



# Endpoint Security

powered by HEAT Software

## Device Control Best Practice Guide

Dec 2020

## Contents

<b>Introduction</b>	<b>3</b>
Overview	4
<b>Phase 1: Prepare Your Infrastructure</b>	<b>8</b>
Install the Server Module	9
Configure the Device Control Reboot Behavior Option	10
Enable Audit Mode	14
Install the Endpoint Module	17
Synchronize With Active Directory	20
Configure Options	24
<b>Phase 2: Plan Your Policies</b>	<b>25</b>
Learn Device Control Concepts and Policy Features	25
Create Policy Goals	41
Copy Default Policies	50
Create Custom Policies	53
<b>Phase 3: Enforce Policies</b>	<b>55</b>
Plan Deployment Informational Campaign	56
Enable Enforcement	57
Test Device Control Policies	58
Confirm Policy Functionality	62
Deploy Device Control Policies	65
<b>Phase 4: Daily Operation</b>	<b>67</b>
Dashboard Widgets	68
File Shadowing	69
Temporary Permissions	72
Temporary Policy	73
Password Recovery	74
Policy Maintenance	75
Adding Individual Users	76
Adding New Devices	78
<b>Appendix: References</b>	<b>79</b>
Supported Device Classes	80
Supported Permission Types	81
Default Policy/ Custom Policy Conflict Resolution	84
Configuration Options	85
Encryption Scenarios	87
FAQ	90
Policy Planning Worksheet	93

# Introduction

A module for Ivanti Endpoint Security, Ivanti Device Control enforces policies for removable devices, removable media, and data (such as read / write and encryption). These flexible policies allow workers to use productivity-enhancing tools while these same tools from being used maliciously.

Device Control features include:

- **Productivity Enhancement and Risk Reduction:**

Centrally manage security policies for removable devices (like USB flash drives) and media (like CDs and DVDs) through a flexible whitelist approach.

- **Data Encryption:**

Encrypt and secure data on removable devices and media using FIPS 140-2 Level 2 cryptography, a U.S. government computer security standard used to accredit cryptographic modules.

- **Malware Prevention:**

Block removable devices and media that contain malicious software.

- **Roaming Protection:**

Prevent use of unauthorized devices and media, regardless of whether the endpoint is connected to your network.

- **Device Control Metrics:**

View reports and copies of files that prove your organization complies with regulatory laws.

This document is a practical guide intended to assist you with the deployment of Device Control module within your organization.

## Overview

Implement Device Control in four different phases:



"Phase 1: Prepare Your Infrastructure" on page 8

Before you can enforce Device Control Policies in your organization, you have to install and configure Device Control. During this phase, you will:

1. "Install the Server Module" on page 9

First things first: install the Device Control server module on the Endpoint Security platform.

2. "Configure the Device Control Reboot Behavior Option" on page 10

When you install the Device Control module on your endpoints, they require a reboot to complete installation. This reboot can disrupt your employees' work. However, the Endpoint Security Agent Policy Set feature includes options for handling this reboot with minimal effect on your users. Choose an option before installing the endpoint module.

3. "Enable Audit Mode" on page 14

Next, enable Audit mode, a setting within the Global Device Policy. This mode does two things:

- It logs all devices that users connect to their endpoints, which is helpful information while planning your Device Control Policies.
- It turns off policy enforcement. Since you still need to plan your policies, policy enforcement is not appropriate at this time.

4. "Install the Endpoint Module" on page 17

Use the Endpoint Security Console to install the Device Control module on your endpoints.

5. "Synchronize With Active Directory" on page 20

Device Control assigns Device Control Policies using user and endpoint data from your Active Directory. Synchronize your Endpoint Security Server with your Active Directory so that Device Control can use these objects to assign policies.

6. "Configure Options" on page 24

Configure the Device Control default options. These options include some settings that apply globally to your Device Control installation. You should configure these options as early as possible.

"Phase 2: Plan Your Policies" on page 25

Before you begin enforcing Device Control Policies on your endpoints, determine which devices and users require policies in the first place. This chapter covers policy planning and creation.

