jamf | PRO

jamf | PROTECT

# Configure Custom
# USB Drive Restrictions with Notifications


*Rev 20260106*

## Contents

## 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)

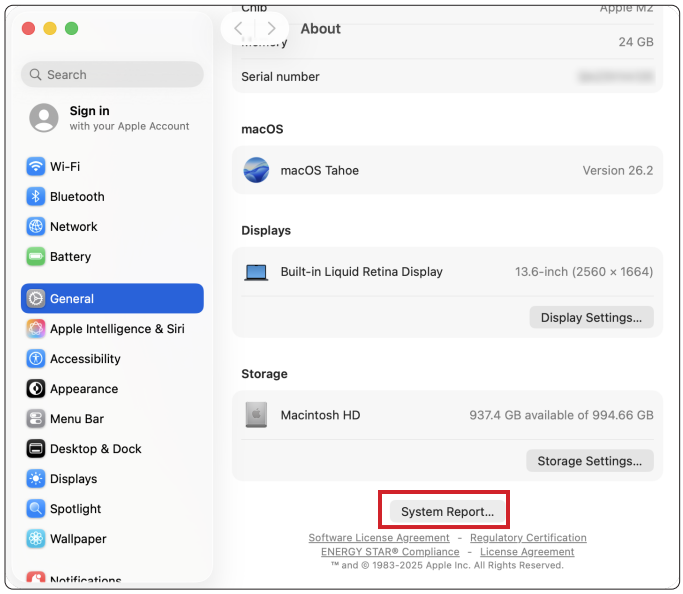
NOTE: You will use the Vendor ID and Product ID from System Report, not the display names. These are technical identifiers that uniquely identify device types.

**Find Your Device's Vendor ID**

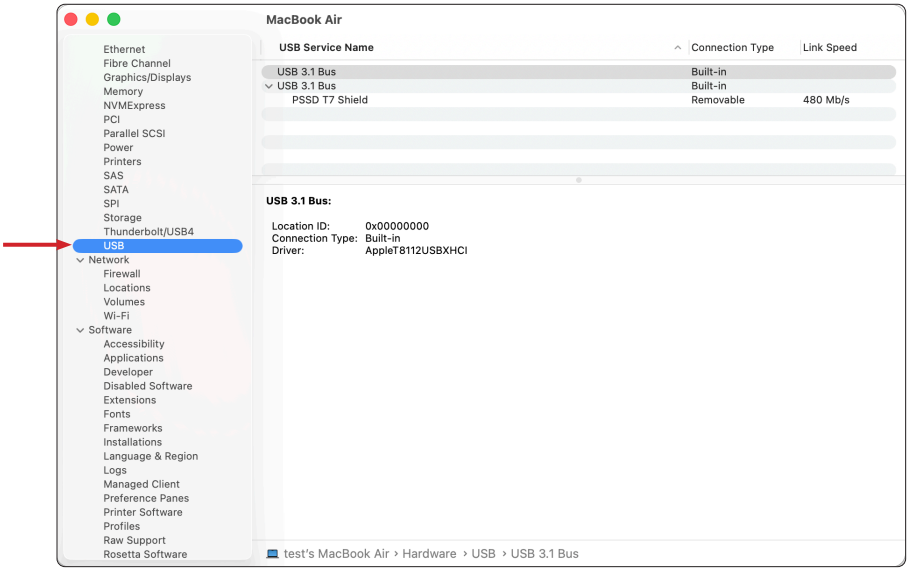
1. On a Mac, connect the USB drive you want to approve.
2. Click the Apple menu.
3. Select About This Mac.


4. Click More Info.

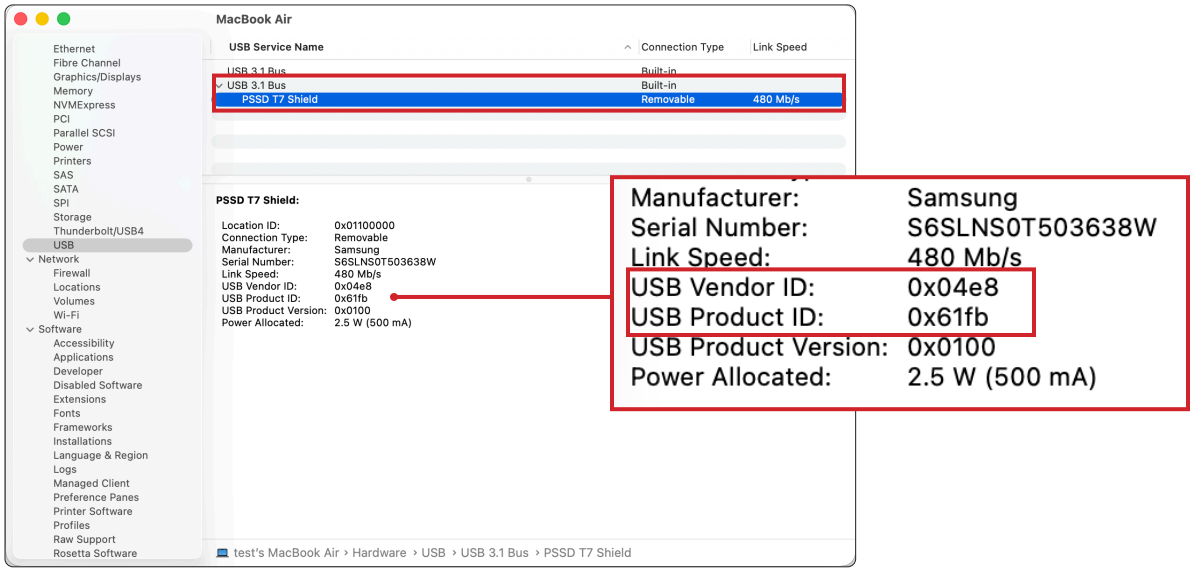
5. Scroll down and click System Report.



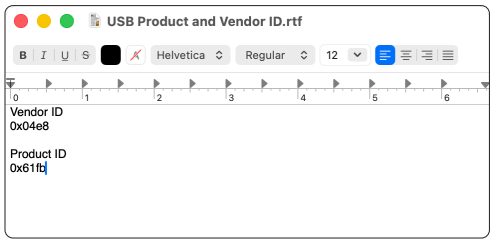

6. In the sidebar, click USB.



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

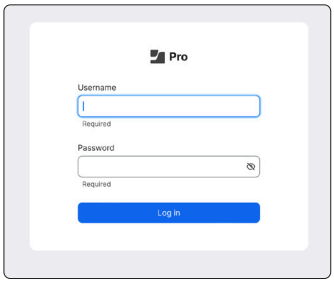
In this section, you will deploy the HCS logo image that will be displayed in the Jamf Helper pop-up notifications. This branding ensures users recognize the notification as coming from an official IT source.

**Download the Branding Package**

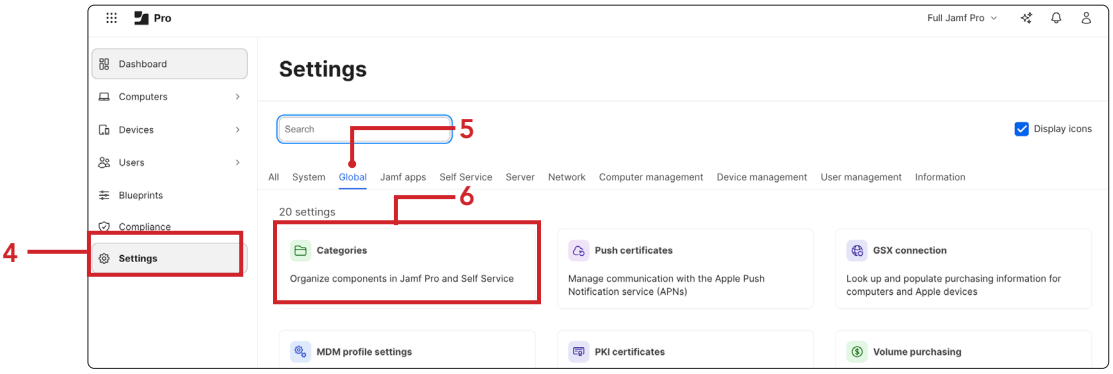
1. Download the the HCS Branding Package and Script from https://github.hcsonline.com/jpusb
2. Unzip the downloaded file to extract the HCS-USB-Alert-Branding.pkg.

