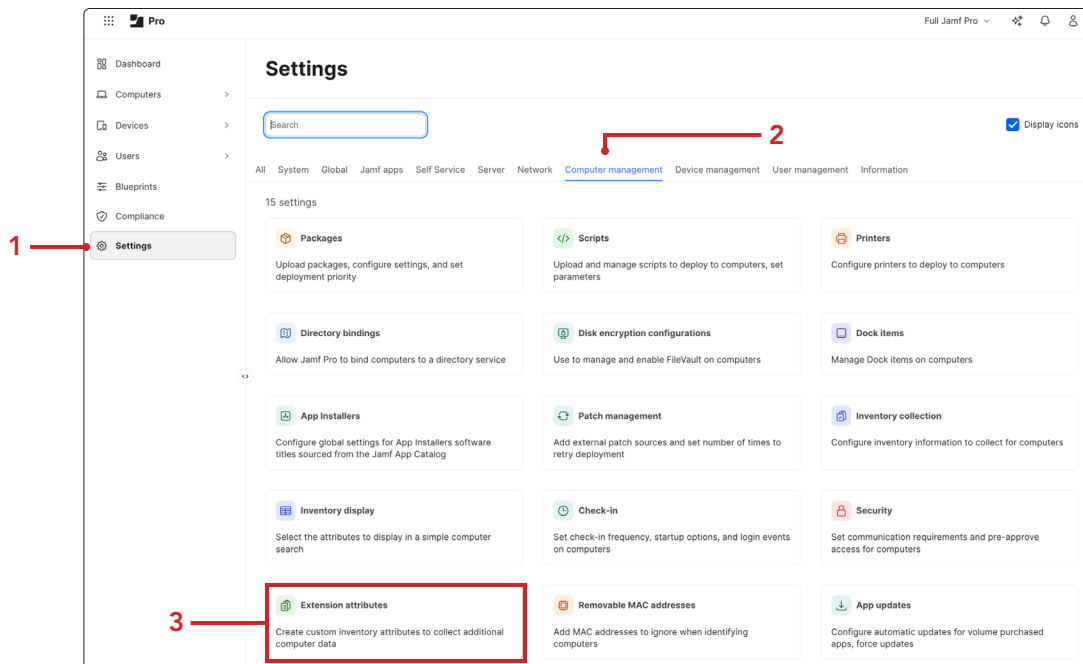
The Analytic Remediation workflow uses a custom identifier to link Jamf Protect and Jamf Pro. When Jamf Protect detects an unapproved USB disk:

- Jamf Protect writes the identifier to the computer at /Library/Application Support/JamfProtect/groups/
- The Extension Attribute collects the identifier during inventory
- The Smart Group matches computers with that identifier
- Policies scoped to the Smart Group execute

You define this identifier yourself. This guide uses "unapproved_usb" but you can name it anything meaningful to your organization (e.g., "usb_violation", "blocked_device"). The identifier must match exactly in both Jamf Pro and Jamf Protect.

Create the Extension Attribute

1. In Jamf Pro, click Settings (⚙️).
2. Click Computer Management.
3. Click Extension Attributes.





4. Click New From Template.

Settings : Computer management

← **Extension attributes**

+ New **New from template** Upload

5. In the search field, enter: **Jamf Protect**

6. Click Jamf Protect Smart Groups in the results.

Settings : Computer management

← **Extension attributes**

5 × 1 1 - 8 of 8

NAME	CATEGORY
Jamf Protect - Binary Version	Jamf Applications
Jamf Protect - Last Check-in	Jamf Applications
Jamf Protect - Last Insights Check-in	Jamf Applications
Jamf Protect - Plan Hash	Jamf Applications
Jamf Protect - Plan ID	Jamf Applications
6 Jamf Protect - Smart Groups	Jamf Applications
Jamf Protect - Tenant	Jamf Applications
Jamf Protect - Threat Prevention Version	Jamf Applications

7. Click Save.

Settings : Computer management > Extension attributes

← **Jamf Protect - Smart Groups**

☒ Enable (script input type only)

Display Name
Display name for the extension attribute

Required

Description
Description for the extension attribute

Data type
Type of the data being collected
String

Inventory display
Category in which to display the extension attribute in Jamf Pro
General

Input type
Input type to use to populate the extension attribute
Script

Script
Mode: Shell/Bash Theme: Default

```
1 #!/bin/bash
2
3 SMARTGROUPS_DIR=/Library/Application\ Support/JamfProtect/groups
4 if [ -d "$SMARTGROUPS_DIR" ]; then
5     SMART_GROUPS="/bin/ls "$SMARTGROUPS_DIR" | tr '\n' ','
6     echo "<result>${SMART_GROUPS?}</result>"
7 else
8     echo "<result></result>"
9 fi
10
11 exit 0
```

Cancel **Save**



Create a Smart Computer Group

8. In Jamf Pro, click Computers (🖥️) in the sidebar.

9. Click Smart Computer Groups.

10. Click New (+).

The screenshot shows the Jamf Pro interface. On the left sidebar, the 'Computers' icon is highlighted with a red callout 8. Below it, the 'Smart Computer Groups' link is highlighted with a red callout 9. On the right, the 'Smart Computer Groups' table is displayed. The table has columns for NAME, DESCRIPTION, and COUNT. The table contains the following data:

NAME	DESCRIPTION	COUNT
All Managed Clients		3
All Managed Servers		0
Macs with Less than 50% Space left		3
My Macs		1
SentinelOne Installed		2

The '+ New' button is highlighted with a red callout 10.

11. In the Display Name field, enter: Unapproved USB Detected.

12. Click Criteria.

The screenshot shows the 'New Smart Computer Group' form. The 'Computer Group' tab is selected, and the 'Criteria' tab is highlighted with a red callout 12. The 'Display Name' field is highlighted with a red callout 11 and contains the text 'Unapproved USB Detected'. The 'Description' field is empty. The 'Send email notification on membership change' checkbox is unchecked. The 'Site' dropdown menu is set to 'None'.



13. Click Add (+).

Computers : Smart Computer Groups

← **New Smart Computer Group**

Computer Group [Criteria](#)

AND/OR	CRITERIA	OPERATOR	VALUE
No Criteria Specified			

+ Add

14. Click Show Advanced Criteria.

15. Scroll down to Jamf Protect - Smart Groups.

16. Click Choose.

Computers : Smart Computer Groups

← **New Smart Computer Group**

Computer Group [Criteria](#)

FileVault 2 User	Choose
FileVault Status	Choose
Firewall Enabled	Choose
Full Name	Choose
Gatekeeper	Choose
Here file AdminOn Demand	Choose
IP Address	Choose
iTunes Store Account	Choose
Jamf Binary Version	Choose
Jamf Protect - Smart Groups	Choose

17. Click the Operator dropdown and select like.

18. In the Value field, enter: `unapproved_usb`

Computers : Smart Computer Groups

← **Unapproved USB Detected**

Computer Group [Criteria](#) Reports

AND/OR	CRITERIA	OPERATOR	VALUE
	Jamf Protect - Smart Groups	like	unapproved_usb

+ Add

NOTE: The value "unapproved_usb" is a custom identifier that YOU define. You can name it anything meaningful to your organization (e.g., "usb_violation", "blocked_device"). This value must match exactly the Identifier you will enter in Jamf Protect in Section 6.

