



CROWDSTRIKE

FALCON DEVICE CONTROL TRIAL GUIDE

TABLE OF CONTENTS

3	INTRODUCTION
4	GETTING STARTED
5	CREATING A DEVICE CONTROL POLICY
9	USING ASSIGNED HOST GROUPS
12	CONFIGURING GROUPS FOR USB DEVICE CONTROL
15	TESTING
16	CREATING AN EXCEPTION IN A USB DEVICE POLICY
20	SUMMARY
20	ABOUT CROWDSTRIKE

INTRODUCTION

CrowdStrike Falcon Device Control™ enables safe and accountable USB device use across your organization. Built on the CrowdStrike Falcon® platform, it uniquely combines visibility and granular control, allowing administrators to ensure that only approved devices are used in your environment. When used with Falcon Insight™, CrowdStrike's endpoint detection and response (EDR) solution, visibility is extended to include historical detailed logging and reporting capabilities.

This user guide allows you to realize the value of device control in context with the rest of the Falcon interface. In this guide, we explore a few use cases for the Falcon Device Control module to help you easily create, enforce and maintain policies using a simple, centralized approach.

GETTING STARTED

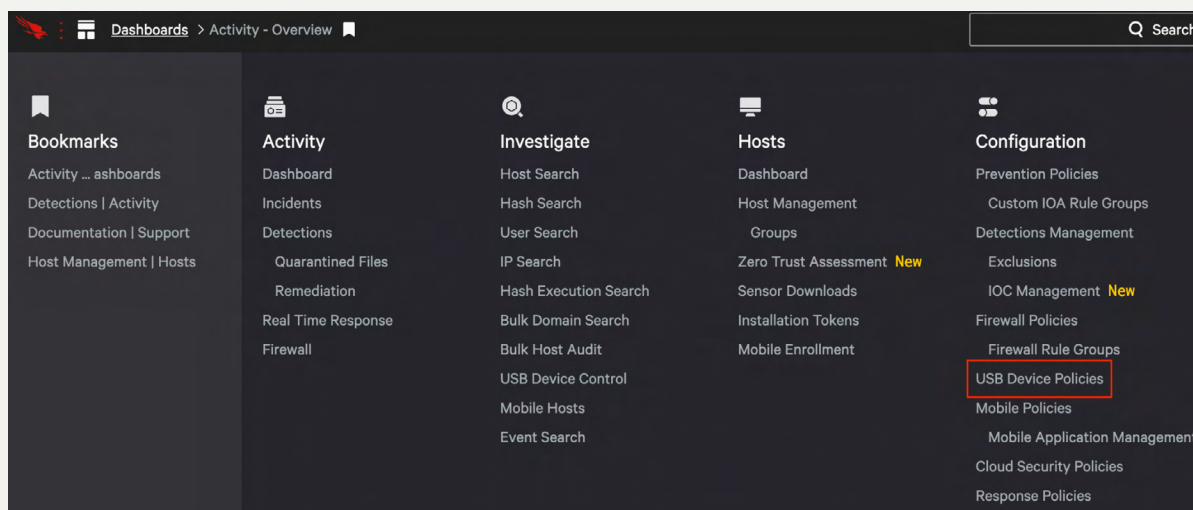
In this guide, we introduce you to the USB device management process to get you started. For a more in-depth understanding of Falcon Device Control configuration options, refer to the [USB Device Control Feature Guide](#) in the Falcon console.

Applying a device control policy to a system or systems has two basic steps:

1. Create a policy
2. Apply that policy to a group

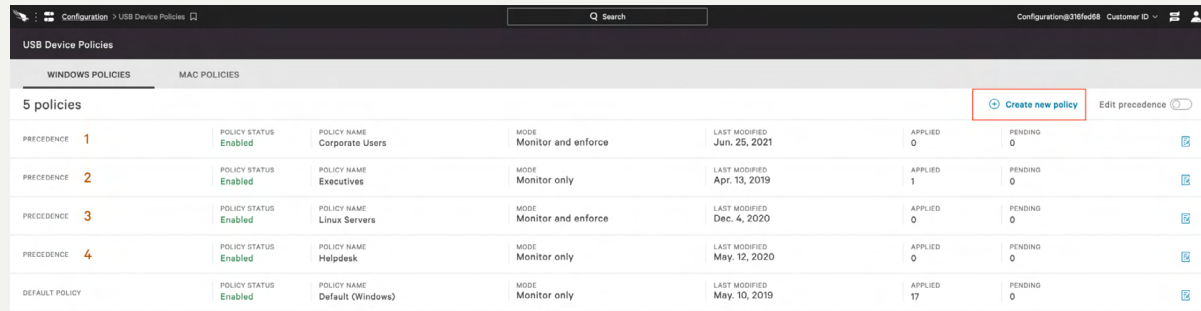
After logging in to the CrowdStrike Falcon user interface (UI), you can access the USB Device Control policies in the Configuration App. Creating a device control policy is simple. All policies can be managed from the policy page. The policy page allows you to create hierarchical policies to ensure the right devices receive the correct policies.

To get started, click on the Falcon logo in the upper left corner and navigate to “USB Device Policies.”



