



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://hcsonline.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.

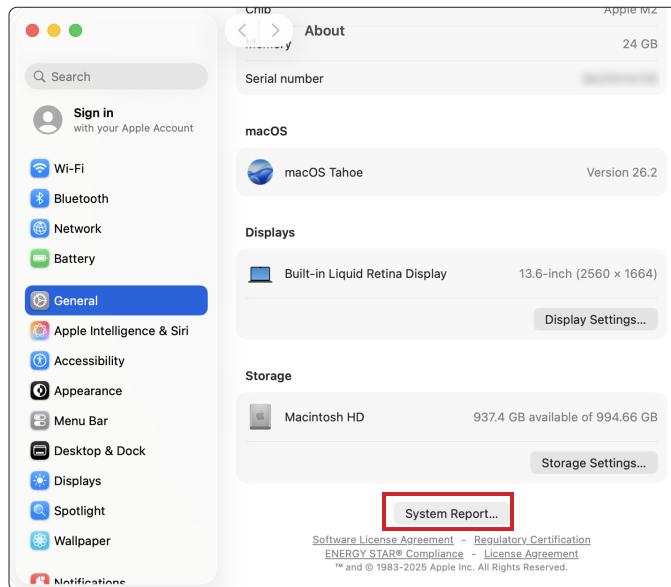


4. Click More Info.

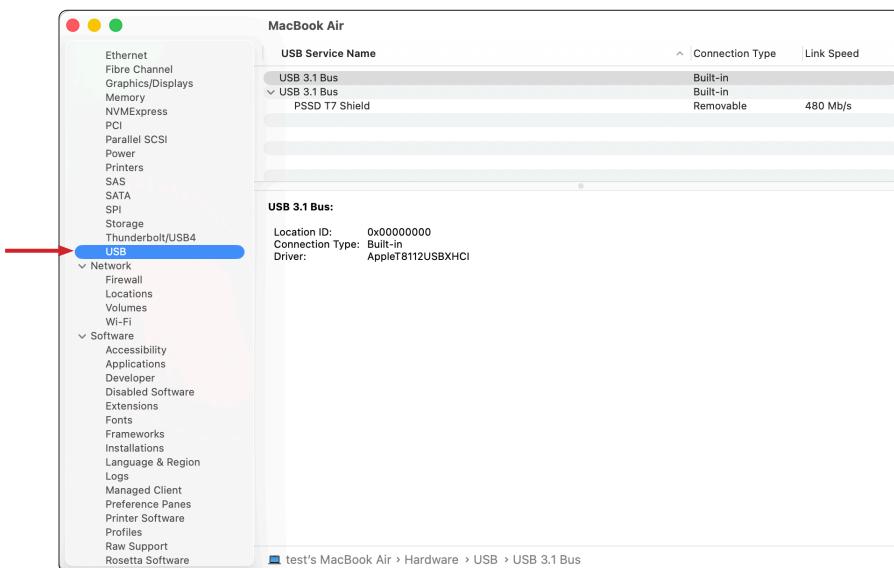




5. Scroll down and click System Report.

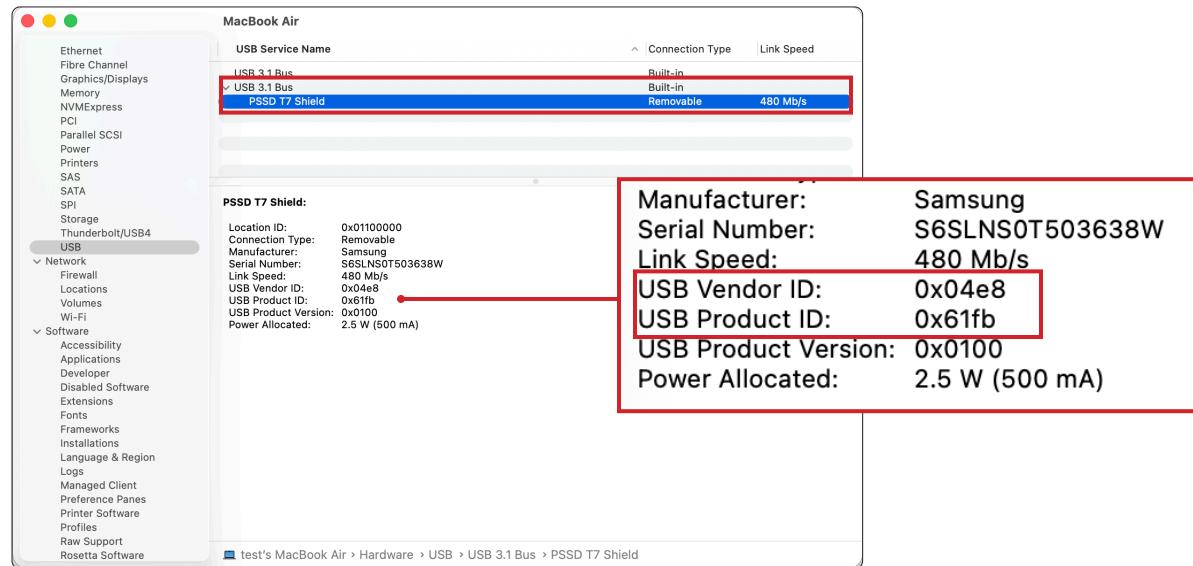


6. In the sidebar, click USB.





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 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 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.

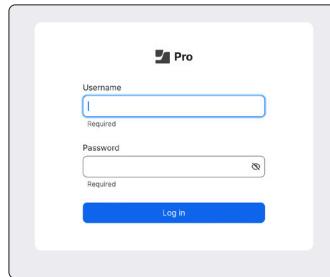
Download the Branding Package

1. Download the the HCS Branding Package and Script from <https://github.hcsonline.com/jpusb>

2. Unzip the downloaded file to extract the HCS-USB-Alert-Branding.pkg.

Create a Category for the Package

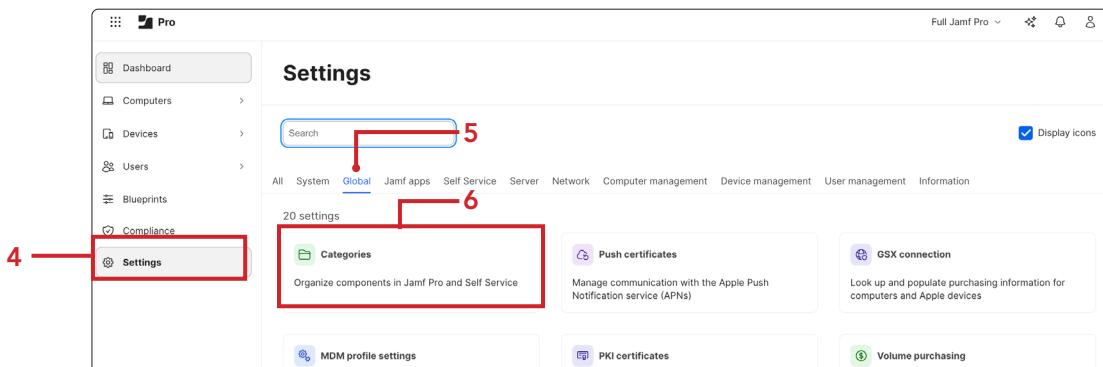
3. In a web browser, log in to your Jamf Pro instance with administrator privileges.