19. Click Save.

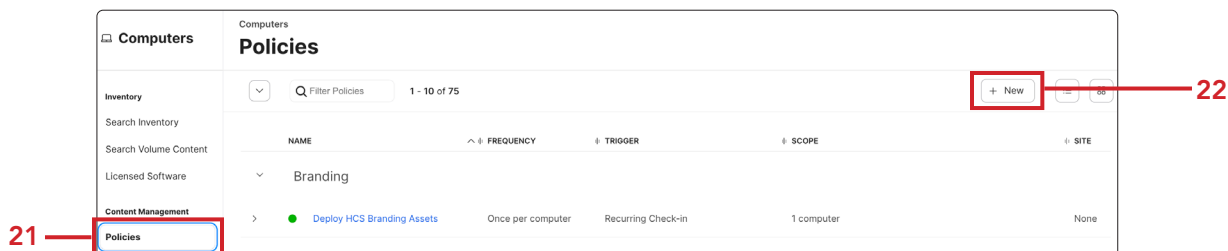


Create the Remediation Policy

20. In Jamf Pro, click Computers in the sidebar.

21. Click Policies.

22. Click New (+).



23. In the Display Name field, enter: **Alert - Unapproved USB Drive**

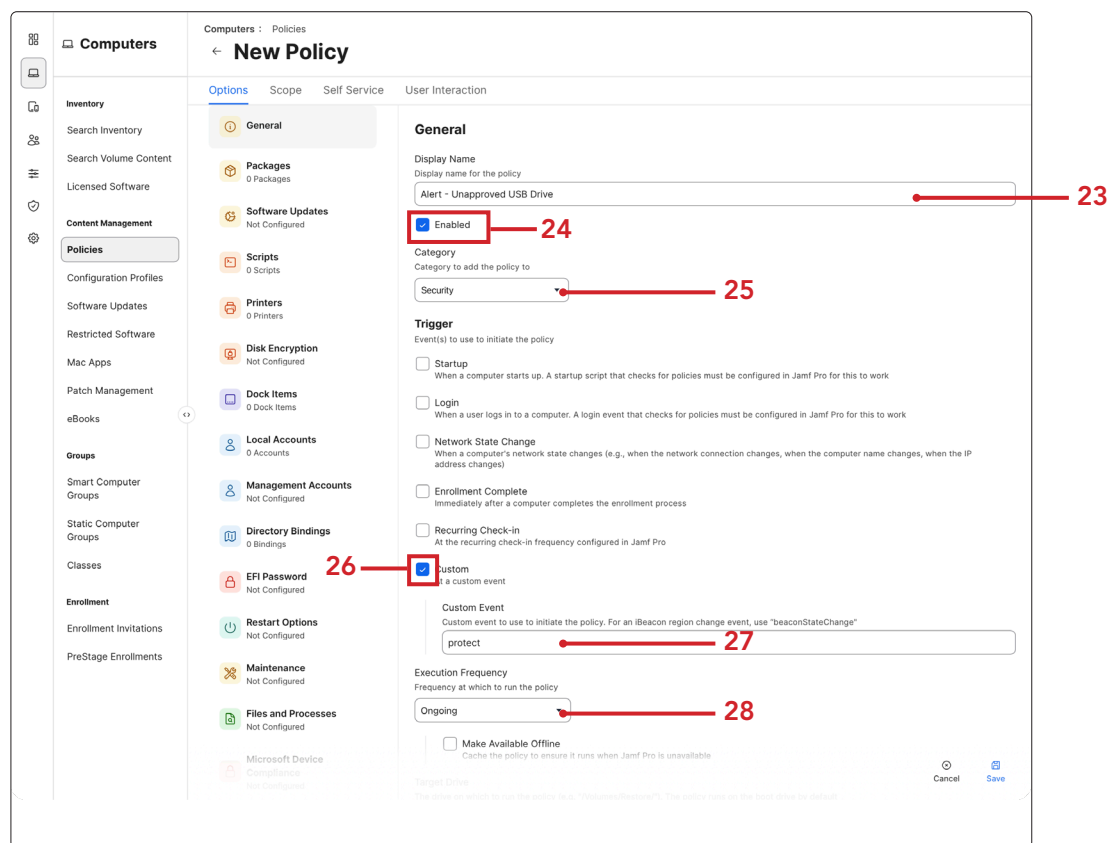
24. Verify Enabled is selected.

25. Select Security for the Category.

26. Select the checkbox for Custom.

27. Enter **protect** in the Custom Event field.

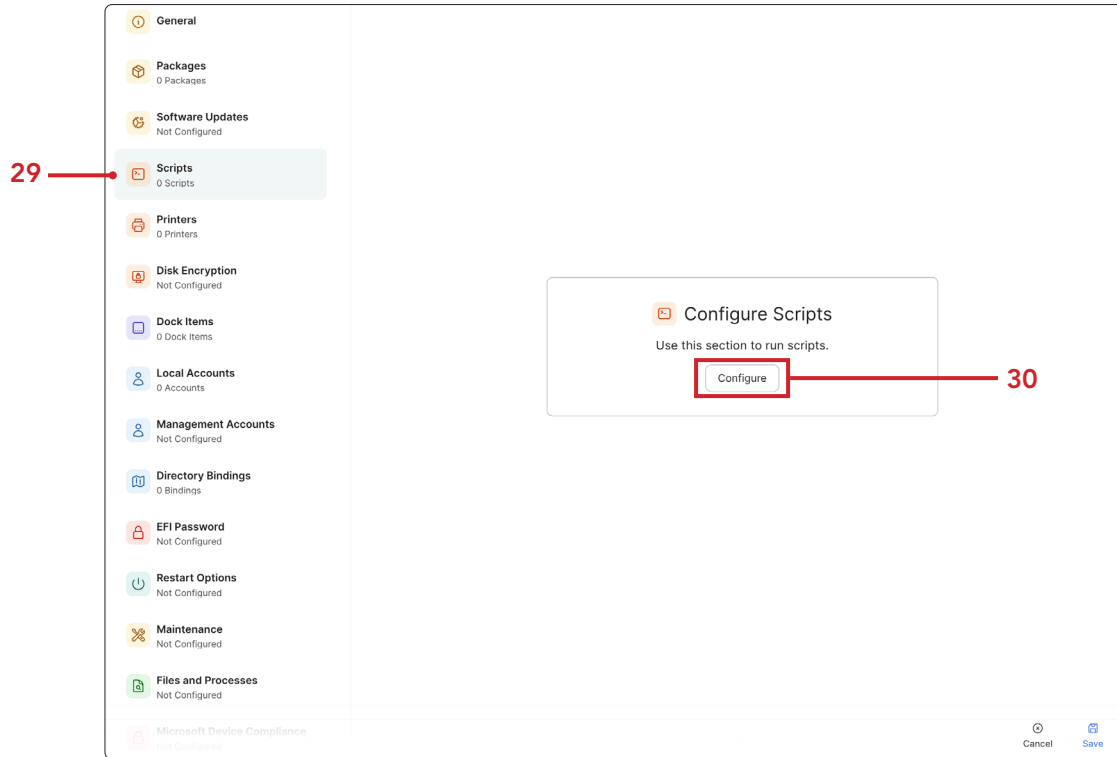
28. Click the Execution Frequency dropdown and select Ongoing.