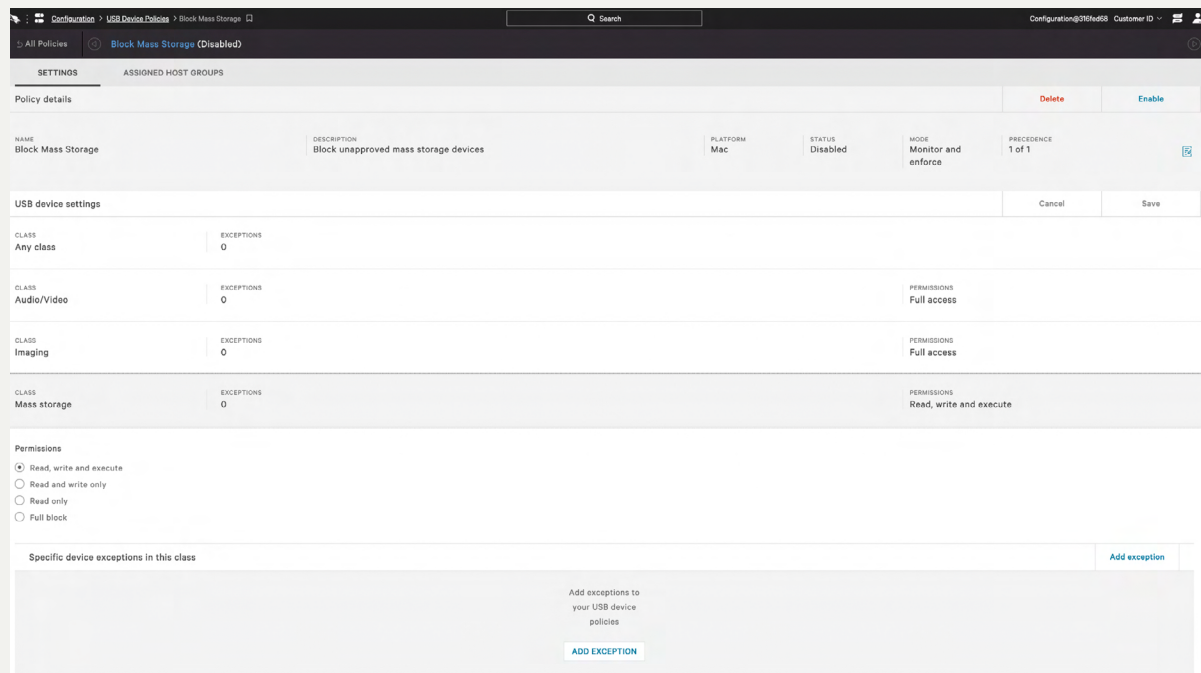
CREATING A DEVICE CONTROL POLICY

On the “USB Device Policies” page, click the “Create new policy” button in the upper right.



USB Device Policies							
WINDOWS POLICIES				MAC POLICIES			
5 policies Create new policy Edit precedence							
PRECEDENCE 1	POLICY STATUS Enabled	POLICY NAME Corporate Users	MODE Monitor and enforce	LAST MODIFIED Jun. 25, 2021	APPLIED 0	PENDING 0	
PRECEDENCE 2	POLICY STATUS Enabled	POLICY NAME Executives	MODE Monitor only	LAST MODIFIED Apr. 13, 2019	APPLIED 1	PENDING 0	
PRECEDENCE 3	POLICY STATUS Enabled	POLICY NAME Linux Servers	MODE Monitor and enforce	LAST MODIFIED Dec. 4, 2020	APPLIED 0	PENDING 0	
PRECEDENCE 4	POLICY STATUS Enabled	POLICY NAME Helpdesk	MODE Monitor only	LAST MODIFIED May. 12, 2020	APPLIED 0	PENDING 0	
DEFAULT POLICY	POLICY STATUS Enabled	POLICY NAME Default (Windows)	MODE Monitor only	LAST MODIFIED May. 10, 2019	APPLIED 17	PENDING 0	

Next, select the “Platform” (Windows or Mac), give the new policy a “Name” and “Description (Optional)” and then select the “Mode.”



Configuration > USB Device Policies > Block Mass Storage					
Configuration USB Device Policies Block Mass Storage Search Configuration@316fed59 Customer ID					
All Policies Block Mass Storage (Disabled)					
SETTINGS ASSIGNED HOST GROUPS					
Policy details Delete Enable					
NAME	DESCRIPTION	PLATFORM	STATUS	MODE	PRECEDENCE
Block Mass Storage	Block unapproved mass storage devices	Mac	Disabled	Monitor and enforce	1 of 1
USB device settings Cancel Save					
CLASS	EXCEPTIONS	PERMISSIONS			
Any class	0				
CLASS	EXCEPTIONS	PERMISSIONS			
Audio/Video	0	Full access			
CLASS	EXCEPTIONS	PERMISSIONS			
Imaging	0	Full access			
CLASS	EXCEPTIONS	PERMISSIONS			
Mass storage	0	Read, write and execute			
Permissions Read, write and execute Read and write only Read only Full block					
Specific device exceptions in this class Add exception					
Add exceptions to your USB device policies ADD EXCEPTION					

New policy details

PLATFORM

Mac

NAME

Block Mass Storage

DESCRIPTION (OPTIONAL)

Block unapproved mass storage devices

MODE

☒ Monitor and enforce
☐ Monitor only
☐ Off

☐ Start with a copy of the default policy

CANCEL

CREATE POLICY

After you fill in the details, click “Create Policy” to be sent to the “Policy details” page, which lists the various USB class types. Policy settings can be set according to specific class types or by using the “Any class” option near the top. The different class types include “Audio/Video” (e.g., cameras and microphones), “Imaging” (e.g., digital cameras), “Mass storage,” “Mobile” (e.g., cell phones), “Printers,” and “Wireless” devices. You can see the default settings are set to “Full access” in the “Permissions” column. (“Mass storage” is set to “Read, write and execute” by default, which is the same as “Full access.”)