**Create a Category for the Package**

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

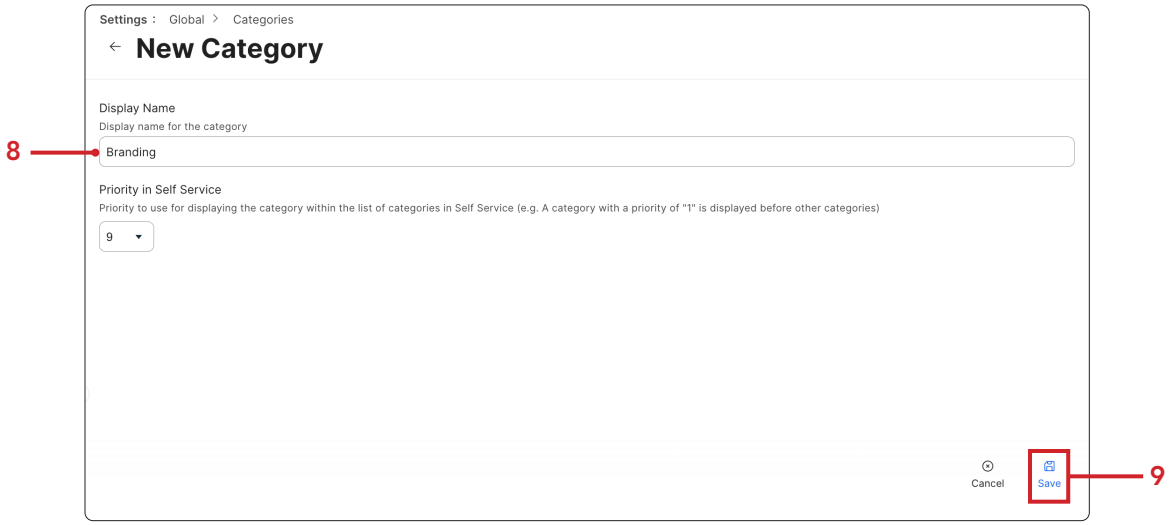



4. In Jamf Pro, click Settings(⚙).
5. Click Global.
6. Click Categories.



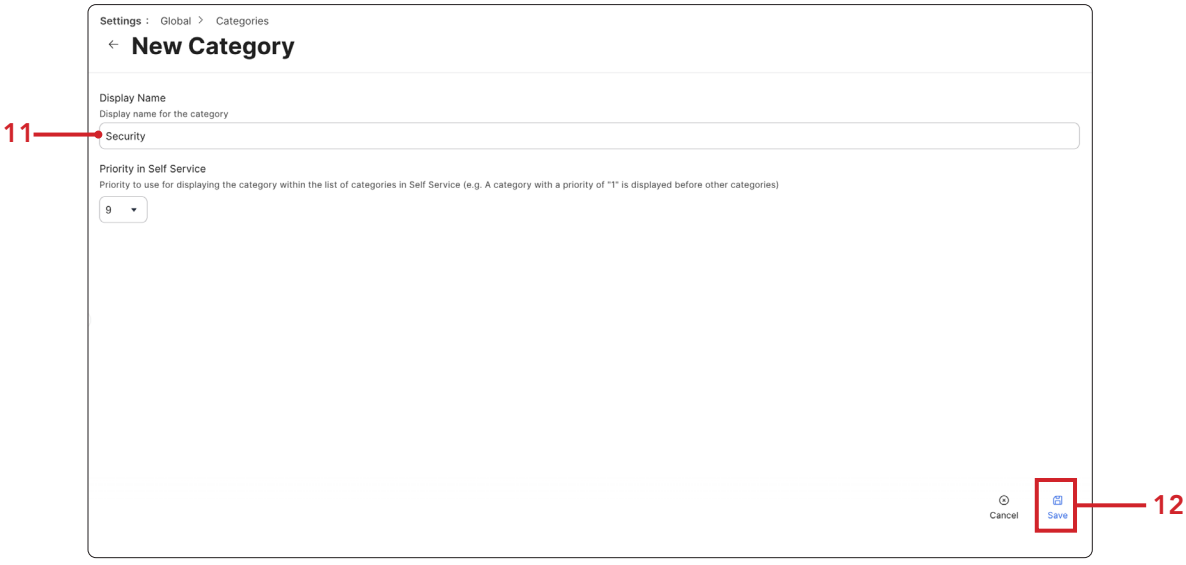

7. Click New (+).

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



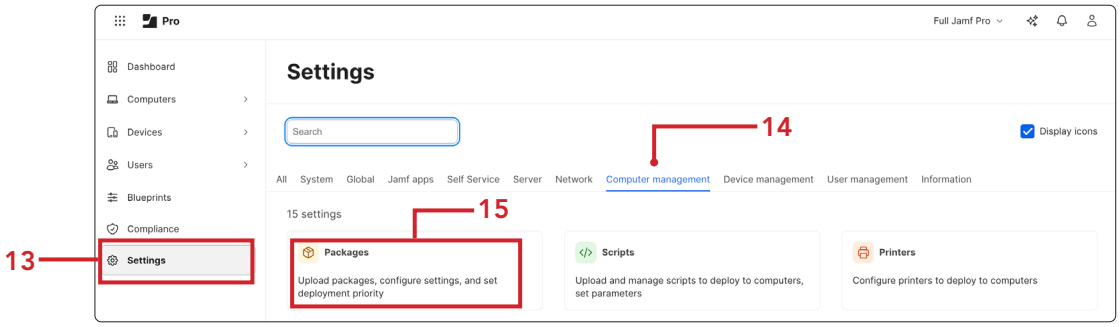

10. Click New (+).


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



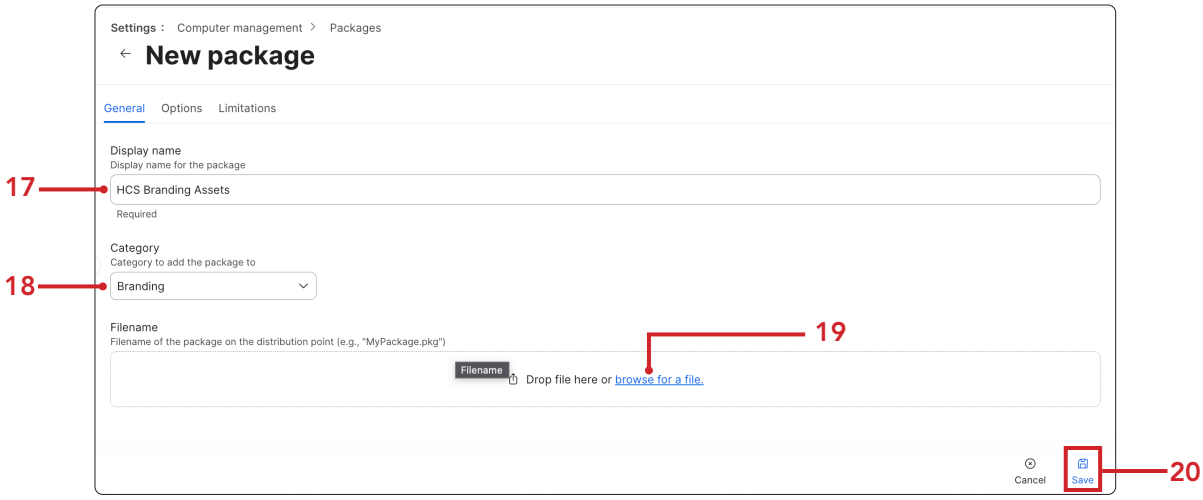
### Upload the Branding Package

13. In Jamf Pro, click Settings(⚙).
14. Click Computer Management
15. Click Packages.



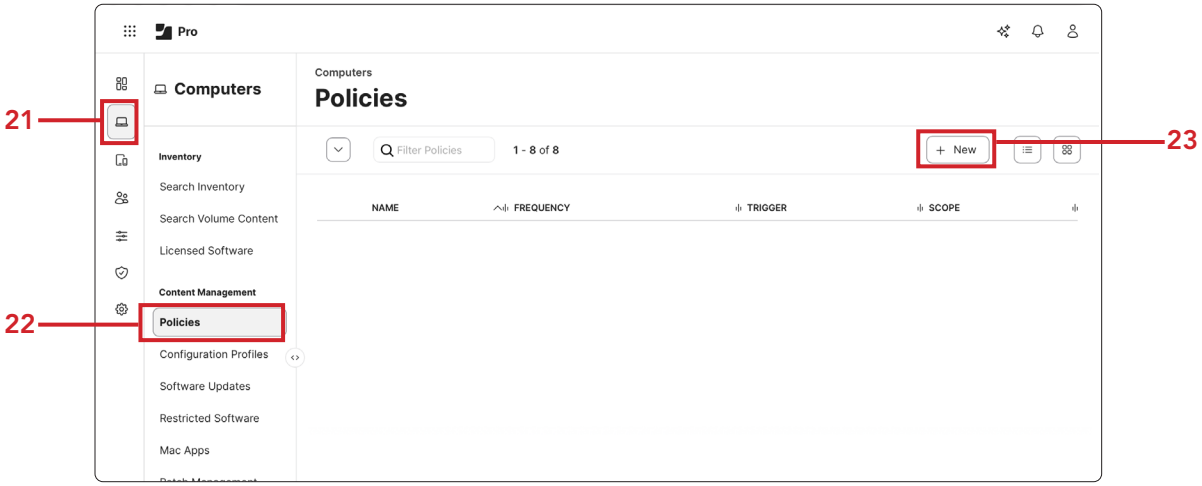

16. Click New (+) to create a new package.


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.

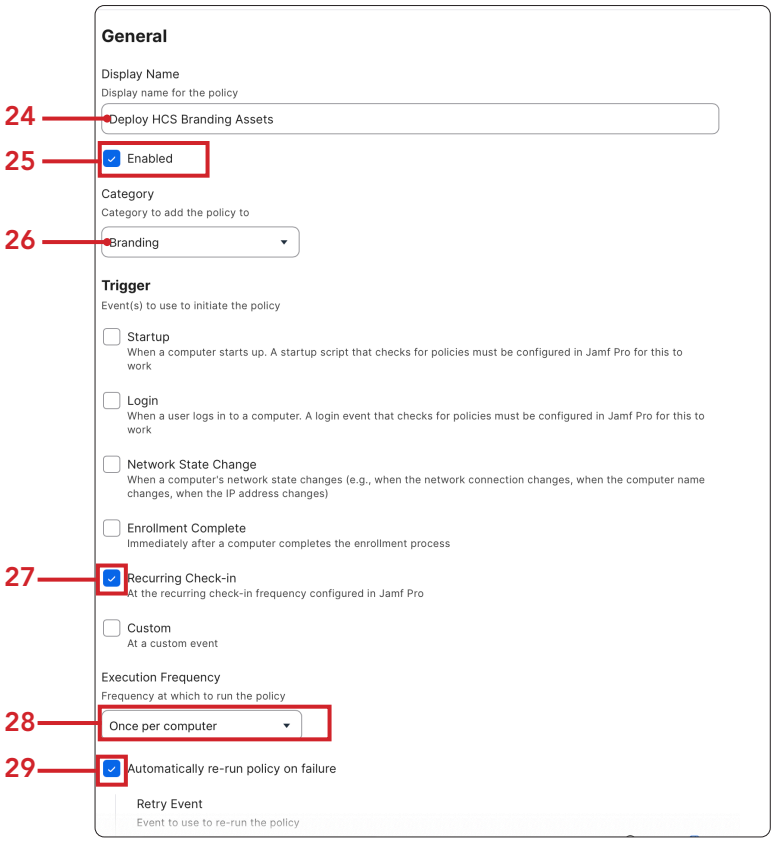


## Create a Policy to Deploy the Branding Package

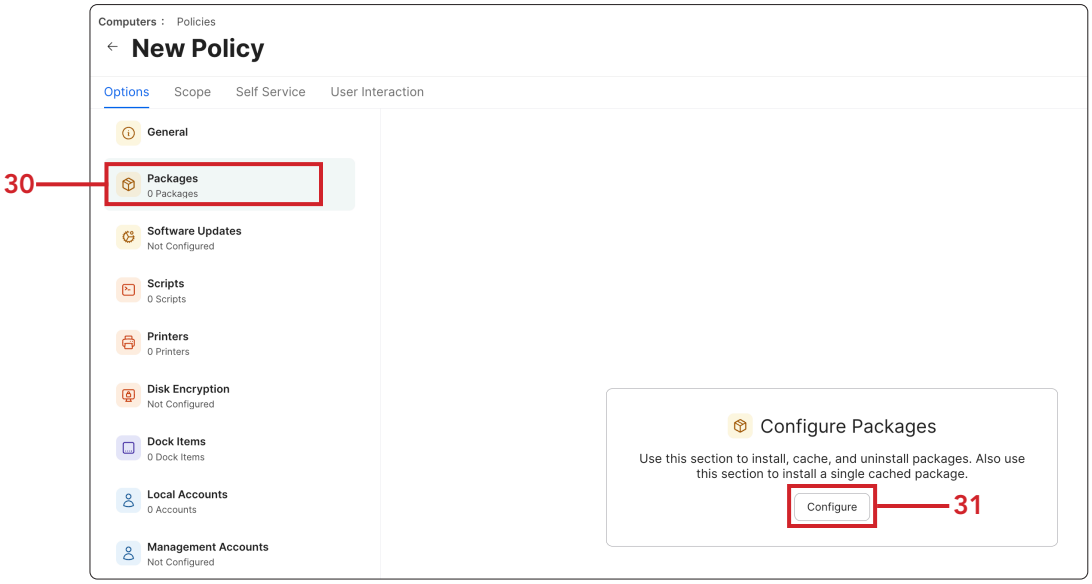
21. In Jamf Pro, click Computers (💻) in the sidebar.
22. Click Policies.
23. Click New (+).



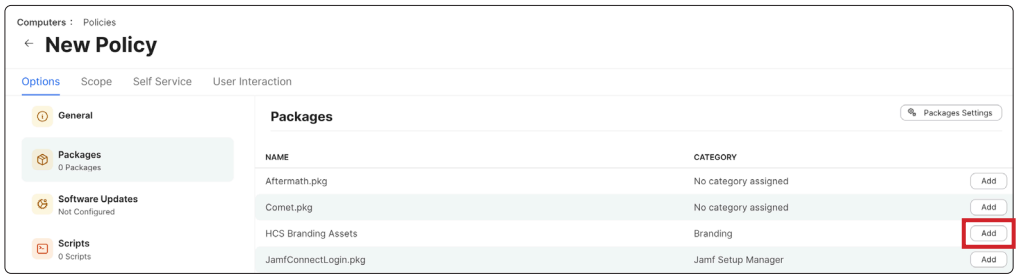

24. In the Display Name field, enter: **Deploy HCS Branding Assets**.
25. Verify Enabled is selected.
26. Select Branding for the Category.
27. Under Trigger, select the checkbox for Recurring Check-in.
28. Click the Execution Frequency menu and select Once per computer.
29. Select the checkbox for Automatically re-run policy on failure.



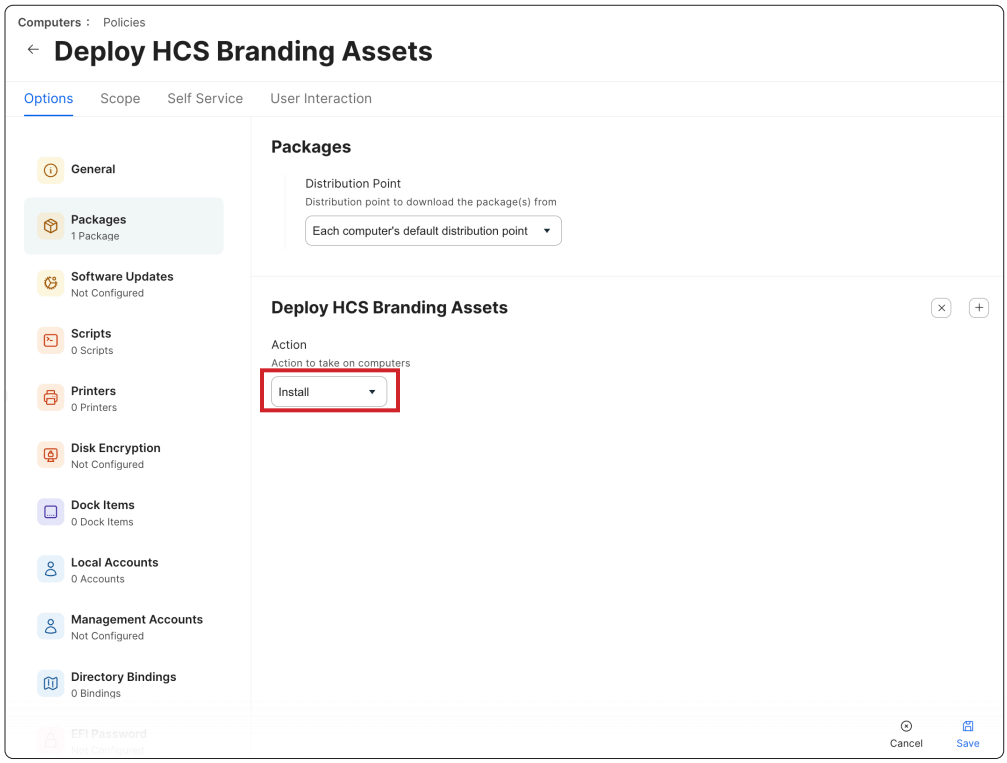
30. In the left sidebar, click Packages.
31. Click Configure.



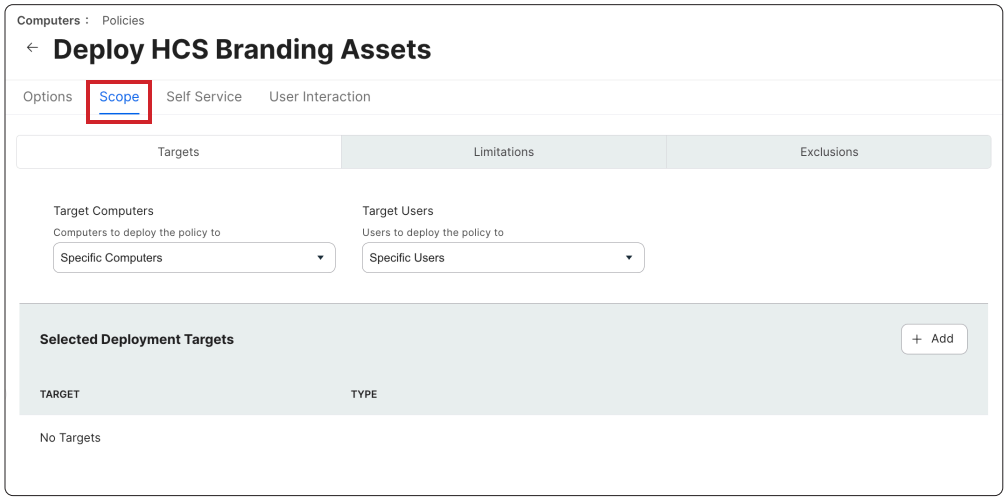

32. Locate the HCS Branding Assets package in the list.
33. Click Add next to HCS Branding Assets.



34. Verify Action is set to Install.

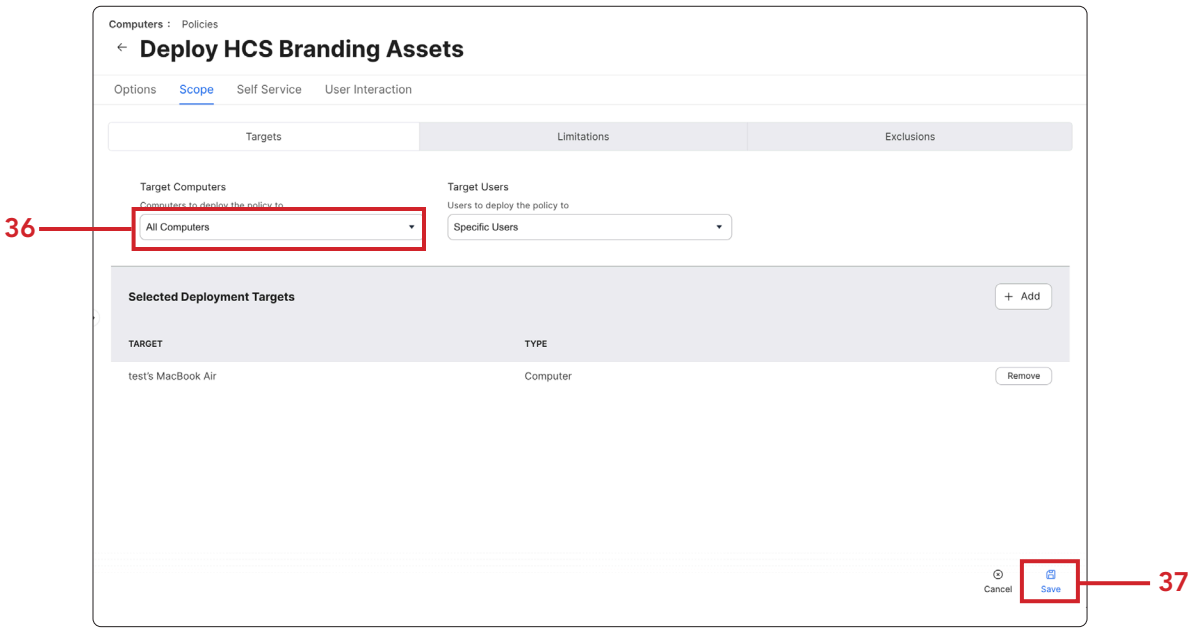



35. Click Scope.



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.




