Device Control

Last Updated: November 14, 2022

Cisco Systems, Inc. www.cisco.com

INTRODUCTION

This demonstration shows how Device Control enhances the capabilities of Cisco Secure Endpoint to prevent and detect attacks from external devices. With visibility into USB mass storage devices, endpoint administrators can review device connect/disconnect events, access violation events, among others. With control, administrators define the default behavior when devices are connected, with configurations ranging from allowing full access to totally blocking devices. Granular rules with multiple conditions can also be created to further support varied approaches to controlling these devices.

Ultimately, removable devices can represent a security risk and may be attack vectors. Threat actors often use these devices to deliver malware to endpoints. By having visibility and control over these devices, administrators can prevent and detect attacks.

The Attack Surface

A targeted attack may start with an infected USB, which could be connected to an endpoint by a company employee who may be unaware that the device is compromised. Such type of attack is exemplified under the MITRE ATT&CK T1091, with associated tactics including initial access and lateral movement. These attacks can be specific to the company being attacked and may even allow adversaries to move into disconnected or air-gapped networks. Other examples include MITRE ATT&CK T1025, in which adversaries may search and collect data from removable storage.

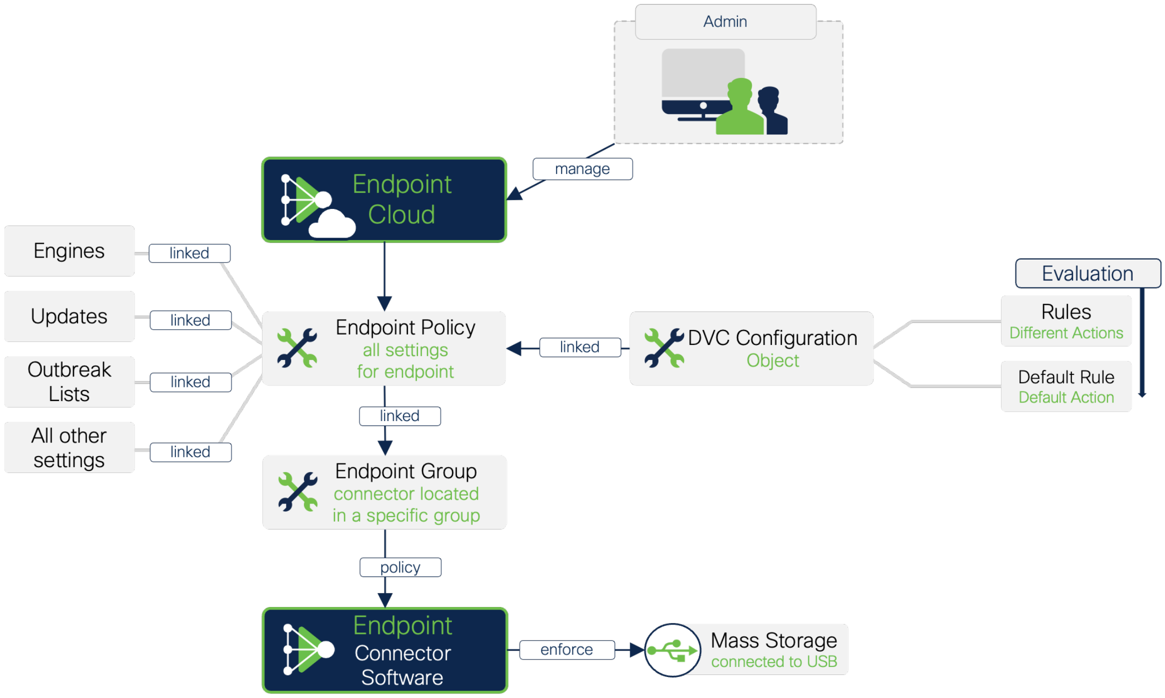
To prevent such attacks and reduce the attack Surface, Device Control policies can be configured in Secure Endpoint. Besides setting a default behaviour, rules can be further tweaked, with granular controls to achieve a balance between security and avoidance of business disruption.

Prepare the Environment

By enabling demo data, Device Control rules and events are automatically created. These rules can be reviewed in the Secure Endpoint Console under Management → Device Control.