1. "Learn Device Control Concepts and Policy Features" on page 25

The first step in planning Device Control policies for your organization is:

- To understand the different policy types available
- To understand the options available for each policy type

2. "Create Policy Goals" on page 41

Now that you have learned about the different Device Control policies that are available, create goals for your policies and write down your policy plan.

3. "Copy Default Policies" on page 50

To properly test your custom Device Control Policies, you need to copy the default Device Control policies. These copies provide Read/Write access for your employees while you're custom policies.

4. "Create Custom Policies" on page 53

You've made your plan. Now draft your policies!

### "Phase 3: Enforce Policies" on page 55

Now you need to deploy and enforce your policies. This chapter guides you through the transition to Device Control policy enforcement.

1. "Plan Deployment Informational Campaign" on page 56

Inform your end users that you're deploying your policies. They need to know how Device Control affects them.

2. "Enable Enforcement" on page 57

Switch from **Audit** mode to **Policy enforcement** mode to begin enforcing the default Device Control Policies.

3. "Test Device Control Policies" on page 58

Before deploying your custom Device Control Policies to your production endpoints, test them on a small group of endpoints to confirm they're working correctly.

4. "Confirm Policy Functionality" on page 62

Finally, review device event logs to make sure that your policies are functioning correctly. If they aren't, edit your policies to correct them.

5. "Deploy Device Control Policies" on page 65

After testing your custom policies, deploy them to your production endpoints. When you're done deploying, circle back to "Confirm Policy Functionality" on page 62 to reconfirm that your policies are working properly.

### "Phase 4: Daily Operation" on page 67

Following installation and configuration, you still need to maintain your Device Control installation and perform daily tasks to keep your users productive. This chapter details those tasks and how to perform them.

## Phase 1: Prepare Your Infrastructure



Before you can enforce Device Control policies in your organization, you have to get Device Control up and running.

During this phase, you will:

1. "Install the Server Module" on the next page

First things first: install the Device Control server module on the Endpoint Security platform.

2. "Configure the Device Control Reboot Behavior Option" on page 10

When you install the Device Control module on your endpoints, they require a reboot to complete installation. This reboot can disrupt your employees' work. However, the Endpoint Security Agent Policy Set feature includes options for handling this reboot with minimal effect on your users. Choose an option before installing the endpoint module.

3. "Enable Audit Mode" on page 14

Next, enable Audit mode, a setting within the Global Device Policy. This mode does two things:

- It logs all devices that users connect to their endpoints, which is helpful information while planning your Device Control Policies.
- It turns off policy enforcement. Since you still need to plan your policies, policy enforcement is not appropriate at this time.

4. "Install the Endpoint Module" on page 17

Use the Endpoint Security Console to install the Device Control module on your endpoints.

5. "Synchronize With Active Directory" on page 20

Device Control assigns Device Control Policies using user and endpoint data from your Active Directory. Synchronize your Endpoint Security Server with your Active Directory so that Device Control can use these objects to assign policies.

6. "Configure Options" on page 24

Configure the Device Control default options. These options include some settings that apply globally to your Device Control installation. You should configure these options as early as possible.



## Install the Server Module

Your first practical step toward controlling devices is installation of the Device Control server module. Installation is simple. Open the Endpoint Security Console, and then select **Tools > Launch Installation Manager**. Select the **Device Control** module and complete installation.

The screenshot shows the Ivanti Endpoint Security console. On the left, the 'Tools' menu is open, highlighting 'Launch Installation Manager...'. The main window is the 'Installation Manager' interface, which displays a table of components available for installation or update.

**Installation Manager**  
powered by Heat

Home Tools Help

The components below are available for install/update with the Ivanti Endpoint Security. Select a Suite and one or more of the corresponding components to install and/or update.