This completes this section.

## Section 3: Jamf Pro - Create the Jamf Helper Script

What You'll Need

Hardware and Software

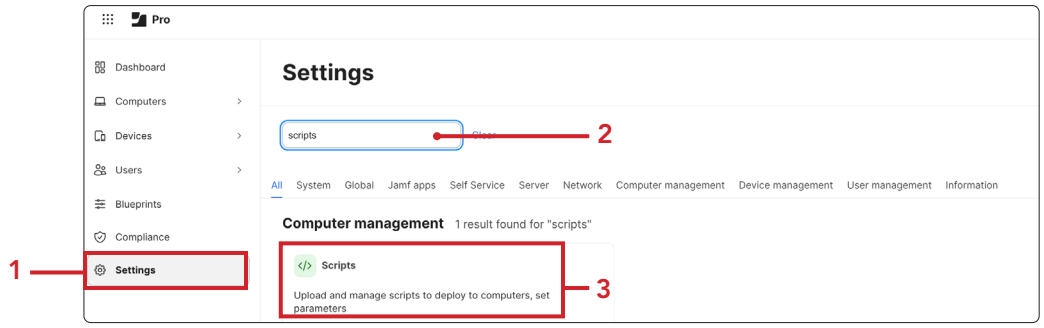
Requirements for following along with this section:

- 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/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.

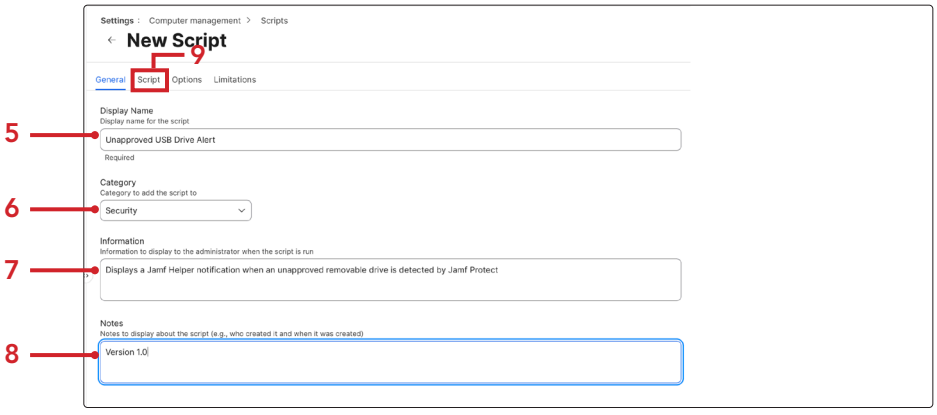
**Add the Script to Jamf Pro**

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

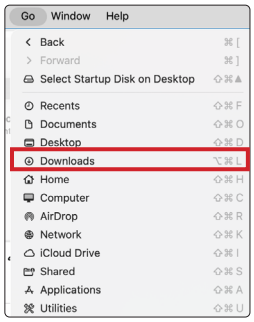



4. Click New (+).

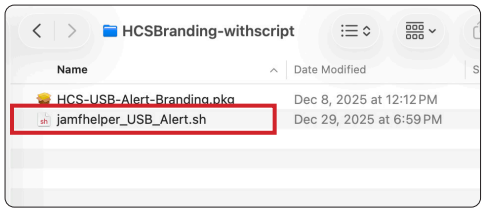

5. In the Display Name field, enter: **Unapproved USB Drive Alert**.
6. Click the Category menu and select Security.
7. In the Information field, enter: **Displays a Jamf Helper notification when an unapproved removable drive is detected by Jamf Protect**.
8. In the Notes field, enter: **Version 1.0**.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



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



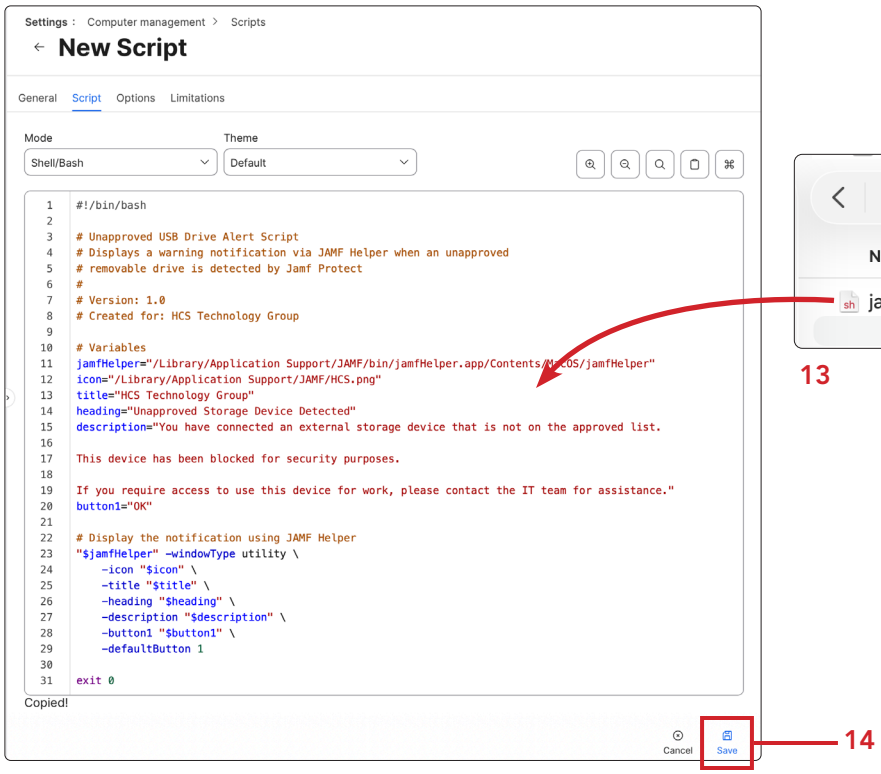

11. Locate the script, jamfhelper_USB_Alert.sh inside the folder, HCSBranding-withscript.




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**

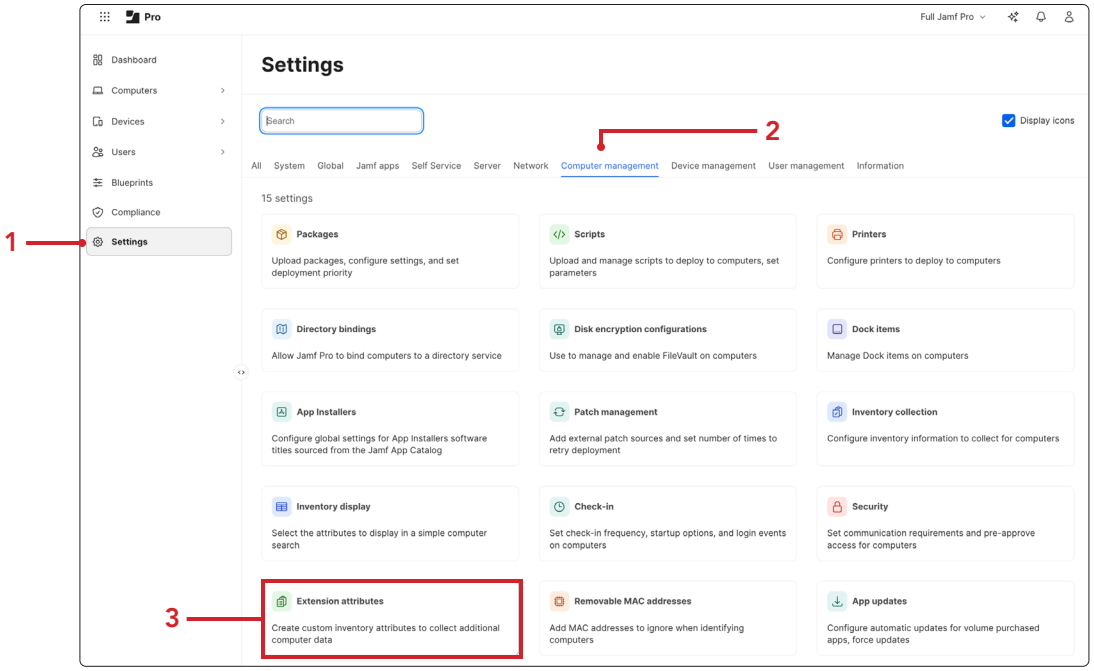
The Analytic Remediation workflow uses a custom identifier to link Jamf Protect and Jamf Pro. When Jamf Protect detects an unapproved USB disk:

- 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.