Configuration > USB Device Policies > Block Mass Storage

Search
Configuration@310fed59 Customer ID

All Policies
Block Mass Storage (Disabled)

SETTINGS
ASSIGNED HOST GROUPS

Policy details
Delete Enable

NAME	DESCRIPTION	PLATFORM	STATUS	MODE	PRIORITY
Block Mass Storage	Block unapproved mass storage devices	Mac	Disabled	Monitor and enforce	1 of 1

USB device settings
Cancel Save

CLASS	EXCEPTIONS	PERMISSIONS
Any class	0	
Audio/Video	0	Full access
Imaging	0	Full access
Mass storage	0	Read, write and execute
Mobile (MTP/PTP)	0	Full access
Printer	0	Full access
Wireless	0	Full access

End User Notifications
0

Send a pop-up notification to the device end user when they trigger this policy.

As an example, let's block all mass storage devices on a Mac for this particular policy. Select "Mass storage" to expand its configuration options (clicking on any class will expand its configuration options). Note that while all other classes offer two permission options — "Full access" or "Full block" — the mass storage device class offers additional options that provide more flexibility.

Configuration > USB Device Policies > Block Mass Storage [1]

Configuration:316fed66 Customer ID

Block Mass Storage (Disabled)

SETTINGS ASSIGNED HOST GROUPS

Policy details

NAME: Block Mass Storage DESCRIPTION: Block unapproved mass storage devices PLATFORM: Mac STATUS: Disabled MODE: Monitor and enforce PRECEDENCE: 1 of 1

USB device settings

CLASS: Any class EXCEPTIONS: 0

CLASS: Audio/Video EXCEPTIONS: 0 PERMISSIONS: Full access

CLASS: Imaging EXCEPTIONS: 0 PERMISSIONS: Full access

CLASS: Mass storage EXCEPTIONS: 0 PERMISSIONS: Read, write and execute

Permissions

☒ Read, write and execute

☐ Read and write only

☐ Read only

☐ Full block

Specific device exceptions in this class

Add exception

Add exceptions to your USB device policies

ADD EXCEPTION

Let's change this policy so that mass storage devices in this policy are all blocked by selecting the "Full block" radio button. After making any change to a policy, a banner will appear reminding the user that there are unsaved changes. Scroll to the bottom of the page and enable "End User Notifications" (this will make validating the policy easier).

CLASS	EXCEPTIONS	PERMISSIONS
Mass storage	0	Full block
Mobile (MTP/PTP)	0	Full access
Printer	0	Full access
Wireless	0	Full access

End User Notifications ☒

Send a pop-up notification to the device end user when they trigger this policy.

After making a change to the policy, scroll to the top of the page (if necessary) and select “Save.” Because this is a new policy, there is one more step after making changes and saving it: The policy must be set to “Enable” before it will be applied.

The screenshot shows the 'Block Mass Storage (Disabled)' policy configuration page. At the top, a message states: 'There are unsaved changes on the Policy Settings tab'. The interface is divided into two main tabs: 'SETTINGS' and 'ASSIGNED HOST GROUPS'. The 'SETTINGS' tab is active and contains the following sections:

- Policy details:** Includes a 'Delete' button and an 'Enable' button (highlighted with a red box).
- NAME:** Block Mass Storage
- DESCRIPTION:** Block unapproved mass storage devices
- PLATFORM:** Mac
- STATUS:** Disabled
- MODE:** Monitor and enforce
- PRIORITY:** 1 of 1

Below these details is the 'USB device settings' section, which includes a 'Cancel' button and a 'Save' button (highlighted with a red box). This section lists three device classes with their respective permissions:

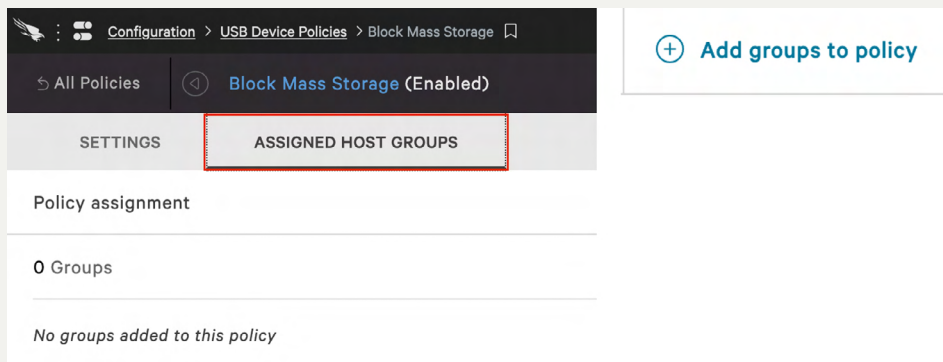
CLASS	EXCEPTIONS	PERMISSIONS
Any class	0	
Audio/Video	0	Full access
Imaging	0	Full access
Mass storage	0	Full block

At the bottom, the 'Permissions' section shows three radio button options: 'Read, write and execute', 'Read and write only', and 'Full block' (which is selected and highlighted with a red box).

Let's quickly review this example policy. The platform selected was Mac systems. The policy to block all mass storage devices was chosen, saved and enabled. The policy must now be assigned to a host group.

USING ASSIGNED HOST GROUPS

Recall that changes to the policy were made on the “Settings” tab. A quick way to pivot to host groups is to use the “Assigned Host Groups” tab. Clicking on it shows that no groups are currently assigned to this policy. Let’s change that.



On the right-hand side of the “Assigned Host Groups” tab, there is an “Add groups to policy” button. Select the “+” icon to add the policy to existing groups or pivot to the “Groups” page in the Host Management app.