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.

Settings : Global > Categories

← New Category

Display Name
Display name for the category

Branding

Priority in Self Service
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)

9 ▾

Cancel

Save

10. Click New (+).

Settings : Global

← Categories

+ New

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

12. Click Save.

Settings : Global > Categories

← New Category

Display Name
Display name for the category

Security

Priority in Self Service
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)

9

Cancel

Save



Upload the Branding Package

13. In Jamf Pro, click Settings (⚙️).

14. Click Computer Management

15. Click Packages.

The screenshot shows the Jamf Pro Settings interface. The left sidebar has 'Settings' selected. The main content area has 'Computer management' selected. A red box labeled '14' highlights the 'Computer management' tab. A red box labeled '15' highlights the 'Packages' button. A red box labeled '13' highlights the 'Settings' menu item.

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

The screenshot shows the 'Packages' list page. A red box labeled '16' highlights the 'New' button.

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.

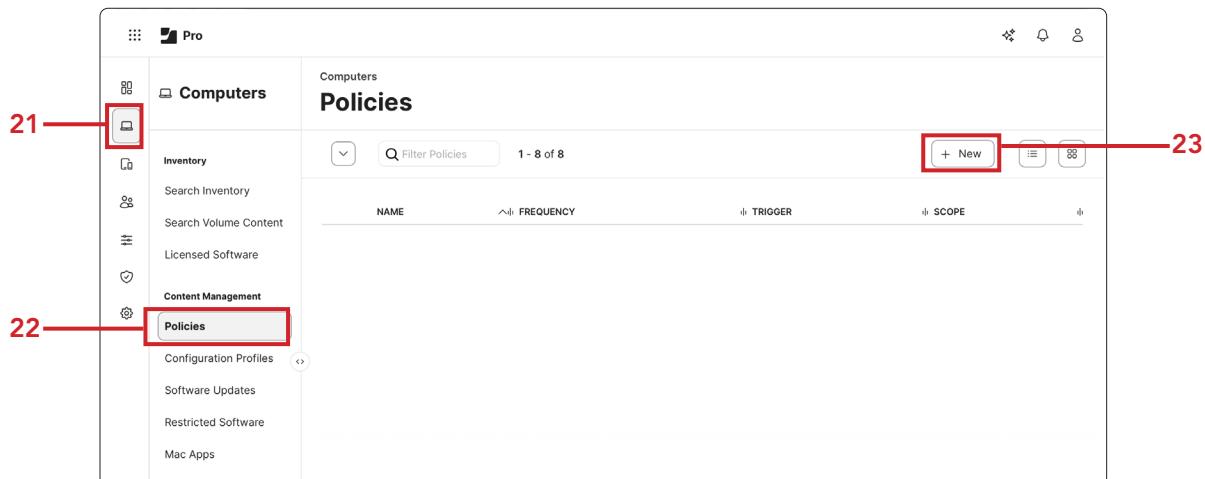
20. Click Save.

The screenshot shows the 'New package' dialog. A red box labeled '17' highlights the 'Display name' field with 'HCS Branding Assets'. A red box labeled '18' highlights the 'Category' dropdown set to 'Branding'. A red box labeled '19' highlights the 'Filename' browse field. A red box labeled '20' highlights the 'Save' button.



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.

General

Display Name
Display name for the policy
24 Deploy HCS Branding Assets

Enabled
25

Category
Category to add the policy to
26 Branding

Trigger
Event(s) to use to initiate the policy

Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

Login
When a user logs in to a computer. A login event that checks for policies must be configured in Jamf Pro for this to work

Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

Enrollment Complete
Immediately after a computer completes the enrollment process

27 Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

Custom
At a custom event

Execution Frequency
Frequency at which to run the policy
28 Once per computer

29 Automatically re-run policy on failure

Retry Event
Event to use to re-run the policy



30. In the left sidebar, click Packages.

31. Click Configure.

The screenshot shows the 'New Policy' configuration interface. The left sidebar has tabs for Options, Scope, Self Service, and User Interaction. The 'Options' tab is selected. Under 'General', the 'Packages' section is highlighted with a red box and the number '30' to its left. Other sections include Software Updates, Scripts, Printers, Disk Encryption, Dock Items, Local Accounts, and Management Accounts. To the right, a 'Configure Packages' section is shown with a 'Configure' button, which is also highlighted with a red box and the number '31' to its right. The text in this section says: 'Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.'

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

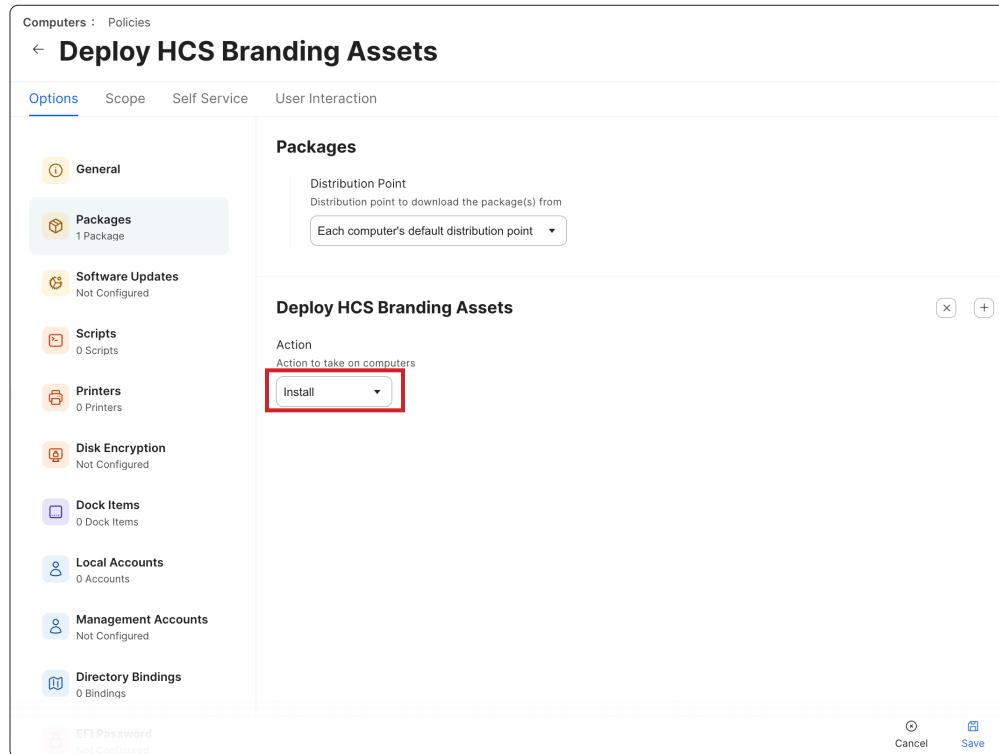
33. Click Add next to HCS Branding Assets.