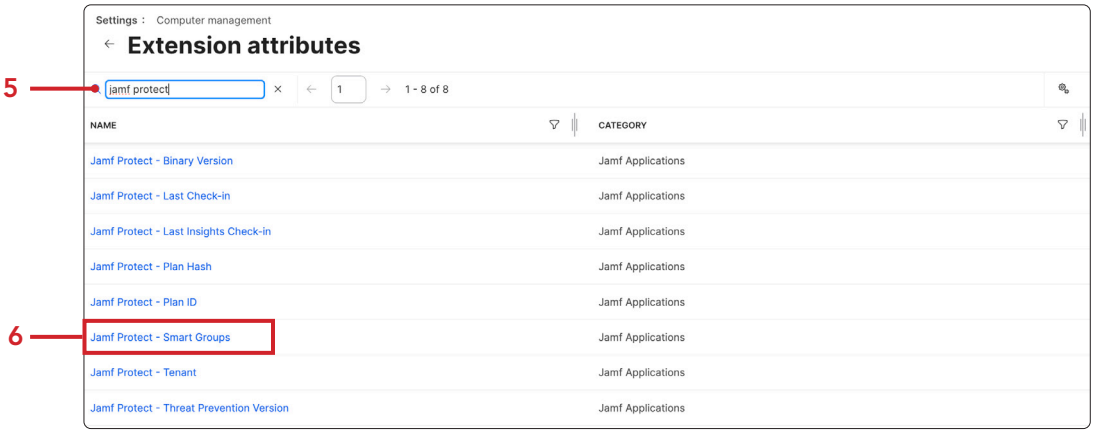
**Create the Extension Attribute**

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

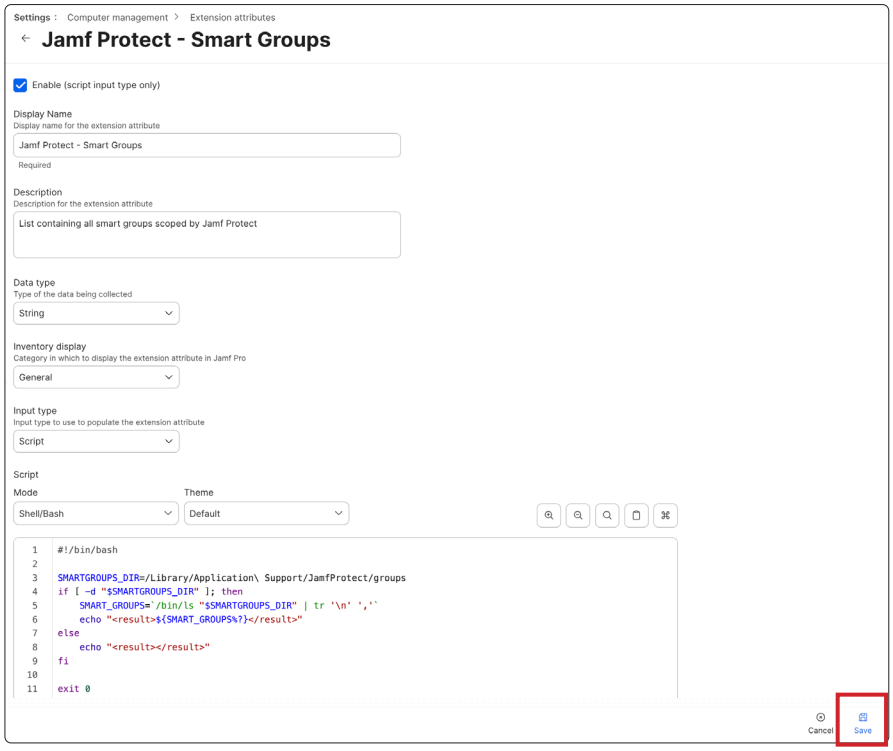


4. Click New From Template.


5. In the search field, enter: **Jamf Protect**
6. Click Jamf Protect Smart Groups in the results.

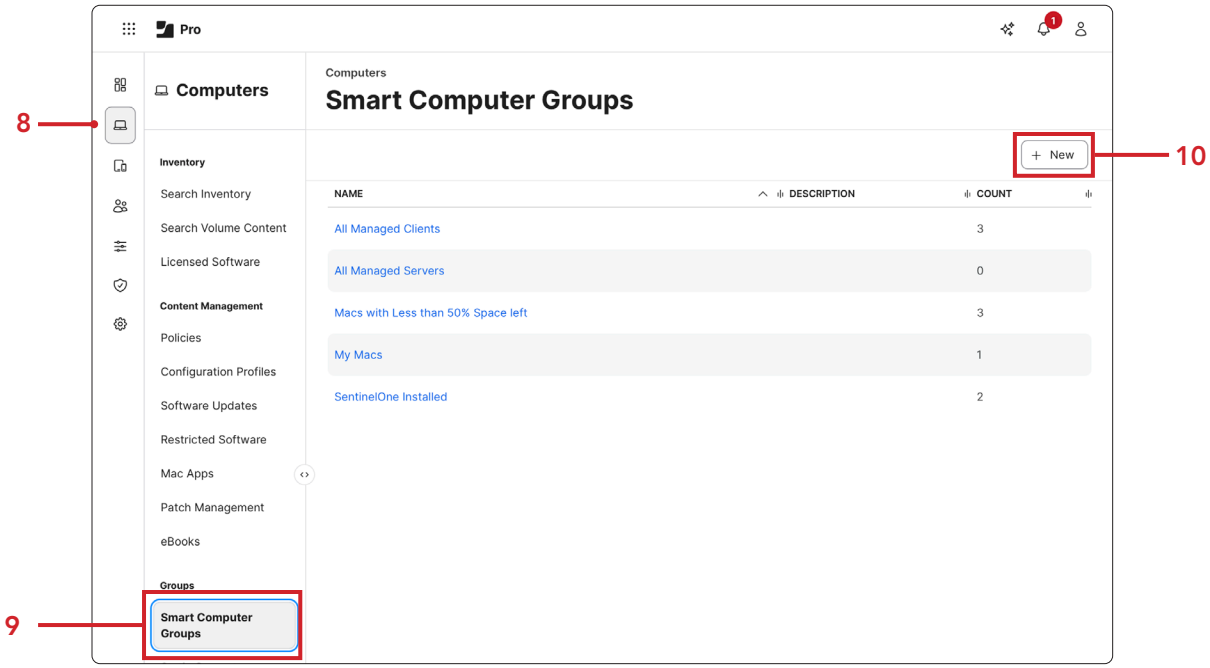



7. Click Save.

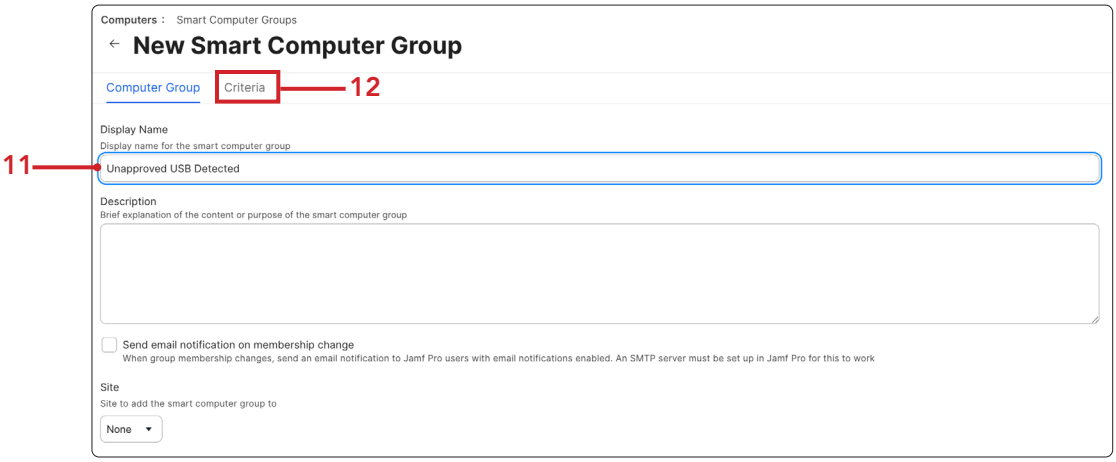


### Create a Smart Computer Group

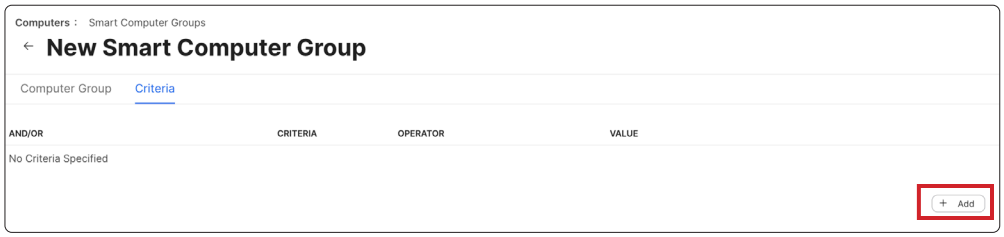
8. In Jamf Pro, click Computers (💻) in the sidebar.
9. Click Smart Computer Groups.
10. Click New (+).




11. In the Display Name field, enter: **Unapproved USB Detected**.
12. Click Criteria.



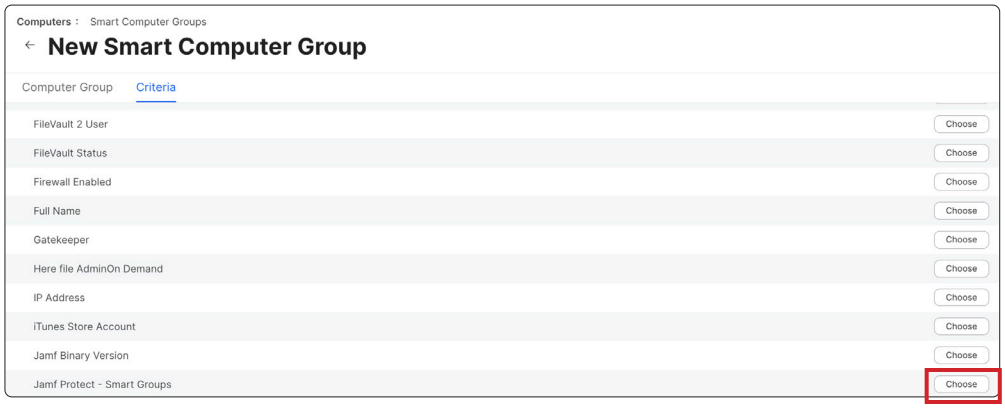
13. Click Add (+).




14. Click Show Advanced Criteria.

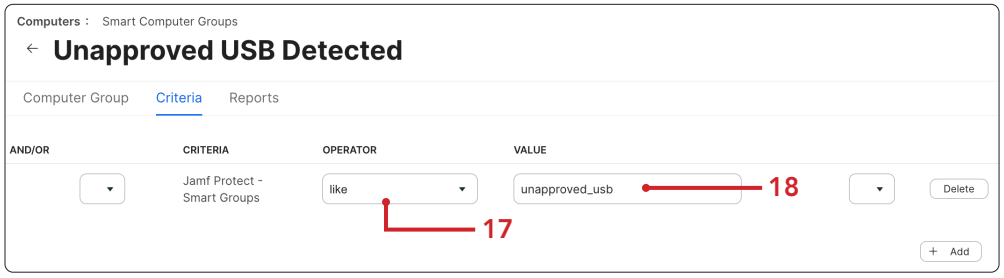
15. Scroll down to Jamf Protect - Smart Groups.

16. Click Choose.




17. Click the Operator dropdown and select like.

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

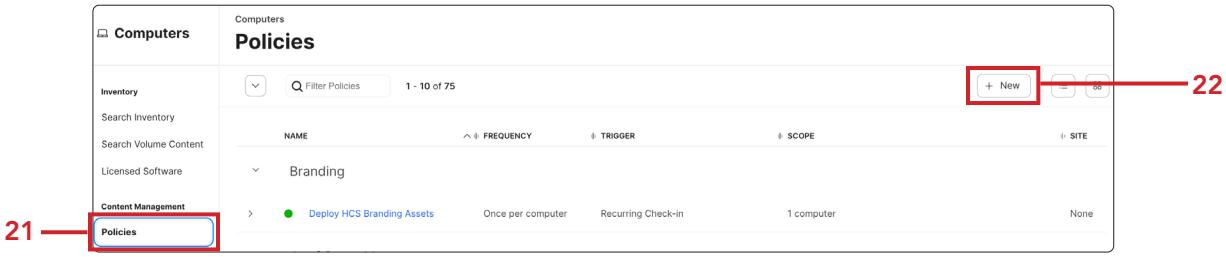



NOTE: The value "unapproved_usb" is a custom identifier that YOU define. You can name it anything meaningful to your organization (e.g., "usb_violation", "blocked_device"). This value must match exactly the Identifier you will enter in Jamf Protect in Section 6.

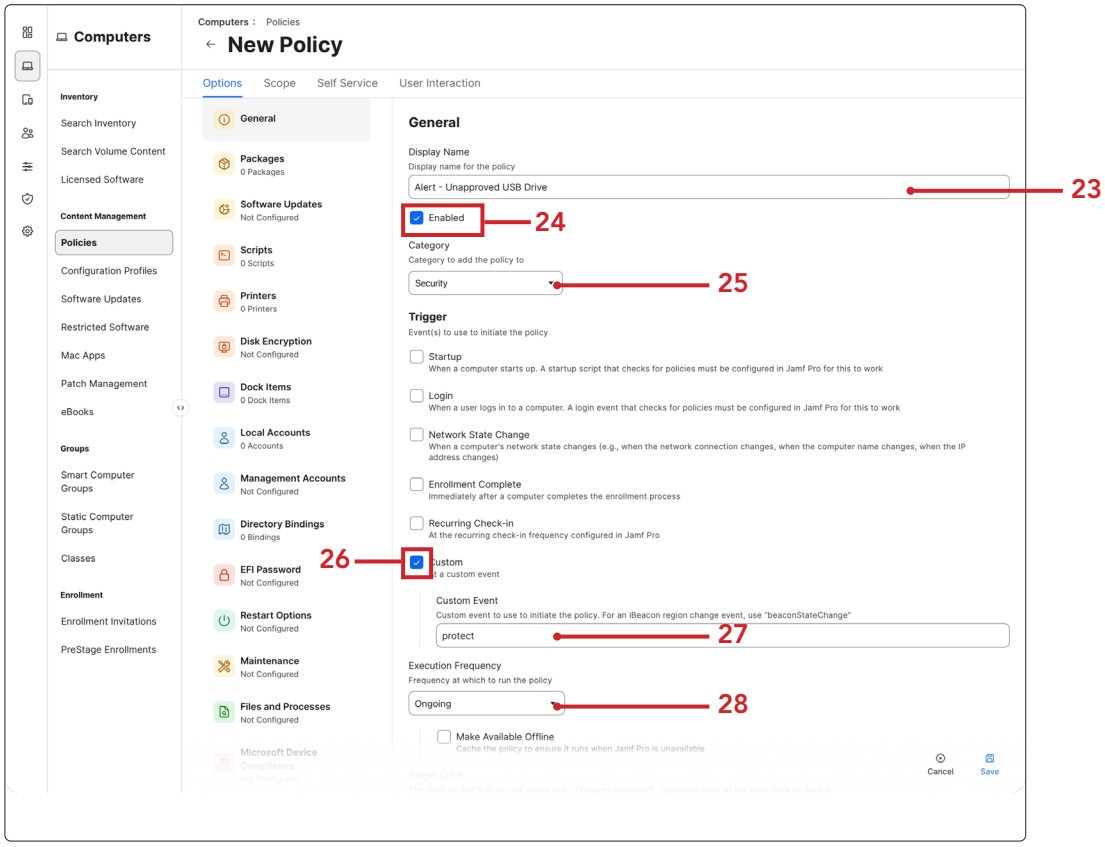
19. Click Save.

**Create the Remediation Policy**

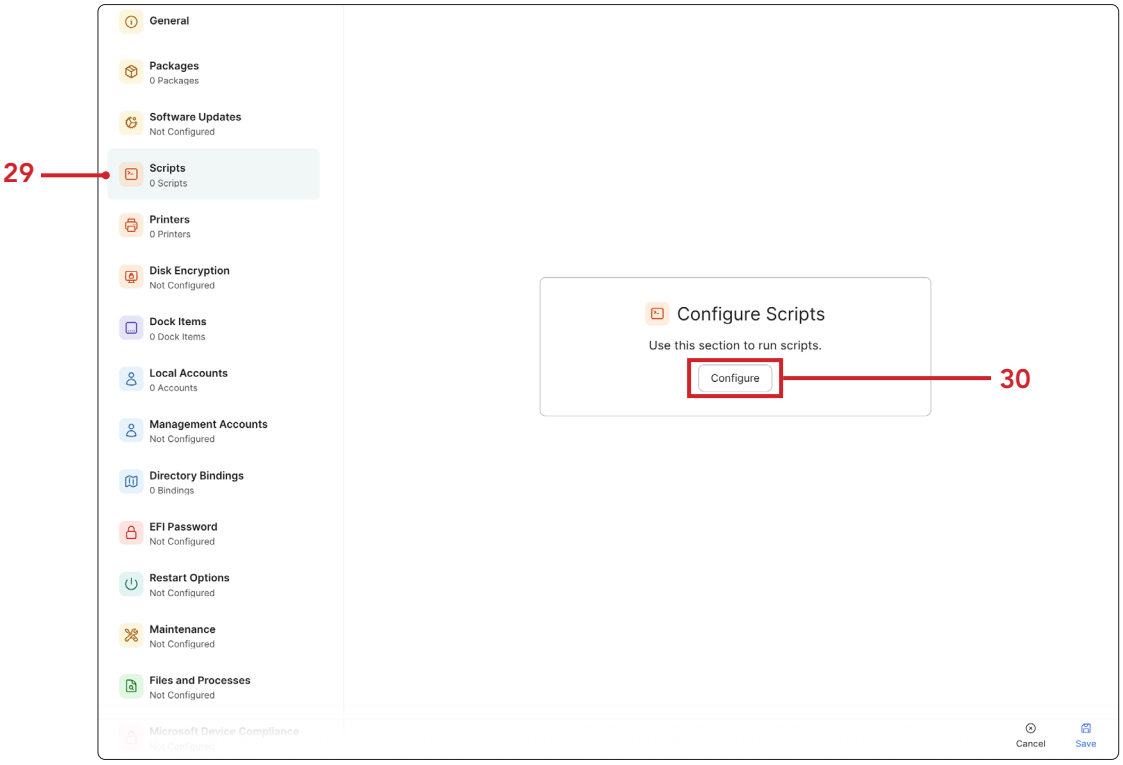
20. In Jamf Pro, click Computers in the sidebar.
21. Click Policies.
22. Click New (+).




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.