Any Device Configuration includes a "Default Rule". The Default Rule gets enforced if no other rule matches the connected device. The Default Rule also represents the overall strategy for the Device Control Settings, which can be configured in one of the following settings:

- Block
- Read Only
- Read and Write Only
- Read, Write and Execute

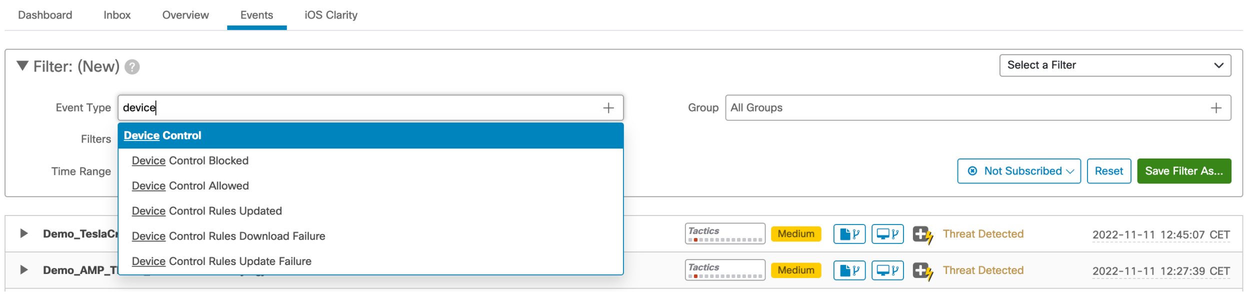


The connector software enforces the rules from top to bottom on first match. If a rule is matched, the connector enforces the configured action and stops processing other Device Rules.

Device Control allows flexible control: Administrators can define different rulesets and associate them to one or multiple Secure Endpoint Connector Policies. By enabling demo data, a demo ruleset will be created, along with device control events visible on the events page and in device trajectory.

Event visibility & control

Secure Endpoint Device Control generates multiple types of events. To filter all available Device Control Events generated by Secure Endpoint, select the event type "Device Control" in the Events filter, or select the specific event type you may want to review.



Event Type: device

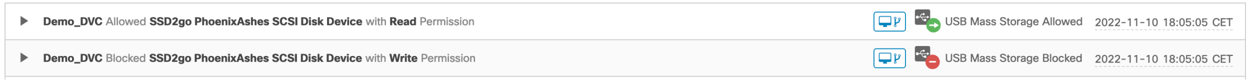
Group: All Groups

- Device Control
- Device Control Blocked
- Device Control Allowed
- Device Control Rules Updated
- Device Control Rules Download Failure
- Device Control Rules Update Failure

Demo_TeslaCr Medium Threat Detected 2022-11-11 12:45:07 CET

Demo_AMP_T Medium Threat Detected 2022-11-11 12:27:39 CET

For instance, the two events shown below have been generated for a single Device Control connection and show exactly what happened: Write Access was blocked, and Read Permission was allowed

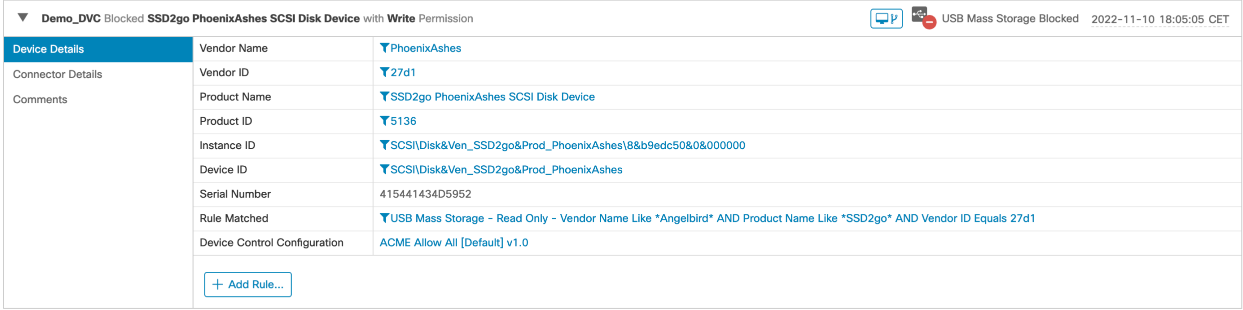


Demo_DVC Allowed SSD2go PhoenixAshes SCSI Disk Device with Read Permission — USB Mass Storage Allowed — 2022-11-10 18:05:05 CET

Demo_DVC Blocked SSD2go PhoenixAshes SCSI Disk Device with Write Permission — USB Mass Storage Blocked — 2022-11-10 18:05:05 CET

The Event details provide more information about the connected device, including the Vendor Name, Vendor ID, among others. Details also include any assigned Device Control configuration and the matched rule.