The screenshot shows the 'New Policy' configuration interface with the 'Packages' section selected in the left sidebar. The 'Packages' table lists several packages: Aftermath.pkg, Comet.pkg, HCS Branding Assets, and JamfConnectLogin.pkg. The 'HCS Branding Assets' row has an 'Add' button to its right, which is highlighted with a red box and the number '32' to its right. The table has columns for NAME and CATEGORY.

NAME	CATEGORY	Add
Aftermath.pkg	No category assigned	Add
Comet.pkg	No category assigned	Add
HCS Branding Assets	Branding	Add
JamfConnectLogin.pkg	Jamf Setup Manager	Add



34. Verify Action is set to Install.



The screenshot shows the 'Deploy HCS Branding Assets' policy configuration page. The 'Action' dropdown is highlighted with a red box and set to 'Install'. Other options in the dropdown are 'Not Configured' and 'Uninstall'.

Packages

Distribution Point: Each computer's default distribution point

Deploy HCS Branding Assets

Action: Install

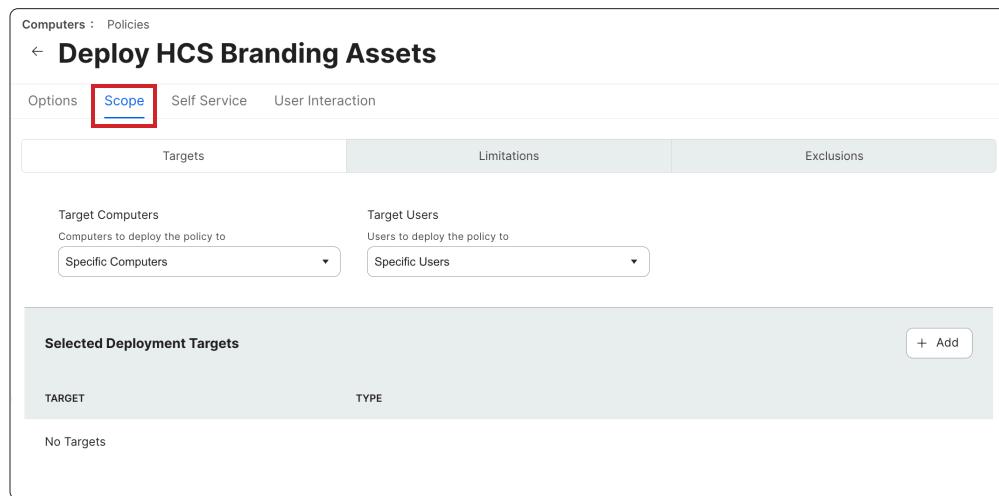
General

- 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

EFI Password: Not Configured

Cancel Save

35. Click Scope.



The screenshot shows the 'Deploy HCS Branding Assets' policy configuration page with the 'Scope' tab selected. The 'Targets' section is highlighted with a red box.

Targets

Target Computers: Specific Computers

Target Users: Specific Users

Selected Deployment Targets

Target: No Targets

+ Add



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.

The screenshot shows the 'Deploy HCS Branding Assets' dialog box. The 'Scope' tab is selected. In the 'Targets' section, the 'Target Computers' dropdown is set to 'All Computers'. In the 'Selected Deployment Targets' table, there is one entry: 'test's MacBook Air' under 'TARGET' and 'Computer' under 'TYPE'. The 'Save' button at the bottom right is highlighted with a red box and labeled '37'.

This completes this section.



Section 3: Jamf Pro - Create the Jamf Helper Script

What You'll Need

Hardware and Software

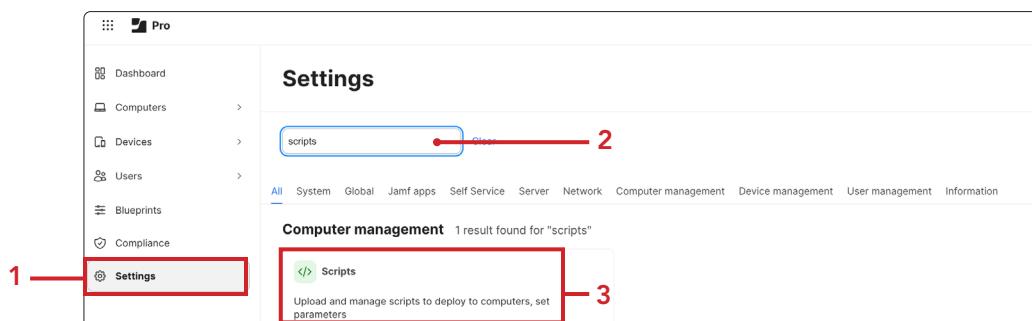
Requirements for following along with this section:

- 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.hcsonline.com/jpush>

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

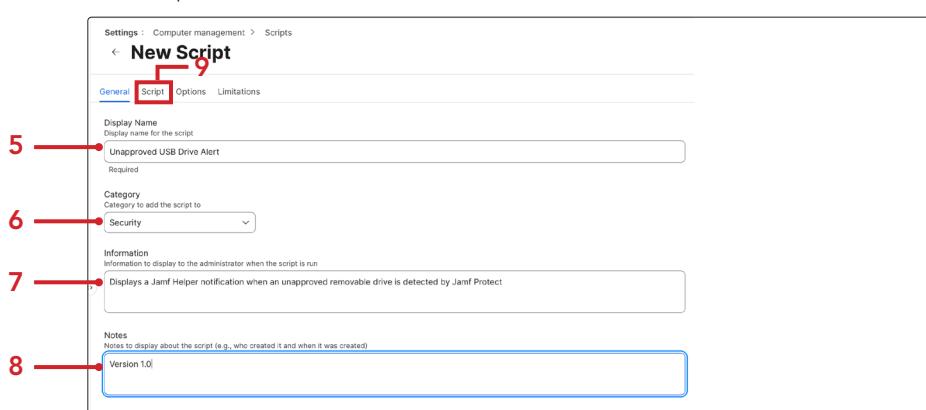
1. In Jamf Pro, click Settings (⚙️).
2. Enter scripts in the search field.
3. Click Scripts.



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.