29. In the payload sidebar, click Scripts.

30. Click Configure.



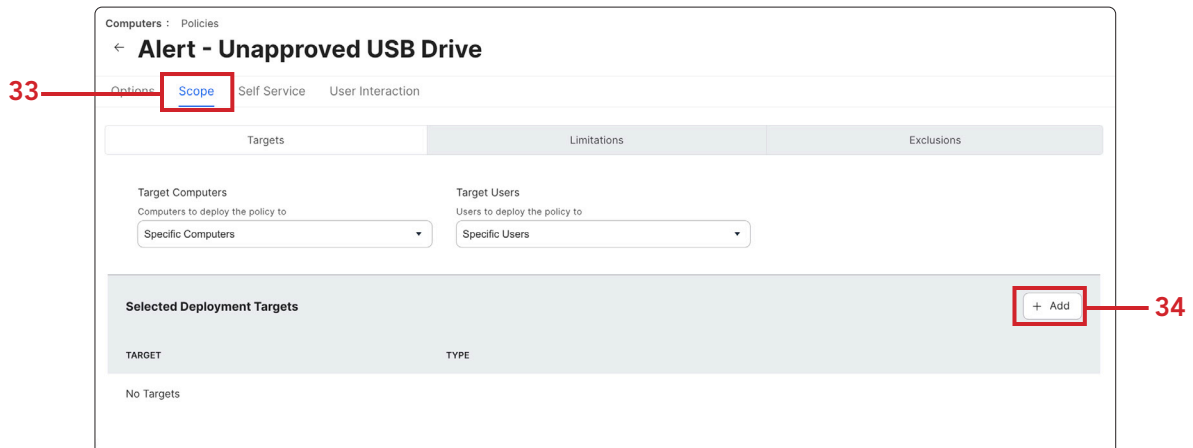
31. Locate the "Unapproved USB Drive Alert" script in the list.

32. Click Add next to "Unapproved USB Drive Alert".



33. Click Scope.

34. Click Add (+).





35. Click Computer Groups.

Computers : Policies

← **Alert - Unapproved USB Drive**

Options Scope Self Service User Interaction

Targets Limitations Exclusions

Add Deployment Targets Done

Computers **Computer Groups** Users User Groups Buildings Departments

Filter results 1 - 10 of 90

GROUP NAME

All Managed Clients	Add
anyorg_it does exist	Add
Macs running macOS 14.5 or later	Add
User is an Admin account settings are dimmed	Add
User is an admin	Add
Computers that are enrolled - Application Install	Add
TESTDATA_2ec1d570_Static_Group_1	Add
TESTDATA_2ec1d570_Static_Group_2	Add
TESTDATA_2ec1d570_Static_Group_3	Add
TESTDATA_2ec1d570_Static_Group_4	Add

36. Search for Unapproved USB Detected.

37. Click Add.

38. Done

Computers : Policies

← **Alert - Unapproved USB Drive**

Options Scope Self Service User Interaction

Targets Limitations Exclusions

Add Deployment Targets Done

Computers Computer Groups Users User Groups Buildings Departments

36 1 - 1 of 1

GROUP NAME

Unapproved USB Detected	37 Add
-------------------------	----------------------------------

39. Click Save.

This completes this section.



Section 5: Jamf Protect - Create a Removable Storage Control Set

What You'll Need

Hardware and Software

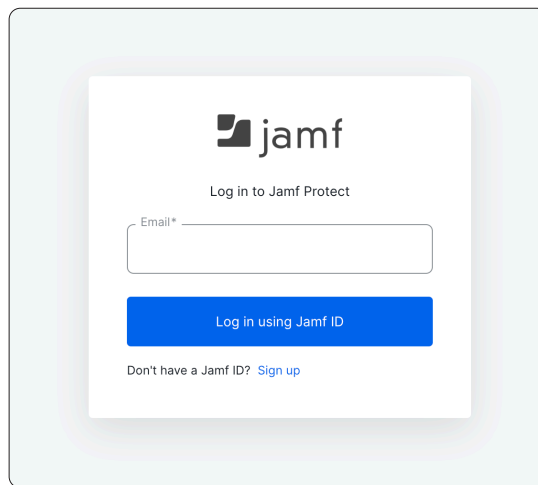
Requirements for following along with this section:

- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)
- The Vendor and Product ID's of your USB disks that you saved in Section 1 of this guide.

In this section, you will configure Jamf Protect to monitor and control USB and external drive connections. You will create a Removable Storage Control Set and add your approved devices as overrides.

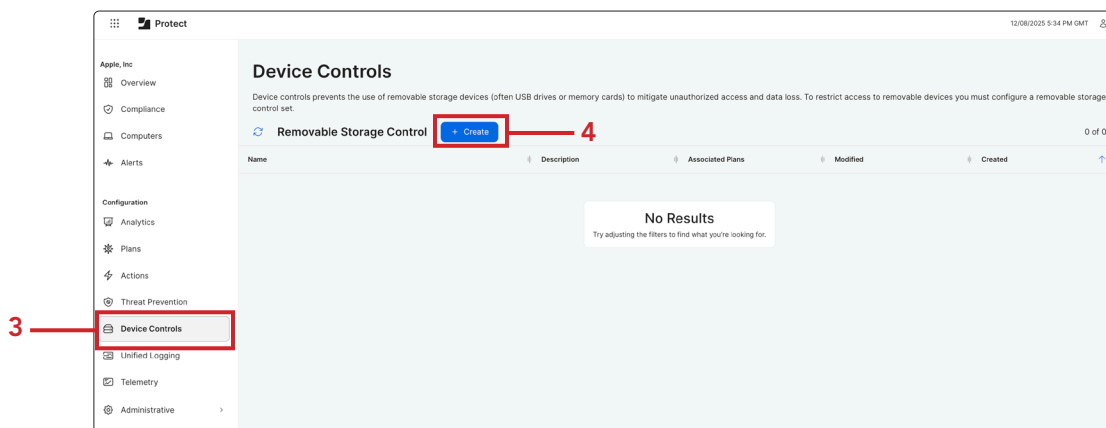
Access Jamf Protect

1. Open a web browser and navigate to your macOS Security portal (Jamf Protect web app) URL.
2. Log in with your administrator credentials.



Create a Removable Storage Control Set

3. In the left sidebar, click Device Controls.
4. Click Create.





5. In the Name field, enter: **USB Drive Control Set**.
6. In the Description field, enter: **Blocks unauthorized USB devices from mounting while allowing Read-Only access to approved devices.**
7. Verify that Default Permission is set to Prevent.
NOTE: The Prevent permission blocks unapproved devices from mounting. Read Only allows reading but not writing. Read and Write allows full access.

Add Approved Device Overrides

8. Scroll down to the Total Overrides section.
9. Under Total Overrides, click Add (+).

Device Controls / Create

Create Removable Storage Control Set

Save

Name: USB Drive Control Set

Description: Blocks unauthorized USB devices from mounting while allowing Read-Only access to approved devices.

Default Permission: Prevent

Default Local Notification Message: Enter a notification displayed to users when a removable storage device is restricted. This removable storage device is not allowed.

Total Overrides (0) + Add

10. Under the Removable Storage Override Type, click the menu and select Product ID.
11. Click Add (+).

Removable Storage Override Type

Encrypted Devices

An identifier used to target removable storage devices and override default settings

Encrypted Devices

Vendor ID

Serial Number

Product ID

Details

Cancel + Add



12. Navigate to the Product ID Override Details section, under Product ID Overrides, click Add (+).

13. In the Vendor ID field, enter the Vendor ID from Section 1 (e.g., 0x5583).

14. In the Product ID field, enter the Product ID from Section 1 (e.g., 0x0781).

15. Click Add.



16. Under Product ID Override Details click the Permission menu and select Read and Write.
NOTE: Select Read and Write to allow approved devices full access. Select Read Only if you want to allow reading but prevent writing to the device.
17. Click Save.

Device Controls / **Removable Storage Control Set**

← USB Drive Control Set **Save** —17 Delete

Name: USB Drive Control Set

Default Permission: Prevent

Description: Blocks unauthorized USB devices from mounting while allowing Read-Only access to approved devices.

Default Local Notification Message: Enter a notification displayed to users when a removable storage device is restricted. This removable storage device is not allowed.

Total Overrides (1) + Add

Type	Permission	Apply to
Product ID	Read and Write	All

1 added Product IDs

Product ID Override Details

Permission: Read and Write Apply to: All —16

Product ID Overrides

Search... Export Upload CSV + Add Delete 1 ...