New/Update Components Existing Components

Suite	Suite Version	Release Date
+	Suite 8.5.0.148	4/25/2017

Component	Version	Type	Description	Dependencies	Download Size
<input type="checkbox"/> AntiVirus	8.5.0.177	Module	Protects against malware via signature-matching capabilities as well as proactive behavioral analysis technologies.		10.65 MB
<input type="checkbox"/> Application Control	8.5.0.171	Module	Prevents unwanted or dangerous programs from executing via basic snapshot, application whitelist and Trust Engine capabilities.		3.35 MB
<input checked="" type="checkbox"/> Device Control	8.5.0.179	Module	Protects against data theft via blocking of externally attachable devices, monitoring of data transfer, and enforcement of encryption policies on transient data storage technologies.		44.68 MB

Download Only... Install Close

## Configure the Device Control Reboot Behavior Option

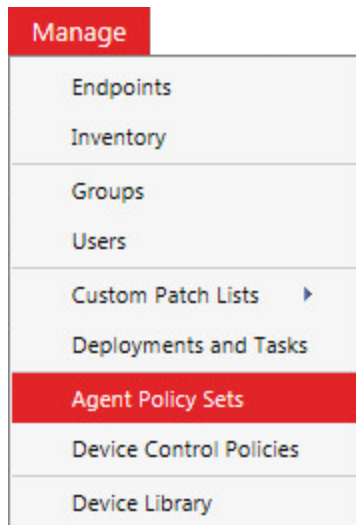
After the server module is installed, configure your Agent Policy Sets for Device Control. These configuration determine how the Endpoint Security Agent handles the reboot that's required to complete installation of the Device Control endpoint module.



Agent Policy Sets are not the same as Device Control Policies. They are two different types of policies.

### To Configure the Device Control Reboot Behavior Option:

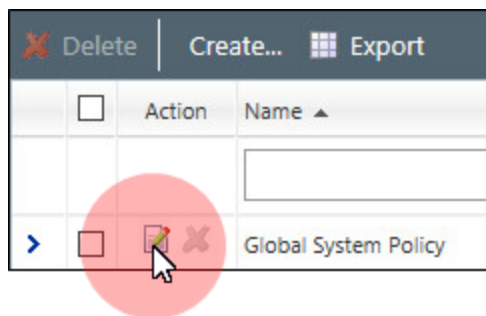
1. From the Endpoint Security Console, select **Manage > Agent Policy Sets**.



- Click the  icon for an Agent Policy Set assigned to a user group that you want to use Device Control on.



You may need to create/edit multiple Agent Policy Sets so that you can choose different options for different groups of endpoints.



The **Edit A Policy Set** dialog opens.

3. Scroll down to the **Reboot Behavior Defaults** section and set the **Reboot behavior** policy.

Show alerts on endpoint	True
<b>Reboot Behavior Defaults</b>	
Reboot behavior	Notify user, user response required before reboot
<b>Batch Agent Communication</b>	

#### What's the Reboot Behavior Policy?

When you install the Device Control module on your endpoints (which you'll do later in "Install the Endpoint Module" on page 17), those endpoints require a reboot.

The **Reboot behavior** policy lets you control how each endpoint handles this reboot. Reboots are disruptive, so Device Control offers three options for how to handle them:

- **Notify user, user response required before reboot**

This option prompts end users to reboot their system with no deadline, so they have time to save their work. We recommend using this option for desktop and laptop endpoints that employees use for productivity.

- **Notify user, automatically reboot with 5 minute timer**

This option prompts end users to reboot their system. However, this option imposes the reboot after 5 minutes. We recommend using this option for servers and other systems that you suspect might have someone working on them.

- **Don't notify user, wait for the next user-initiated reboot**

This option does not prompt a reboot, nor does it impose a reboot. Use this option when installing Device Control on unmanned endpoints like servers, ATMs, or kiosks that can be rebooted in a scheduled maintenance window.

4. Scroll down to the **Device Control** section and set each of the DC policies.

Device Control	
DC install SK-NDIS driver	Install enabled
DC detection interval	5 minutes
DC device event upload interval	5 minutes
DC agent reboot behavior	Set or view this setting in the Reboot Behavior Defaults section above.