Settings : Computer management > Scripts
← New Script

General Script Options Limitations

Mode Theme

Shell/Bash Default

```
1 #!/bin/bash
2
3 # Unapproved USB Drive Alert Script
4 # Displays a warning notification via JAMF Helper when an unapproved
5 # removable drive is detected by Jamf Protect
6 #
7 # Version: 1.0
8 # Created for: HCS Technology Group
9
10 # Variables
11 jamfHelper="/Library/Application Support/JAMF/bin/jamfHelper.app/Contents/MacOS/jamfHelper"
12 icon="/Library/Application Support/JAMF/HCS.png"
13 title="HCS Technology Group"
14 heading="Unapproved Storage Device Detected"
15 description="You have connected an external storage device that is not on the approved list.
16
17 This device has been blocked for security purposes.
18
19 If you require access to use this device for work, please contact the IT team for assistance."
20 button1="OK"
21
22 # Display the notification using JAMF Helper
23 "$jamfHelper" -windowType utility \
24   -icon "$icon" \
25   -title "$title" \
26   -heading "$heading" \
27   -description "$description" \
28   -button1 "$button1" \
29   -defaultButton 1
30
31 exit 0
```

Copied!

Cancel Save

13

14

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.

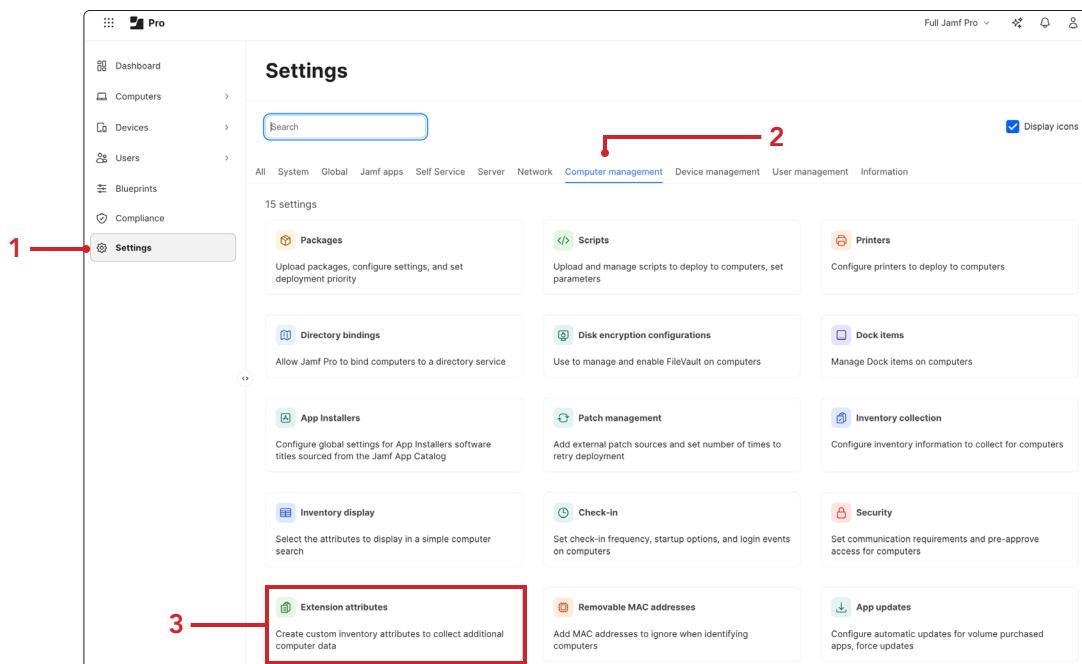
When Jamf Protect detects an unapproved USB disk:

- 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., "usbViolation", "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.



5. In the search field, enter: Jamf Protect

6. Click Jamf Protect Smart Groups in the results.

5

6

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
Jamf Protect - Smart Groups	Jamf Applications
Jamf Protect - Tenant	Jamf Applications
Jamf Protect - Threat Prevention Version	Jamf Applications

7. Click Save.

Enable (script input type only)