Vendor ID	Product ID
<input type="checkbox"/> 0x04e8	<input type="checkbox"/> 0x6300

18. Repeat steps 10-15 for each additional approved drive.

This completes this section.



Section 6: Jamf Protect - Create an Analytic Set

What You'll Need

Hardware and Software

Requirements for following along with this section:

- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)

In this section, you will create a Custom Analytic that detects unapproved USB devices and triggers the Jamf Pro Smart Group.

How This Connects to Jamf Pro

In Section 4, you created the following in Jamf Pro:

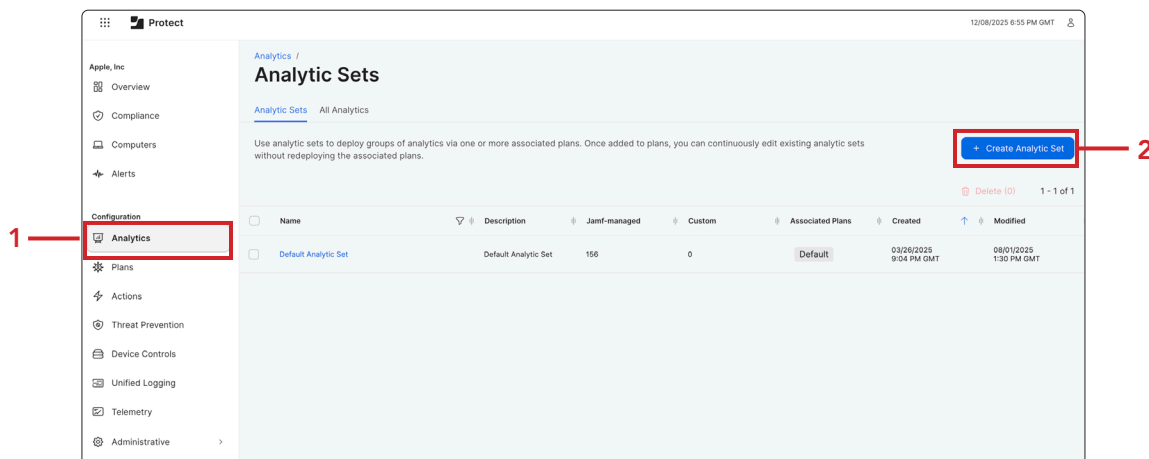
- Extension Attribute: Jamf Protect Alerts - collects identifiers written by Jamf Protect
- Smart Computer Group: Unapproved USB Detected - matches computers with the identifier "unapproved_usb"
- Policy: Alert - Unapproved USB Drive - runs the notification script when computers join the Smart Group

Now in the macOS Security portal (Jamf Protect web app), you will configure the Analytic to write the identifier "unapproved_usb" to computers when an unapproved USB drive is detected. This creates the link between the two systems:

- Unapproved USB drive Inserted
- Jamf Protect writes identifier "unapproved_usb" to computer
- Extension Attribute collects identifier during inventory
- Computer joins "Unapproved USB Detected" Smart Group
- Policy runs and displays Jamf Helper notification

Create an Analytic Set

1. In the macOS Security portal (Jamf Protect web app), click Analytics in the left sidebar.
2. Click Create Analytic Set.





3. In the Name field, enter: **Unapproved USB Drive Detected**.
4. In the Description field enter, Tracks and logs unapproved USB device detection events
5. Click Save.
6. Click Analytics.

6 — **Analytics** / Analytic Sets /

Create

← Create Analytic Set **Save** — 5

Name
Unapproved USB Drive Detected — 3

Description
Tracks and logs unapproved USB device detection events. — 4

Analytics in this set

Jamf-managed (0) Custom (0)

Search all... Group by: Category 1 - 156 of 156

<input type="checkbox"/>	Name	Description	Severity	Smart Group	Category	Created	Modified
<input type="checkbox"/>	Living Off the Land (13) 0 selected		8	5			
<input type="checkbox"/>	Reverse Shell Perl (Deprecated)	Reverse shell creation ...	3		Living Off the Land	03/26/2025 8:17 PM GMT	05/06/2025 4:14 PM GMT
<input type="checkbox"/>	Cat Piped to NC	Reverse shell creation ...	3		Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT
<input type="checkbox"/>	Reverse Shell Generic (Deprecated)	Reverse shell creation ...	3		Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT
<input type="checkbox"/>	Reverse Shell Netcat	Reverse shell creation ...	3		Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT
<input type="checkbox"/>	Reverse Shell PHP (Deprecated)	Reverse shell creation ...	3		Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT

Create the Custom Analytic

7. Click Create Custom Analytic.

Analytics

Analytic Sets / All Analytics

Analytics detect suspicious user behavior and system activity. Jamf-managed analytics and categories are maintained by Jamf. Create custom analytics to detect activity specific to your security needs. To deploy analytics, add individual analytics to one or more analytic sets, and then add each analytic set to one or more plans.

Jamf-managed Custom

Search all... Group by: Category 1 - 156 of 156

>	Name	Description	Severity	Tags	Smart Group	Category	Created	Modified
>	Living Off the Land (13)		8	5				
>	System Visibility (13)		1	2	10			
>	Known Malicious File (66)		58	8				
>	Persistence (15)		2	13				
>	Credential Harvesting (3)		1	2				
>	Common Attacker Technique (13)		3	8	1	1		
>	Evasion (11)		3	7	1			
>	System Tampering (8)		2	1	2	3		
>	Apple Security (4)		1	1	2			
>	Privilege Escalation (5)		4	1				



8. In the Name field, enter: **Unauthorized USB Inserted**
9. Under Categories, select System Visibility.
10. In the Description field, enter: **Detects when an unapproved removable USB storage device is inserted. Approved vendors are excluded from triggering this analytic.**
11. Set Severity to High.
12. For Sensor Type, select USB Event.
13. Under Analytic Filter, select Filter Text View and enter the following:
`$event.type == 0 AND $event.device.removable == 1 AND $event.device.writable == 1 AND $event.device.vendorName != "Samsung"`

The screenshot shows the 'Create Analytic' form in the Jamf Protect interface. Red callout numbers 8 through 13 point to specific fields:

- 8:** Points to the 'Analytic Name' field, which contains 'Unauthorized USB Device'.
- 9:** Points to the 'Categories' dropdown menu, which is set to 'System Visibility'.
- 10:** Points to the 'Description' text area, which contains the text: 'Detects when an unapproved removable USB storage device is inserted. Approved vendors are excluded from triggering this analytic.'
- 11:** Points to the 'Severity' dropdown menu, which is set to 'High'.
- 12:** Points to the 'Sensor Type' dropdown menu, which is set to 'USB Event'.
- 13:** Points to the 'Filter' text area, which contains the predicate: '\$event.type == 0 AND \$event.device.removable == 1 AND \$event.device.writable == 1 AND \$event.device.vendorName != "Samsung"'. The 'Filter Text View' tab is selected.

NOTE: Replace "Samsung" with your approved manufacturer name. To find the manufacturer name, connect the approved USB device to a Mac and check System Information > Hardware > USB. Use the exact manufacturer name string shown there. To add multiple approved vendors, extend the predicate with additional AND statements. For example:

```
$event.type == 0 AND $event.device.removable == 1 AND $event.device.writable == 1 AND $event.device.vendorName != "Samsung" AND $event.device.vendorName != "SanDisk"
```

NOTE: For more granular control, you can also filter by product name. See Jamf Protect documentation for additional predicate options.

https://learn.jamf.com/en-US/bundle/jamf-protect-documentation/page/Creating_Analytics.html

Understanding the Predicate

The predicate uses NSPredicate syntax to filter USB events:

- `$event.type == 0`: Matches insertion events only
- `$event.device.removable == 1`: Matches removable devices
- `$event.device.writable == 1`: Matches writable devices
- `$event.device.vendorName != "Samsung"`: Excludes devices from Samsung

This combination ensures the analytic only triggers when an unapproved, removable, writable USB device is inserted.