If host groups already exist, a page will open to allow you to apply the new USB device policy to those existing host groups. For this example, create a new host group by selecting the “Go to Groups page” link at the bottom center of the page.

Add groups to policy

	NAME	DESCRIPTION
☐	Automated Remediation	
☐	Corp Demo 2019	
☐	Corporate Laptops	
☐	Default Pod Namespace Group	
☐	Demo Prevention	
☐	Detect Mode AID	
☐	Detect Mode_Static	Group created from Migrating Assignment Rule from Policy Detect Mode
☐	DRAGOS DEMO	
☐	Enterprise_Protection_Static	Group created from Migrating Assignment Rule from Policy Enterprise_Protection
☐	Full Detection	
☐	Full RTR	
☐	Linux Servers - Prevention	Linux
☐	Mac Detect	Detection policy for Mac systems
☐	MAC trial testing	
☐	Malware Testing Lab	This group is for systems in the isolated lab. Since live malware and ransomware will be tested I've created a dynamic group based on hostname so anything cs-IMN* will automatically be assigned to this group.
☐	Malware Testing Static	

Need to create a new group? [Go to Groups page](#)

CANCELADD GROUPS TO POLICY

On the “Groups” page, find the “Add New Group” button on the right side of the page and click the “+” icon.

Hosts > Groups

Search

Hosts@141c3877 Customer ID

Groups

+ Add New Group

Hosts can be added to a group through multiple criteria, either dynamically through user-defined filters, statically through static host ID or statically by hostname. For this example, let's add systems dynamically. Dynamic host groups will automatically add systems that meet the selected criteria. This option allows policies to automatically be applied to new systems brought into the organization that meet the dynamic criteria, reducing the need to manually add systems to policies or groups.

New Group Details

NAME
Mac Mass Storage Device Block

DESCRIPTION
Block mass storage devices on Mac systems.

Group Type

One type per group, and type can't be switched later. [About host groups](#)

☒ **Dynamic**
Create a rule to automatically add and remove hosts based on filters

☐ **Static by host ID**
Add or remove hosts based on host ID

☐ **Static by hostname**
Add or remove hosts based on hostname

CANCEL ADD GROUP

Select the radio button that best fits your requirements.

Note: If this is your first time testing Falcon Device Control, testing on specific hosts is easy. Simply select the radio button “Static by host ID,” then select your specific test system.

Select “Add Group” after filling out the “New Group Details.”

CONFIGURING GROUPS FOR USB DEVICE CONTROL

In this example, the next step is to add attributes to the newly created group. Select the “Add Group” button from the “New Group Details” pop-up to be taken to the group details page.

Scroll to the bottom of the “Details” page to add hosts to this new group. Note that no hosts have been assigned to this group; to change that, click the “Edit assignment rule” button.

Hosts currently targeted by this group

[Edit assignment rule](#)  

Hostname	Last Seen	First Seen	OS Version	OU	Prevention Pol...	Firewall Policy	Response Policy	Sensor Update ...	USB Device Pol...	Containmen...	Sensor Vers...	Grouping Tags
 No Hosts Currently in Group ADD HOSTS												

Multiple attributes can be used to assign hosts to a group. In a static group you can simply select the specific host. Recall that in this example, the policy was configured as a dynamic group that will add systems according to platform. You can see below that all Mac systems will be automatically added to this group.

After adding systems, either statically or dynamically, click “Save” in the upper right.

Hosts > Groups > Mac Mass Storage Device Block

Back to Mac Mass Storage Device Block Details

Choose filter values for "Mac Mass Storage Device Block". Matching hosts are automatically assigned to this group. [CANCEL](#) [SAVE](#)

Platform: Mac X 2 Hosts found

Hostname	Sensor	Version	Grouping	Domain	OS Version	OU	Site	Platform	Pod ID	Pod Labels	Pod Name	Pod Namespace	Pod Service Account	Type	Status	Cloud
LabMac2...	1	5.41.1220...	1	N/A	2	Big Sur (11.0)	1	N/A	2	N/A	2	N/A	2	Workstat...	2	Normal
TMM-De...	1	5.41.1220...	1	N/A	2	Catalina (10.15)	1	N/A	2	N/A	2	N/A	2	Server	0	Normal
CSFALC...	0	6.28.1410...	1	N/A	2	Windows...	0	N/A	2	N/A	2	N/A	2	Server	0	Normal
CS-PING...	0	6.28.1410...	1	N/A	2	Windows...	0	N/A	2	N/A	2	N/A	2	Server	0	Normal
CS-PING...	0	6.28.139...	0	N/A	2	SLES 11.4	0	N/A	2	N/A	2	N/A	2	Server	0	Normal
CS-PING...	0	6.28.1230...	0	N/A	2	SLES 11.4	0	N/A	2	N/A	2	N/A	2	Server	0	Normal

2 Hosts

Hostname	Last Seen	Sensor Version	Domain	OS Version	Model	Type	OU	Site	Host ID	Status
LabMac2.local	Aug. 25, 2021 11:50...	6.28.14102.0		Catalina (10.15)	Macmini7,1				b6e64d9b0382434...	Normal
TMM-DemoMac-01	Aug. 20, 2021 13:20...	5.41.12209.0		Big Sur (11.0)	MacBookPro12,1				c95d5d2155a649a7...	Normal

LOAD MORE

You'll now be returned to the "Group Details" page and see that two systems have been added to the sample policy. Note that while systems have been applied to this group, no policies have yet been assigned to it. To add the sample USB policy to this group, click the edit icon to the right of the "USB Devices Policies" section.