Display Name
Display name for the extension attribute

Description
Description for the extension attribute

Data type
Type of the data being collected

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

Input type
Input type to use to populate the extension attribute

Script
Mode Theme

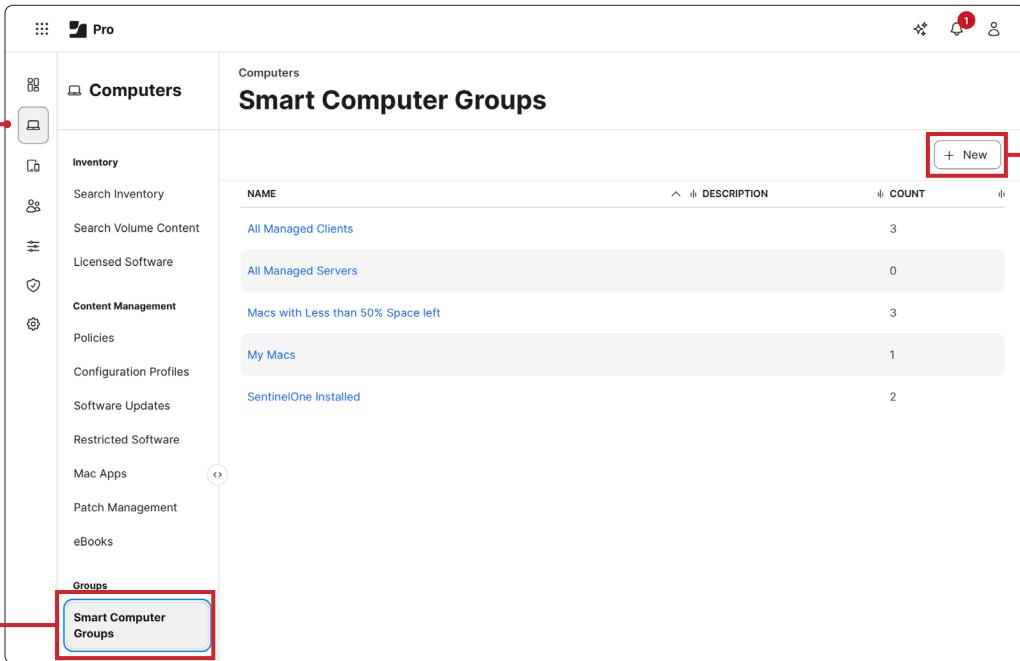
```
1  #!/bin/bash
2
3  SMARTGROUPS_DIR="/Library/Application\ Support/JamfProtect/groups"
4  if [ -d "$SMARTGROUPS_DIR" ]; then
5      SMART_GROUPS=$(ls "$SMARTGROUPS_DIR" | tr '\n' ',' )
6      echo "<result>${SMART_GROUPS}</result>">>results
7  else
8      echo "<result></result>">>results
9  fi
10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

Cancel



Create a Smart Computer Group

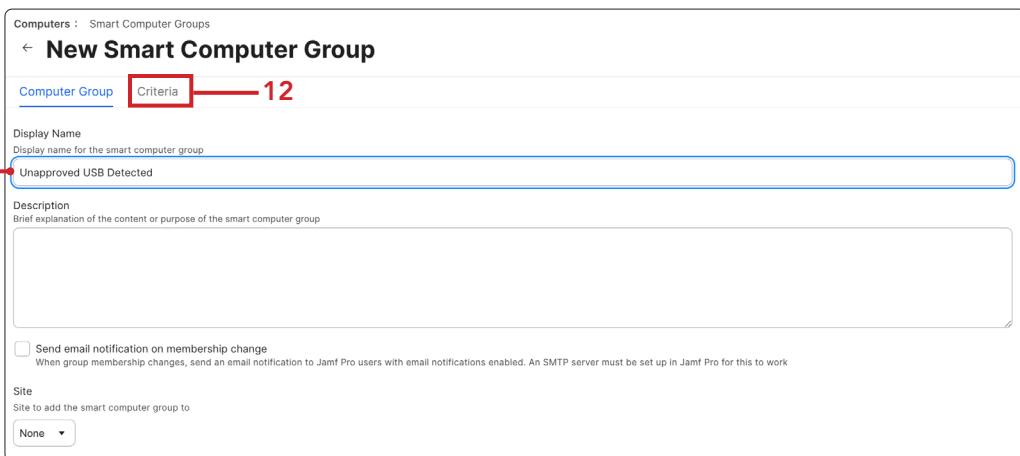
8. In Jamf Pro, click Computers (□) in the sidebar.
9. Click Smart Computer Groups.
10. Click New (+).



The screenshot shows the 'Smart Computer Groups' page in Jamf Pro. The sidebar on the left is titled 'Computers' and includes options like 'Inventory', 'Search Inventory', 'Search Volume Content', 'Licensed Software', 'Content Management' (with 'Policies' and 'Configuration Profiles'), 'Software Updates', 'Restricted Software', 'Mac Apps', 'Patch Management', and 'eBooks'. Under 'Groups', the 'Smart Computer Groups' option is highlighted with a red box and the number '9'. The main area is titled 'Smart Computer Groups' and lists existing groups: 'All Managed Clients' (3), 'All Managed Servers' (0), 'Macs with Less than 50% Space left' (3), 'My Macs' (1), and 'SentinelOne Installed' (2). A red box surrounds the 'New' button in the top right corner, labeled '10'.

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

12. Click Criteria.



The screenshot shows the 'New Smart Computer Group' creation page. The 'Computer Group' tab is selected, and the 'Criteria' tab is highlighted with a red box and the number '12'. The 'Display Name' field is filled with 'Unapproved USB Detected', which is also highlighted with a blue box and the number '11'. The 'Description' field is empty. Below the fields, there is a checkbox for 'Send email notification on membership change' and a dropdown for 'Site' 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

17

18

[+ Add](#)

NOTE: The value "unapproved_usb" is a custom identifier that YOU define. You can name it anything meaningful to your organization (e.g., "usbViolation", "blockedDevice"). 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 (+).

The screenshot shows the 'Computers' sidebar with 'Policies' selected. The main area displays a table of policies, with one named 'Branding' visible. In the top right corner, there is a red box around the '+ New' button, with the number '22' to its right.

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.

The screenshot shows the 'New Policy' configuration page. The sidebar on the left has 'Policies' selected. The main area has several sections: 'General' (Display Name: Alert - Unapproved USB Drive, Enabled checked, highlighted with a red box and labeled 24), 'Category' (Security selected, highlighted with a red box and labeled 25), 'Trigger' (checkboxes for Startup, Login, Network State Change, Enrollment Complete, Recurring Check-in, and Custom (selected), highlighted with a red box and labeled 26), 'Custom Event' (protect entered, highlighted with a red box and labeled 27), and 'Execution Frequency' (Ongoing selected, highlighted with a red box and labeled 28). The bottom right has 'Cancel' and 'Save' buttons.



29.In the payload sidebar, click Scripts.

30.Click Configure.

The screenshot shows the payload sidebar with various configuration categories. The 'Scripts' category is highlighted with a green background and a red arrow labeled '29' pointing to it. To the right, a 'Configure Scripts' dialog box is open, containing a 'Configure' button which is also highlighted with a red box and labeled '30'.

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

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

The screenshot shows a list of scripts. The 'Unapproved USB Drive Alert' script is listed, and a red box labeled 'Add' is positioned next to it, indicating where to click to add it.

33.Click Scope.

34.Click Add (+).

The screenshot shows the 'Alert - Unapproved USB Drive' configuration page. The 'Scope' tab is selected, indicated by a red box labeled '33'. In the 'Selected Deployment Targets' table, a red box labeled '34' is on the '+ Add' button.



35. Click Computer Groups.

A screenshot of a software interface titled 'Alert - Unapproved USB Drive'. The 'Scope' tab is selected. Below it is a 'Targets' section with tabs for 'Targets', 'Limitations', and 'Exclusions'. A sub-dialog titled 'Add Deployment Targets' is open, showing tabs for 'Computers', 'Computer Groups' (which is highlighted with a red box), 'Users', 'User Groups', 'Buildings', and 'Departments'. A search bar shows 'Filter results' and '1 - 10 of 90'. Below the search is a table with columns for 'GROUP NAME' and 'Add' buttons. The table lists several computer groups, including 'All Managed Clients', 'anyorg_it does exist', 'Macs running macOS 14.5 or later', 'User is an Admin account settings are dimmed', 'User is an admin', 'Computers that are enrolled - Application Install', 'TESTDATA_2ec1d570_Static_Group_1', 'TESTDATA_2ec1d570_Static_Group_2', 'TESTDATA_2ec1d570_Static_Group_3', and 'TESTDATA_2ec1d570_Static_Group_4'.

36. Search for Unapproved USB Detected.

37. Click Add.

38. Done