Configure Analytic Actions

14. Select the checkbox for Add to Jamf Pro Smart Group.

15. In the Identifier field, enter: **unapproved_usb**

NOTE: This identifier MUST match exactly the Value you entered in the Smart Group criteria in Section 4, Step 20. If these do not match, the workflow will not function.

14

15

The screenshot shows a form titled 'Analytic Actions'. It has a checkbox labeled 'Add to Jamf Pro Smart Group' which is checked. Below it is a text field labeled 'Identifier' with the placeholder text 'This value must match a pre-configured Jamf Pro extension attribute.' and the value 'unapproved_usb'. There is also a 'Tags' section with a dropdown menu labeled 'Select value'. Below the 'Analytic Actions' section are two sections: 'Analytic Context Items' with a '+ Add Context Item' button, and 'Snapshot Files' with a '+ Add Snapshot File' button.

16. Click Save.

The screenshot shows a 'Create' page for an analytic. At the top, there is a 'Create Analytic' button and a 'Save' button. Below this is the 'Analytic Description' section, which includes an 'Analytic Name' field with the value 'Unapproved USB Device' and a 'Level' field with the value '0'. There is also a 'Categories' section at the bottom.



Add the Custom Analytic to the Analytic Set

17. Click Analytics.

18. Click Analytics Sets

19. Click the Unapproved USB Detected analytic set.

20. Under Analytics in this set, click Custom.

21. In the search field, enter: **Unauthorized USB**.

22. Click the disclosure triangle next to System Visibility (1).

23. Select the checkbox next to the custom analytic you created.

24. Click Save.

Analytics / Analytic Sets /

Analytic Set

← Unapproved USB Detected **Save** 24 Clone Delete

Name: Unapproved USB Detected Associated Plans: USB Drive Control Plan

Description:

Analytics in this set

Jamf-managed (0) **Custom (1)** 20

21 Unauthorized USB Group by: Category 1 - 156 of 1

	Name	Description	Severity	Smart Group	Category	Created	Modified
22	System Visibility (1) 1 selected						
23	<input checked="" type="checkbox"/> Unauthorized USB				System Visibility	12/09/2025 12:06 AM GMT	12/09/2025 12:06 AM GMT

For this guide we will not be using tags

NOTE: Tags help you connect different security rules together, like building blocks that work as a team. Click the link below to learn more about tags.

https://learn.jamf.com/en-US/bundle/jamf-protect-documentation/page/Analytic_Chains.html

Related Documentation

- Jamf Protect Documentation: Prohibited USB Insertion Detections
https://learn.jamf.com/en-US/bundle/jamf-trusted-access-solution-guide-business/page/trustedAccess_macOSDeviceControls.html
- Jamf Protect Documentation: Creating Analytics
https://learn.jamf.com/en-US/bundle/jamf-protect-documentation/page/Creating_Analytic_Sets.html
- Jamf Protect GitHub Repository: <https://github.com/jamf/jamfprotect>
Contains custom analytic predicates and examples, including USB detection samples

This completes this section.



Section 7: Jamf Protect - Create and Configure the Plan

What You'll Need

Hardware and Software

Requirements for following along with this section:

- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)
- The USB Drive Control Set from Section 5
- The Unapproved USB Detected Analytic Set from Section 6

In this section, you will create a Jamf Protect Plan and assign the Removable Storage Control Set and Analytic Set to it. Plans are used to deploy configurations to your managed computers.

How This Connects Everything

The Plan brings together everything you have configured:

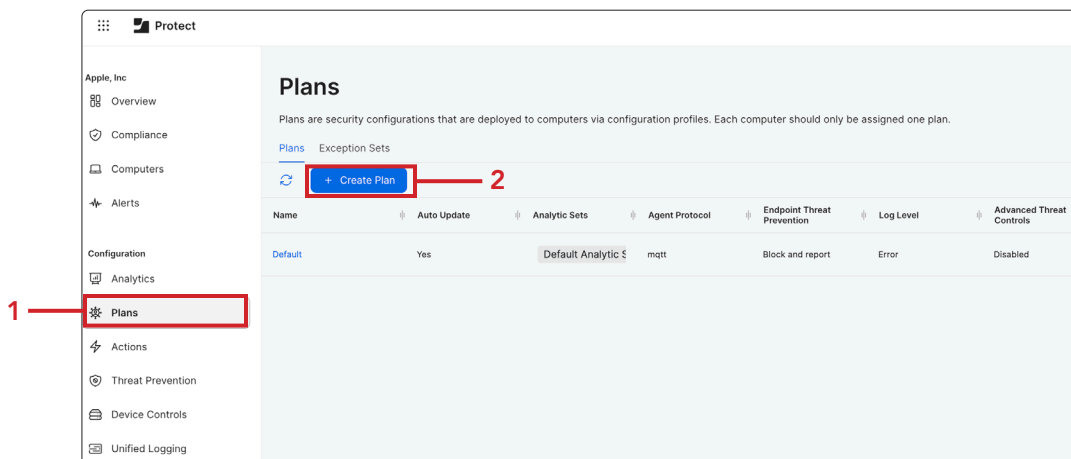
- USB Drive Control Set (Section 5): Blocks unapproved devices, allows approved devices
- Unapproved USB Detected Analytic Set (Section 6): Detects USB insertions and triggers Jamf Pro workflow

When you assign both to a Plan, computers receiving the Plan will:

1. Block unapproved USB devices from mounting (Control Set)
2. Trigger the Jamf Helper notification via Jamf Pro (Analytic Set)

Create a Plan

1. In the macOS Security portal (Jamf Protect web app), click Plans.
2. Click Create Plan.





3. In the Name field, enter: **USB Drive Control Plan**.
4. In the Description field, enter: **Prevent unauthorized USB drive usage and data loss**.
5. Under Threat Preventions, we are using the default settings.
6. Scroll down to the Analytics sets and select Unapproved USB Detected.
7. Select None for Telemetry.
8. Scroll down to Device Controls.
9. Click the dropdown menu and select USB Drive Control Set.
10. Click Save.

The screenshot shows the 'Create Plan' interface with the following elements and annotations:

- 10**: Points to the **Save** button at the top right of the 'Create Plan' section.
- 3**: Points to the **Name** field, which contains 'USB Drive Control Plan'.
- 4**: Points to the **Description** field, which contains 'Prevent unauthorized USB drive usage and data loss'.
- 6**: Points to the **Analytic sets** dropdown menu, which is set to 'Unapproved USB Detected'.
- 7**: Points to the **Telemetry configuration** dropdown menu, which is set to 'None'.
- 9**: Points to the **Control set** dropdown menu, which is set to 'USB Drive Control Set'.

The interface includes sections for **General**, **Threat Prevention** (with sub-sections for Endpoint Threat Prevention, Tamper Prevention, and Advanced Threat Controls), **Analytic sets**, **Telemetry**, and **Device Controls**.

This completes this section.