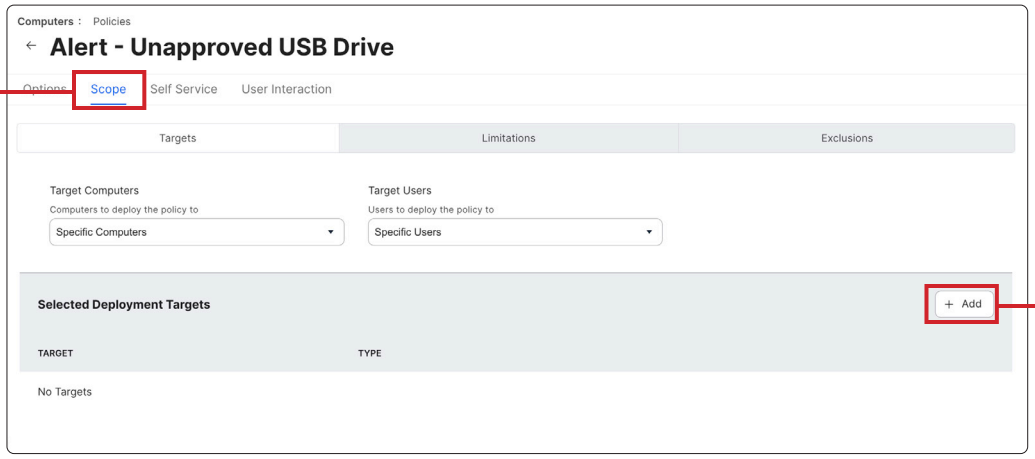


29. In the payload sidebar, click Scripts.
30. Click Configure.

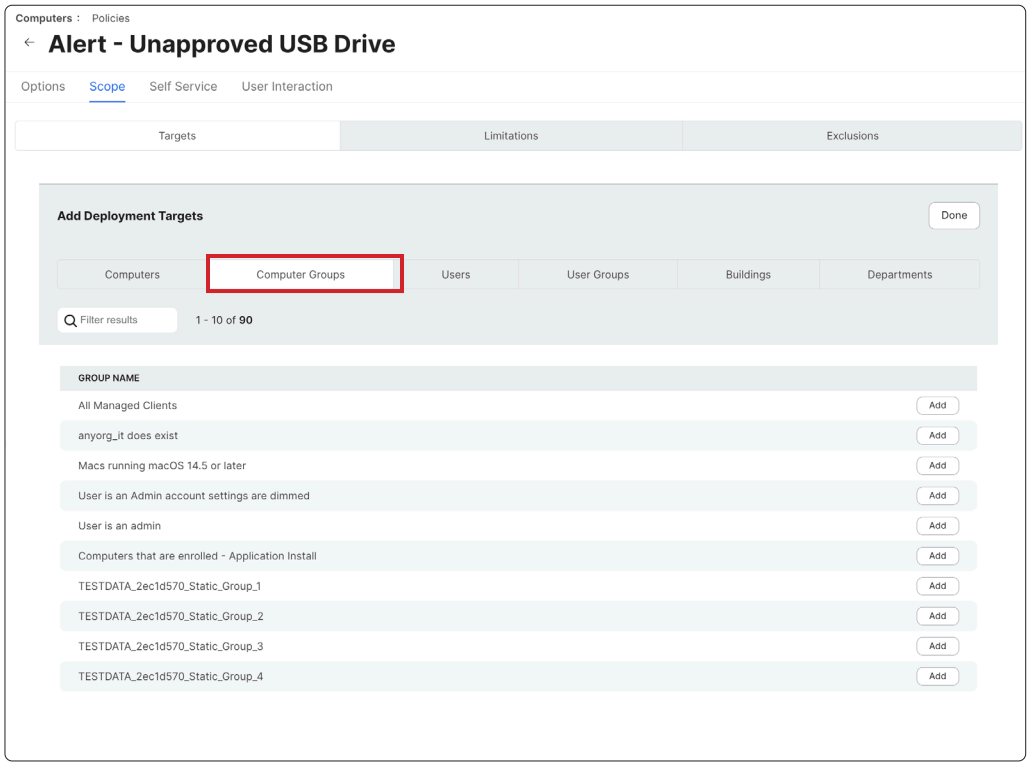



31. Locate the "Unapproved USB Drive Alert" script in the list.
32. Click Add next to "Unapproved USB Drive Alert".


33. Click Scope.
34. Click Add (+).



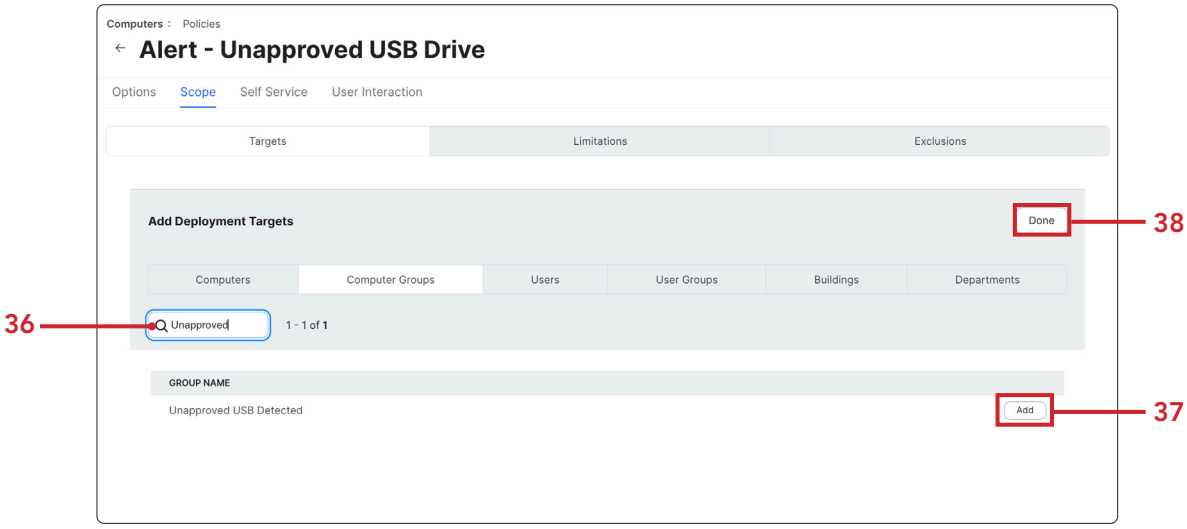
35. Click Computer Groups.




36. Search for Unapproved USB Detected.

37. Click Add.

38. Done




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.

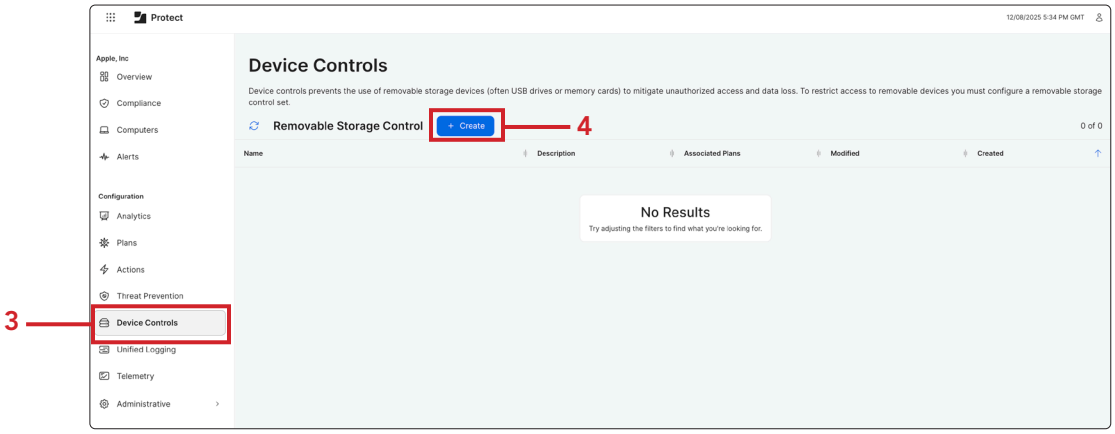
In this section, you will configure Jamf Protect to monitor and control USB and external drive connections. You will create a Removable Storage Control Set and add your approved devices as overrides.

**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**

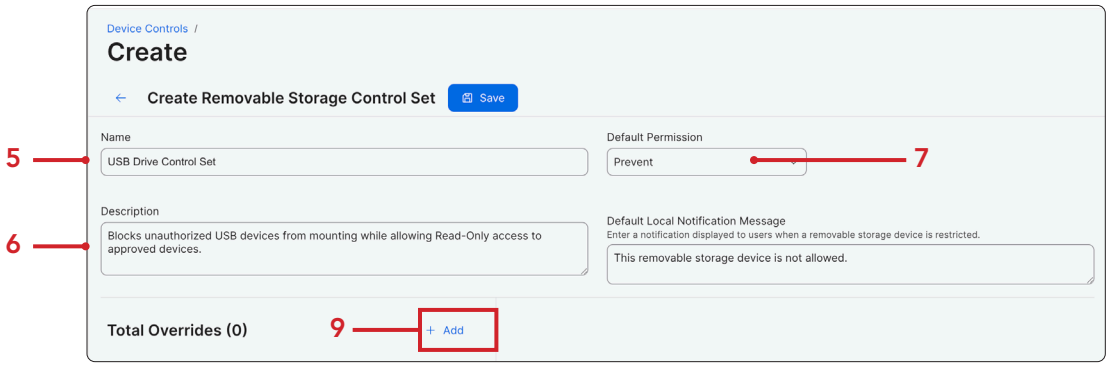
3. In the left sidebar, click Device Controls.
4. Click Create.



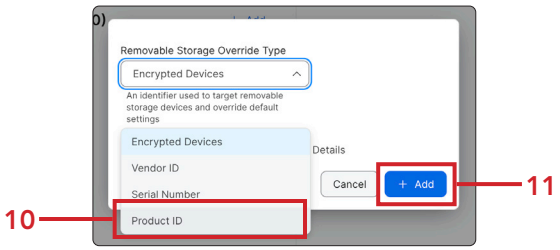
5. In the Name field, enter: **USB Drive Control Set**.
6. In the Description field, enter: **Blocks unauthorized USB devices from mounting while allowing Read-Only access to approved devices**.
7. Verify that Default Permission is set to Prevent.
   NOTE: The Prevent permission blocks unapproved devices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

**Add Approved Device Overrides**

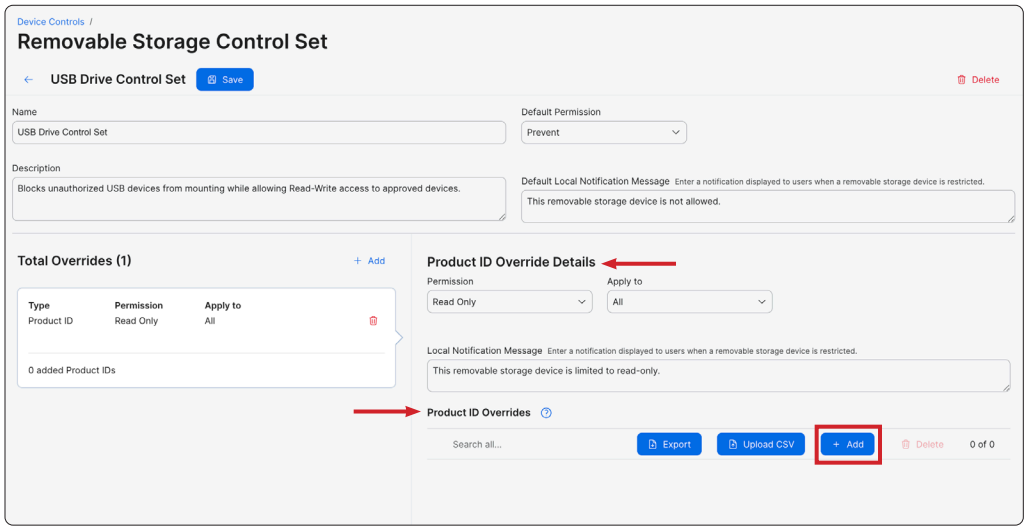
8. Scroll down to the Total Overrides section.
9. Under Total Overrides, click Add (+).



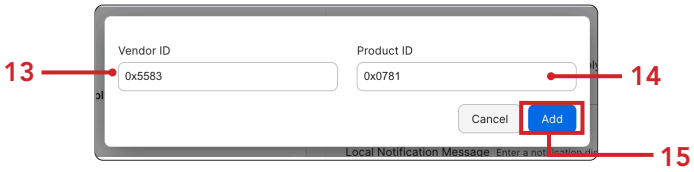

10. Under the Removable Storage Override Type, click the menu and select Product ID.
11. Click Add (+).



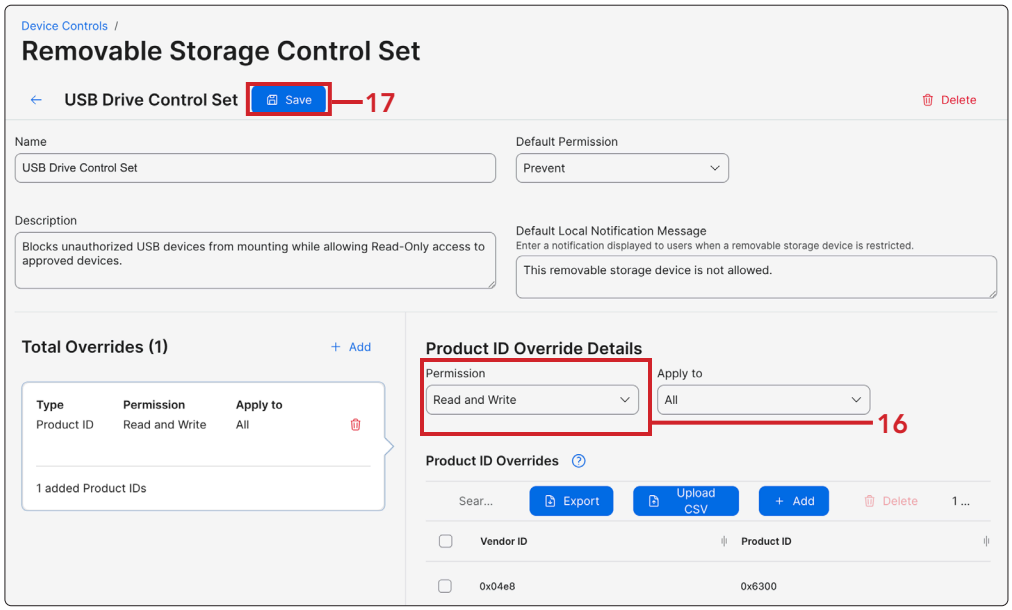
12. Navigate to the Product ID Override Details section, under Product ID Overrides, click Add (+).




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.




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:

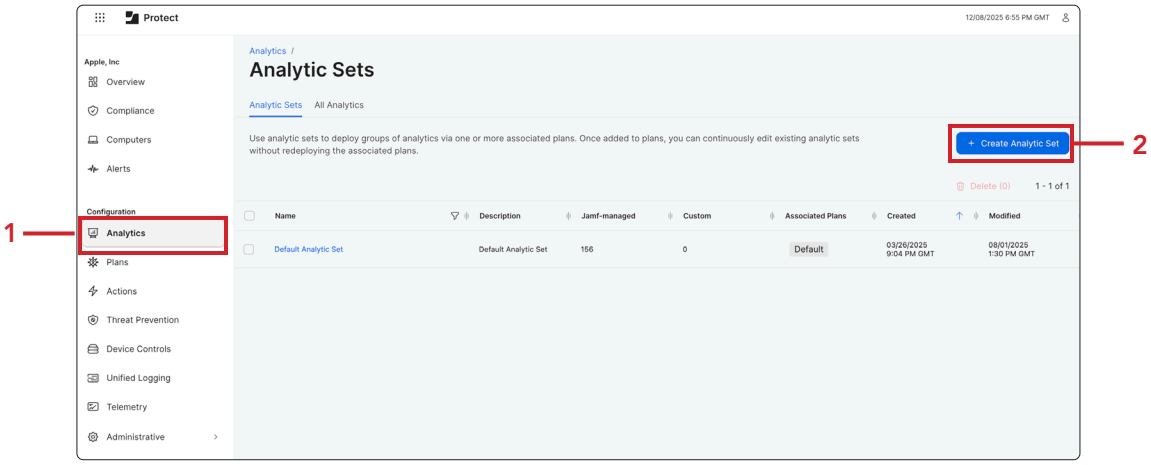
- Extension Attribute: Jamf Protect Alerts - collects identifiers written by Jamf Protect
- Smart Computer Group: Unapproved USB Detected - matches computers with the identifier "unapproved_usb"
- Policy: Alert - Unapproved USB Drive - runs the notification script when computers join the Smart Group

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:

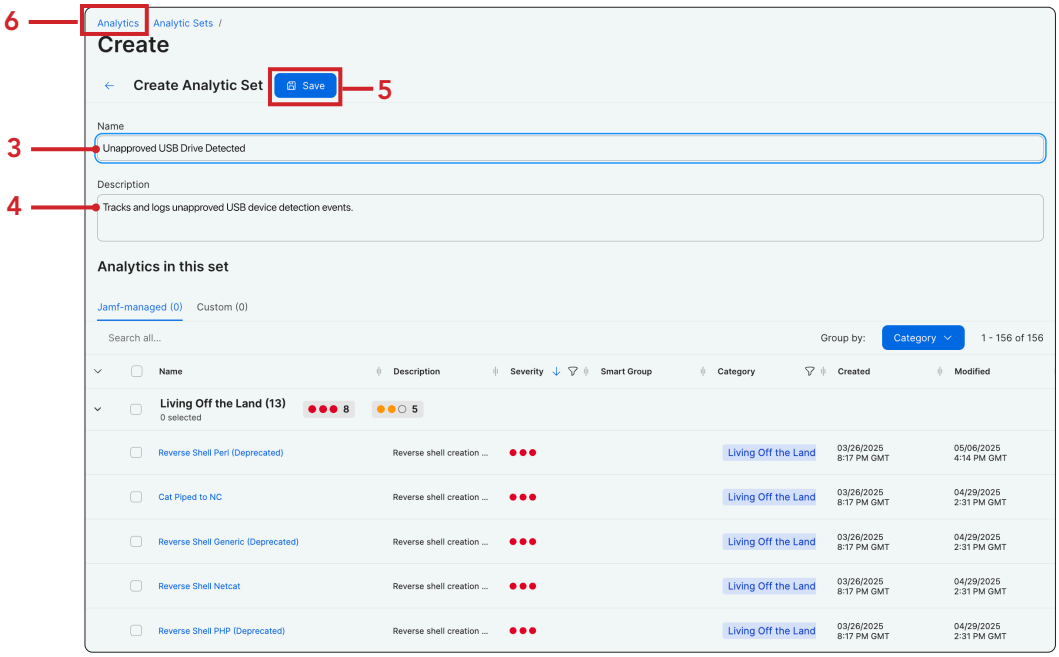
- Unapproved USB drive Inserted
- Jamf Protect writes identifier "unapproved_usb" to computer
- Extension Attribute collects identifier during inventory
- Computer joins "Unapproved USB Detected" Smart Group
- Policy runs and displays Jamf Helper notification

**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.

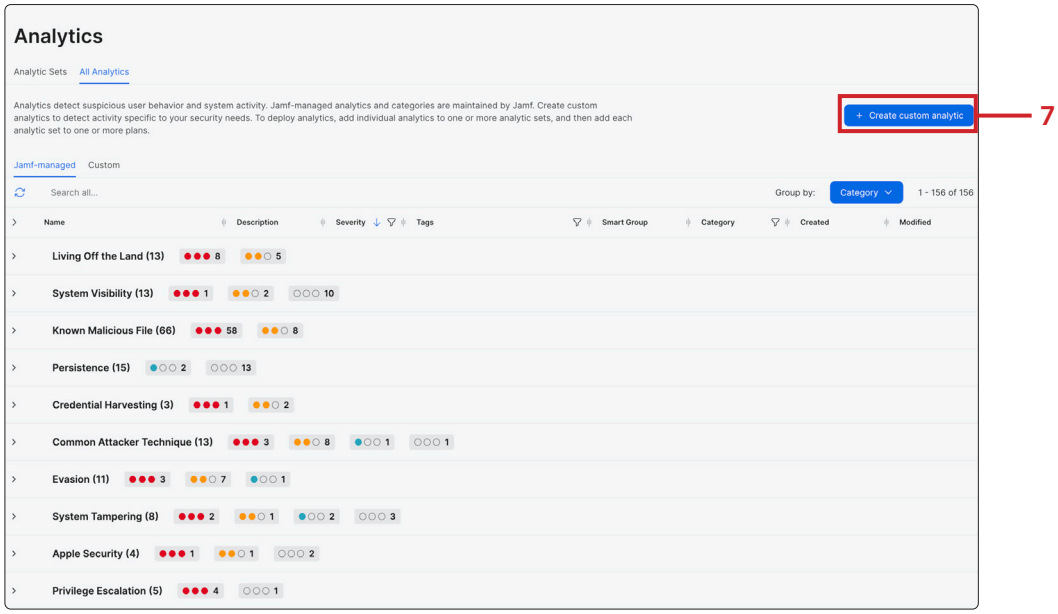


3. In the Name field, enter: **Unapproved USB Drive Detected.**
4. In the Description field enter, Tracks and logs unapproved USB device detection events
5. Click Save.
6. Click Analytics.