A screenshot of the same software interface as the previous step. The 'Computer Groups' tab is selected in the 'Add Deployment Targets' dialog. A red arrow labeled '36' points to the search bar containing 'Unapproved'. A red box highlights the 'Add' button in the 'GROUP NAME' section. A red arrow labeled '37' points to the 'Add' button. A red arrow labeled '38' points to the 'Done' button in the top right corner of the dialog.

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.

A screenshot of the Jamf Protect Device Controls page. The left sidebar shows a navigation menu with 'Device Controls' highlighted and a red box labeled '3'. The main content area is titled 'Device Controls' and contains a sub-section 'Removable Storage Control'. A red box labeled '4' highlights the '+ Create' button. The table below the section shows a single row with the status 'No Results'. The table has columns for 'Name', 'Description', 'Associated Plans', 'Modified', and 'Created'. The top right corner of the page shows the date '12/08/2025 5:34 PM GMT'.



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 (+).

The screenshot shows the 'Create Removable Storage Control Set' page. The 'Name' field (5) contains 'USB Drive Control Set'. The 'Default Permission' dropdown (7) is set to 'Prevent'. The 'Description' field (6) contains 'Blocks unauthorized USB devices from mounting while allowing Read-Only access to approved devices.' The 'Total Overrides (0)' section (9) has an 'Add' button highlighted with a red box.

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

The screenshot shows the 'Removable Storage Override Type' dialog box. The 'Encrypted Devices' dropdown (10) is selected. The 'Product ID' field (11) is highlighted with a red box.



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

The screenshot shows the 'Removable Storage Control Set' configuration page. The 'Product ID Override Details' section is highlighted with a red arrow. The 'Product ID Overrides' section is also highlighted with a red arrow and contains a red box around the '+ Add' button.

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.

The dialog box shows the 'Add Product ID Override' interface. Step 13 points to the 'Vendor ID' field containing '0x5583'. Step 14 points to the 'Product ID' field containing '0x0781'. Step 15 points to the 'Add' button, which is highlighted with a red box.



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.

A screenshot of a web-based configuration interface for a 'Removable Storage Control Set'. The page title is 'Removable Storage Control Set'. At the top, there is a 'Save' button with a red box around it and the number '17' to its right. Below the title, there are fields for 'Name' (set to 'USB Drive Control Set') and 'Default Permission' (set to 'Prevent'). A 'Description' section notes that it blocks unauthorized USB devices while allowing Read-Only access to approved devices. A 'Default Local Notification Message' field contains the text 'This removable storage device is not allowed.' In the center, there is a 'Product ID Override Details' section with a 'Permission' dropdown set to 'Read and Write' and an 'Apply to' dropdown set to 'All', both highlighted with a red box and the number '16' to its right. To the left, a 'Total Overrides (1)' section shows a table with one row: 'Type' (Product ID), 'Permission' (Read and Write), and 'Apply to' (All). The table shows '1 added Product IDs'. At the bottom, there is a 'Product ID Overrides' section with a table showing two rows: 'Vendor ID' (0x04e8) and 'Product ID' (0x6300).

Type	Permission	Apply to
Product ID	Read and Write	All

Vendor ID	Product ID
0x04e8	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.

The screenshot shows the Jamf Protect web app interface. The left sidebar is titled 'Apple, Inc' and contains the following sections: Overview, Compliance, Computers, Alerts, Configuration (with 'Analytics' selected and highlighted by a red box labeled '1'), Plans, Actions, Threat Prevention, Device Controls, Unified Logging, Telemetry, and Administrative. The main content area is titled 'Analytics / Analytic Sets' and shows a table of 'Analytic Sets'. The table has columns for Name, Description, Jamf-managed, Custom, Associated Plans, Created, and Modified. One row is visible: 'Default Analytic Set' (Description: Default Analytic Set, Jamf-managed: 156, Custom: 0, Associated Plans: Default, Created: 03/26/2025 9:04 PM GMT, Modified: 08/01/2025 1:30 PM GMT). At the top right of the main content area, there is a blue button labeled '+ Create Analytic Set' (highlighted by a red box labeled '2').



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.

Create

← Create Analytic Set **Save**

Name: **Unapproved USB Drive Detected**

Description: **Tracks and logs unapproved USB device detection events.**

Analytics in this set

Name	Description	Severity	Smart Group	Category	Created	Modified
Living Off the Land (13)	Reverse shell creation ...	●●●	Living Off the Land	03/26/2025 8:17 PM GMT	05/06/2025 4:14 PM GMT	
Cat Piped to NC	Reverse shell creation ...	●●●	Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Reverse Shell Generic (Deprecated)	Reverse shell creation ...	●●●	Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Reverse Shell Netcat	Reverse shell creation ...	●●●	Living Off the Land	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Reverse Shell PHP (Deprecated)	Reverse shell creation ...	●●●	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.