Section 8: Jamf Protect - Configure Email Notifications

What You'll Need

Hardware and Software

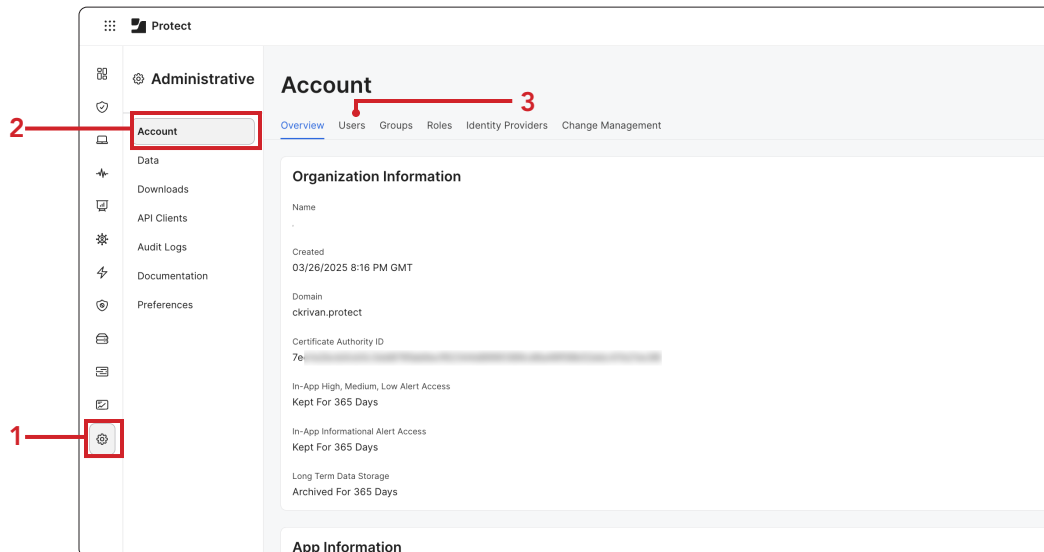
Requirements for following along with this section:

- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)
- A Jamf Protect user account for the IT team member who should receive alerts

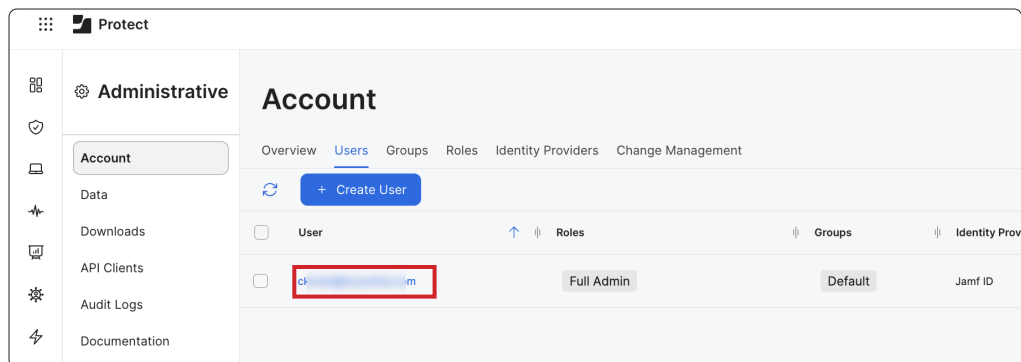
In this section, you will configure Jamf Protect to send email notifications to your IT team when security alerts are generated. Email notifications are enabled per user in Jamf Protect.

Enable Email Notifications for IT Users

1. In Jamf Protect, click Administrative (⚙️).
2. Click Account.
3. Click Users.



4. Click on the user account that should receive email alerts.





5. Locate the Send Email Notifications checkbox.
6. Select the checkbox for Send Email Notifications.
7. Change Email Severity to High.
8. Click Save.

A screenshot of the 'Account' page in the Jamf Protect interface. The page has a header with tabs: Overview, Users, Groups, Roles, Identity Providers, and Change Management. Below the header, there's a user profile section with fields for Email, Last Login, Origin, and Identity Provider. A red box labeled '8' highlights the 'Save' button. Below the profile section, there are sections for Groups, Roles, and Email Notifications. A red box labeled '6' highlights the 'Send Email Notifications' checkbox, which is checked. Below that, a red box labeled '7' highlights the 'Email Severity' dropdown menu, which is set to 'High'. The page also includes a 'Delete' button in the top right corner and an 'Add Group' dropdown in the Groups section.

9. Repeat steps 2-5 for each IT team member who should receive alerts.
NOTE: When enabled, users will receive email notifications for all alerts generated in Jamf Protect, including removable storage violations. The email will include details about the alert, the affected computer, and the user.

This completes this section.



Section 9: Jamf Protect - Assign Plan to Computers

What You'll Need

Hardware and Software

Requirements for following along with this section:

- Jamf Pro server with the Jamf Protect integration configured
- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)
- The USB Drive Control Plan fully configured from Sections 5-8
- Target computers or computer groups to receive the plan

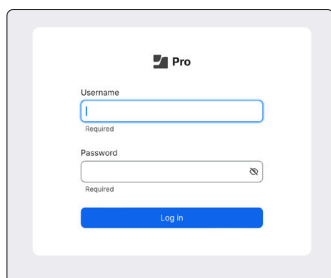
In this section, you will deploy the USB Drive Control Plan to your target computers. Plan assignments are configured in Jamf Pro through the Jamf Protect integration. Once assigned, computers will receive the plan and begin enforcing the USB drive restrictions.

How Plan Assignment Works

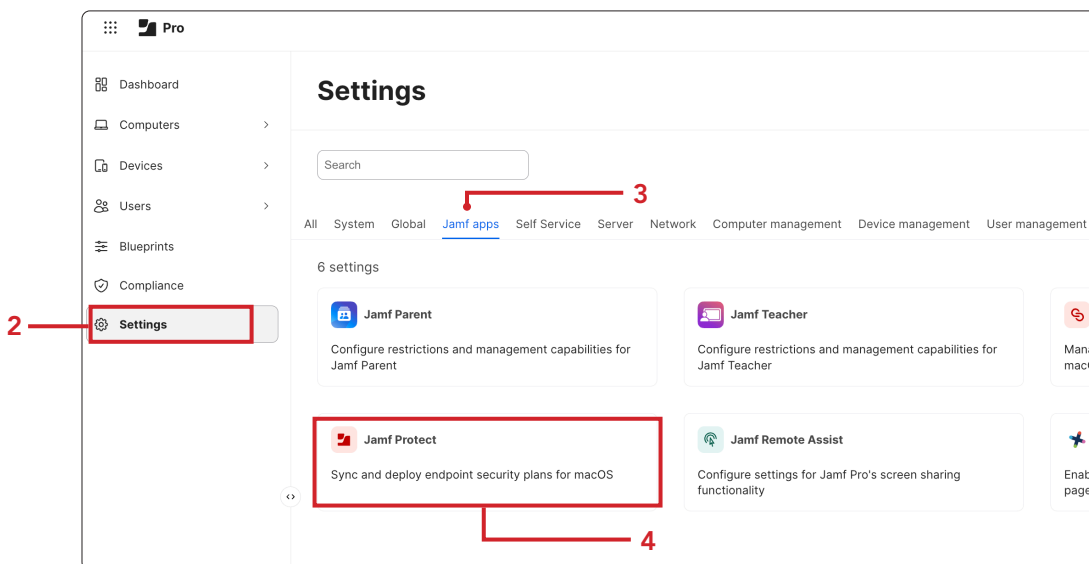
Jamf Protect plans are assigned to computers through Jamf Pro, not directly in the macOS Security portal (Jamf Protect web app). This allows you to use your existing Jamf Pro computer groups and scoping logic to determine which computers receive each plan.

Assign the Plan in Jamf Pro

1. Log in to your Jamf Pro server.



2. Click the Settings (⚙️).
3. Click Jamf apps.
4. Click Jamf Protect.





5. Verify that your Jamf Protect integration is connected (a shows a successful connection.)
6. Scroll down to the Plans section.
7. Locate your USB Drive Control Plan in the list. If you do not see your plan, click Sync
8. Click on the plan.