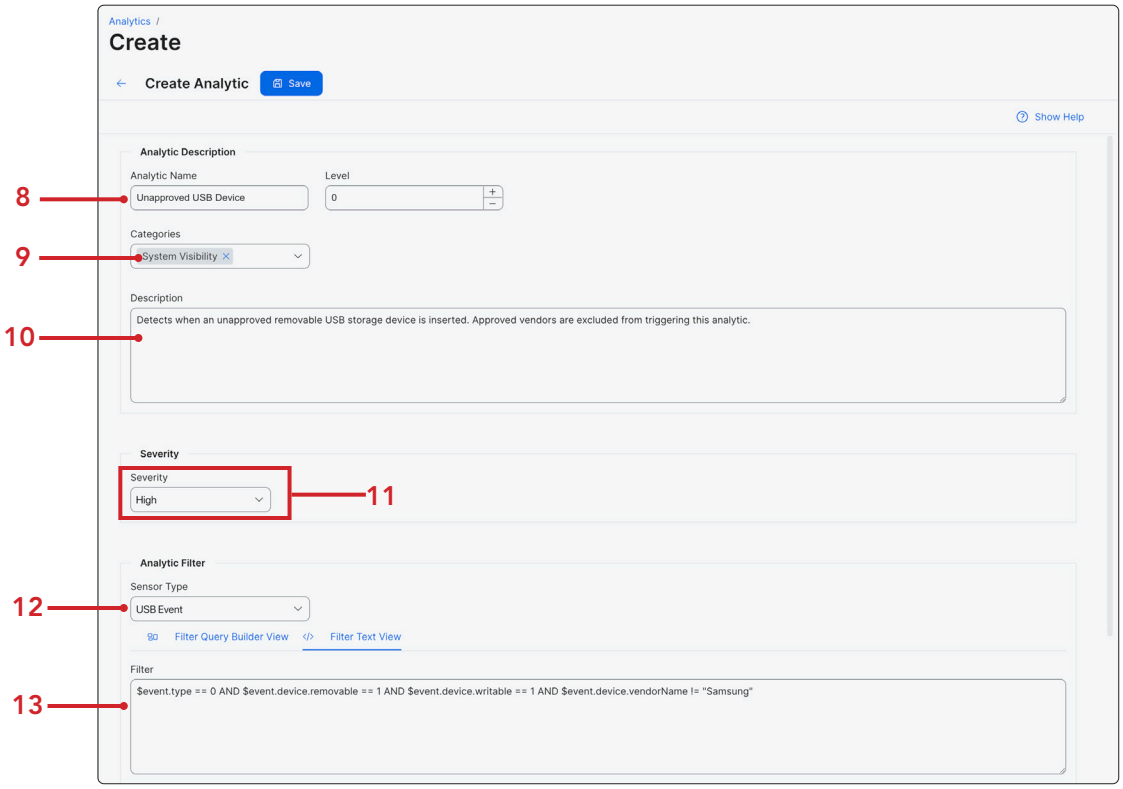

## Create the Custom Analytic

7. Click Create Custom Analytic.



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"
```




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

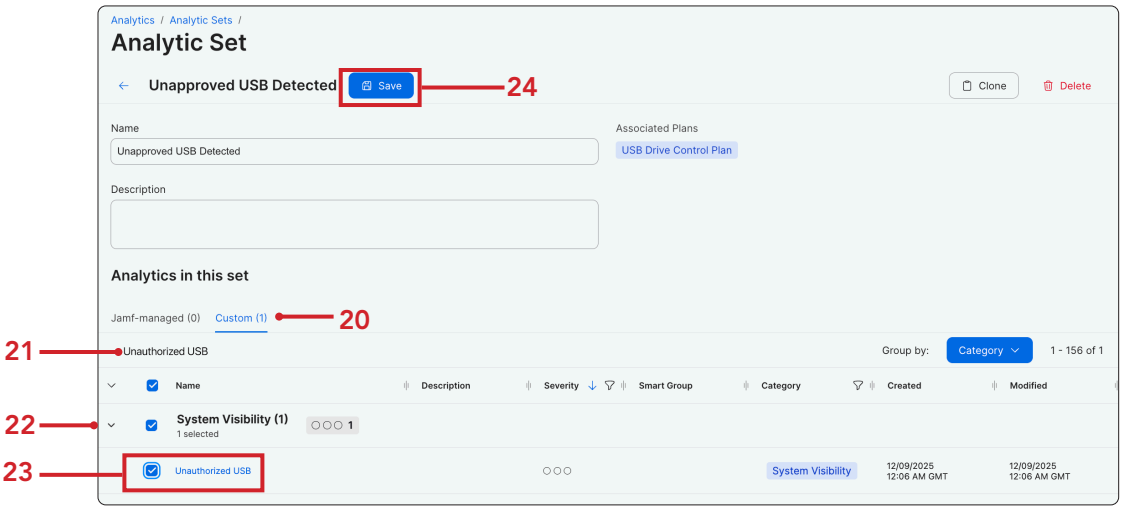
14. Select the checkbox for Add to Jamf Pro Smart Group.

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.


16. Click Save.

**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.




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

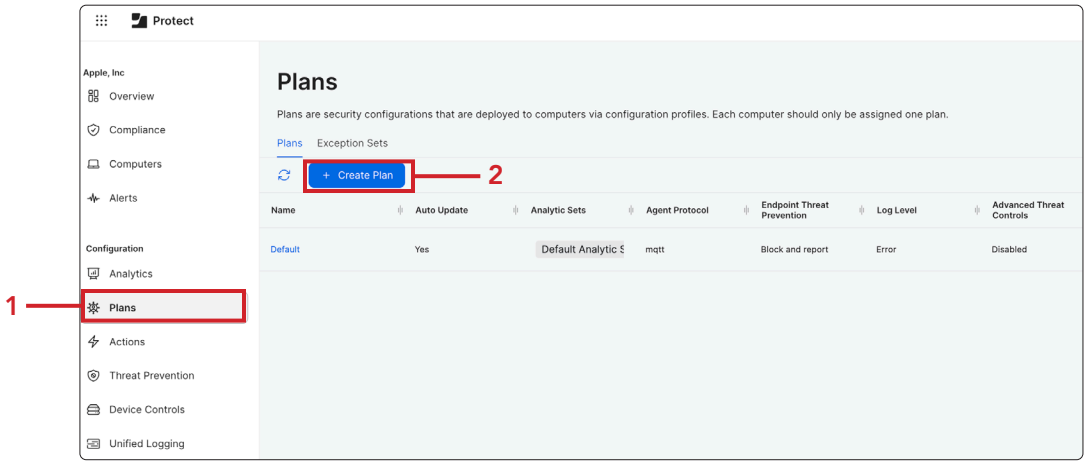
When you assign both to a Plan, computers receiving the Plan will:

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

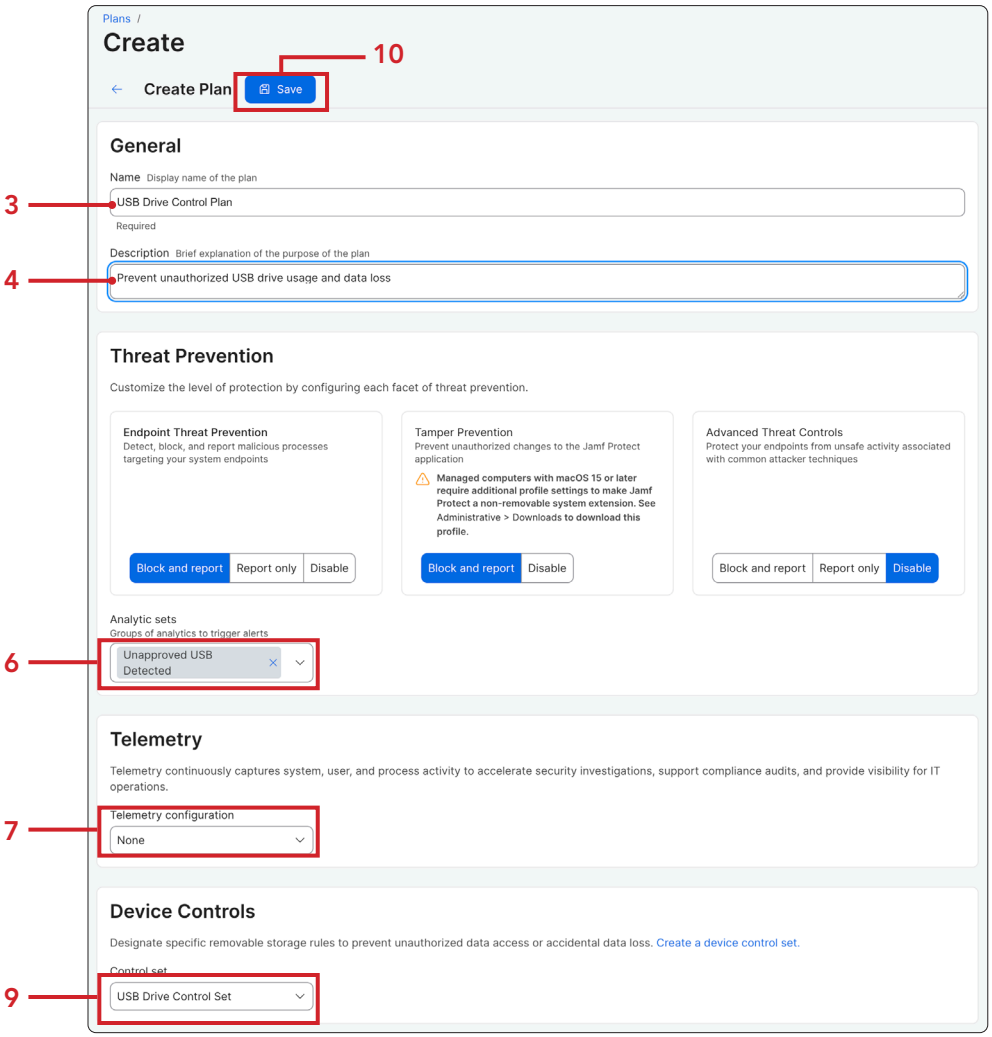
**Create a Plan**

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.




This completes this section.

## Section 8: Jamf Protect - Configure Email Notifications

What You'll Need

Hardware and Software

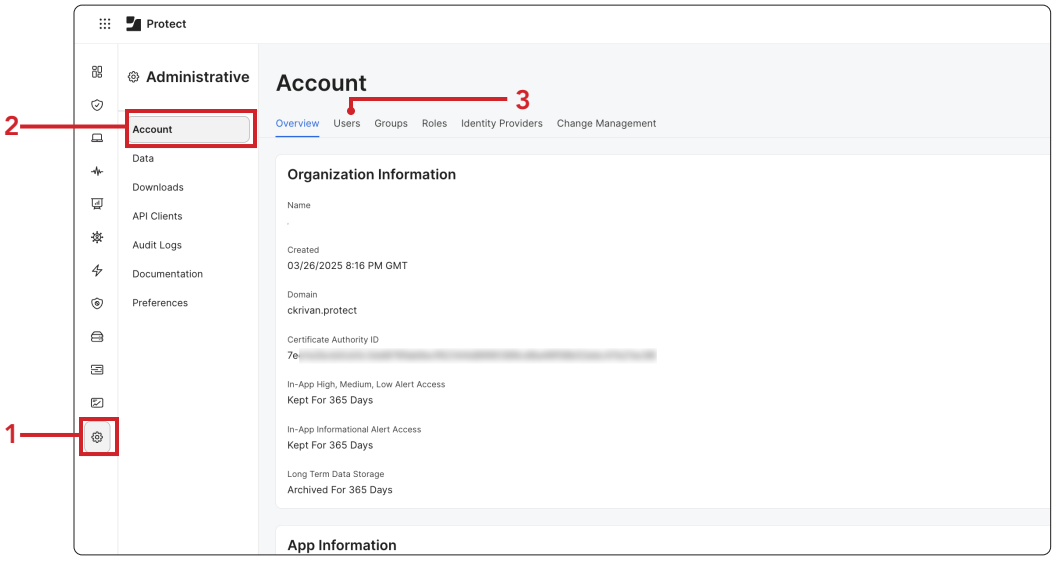
Requirements for following along with this section:

- 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

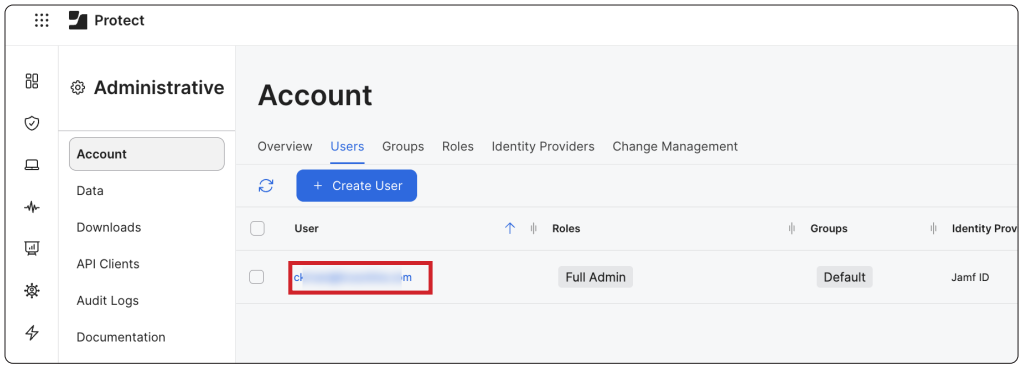
In this section, you will configure Jamf Protect to send email notifications to your IT team when security alerts are generated. Email notifications are enabled per user in Jamf Protect.

**Enable Email Notifications for IT Users**

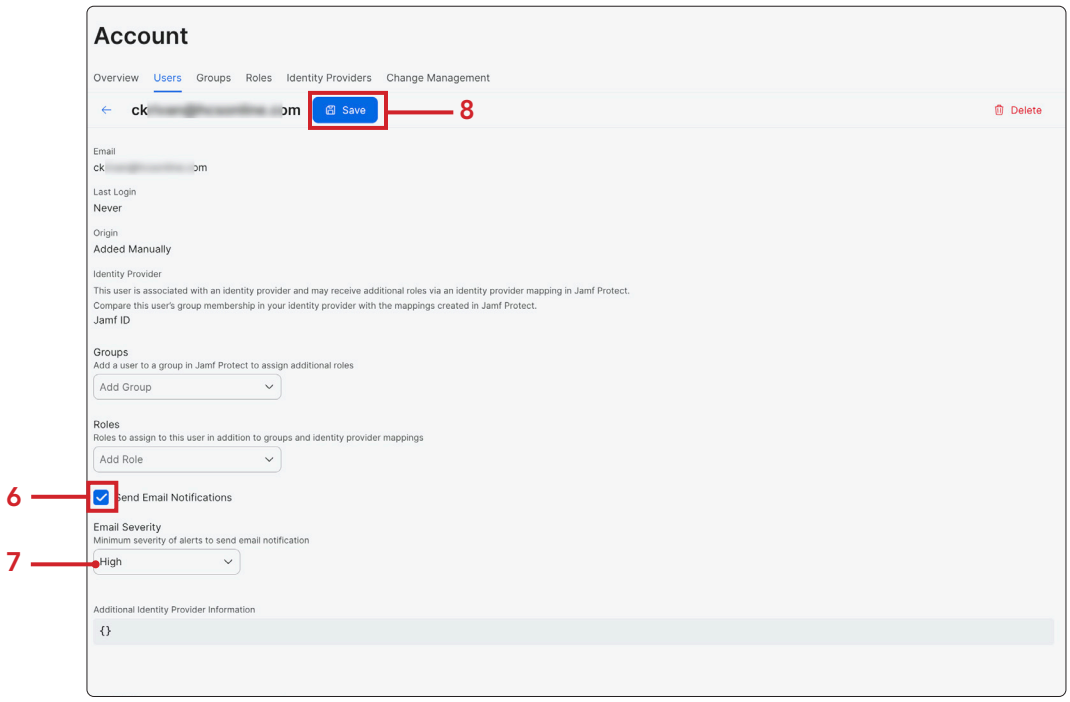
1. In Jamf Protect, click Administrative (⚙).
2. Click Account.
3. Click Users.




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.




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:

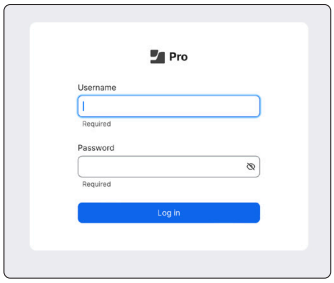
- Jamf Pro server with the Jamf Protect integration configured
- Jamf Protect with administrator privileges to the macOS Security portal (Jamf Protect web app)
- The USB Drive Control Plan fully configured from Sections 5-8
- Target computers or computer groups to receive the plan

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.

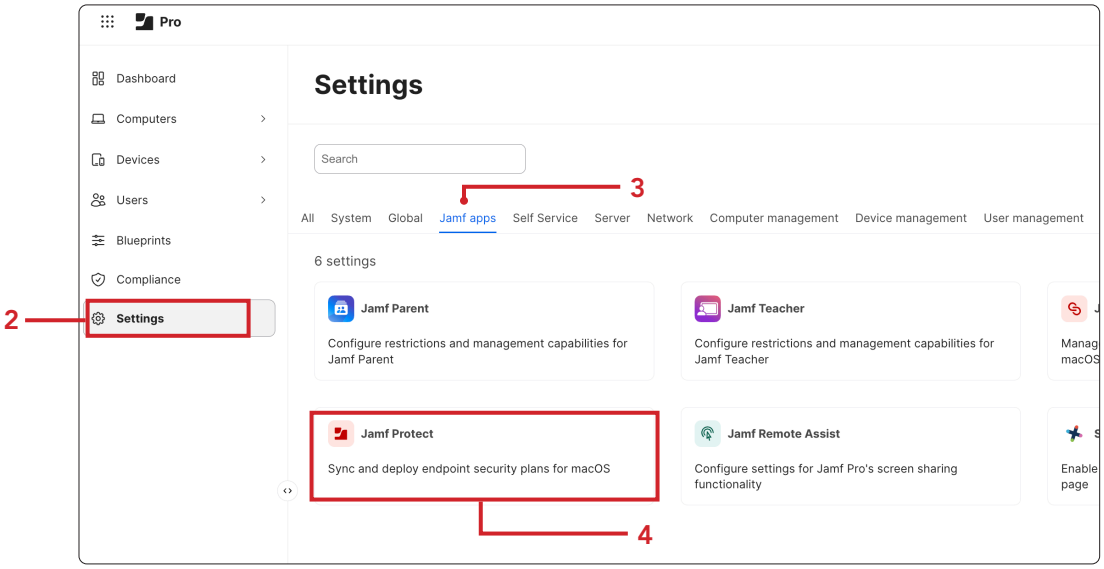
**How Plan Assignment Works**
Jamf Protect plans are assigned to computers through Jamf Pro, not directly in the macOS Security portal (Jamf Protect web app). This allows you to use your existing Jamf Pro computer groups and scoping logic to determine which computers receive each plan.