+ Create custom analytic

Name	Description	Severity	Smart Group	Category	Created	Modified
Living Off the Land (13)	Reverse shell creation ...	●●●	Living Off the Land	03/26/2025 8:17 PM GMT	05/06/2025 4:14 PM GMT	
System Visibility (13)	Reverse shell creation ...	●●●	System Visibility	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Known Malicious File (66)	Reverse shell creation ...	●●●	Known Malicious File	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Persistence (15)	Reverse shell creation ...	●●●	Persistence	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Credential Harvesting (3)	Reverse shell creation ...	●●●	Credential Harvesting	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Common Attacker Technique (13)	Reverse shell creation ...	●●●	Common Attacker Technique	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Evasion (11)	Reverse shell creation ...	●●●	Evasion	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
System Tampering (8)	Reverse shell creation ...	●●●	System Tampering	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Apple Security (4)	Reverse shell creation ...	●●●	Apple Security	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	
Privilege Escalation (5)	Reverse shell creation ...	●●●	Privilege Escalation	03/26/2025 8:17 PM GMT	04/29/2025 2:31 PM GMT	



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' page for a new analytic. The fields are as follows:

- Analytic Name:** Unapproved USB Device (Step 8)
- Level:** 0 (Step 8)
- Categories:** System Visibility (Step 9)
- Description:** Detects when an unapproved removable USB storage device is inserted. Approved vendors are excluded from triggering this analytic. (Step 10)
- Severity:** High (Step 11)
- Sensor Type:** USB Event (Step 12)
- Analytic Filter:** \$event.type == 0 AND \$event.device.removable == 1 AND \$event.device.writable == 1 AND \$event.device.vendorName != "Samsung" (Step 13)

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.

The screenshot shows the 'Analytic Actions' configuration interface. Step 14 points to the 'Add to Jamf Pro Smart Group' checkbox, which is checked. Step 15 points to the 'Identifier' field, which contains the value 'unapproved_usb'. Other sections visible include 'Tags' (with a dropdown menu 'Select value'), 'Analytic Context Items' (with a '+ Add Context Item' button), and 'Snapshot Files' (with a '+ Add Snapshot File' button).

16. Click Save.

The screenshot shows the 'Create' screen for a new analytic. Step 16 points to the 'Save' button, which is highlighted with a red box. The screen also shows fields for 'Analytic Name' (set to 'Unapproved USB Device') and 'Level' (set to '0'). A 'Show Help' link is visible in the top right corner.



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.

The screenshot shows the 'Analytic Set' page for 'Unapproved USB Detected'. The 'Save' button is highlighted with a red box and labeled '24'. The 'Custom (1)' link under 'Analytics in this set' is highlighted with a red box and labeled '20'. The 'Unauthorized USB' checkbox is highlighted with a red box and labeled '21'. The 'System Visibility (1)' section is highlighted with a red box and labeled '22'. The 'Unauthorized USB' checkbox in the list is highlighted with a red box and labeled '23'.

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.

A screenshot of the Jamf Protect web application interface. The left sidebar shows navigation links for Apple, Inc., Overview, Compliance, Computers, Alerts, Configuration, Analytics, Actions, Threat Prevention, Device Controls, and Unified Logging. The 'Plans' link is highlighted with a red box and the number '1'. The main content area is titled 'Plans' and contains a sub-header 'Plans are security configurations that are deployed to computers via configuration profiles. Each computer should only be assigned one plan.' Below this is a table with two rows. The first row is a header row with columns: Name, Auto Update, Analytic Sets, Agent Protocol, Endpoint Threat Prevention, Log Level, and Advanced Threat Controls. The second row is a data row for 'Default' with values: Yes, Default Analytic Set (with a dropdown menu), mqtt, Block and report, Error, and Disabled. A red box labeled '2' highlights the '+ Create Plan' button in the top right of the main content area.



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. The 'General' section is filled with the following information:

- Name:** USB Drive Control Plan (Step 3)
- Description:** Prevent unauthorized USB drive usage and data loss (Step 4)

The 'Threat Prevention' section shows three facets:

- Endpoint Threat Prevention:** Block and report (Step 5)
- Tamper Prevention:** Block and report (Step 5)
- Advanced Threat Controls:** Block and report (Step 5)

The 'Analytics sets' section (Step 6) contains a dropdown menu with 'Unapproved USB Detected' selected.

The 'Telemetry' section (Step 7) has a dropdown menu set to 'None'.

The 'Device Controls' section (Step 9) has a dropdown menu set to 'USB Drive Control Set'.

A red box highlights the 'Save' button in the top right corner, and a red number '10' is placed above it, indicating the final step in the process.

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.