Assuming this is trusted device that should have write access allowed, administrators can add a rule based on any combination of the identifiers for this device. By clicking the "Add Rule" button, a new rule gets directly added to the assigned Device Control Configuration. Details of the device are automatically populated to the new rule, though administrators can further adjust the desired conditions of the rule.



Demo_DVC Blocked **SSD2go PhoenixAshes SCSI Disk Device** with **Write** Permission

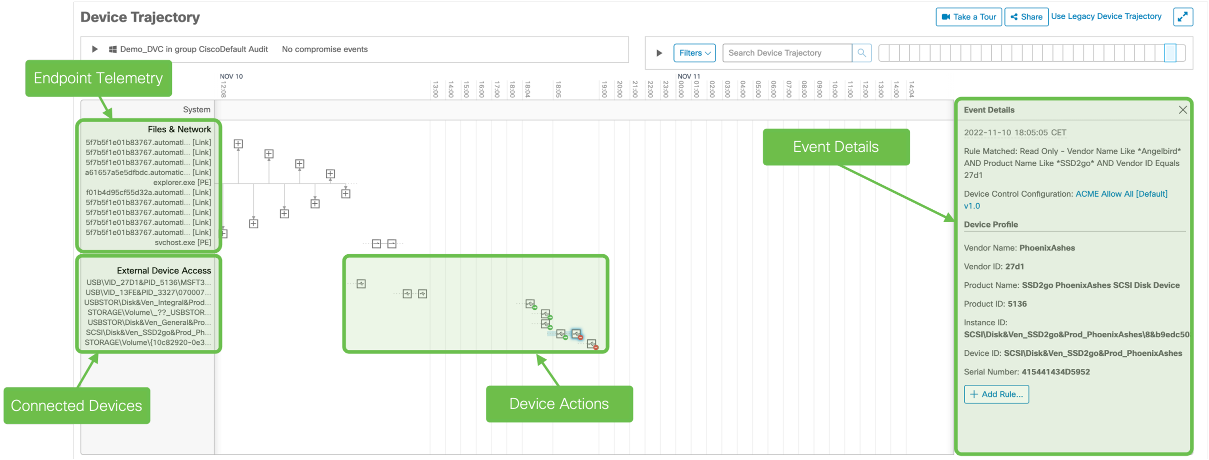
USB Mass Storage Blocked 2022-11-10 18:05:05 CET

Vendor Name	PhoenixAshes
Vendor ID	27d1
Product Name	SSD2go PhoenixAshes SCSI Disk Device
Product ID	5136
Instance ID	SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes\8&b9edc50&0&000000
Device ID	SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes
Serial Number	415441434D5952
Rule Matched	USB Mass Storage - Read Only - Vendor Name Like *Angelbird* AND Product Name Like *SSD2go* AND Vendor ID Equals 27d1
Device Control Configuration	ACME Allow All [Default] v1.0

Investigating with Device Trajectory

The Device Trajectory page in Secure Endpoint correlates available Endpoint Telemetry and Events with Device Control activity. If malicious activity relates to a USB device, a Security Analyst can identify so by using Device Trajectory.

By looking into the Device Trajectory of host "Demo_DVC", click the Device Action to see further event details, which include device identifiers and any matched rules. Adding a rule is one of the potential actions Analysts can take from Device Trajectory, which allows them to continue the investigation without having to lose context from the compromise being investigated.



Demo_DVC in group CiscoDefault Audit   No compromise events

Files & Network
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
a61657a5e5dfbdc.automatic... [Link]
explorer.exe [PE]
f01b4d95cf55d32a.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
svchost.exe [PE]

External Device Access
USB\VID_27D1&PID_5136\MSFT3...
USB\VID_13FE&PID_3327\070007...
USBSTOR\Disk&Ven_Integral&Prod...
STORAGE\Volume_??_USBSTOR...
USBSTOR\Disk&Ven_General&Pro...
SCSI\Disk&Ven_SSD2go&Prod_Ph...
STORAGE\Volume\{10c82920-0e3...