**Assign the Plan in Jamf Pro**

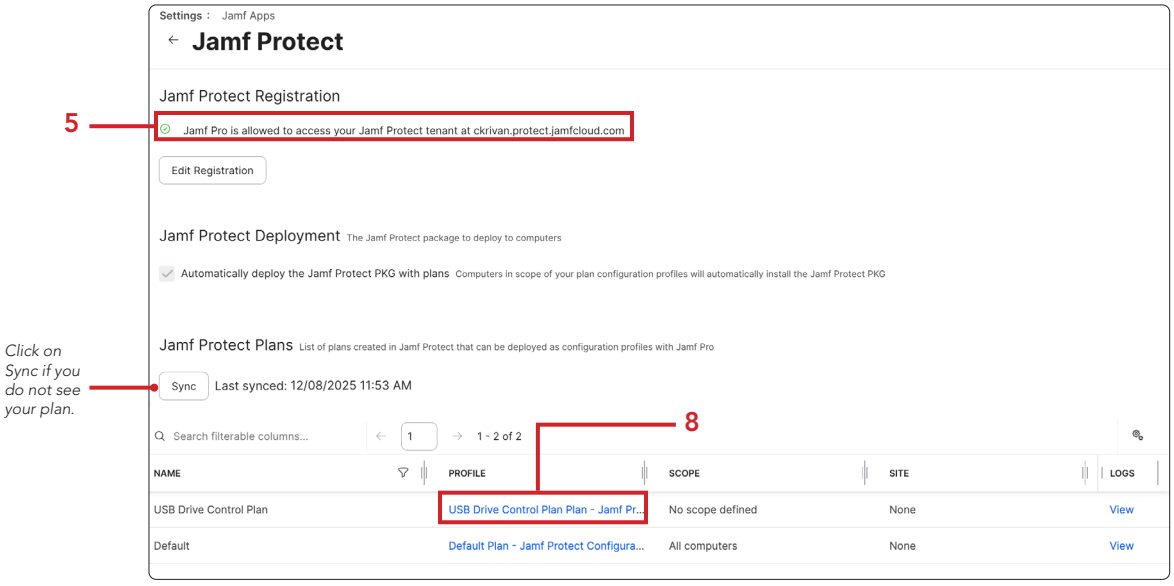
1. Log in to your Jamf Pro server.




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

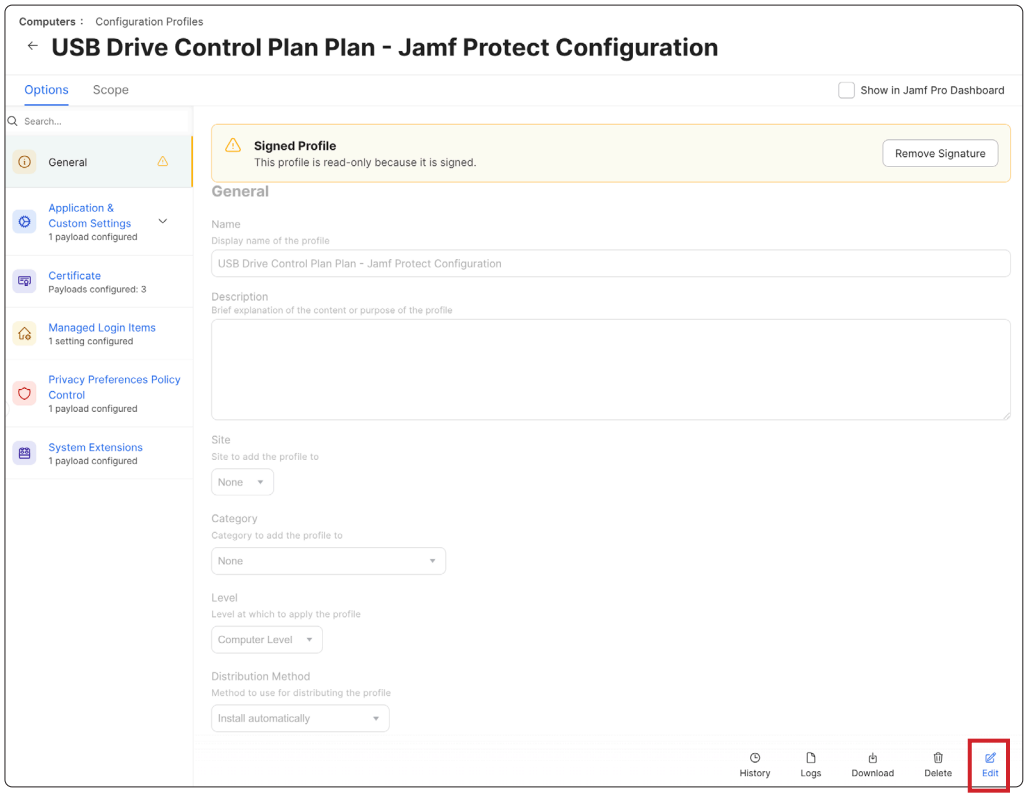


5. Verify that your Jamf Protect integration is connected (a ✓ shows a successful connection.)
6. Scroll down to the Plans section.
7. Locate your USB Drive Control Plan in the list. If you do not see your plan, click Sync
8. Click on the plan.

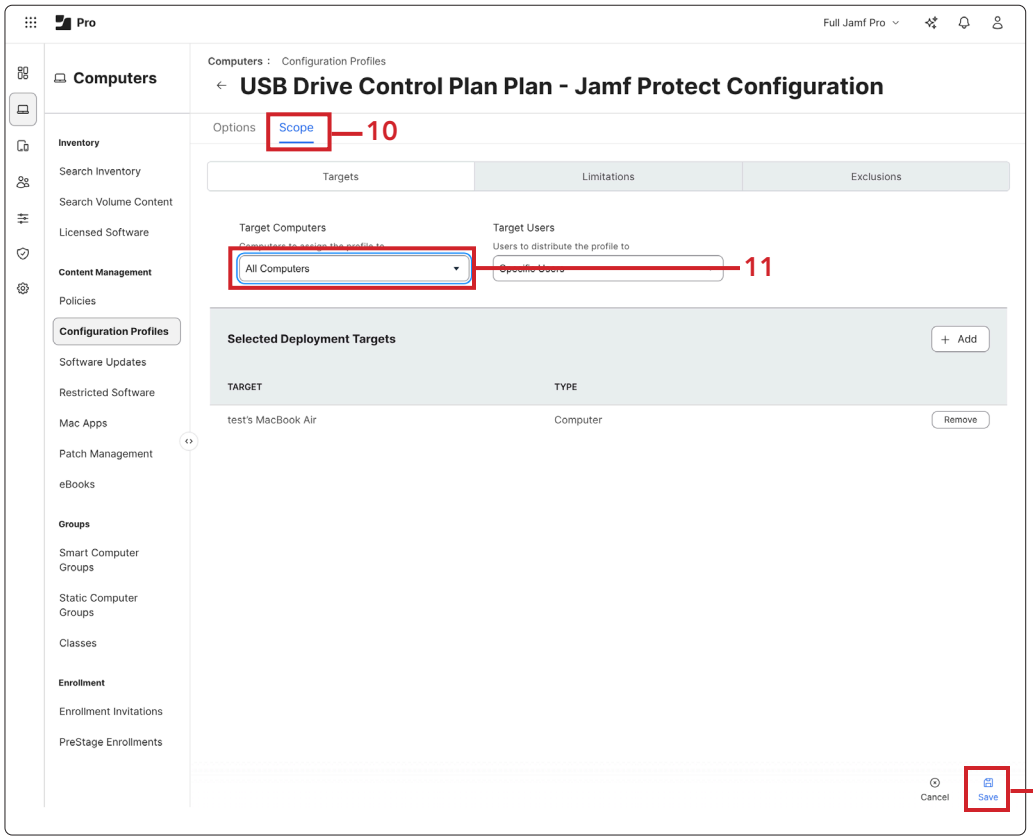



NOTE: Only one plan can be assigned per device. Verify that no conflicting plans are assigned before proceeding.

9. Click Edit.



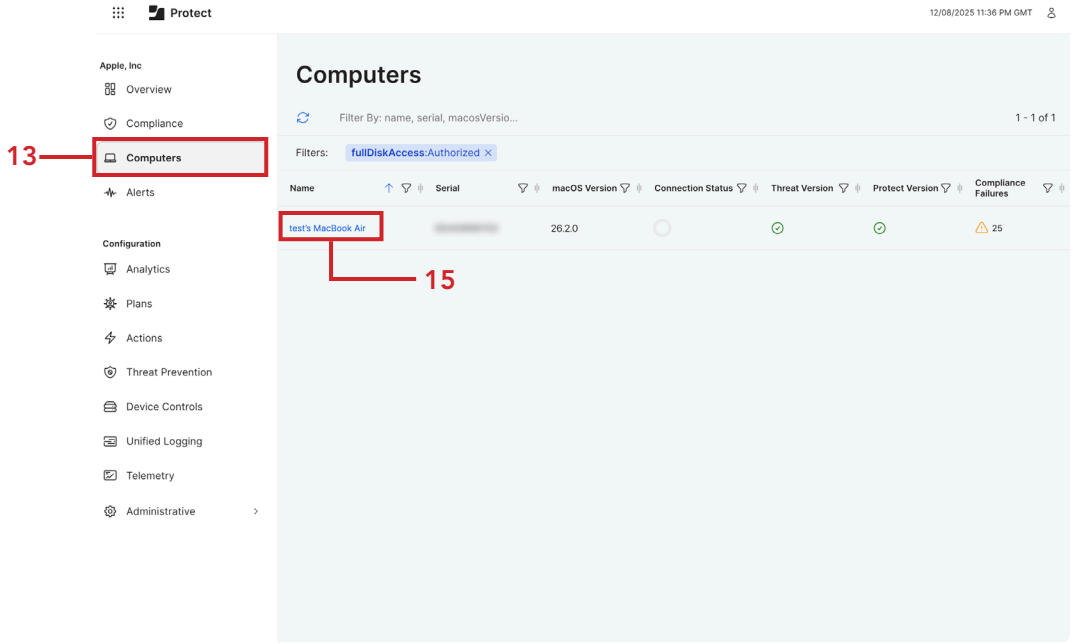
10. Click Scope.
11. Click the Target Computers menu and scope to your needs. This guide will scope to All Computers.
12. Click Save.



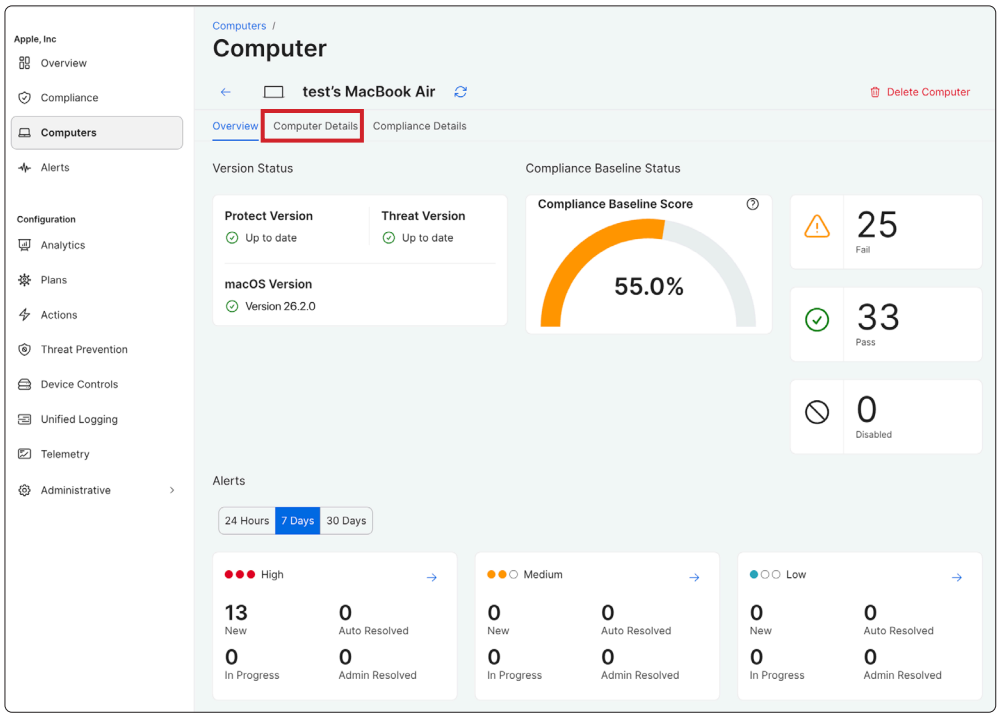

NOTE: You can also scope the plan to specific Smart Computer Groups or individual computers based on your deployment needs. Computers will receive the plan configuration on their next check-in with Jamf Protect. This typically occurs within 15 minutes but can be up to 24 hours depending on your check-in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

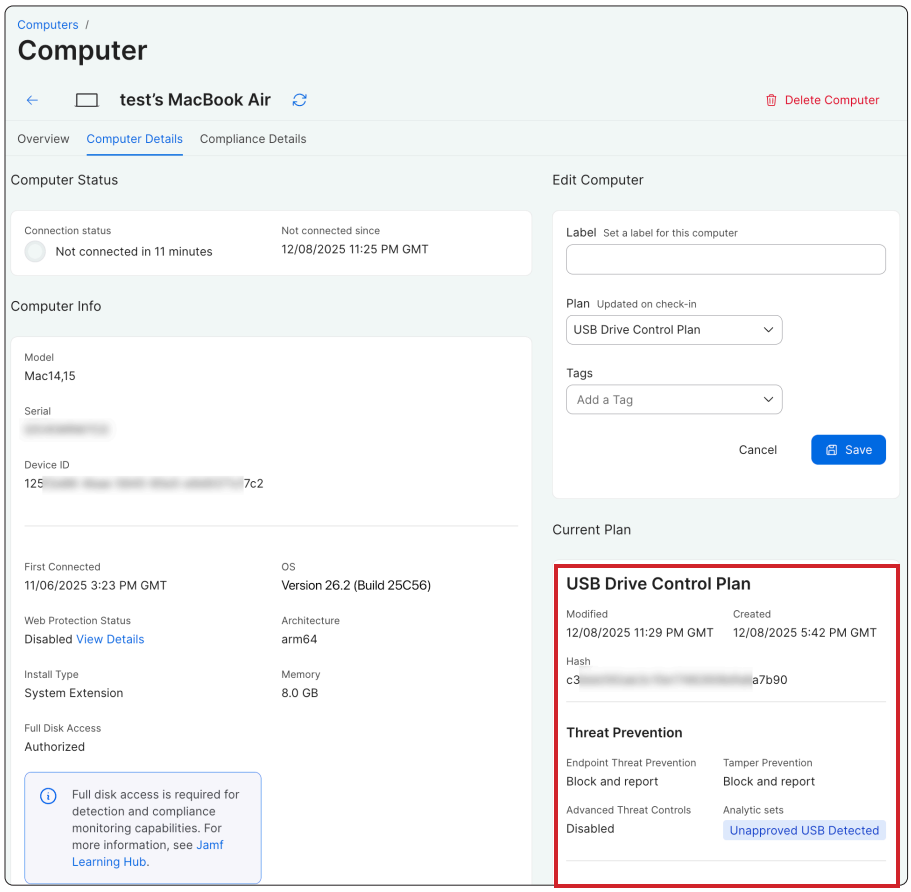



16. Click Computer Details.



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.




This completes this section.

## Section 10: Test the Configuration

What You'll Need

Hardware and Software

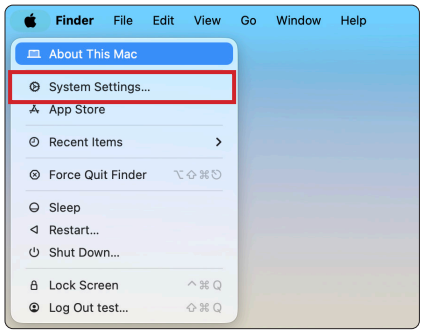
Requirements for following along with this section:

- 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)

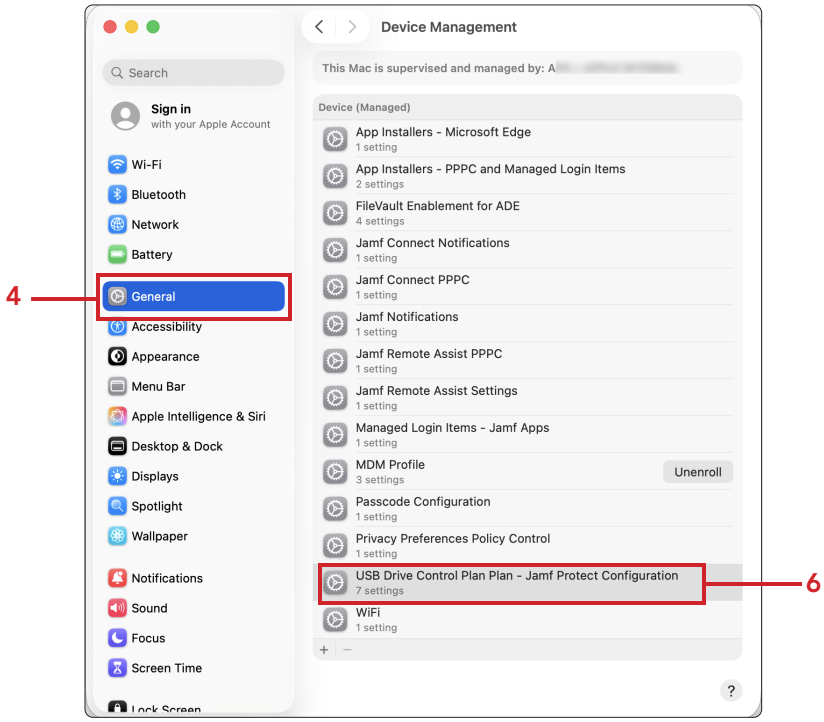
In this section, you will verify that the entire configuration works as expected. Testing should be performed on a non-production Mac computer before deploying to your entire fleet.

**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.

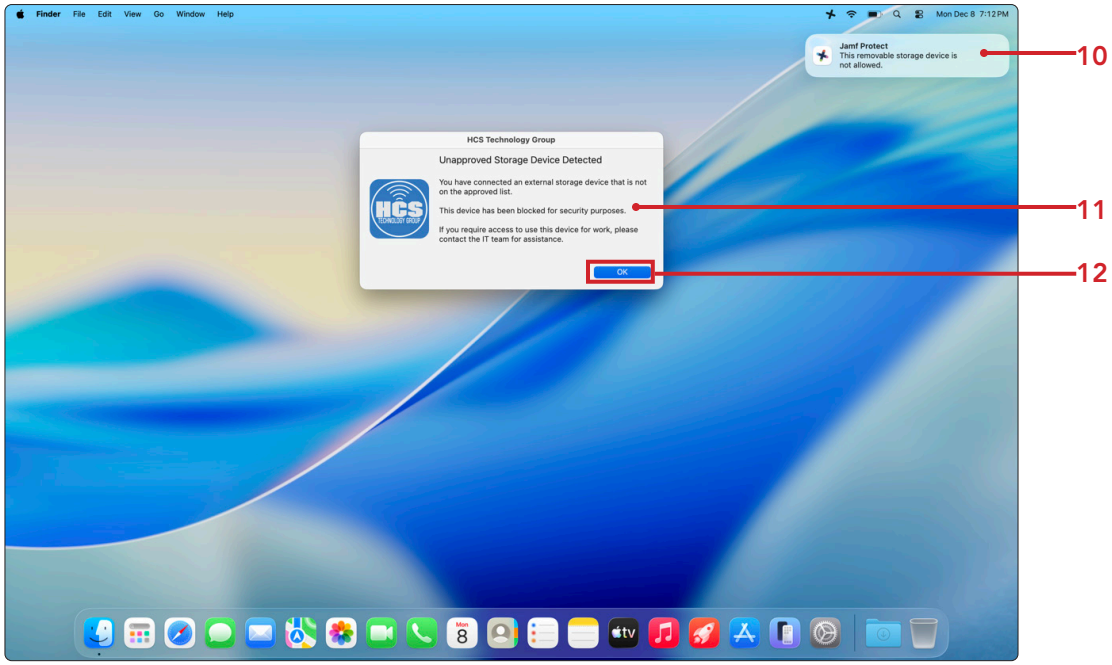


4. In the sidebar, click General.
5. Scroll down and click Device Management.
6. Verify the Jamf Protect configuration profile is installed. This is the plan from Jamf Protect.

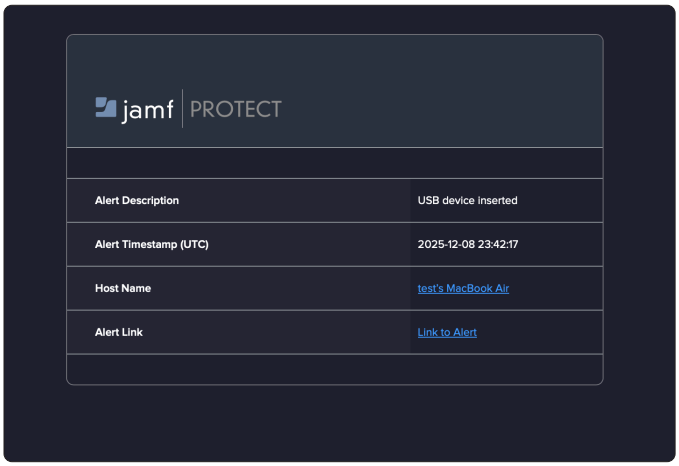


**Test with an Unapproved Drive**

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.