The screenshot shows the Jamf Protect administrative interface. The left sidebar has a 'Administrative' section with icons for Data, Downloads, API Clients, Audit Logs, Documentation, and Preferences. Step 1 is marked with a red box around the gear icon. Step 2 is marked with a red box around the 'Account' button in the sidebar. Step 3 is marked with a red box around the 'Users' tab in the top navigation bar. The main content area is titled 'Account' and shows 'Organization Information' with details like Name, Created date, Domain, and Certificate Authority ID. Below that is 'App Information'.

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

The screenshot shows the 'Users' page in the Jamf Protect administrative interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Account' and shows the 'Users' tab selected. It displays a table with columns for User, Email, Roles, Groups, and Identity Providers. Step 1 is marked with a red box around the 'User' table header. Step 2 is marked with a red box around the 'Email' column header. The table shows a single user entry with 'Full Admin' in the Roles column and 'Default' in the Groups column.



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

The screenshot shows the 'Account' configuration page for a user. The user's name is 'ck' and their email is 'ck@hcs.com'. The 'Save' button is highlighted with a red box and labeled '8'. The 'Send Email Notifications' checkbox is checked and highlighted with a red box and labeled '6'. The 'Email Severity' dropdown is set to 'High' and highlighted with a red box and labeled '7'. The 'Groups' and 'Roles' sections are also visible.

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

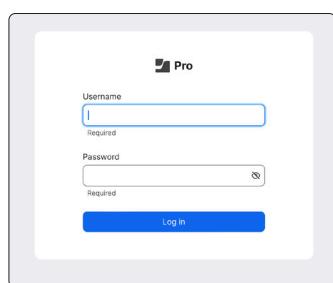
In this section, you will deploy the USB Drive Control Plan to your target computers. Plan assignments are configured in Jamf Pro through the Jamf Protect integration. Once assigned, computers will receive the plan and begin enforcing the USB drive restrictions.

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

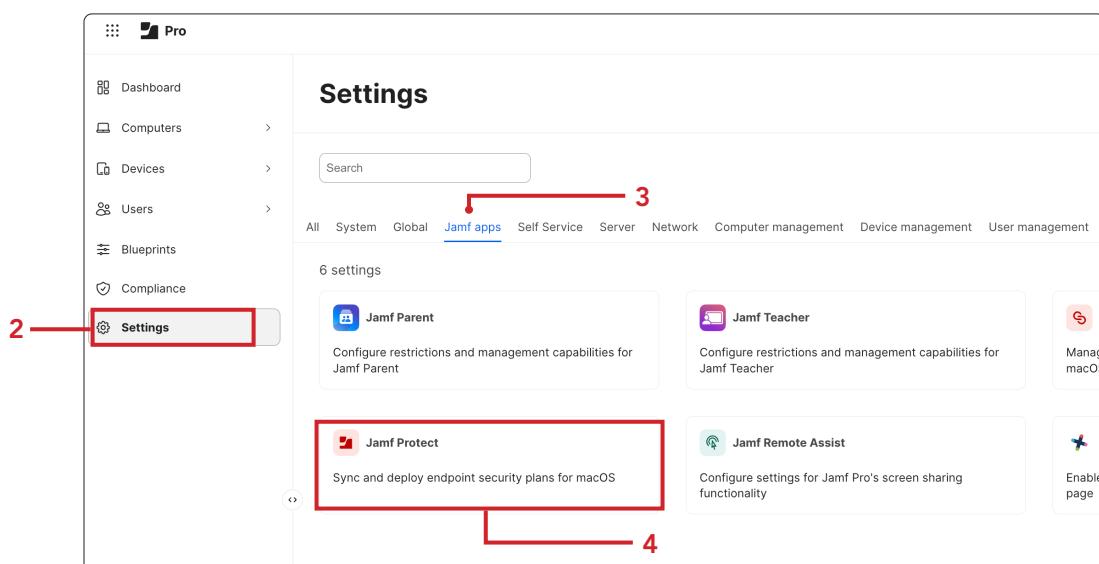
1. Log in to your Jamf Pro server.



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.

The screenshot shows the Jamf Protect registration page. A red arrow labeled '5' points to a green checkmark icon indicating a successful connection to the Jamf Protect tenant. Another red arrow labeled '8' points to the 'USB Drive Control Plan Plan - Jamf Protect Configuration' row in the Jamf Protect Plans list. A note on the left says 'Click on Sync if you do not see your plan.'

NAME	PROFILE	SCOPE	SITE	LOGS
USB Drive Control Plan	USB Drive Control Plan Plan - Jamf Protect Configuration	No scope defined	None	View
Default	Default Plan - Jamf Protect Configuration	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.

The screenshot shows the 'USB Drive Control Plan Plan - Jamf Protect Configuration' edit page. A red box highlights the 'Signed Profile' status message: 'This profile is read-only because it is signed.' A red box also highlights the 'Edit' button in the bottom right corner of the page.



10. Click Scope.

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

12. Click Save.

The screenshot shows the 'USB Drive Control Plan' configuration profile in Jamf Protect. The 'Scope' tab is selected. The 'Target Computers' dropdown is set to 'All Computers'. The 'Save' button is highlighted with a red box and the number 12. The 'Selected Deployment Targets' table shows one target: 'test's MacBook Air' (Computer type).

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

The screenshot shows the 'Computers' page in Jamf Protect. On the left sidebar, the 'Computers' option is highlighted with a red box and the number 13. In the main list, a computer named 'test's MacBook Air' is selected, highlighted with a red box and the number 15. The page includes a table with columns for Name, Serial, macOS Version, Connection Status, Threat Version, Protect Version, and Compliance Failures.

- 16.Click Computer Details.

The screenshot shows the 'Computer Details' tab for 'test's MacBook Air' in Jamf Protect. The 'Computer Details' tab is highlighted with a red box and the number 16. The page displays various status metrics and alert counts. Key data points include a Compliance Baseline Score of 55.0%, 25 Failures, 33 Passes, and 0 Disabled items. The 'Alerts' section shows 13 High, 0 Medium, and 0 Low alerts.



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 shows the 'Computer Details' tab for a MacBook Air. The 'Edit Computer' modal is open, showing fields for 'Label' (empty), 'Plan' (set to 'USB Drive Control Plan'), and 'Tags' (empty). The 'Current Plan' section is highlighted with a red box and shows the 'USB Drive Control Plan' assigned. The plan details are: Modified 12/08/2025 11:29 PM GMT, Created 12/08/2025 5:42 PM GMT, Hash c3, and Analytic sets Unapproved USB Detected.

Computer Details

Computer Status

Computer Info

Current Plan

USB Drive Control Plan

Modified: 12/08/2025 11:29 PM GMT

Created: 12/08/2025 5:42 PM GMT

Hash: c3

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.

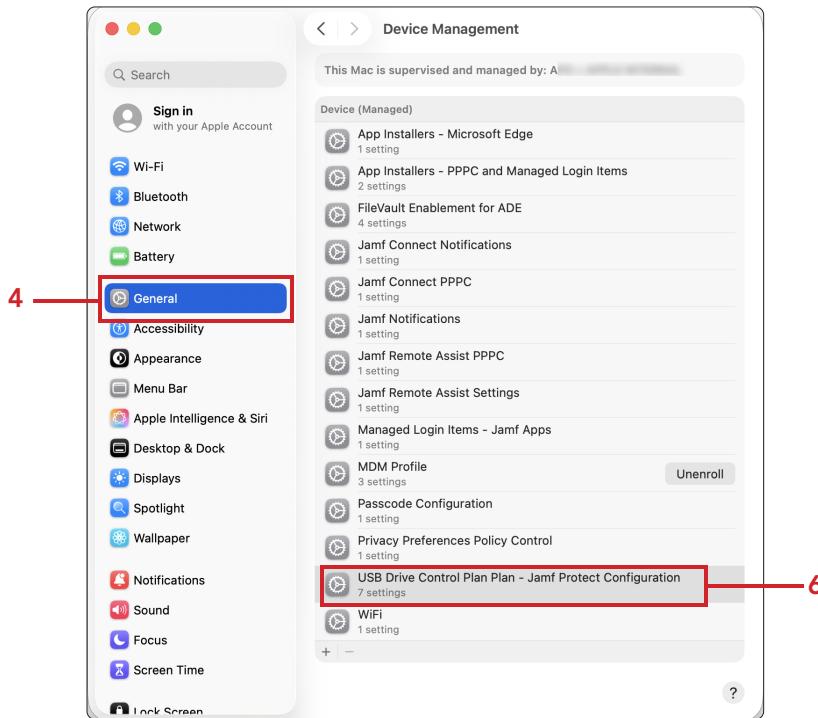
Verify the Plan is Applied

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.





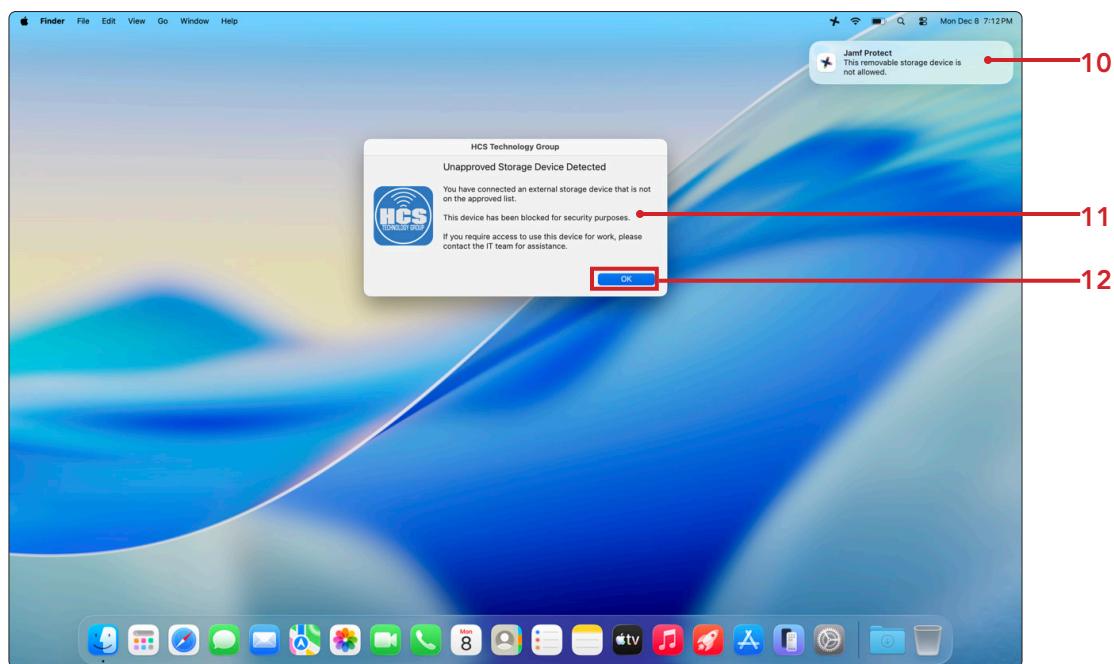
4. In the sidebar, click General.
5. Scroll down and click Device Management.
6. Verify the Jamf Protect configuration profile is installed. This is the plan from Jamf Protect.





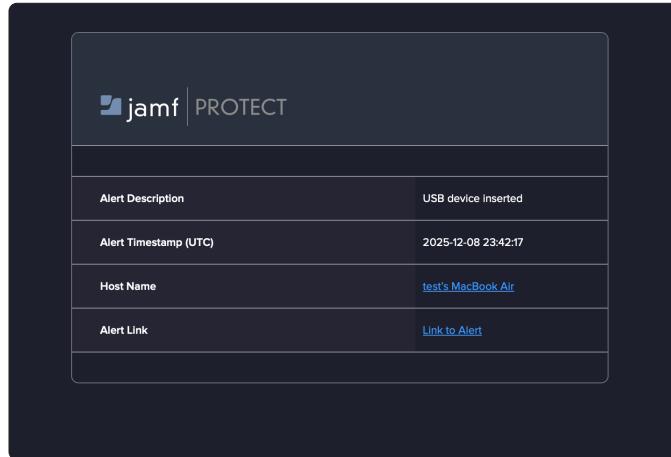
Test with an Unapproved Drive

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.



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://hcsonline.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.