Event Details

2022-11-10 18:05:05 CET

Rule Matched: Read Only - Vendor Name Like *Angelbird* AND Product Name Like *SSD2go* AND Vendor ID Equals 27d1

Device Control Configuration: ACME Allow All [Default] v1.0

Device Profile

Vendor Name: PhoenixAshes

Vendor ID: 27d1

Product Name: SSD2go PhoenixAshes SCSI Disk Device

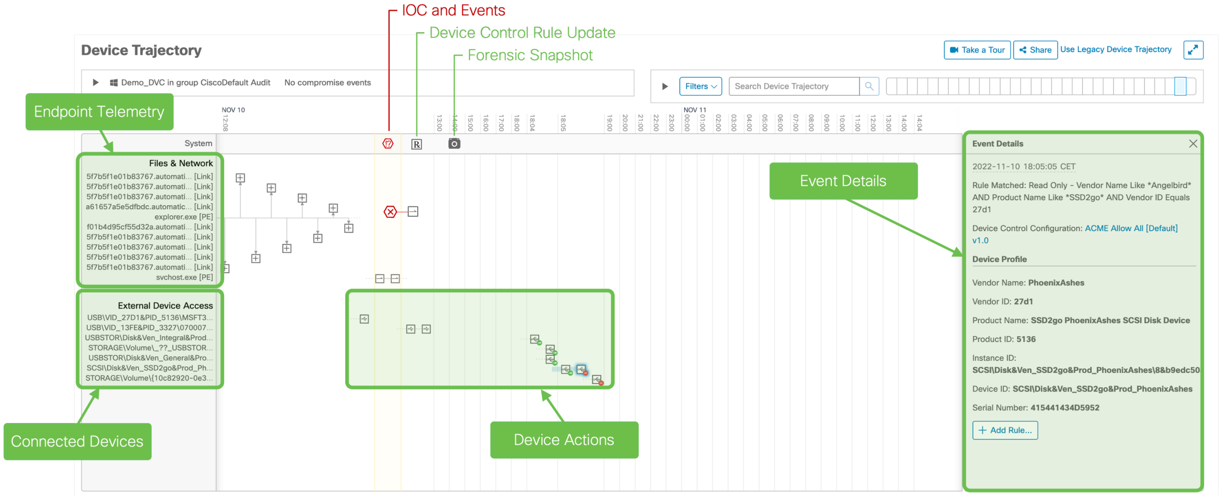
Product ID: 5136

Instance ID: SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes\8&b9edc50

Device ID: SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes

Serial Number: 415441434D5952

While investigating a threat, there may be many other events of interest shown around a connected device. Device Trajectory provides visibility into the events that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware. If the Security Analyst wants to prevent any further lateral movement through any USB devices connected to this potentially compromised endpoint, the Analyst may want create a rule to block this particular USB device, or even move this endpoint to a policy associated with a full block Device Control rule.



Device Trajectory

Demo_DVC in group CiscoDefault Audit   No compromise events

Files & Network
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
a61657a5e5dfbdc.automatic... [Link]
explorer.exe [PE]
f01b4d95cf55d32a.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
5f7b5f1e01b83767.automati... [Link]
svchost.exe [PE]

External Device Access
USB\VID_27D1&PID_5136\MSFT3...
USB\VID_13FE&PID_3327\070007...
USBSTOR\Disk&Ven_Integral&Prod...
STORAGE\Volume_??_USBSTOR...
USBSTOR\Disk&Ven_General&Pro...
SCSI\Disk&Ven_SSD2go&Prod_Ph...
STORAGE\Volume\{10c82920-0e3...

Event Details

2022-11-10 18:05:05 CET

Rule Matched: Read Only - Vendor Name Like *Angelbird* AND Product Name Like *SSD2go* AND Vendor ID Equals 27d1

Device Control Configuration: ACME Allow All [Default] v1.0

Device Profile

Vendor Name: **PhoenixAshes**

Vendor ID: **27d1**

Product Name: **SSD2go PhoenixAshes SCSI Disk Device**

Product ID: **5136**

Instance ID: **SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes\8&b9edc50**

Device ID: **SCSI\Disk&Ven_SSD2go&Prod_PhoenixAshes**

Serial Number: **415441434D5952**

＋ Add Rule...

Summary

This scenario highlights how Secure Endpoint provides visibility and control over external devices. By configuring Device Control policies and assigning them to Endpoint Connector Policies, administrators can prevent and detect malware from external devices. Ultimately, Device Control should be configured based on the Device Management Strategy (E.g., Block All and Allow, Allow and Block specific devices) that better suits the needs of a particular organization.

This scenario also highlights how Device Control expands upon the capabilities available on Device Trajectory by bringing Endpoint Events, Endpoint Telemetry, and Device Control Activity into one view to streamline Incident Response workflows.