USB Devices Policies

No assigned usb devices policies

Machine Learning Exclusions

EXCLUSIONS
0

IOA Exclusions

EXCLUSIONS
0

Sensor Visibility Exclusions

EXCLUSIONS
0

Hosts currently targeted by this group

Type to filter

2 Hosts found

Edit assignment rule

Hostname	Last S...	First Seen	OS Version	OU	Prevention Poli...	Firewall Policy	Response Policy	Sensor Update ...	USB Device Pol...	Containmen...	Sensor Vers...	Grouping Tags
LabMac2.local	Aug. 25, 2...	Jul. 13, 2020 2...	Catalina (10.15)		Default (Mac) Jan. 18, 2021 1...	No policy	TMM - Full RTR Dec. 1, 2020 15...	Default (Mac) Aug. 17, 2021 1...	Default (Mac) Aug. 5, 2021 16...	Normal	6.28.14102.0	
TMM-DemoMac-01	Aug. 20, 2...	Aug. 19, 2021 1...	Big Sur (11.0)		Default (Mac) Changes pendl...	No policy	TMM - Full RTR Changes pendl...	Default (Mac) Changes pendl...	Default (Mac) Changes pendl...	Normal	5.41.12203.0	

On the "USB Device Policies" page, select the platform you want to add a policy to (in this case it's under "Mac Policies"). Then click the "Edit to Add a Group" button.

Configuration > USB Device Policies

Search

Configuration@2e17bb4c Customer ID

USB Device Policies

WINDOWS POLICIES

MAC POLICIES

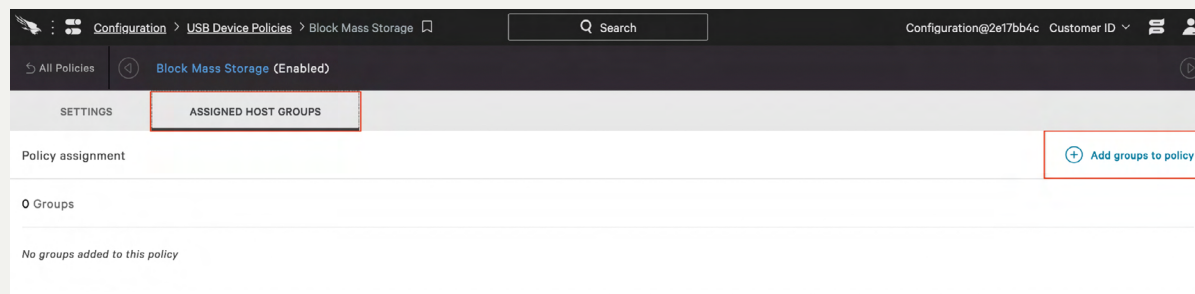
2 policies

Create new policy

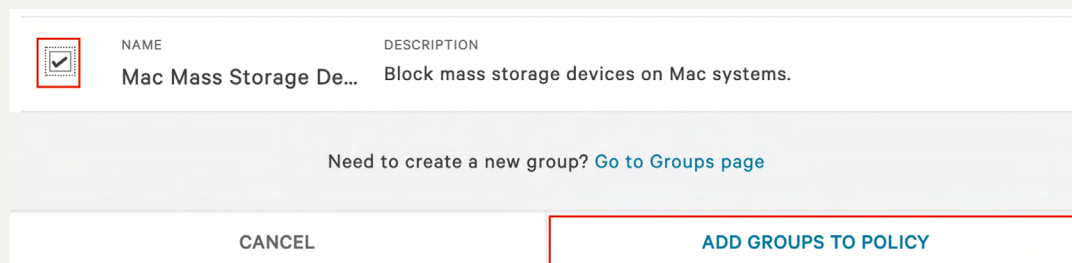
Edit precedence

PRECEDENCE	1	POLICY STATUS	Enabled	POLICY NAME	Block Mass Storage	MODE	Monitor and enforce	LAST MODIFIED	Aug. 20, 2021	APPLIED	0	PENDING	0	
This policy has no groups assigned to it. EDIT TO ADD A GROUP														
DEFAULT POLICY		POLICY STATUS	Enabled	POLICY NAME	Default (Mac)	MODE	Off	LAST MODIFIED	Aug. 5, 2021	APPLIED	1	PENDING	1	

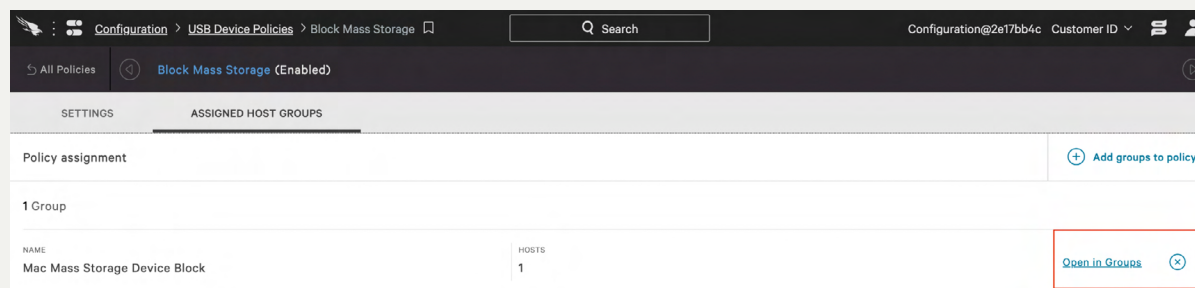
The “Policy assignment” page will open, showing that no groups have yet been assigned to this policy. To change that, click the “+ Add groups to policy” button.