#### DC Install SK-NDIS Driver

Agent Policy Sets contain a few other Device Control options, the most important being **DC install SK-NDIS driver**. SK-NDIS is a driver that lets Device Control access secondary network adapters such as Wi-Fi, Infrared, and Bluetooth devices. Whether you should enable or disable this option depends on your environment.

- Use **Install enabled** if you want to prevent network bridging for wireless network adapters such as 802.11 or bluetooth when an endpoint is connected to your network.
- Use **Do not install** if you have servers that use multiple network adapters simultaneously, as enabling it may disrupt endpoint network connectivity.



If you don't know whether to enable this option, we recommend deploying Device Control to a few test machines that represent a demographic of your organizational endpoints. You can then monitor these test machines to see if SK-NDIS causes issues.

#### DC Detection Interval & DC Device Event Upload Interval

These options:

- Determine how often the Device Control endpoint module verifies its installation to the Endpoint Security Server.
- Determine how often the Device Control endpoint module uploads device events to the Endpoint Security Server.

- After you finish configuring the **Reboot Behavior Defaults** policy and the **Device Control** policies, click **Save**.

The screenshot shows the 'Edit A Policy Set' window with the following sections:

- Patch and Remediation Reboot Notification Defaults**
  - User may cancel: True
  - User may snooze: True
  - Reboot within: 5 minutes
  - Always on top: True
- Discover Applicable Updates (DAU)**
  - Scheduling frequency: 26 hours
- FastPath Servers**
  - Interval: 0 minutes
  - Servers: [Modify button]
- Device Control**
  - DC install SK-NDIS driver: Install enabled
  - DC detection interval: 5 minutes
  - DC device event upload interval: 5 minutes
  - DC agent reboot behavior: Set or view this setting in the Reboot Behavior Defaults section above.

At the bottom, there is a legend: **\* Indicates a required value**. The 'Save' button is highlighted with a red circle and a hand cursor.

- Edit any additional Agent Policy Sets that are applied to endpoint groups you're installing Device Control on.



Remember, since each Agent Policy Set is assigned to different endpoint groups, you need to figure out which Device Control options best suit each group.

## Enable Audit Mode

Device Control contains a feature called **Audit** mode. When this mode is turned on, Device Control logs all devices that connect to your endpoints.

### What is Audit Mode?

After you install the Device Control module on your endpoints, you should place the Global Device Policy in **Audit** mode, a mode that configures your endpoints to:

- Log all device events that occur.
- Continue allowing devices to connect to endpoints. In other words, Device Control does not block devices from connecting.

Why are we turning on **Audit** mode? For two reasons:

- **User activity logging**

Right now, you probably have little data about what device access users require to do their jobs. By placing the Global Device Policy in **Audit** mode, the endpoint will log device events and then upload them to the Endpoint Security Server. You can then use this data to shape your Device Control policies later.

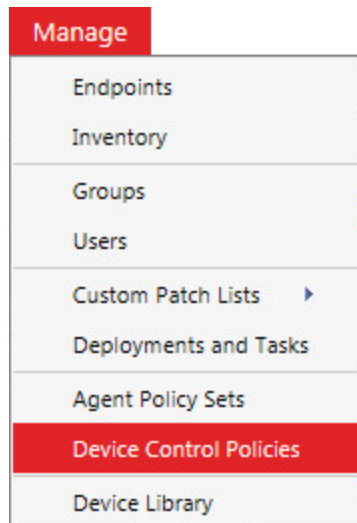
- **Ease of transition**

If the Global Device Policy's other mode (**Policy enforcement** mode) is enabled when you install the Device Control endpoint module, all devices begin enforcing the default Device Control policies.