Settings : Jamf Apps

← Jamf Protect

Jamf Protect Registration

Jamf Pro is allowed to access your Jamf Protect tenant at ckriyan.protect.jamfcloud.com

Edit Registration

Jamf Protect Deployment

The Jamf Protect package to deploy to computers

☒ Automatically deploy the Jamf Protect PKG with plans Computers in scope of your plan configuration profiles will automatically install the Jamf Protect PKG

Jamf Protect Plans

List of plans created in Jamf Protect that can be deployed as configuration profiles with Jamf Pro

Sync Last synced: 12/08/2025 11:53 AM

Click on Sync if you do not see your plan.

Q Search filterable columns... ← 1 → 1 - 2 of 2

NAME	PROFILE	SCOPE	SITE	LOGS
USB Drive Control Plan	USB Drive Control Plan Plan - Jamf Pr...	No scope defined	None	View
Default	Default Plan - Jamf Protect Configura...	All computers	None	View

NOTE: Only one plan can be assigned per device. Verify that no conflicting plans are assigned before proceeding.

9. Click Edit.

Computers : Configuration Profiles

← USB Drive Control Plan Plan - Jamf Protect Configuration

Options Scope ☐ Show in Jamf Pro Dashboard

Q Search...

General

Application & Custom Settings
1 payload configured

Certificate
Payloads configured: 3

Managed Login Items
1 setting configured

Privacy Preferences Policy Control
1 payload configured

System Extensions
1 payload configured

Signed Profile
This profile is read-only because it is signed. [Remove Signature](#)

General

Name
Display name of the profile
USB Drive Control Plan Plan - Jamf Protect Configuration

Description
Brief explanation of the content or purpose of the profile

Site
Site to add the profile to
None

Category
Category to add the profile to
None

Level
Level at which to apply the profile
Computer Level

Distribution Method
Method to use for distributing the profile
Install automatically

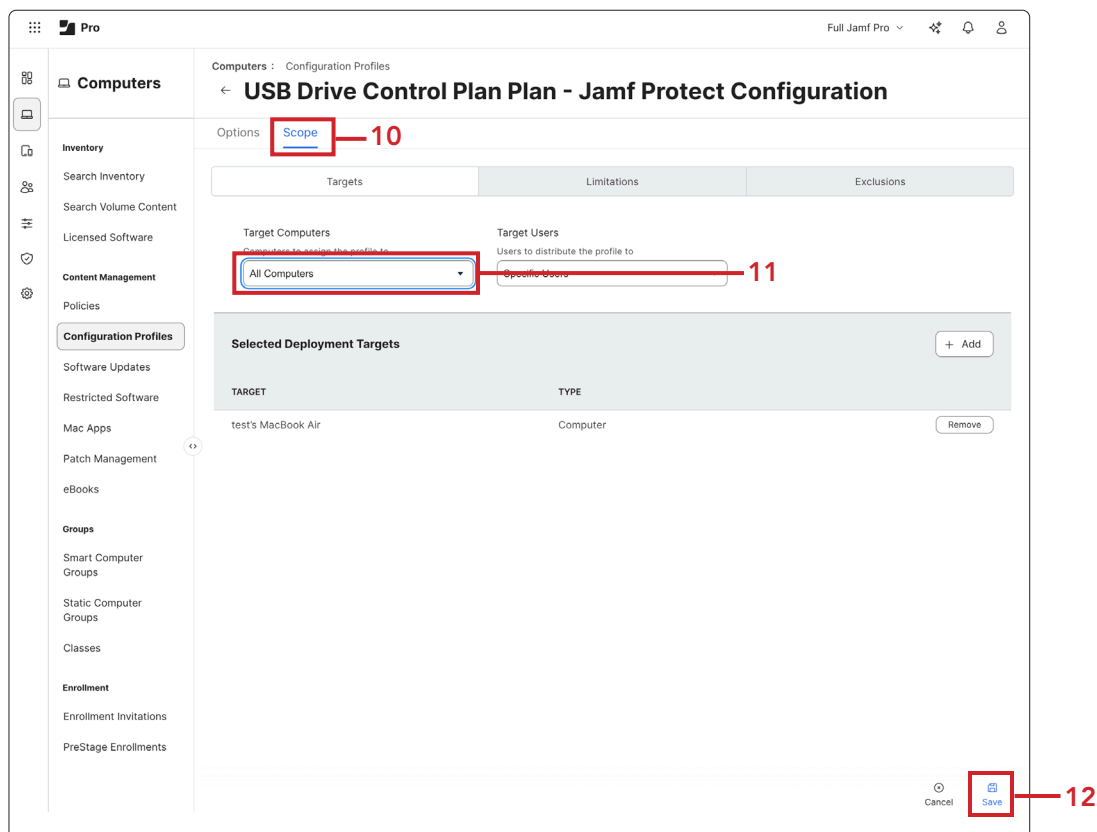
[History](#) [Logs](#) [Download](#) [Delete](#) [Edit](#)



10. Click Scope.

11. Click the Target Computers menu and scope to your needs. This guide will scope to All Computers.

12. Click Save.



NOTE: You can also scope the plan to specific Smart Computer Groups or individual computers based on your deployment needs. Computers will receive the plan configuration on their next check-in with Jamf Protect. This typically occurs within 15 minutes but can be up to 24 hours depending on your check-in configuration.



Verify Plan Assignment

13. In Jamf Protect, click Computers in the left sidebar.

14. Locate a computer that should have received the plan.

15. Click on the computer name

13

15

16. Click Computer Details.

Computer

test's MacBook Air

Computer Details

Version Status

Protect Version: Up to date

Threat Version: Up to date

macOS Version: Version 26.2.0

Compliance Baseline Status

Compliance Baseline Score: 55.0%

25 Fail

33 Pass

0 Disabled

Alerts

24 Hours 7 Days 30 Days

13 High

0 Medium

0 Low



17. Verify the USB Drive Control Plan is listed under the assigned plan.
NOTE: If you do not see your plan, go back to Jamf Protect and click the Sync button. On the test Mac computer, open Terminal and run the following command:
`sudo protectctl checkin`

This forces a Jamf Protect agent check-in on Mac computers.

The screenshot displays the 'Computer' details page in Jamf Protect for a device named 'test's MacBook Air'. The page is divided into several sections:

- Computer Status:** Shows 'Connection status' as 'Not connected in 11 minutes' and 'Not connected since' as '12/08/2025 11:25 PM GMT'.
- Computer Info:** Lists 'Model' as 'Mac14,15', 'Serial' as a redacted value, and 'Device ID' as '125...7c2'.
- Web Protection Status:** Shows 'Disabled' with a 'View Details' link.
- Architecture:** Lists 'arm64'.
- Memory:** Lists '8.0 GB'.
- Full Disk Access:** Shows 'Authorized'.
- Current Plan:** A red box highlights the 'USB Drive Control Plan' section, which includes:
 - Modified:** 12/08/2025 11:29 PM GMT
 - Created:** 12/08/2025 5:42 PM GMT
 - Hash:** c3...a7b90
 - Threat Prevention:**
 - Endpoint Threat Prevention: Block and report
 - Tamper Prevention: Block and report
 - Advanced Threat Controls: Disabled
 - Analytic sets: Unapproved USB Detected

This completes this section.



Section 10: Test the Configuration

What You'll Need

Hardware and Software

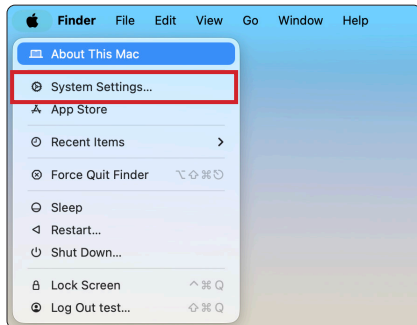
Requirements for following along with this section:

- A non-production Mac computer enrolled in Jamf Pro with Jamf Protect installed
- The USB Drive Control Plan assigned to the test computer (Section 9)
- An approved USB drive (matching a vendor in your custom analytic predicate)
- An unapproved USB drive (not matching any entries in your allowed list)

In this section, you will verify that the entire configuration works as expected. Testing should be performed on a non-production Mac computer before deploying to your entire fleet.