A dialogue box will open with all available policies. Locate the policy created in Step 1, select the box, then click the “Add Groups to Policy” button.



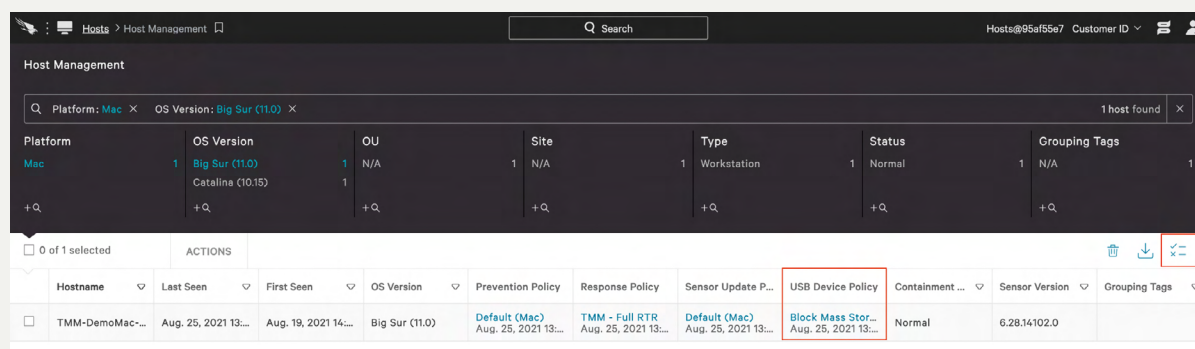
Back on the “Policy assignment” page, you can now see that this policy is assigned in one group. Click the “Open in Groups” button to validate that the group is correct.



Back on the “Groups” page, you can see that the policy has been assigned to this group. Any new Mac system coming online in the organization will be assigned this USB device control policy.

TESTING

To test the policy, first validate that the host has been assigned the correct USB device policy by navigating to the Hosts → Host Management page and filtering for your host(s). In the “USB Device Policy” column, you should see that the newly created policy has been applied. If you don’t see this column, click on the column editor in the upper right corner and check the box next to “USB Device Policy.”



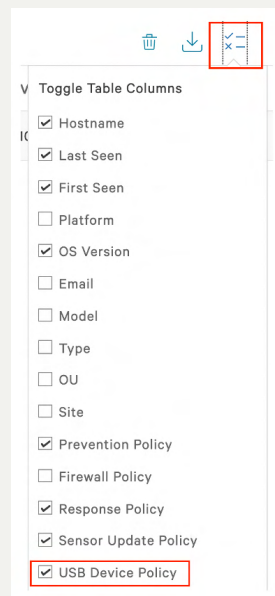
Host Management

Platform: Mac OS Version: Big Sur (11.0) 1 host found

Platform	OS Version	OU	Site	Type	Status	Grouping Tags
Mac	Big Sur (11.0) Catalina (10.15)	N/A	N/A	Workstation	Normal	N/A

0 of 1 selected ACTIONS

Hostname	Last Seen	First Seen	OS Version	Prevention Policy	Response Policy	Sensor Update P...	USB Device Policy	Containment ...	Sensor Version	Grouping Tags
TMM-DemoMac-...	Aug. 25, 2021 13:...	Aug. 19, 2021 14:...	Big Sur (11.0)	Default (Mac) Aug. 25, 2021 13:...	TMM - Full RTR Aug. 25, 2021 13:...	Default (Mac) Aug. 25, 2021 13:...	Block Mass Stor... Aug. 25, 2021 13:...	Normal	6.28.14102.0	



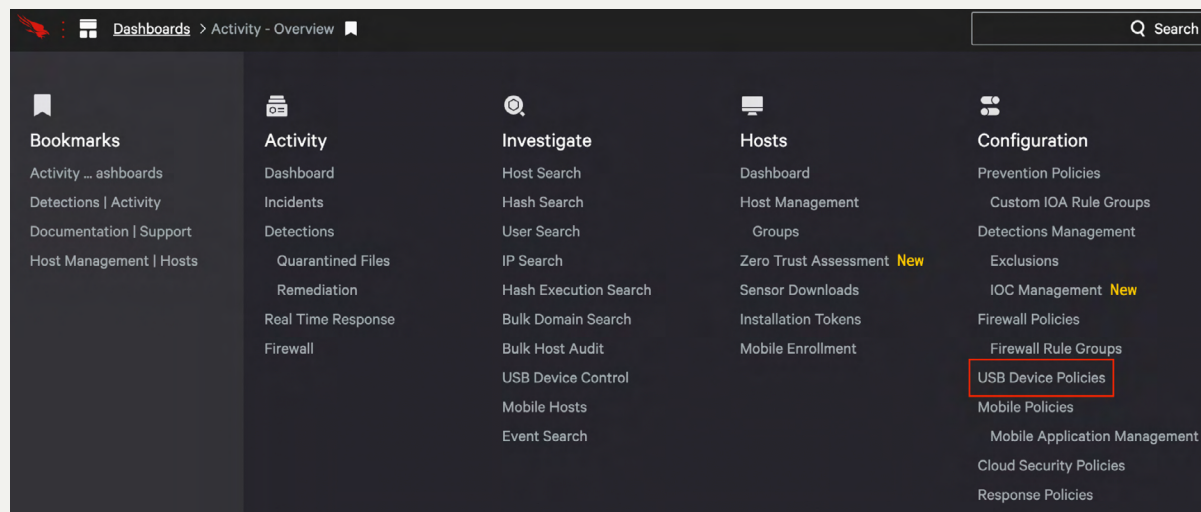
Here you can see that the policy has been applied and is ready to test.