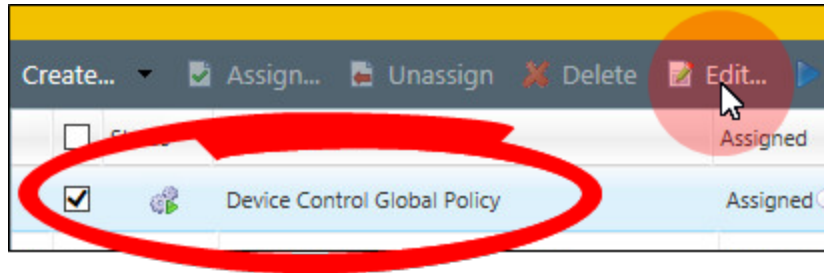
At this time, **Policy enforcement** mode is inappropriate because your default policies will likely conflict with custom Device Control policies as you create them, creating volatile permissions for your users. **Audit** mode allows users to continue accessing their devices while you configure the policy to a level more appropriate for your organization.

**To Enable Audit Mode:**

1. Select **Manage > Device Control Policies**.



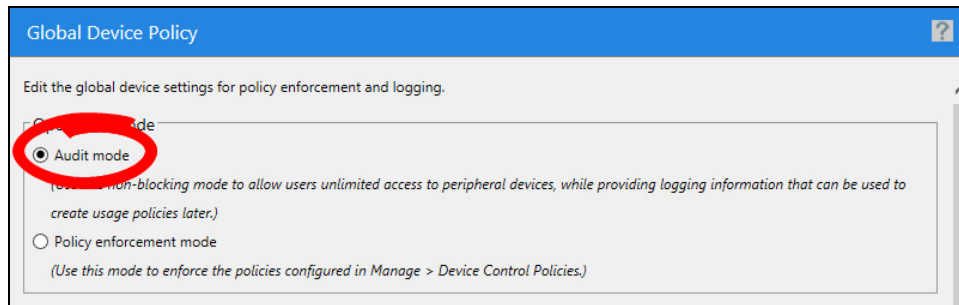
2. Select the **Device Control Global Policy** and click **Edit**.



The **Global Device Policy** dialog opens.

We'll have more information about the default device class policies listed beneath the **Device Control Global Policy** later in "Default Device Class Policies" on page 30. Don't worry about them for now though.

3. Make sure that the Global Device Policy is in **Audit mode**.



4. After you select **Audit mode**, click **Finish**.



## Install the Endpoint Module

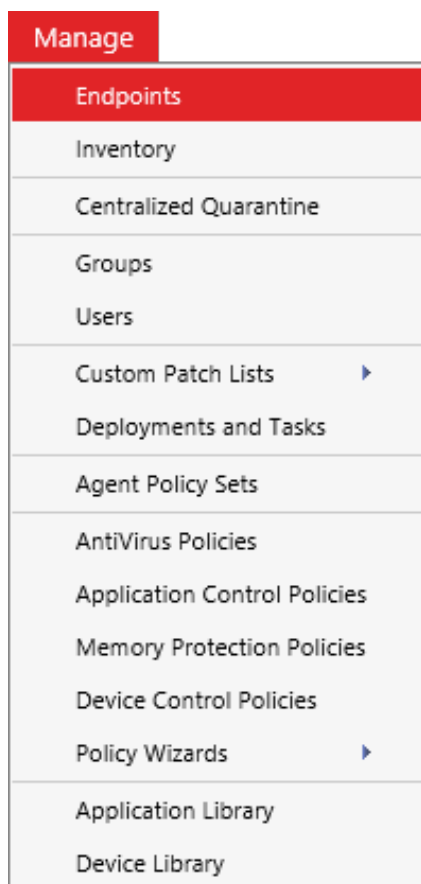
Now that you've created policies that address situations that occur when the Device Control endpoint module is initially installed, you can begin installing the Device Control endpoint module.