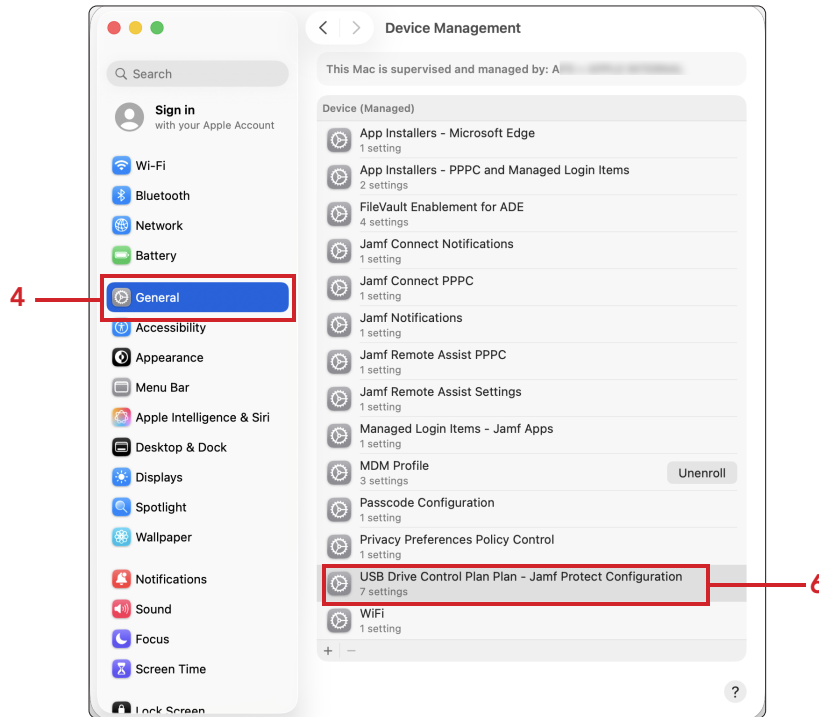
Verify the Plan is Applied

1. Go to a test Mac computer that is enrolled in Jamf Pro with Jamf Protect installed.
2. Click the Apple menu.
3. Click System Settings.





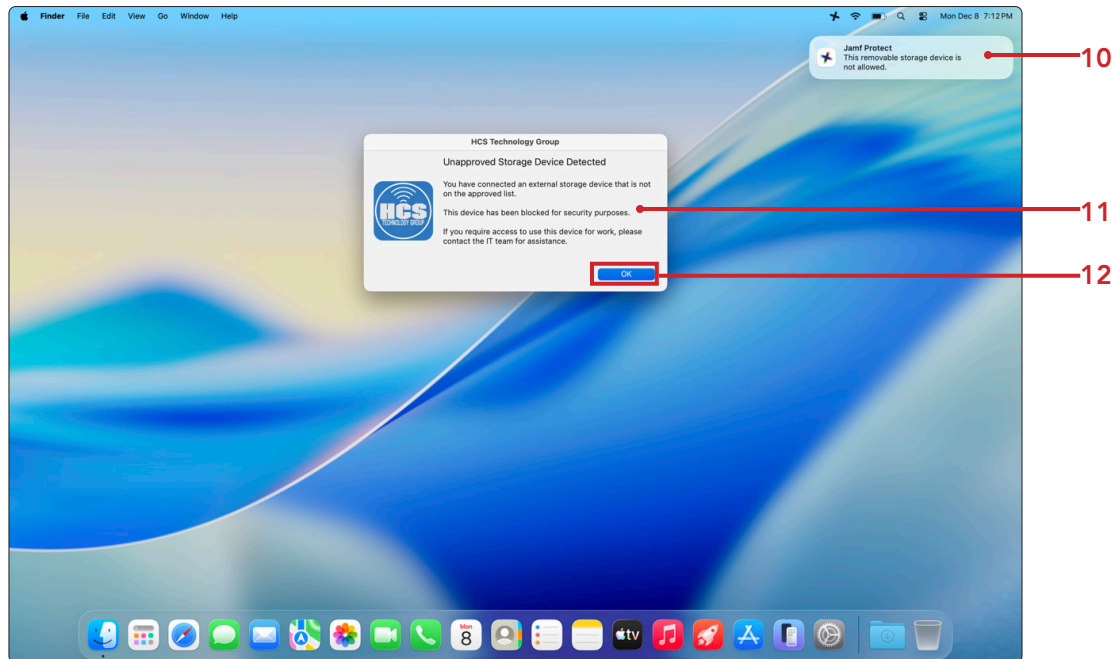
4. In the sidebar, click General.
5. Scroll down and click Device Management.
6. Verify the Jamf Protect configuration profile is installed. This is the plan from Jamf Protect.





Test with an Unapproved Drive

7. Connect an unapproved USB drive to the test Mac computer. Use a drive that does NOT match any vendor and product entries in your approved list.
8. Wait a few seconds for Jamf Protect to detect the device.
9. Verify the drive does NOT appear in Finder. The device should be blocked from mounting.
10. Verify a notification appears on the screen.
11. Verify the Jamf Helper pop-up displays:
 - The HCS logo
 - The heading: Unapproved Storage Device Detected
 - The message explaining the device is blocked
12. Click OK to dismiss the notification.





13. Open your IT team email inbox.
14. Locate the Jamf Protect alert email.
15. Verify the email contains details about the removable storage alert, including the affected computer and user information.

A screenshot of a Jamf Protect alert email. The header shows the Jamf Protect logo. Below it is a table with alert details.

jamf PROTECT	
Alert Description	USB device inserted
Alert Timestamp (UTC)	2025-12-08 23:42:17
Host Name	test's MacBook Air
Alert Link	Link to Alert

16. Remove the unapproved USB drive from the test Mac computer.

Test with an Approved Drive

17. Connect an approved USB drive to the test Mac computer. Use a drive from a vendor listed in your custom analytic predicate (e.g., Samsung if you used the example predicate).
18. Wait a few seconds for the device to mount.
19. Verify the drive DOES appear in Finder. The device should mount normally.
20. Verify the Jamf Helper pop-up does NOT appear.





21. Check your IT team email inbox and verify no alert email was sent for this device.
NOTE: If the Jamf Helper pop-up appears for an approved device, verify that the vendor name in your custom analytic predicate exactly matches the vendor name shown in System Information > Hardware > USB for that device.
22. Remove the approved USB drive from the test Mac.

Summary

You have successfully configured USB Drive Restrictions with Jamf Protect. Your environment now:

1. Allows approved USB devices to mount and function normally without alerts
2. Blocks unapproved USB and external storage devices from mounting
3. Displays a branded pop-up notification to users when they connect an unapproved device
4. Sends an email alert to your IT team for each unapproved device incident

Next Steps

- Review the approved devices list periodically and update as needed
- Monitor the IT email alerts for patterns that may indicate policy violations
- Consider creating reports in Jamf Protect to track removable media incidents over time
- Train end users on the approved USB drive policy and how to request new devices be added

Related Documentation

- How to Use Jamf Helper in Jamf Pro (prerequisite guide)
<https://hconline.com/support/resources/white-papers/how-to-use-jamf-helper-in-jamf-pro>
- Jamf Protect Administrator Guide
https://learn.jamf.com/en-US/bundle/jamf-protect-documentation/page/Jamf_Protect_Documentation.html

This completes this guide.