On your test host, plug in a USB device. With both “End User Notifications” and a full block policy enabled, you should see a CrowdStrike Falcon sensor pop-up appear, indicating that this device has been blocked.

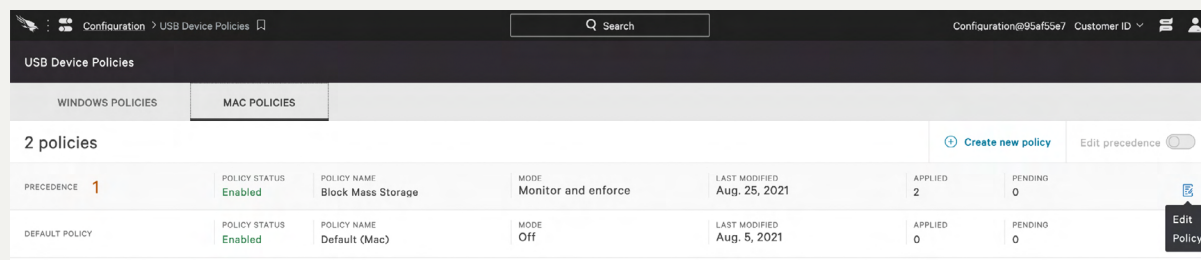


CREATING AN EXCEPTION IN A USB DEVICE POLICY

USB device policies often have exceptions. For example, blocking all mass storage devices might make mandatory tasks more difficult than necessary. For this reason, you have the option to create exceptions for USB device policies. Navigate back to the “USB Device Policies” page to see how this works.



Now open the policy previously created by hitting the “Edit Policy” button to the right of the desired policy.



Notice that under each device class, there is an “Exceptions” column. Scroll down to the “Mass storage” Class and expand it to reveal the “Add Exception” button.

The screenshot shows the 'Block Mass Storage' policy configuration page. The page has a dark header with navigation links and a search bar. Below the header, there are tabs for 'All Policies' and 'Block Mass Storage (Enabled)'. The main content area is divided into 'SETTINGS' and 'ASSIGNED HOST GROUPS'. Under 'SETTINGS', there is a 'Policy details' section with fields for NAME, DESCRIPTION, PLATFORM, STATUS, MODE, and PRECEDENCE. Below this is a 'USB device settings' section with a table of device classes and their permissions. The 'Mass storage' class is highlighted, and its 'Exceptions' column shows '0'. Below the table, there are radio buttons for permissions: 'Read, write and execute', 'Read and write only', 'Read only', and 'Full block' (selected). At the bottom, there is a section for 'Specific device exceptions in this class' with an 'Add exception' button. A red box highlights the 'ADD EXCEPTION' button in the 'Add exceptions to your USB device policies' section.

NAME	DESCRIPTION	PLATFORM	STATUS	MODE	PRECEDENCE
Block Mass Storage	Block unapproved mass storage devices	Mac	Enabled	Monitor and enforce	1 of 1

CLASS	EXCEPTIONS	PERMISSIONS
Any class	0	
Audio/Video	0	Full access
Imaging	0	Full access
Mass storage	0	Full block

Permissions

☐ Read, write and execute
☐ Read and write only
☐ Read only
☒ Full block

Specific device exceptions in this class

Add exceptions to your USB device policies

ADD EXCEPTION

The “Add USB device exception” dialogue box opens, where a “Combined ID” can be used to create an exception.

The 'Add USB device exception' dialog box is shown. It has a title bar with a close button. The main content area has a section 'Choose how to find USB devices for this policy' with two radio buttons: 'Combined ID' (selected) and 'Manual entry'. Below this, there is a text box for 'COMBINED ID' with a red border. Below the text box, there is a dropdown menu for 'DEVICE CLASS' with 'Mass storage' selected. Below the dropdown, there are radio buttons for permissions: 'Read, write and execute' (selected), 'Read and write only', 'Read only', and 'Full block'. At the bottom, there is a checkbox 'Let me add multiple exceptions without leaving this page' and two buttons: 'CANCEL' and 'ADD EXCEPTION'.

Add USB device exception

Choose how to find USB devices for this policy

☒ Combined ID
☐ Manual entry

For USB devices seen in your environment, copy the combined ID from the [USB Device Dashboard](#) and paste it below.