### To Install the Endpoint Module:

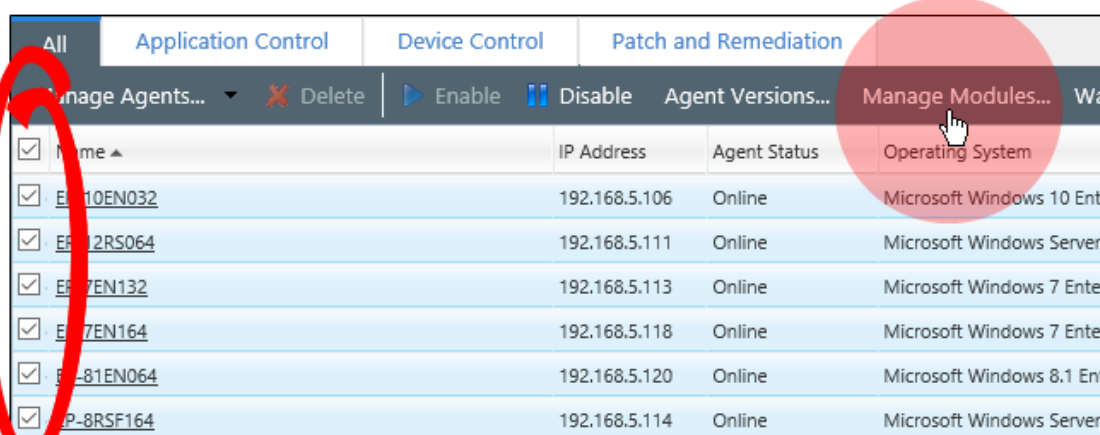


These instructions assume that the Endpoint Security Agent is already installed on your endpoints. If the Agent isn't already installed, refer to the Ivanti Endpoint Security Agent Install Guide available on [Product Documentation](#).

1. From the Endpoint Security Console, select **Manage > Endpoints**.



2. Select the endpoints that you want to install the Device Control endpoint module on. Then click **Manage Modules**.



3. Select the Device Control checkbox for each endpoint that you want to install the module on. Then click **OK**.



Before you install the module on all endpoints, we recommend installing the module on a few endpoints that represent your organization. This test install will reveal any potential software conflicts that to resolve before rolling the module out to your entire organization.

**Add/Remove Modules**

Select the modules you would like to add or deselect the ones you would like to remove.

Licenses	App Control	Dvc Control	Patch
Purchased (non-expired)	100	100	200
In Use	0	0	1
Pending	0	6	0
Available	100	94	199

Endpoint Name	IP Address	Agent Version	App Control	Dvc Control	Patch
SCAPD-MAC-MINI-10	10.19.0.168	7.0306	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-12RS064	192.168.5.111	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-81EN064	192.168.5.120	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-10EN032	192.168.5.106	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-7EN164	192.168.5.118	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-8RSF164	192.168.5.114	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EP-7EN132	192.168.5.113	8.4.0.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rows per page: 100 1 of 7 selected Page 1 of 1

**OK** Cancel

- Device Control module installation begins.
- Module installation progress displays on the **Manage > Endpoints** page.
- Remember, Device Control module installation does not complete until the endpoint is rebooted.

## Synchronize With Active Directory

Within Device Control, you can assign policies to your organization using two types of objects: users or endpoints. Fortunately, your organization may already contain a resource full of these objects: [Active Directory \(AD\)](#).

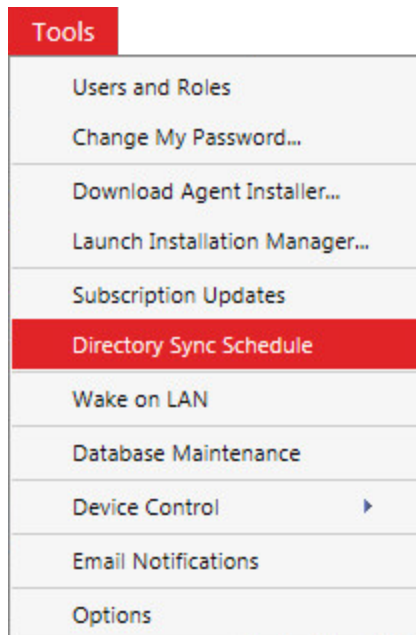
Instead of recreating user and endpoint objects in Endpoint Security by yourself, you can synchronize these objects from your Active Directory using the AD Synchronization feature. This feature scans your existing AD for users and endpoints, and then lists them in the Endpoint Security Console.

While creating your Device Control policies, you can choose users or endpoints for policy assignment.