COMBINED ID

DEVICE CLASS

Mass storage

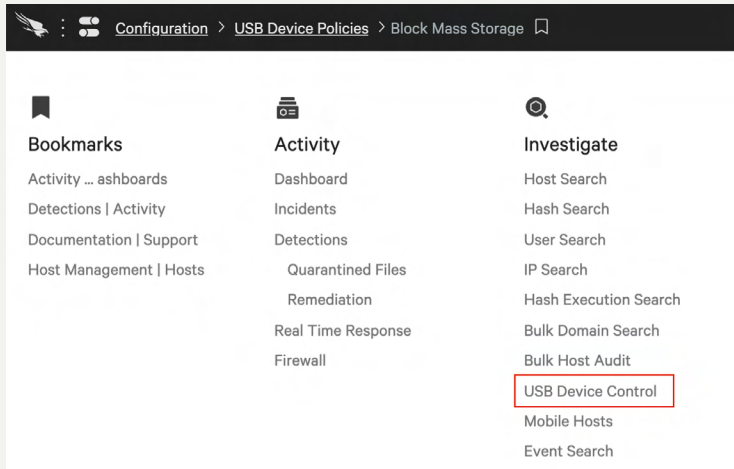
PERMISSIONS

☒ Read, write and execute
☐ Read and write only
☐ Read only
☐ Full block

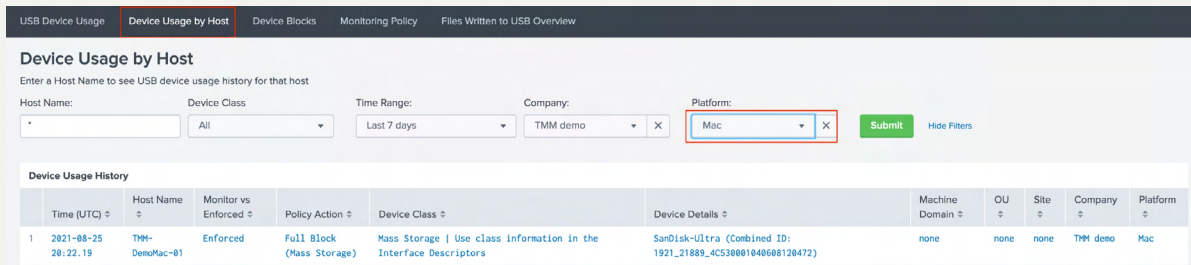
☐ Let me add multiple exceptions without leaving this page

CANCEL ADD EXCEPTION

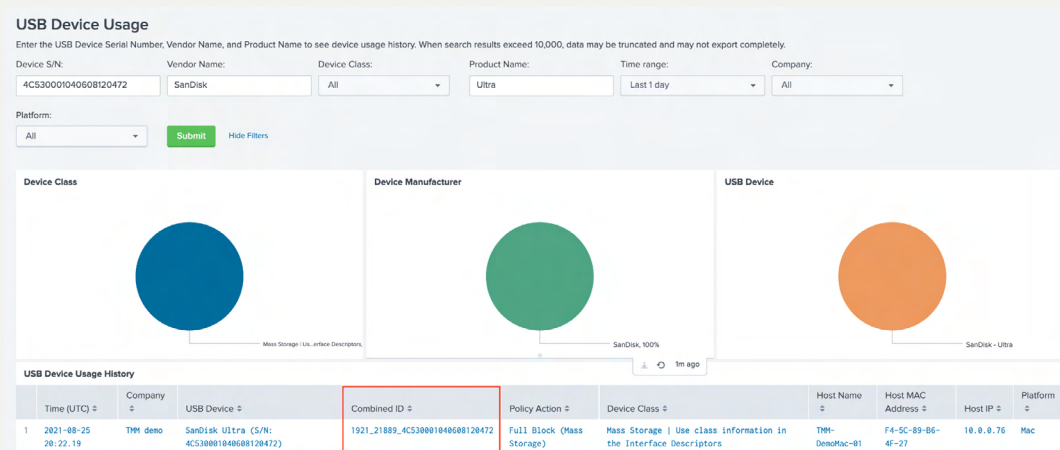
To get the combined ID of devices in your organization, navigate to Investigate → USB Device Control → Device Usage by Host.



Once on the “Device Usage by Host” page, filter using the “Platform” dropdown and select “Mac.”



Click the “Device Usage History” area on any of the blue text to open the “USB Device Usage” page for that specific device and to find that device's “Combined ID” for use in creating an exception.



Copy the “Combined ID” and navigate back to “Add USB device exception” on the “USB Device Policies” page. Select the “Combined ID” radio button, paste in the combined ID from the “USB Device Usage” page, select the “Permissions” you’d like to grant in the exception, and select “Add Exception.”

Add USB device exception

Choose how to find USB devices for this policy

☒ Combined ID
☐ Manual entry

For USB devices seen in your environment, copy the combined ID from the [USB Device Dashboard](#) and paste it below.

COMBINED ID
1921_21889_4C530001040608120472

DEVICE CLASS

Mass storage

PERMISSIONS

☐ Read, write and execute
☒ Read and write only
☐ Read only
☐ Full block

☐ Let me add multiple exceptions without leaving this page

CANCEL
ADD EXCEPTION

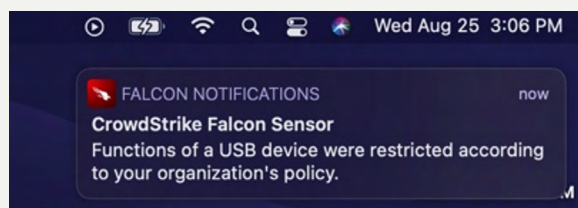
You’ll be returned to the “Policy” page where the exception is listed under the specific “Class” in which it was created. In this example, it’s in the “Mass storage” Class.

CLASS	EXCEPTIONS	PERMISSIONS
Mass storage	1	Full block

Permissions
☐ Read, write and execute
☐ Read and write only
☐ Read only
☒ Full block

Specific device exceptions in this class							Add exception
Vendor ID	Vendor Name	Product ID	Product Name	Serial Number	Combined ID	Permissions	Actions
1921	—	21889	—	4C530001040608120472	1921_21889_4C530001040608120472	Read and wr...	

After the policy has been updated, the user may still see a notification if any restrictions were still enabled for the exception. In this example, this mass storage was allowed to be used, but the ability to execute directly from the device was removed.



SUMMARY

Unlike many security products, CrowdStrike Falcon already leverages the existing console and agent seamlessly integrating device control into existing workflows. Falcon Device Control centralizes visibility, policy creation and management in the Falcon console.

ADDITIONAL RESOURCES

[Falcon Device Control User Guide](#)

[Falcon Device Control Demo Video](#)

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.