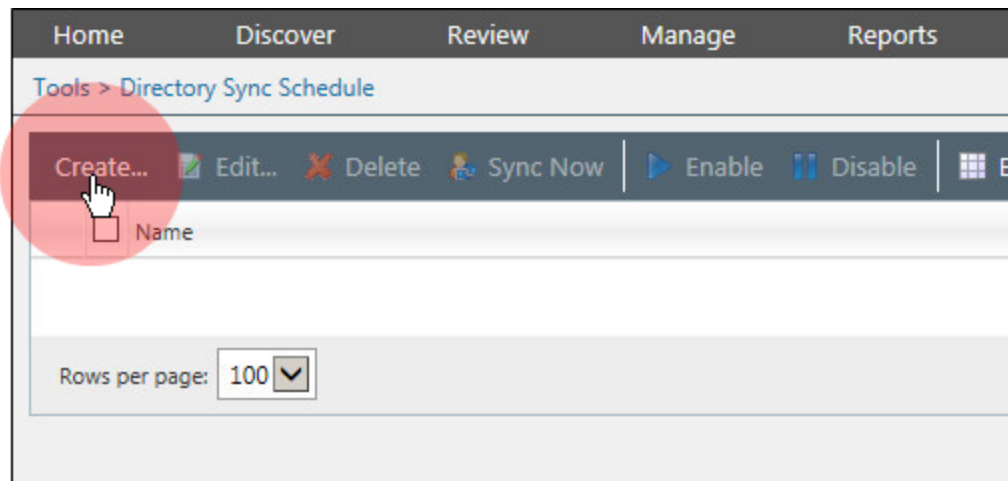
### To Synchronize With Active Directory:

If you also use Application Control, and you've already configured your Endpoint Security Server to synchronize with Active Directory, skip these steps and proceed to "Configure Options" on page 24.

1. From the Endpoint Security Console, select **Tools > Directory Sync Schedule**.



2. Click **Create**.



The **Schedule Directory Sync** wizard opens.

3. Complete each page of the **Schedule Directory Sync** wizard.

**Schedule Directory Sync**

**Specify Sync Server**

Sync results will be limited to the access rights of the login user you specify. It is recommended that you specify a user that holds read-only access to the directory.

**Sync Server**

Directory server/computer: ActiveDirectoryServer x

Domain name: ORG

**Credentials**

Domain\user name: ORG\administrator

Password: .....

Confirm password: .....

**Sync scope**

☒ Sync the entire domain (recommended)

☐ Specify one or more directory containers as sync sources

**Schedule Sync**

Set a recurring time period to perform your directory sync.

Directory sync name: ActiveDirectoryServer - ORG sync

**Scheduling**

☒ Daily ☐ Weekly ☐ Monthly

Start date: 8/1/2016

Start time: 6:00 PM

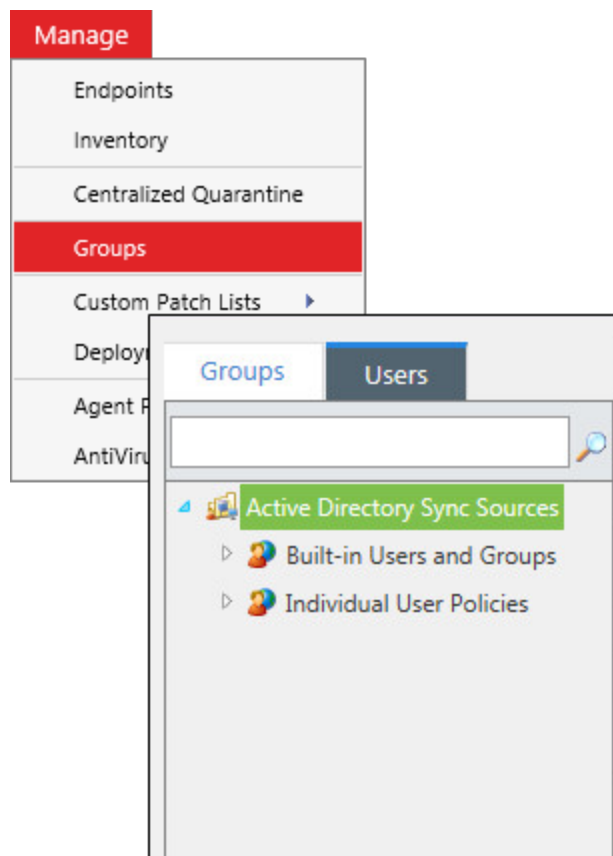
Run every 1 days

☐ End by:

< Back Finish Cancel

- Use this wizard to sync a single domain, multiple domains, or portions of a domain (organizational units).
- For domains that change frequently, schedule daily or weekly syncs.
- For domains that change infrequently, schedule monthly syncs.

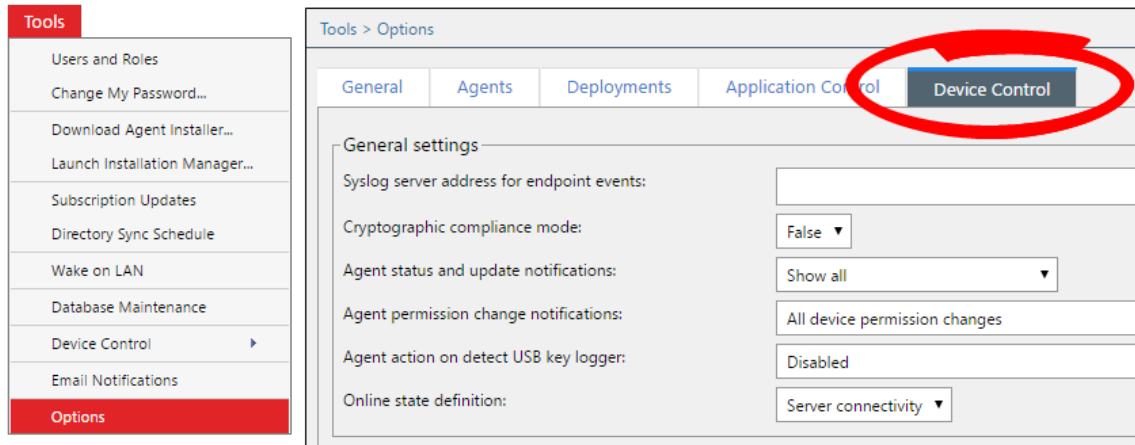
4. Click **Finish** when you're done.
- The synchronization is scheduled. It runs at the time you specified.
  - After the synchronization completes, you can view the objects that it found by selecting **Manage > Groups** and selecting the **Users** tab.



## Configure Options

Now that the Device Control module is installed on your Endpoint Security Server, you can configure the Device Control default options. These options include some settings that apply globally to your Device Control installation. You should configure these options as early as possible. You'll likely only have to set them once.

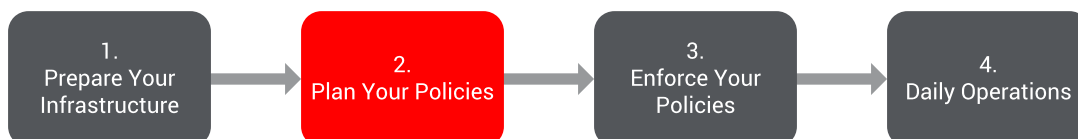
To configure these options, select **Tools > Options**, and then select the **Device Control** tab.



See "Configuration Options" on page 85 for more information on what each option does.



## Phase 2: Plan Your Policies



Before you can begin managing use of devices in your organization, you must create Device Control Policies, which are sets of rules that allow or deny use of different devices.

During this phase, you will:

1. "Learn Device Control Concepts and Policy Features" below

The first step in planning Device Control policies for your organization is:

- To understand the different policy types available
- To understand the options available for each policy type

2. "Create Policy Goals" on page 41

Now that you have learned about the different Device Control policies that are available, create goals for your policies and write down your policy plan.

3. "Copy Default Policies" on page 50

To properly test your custom Device Control Policies, you need to copy the default Device Control policies. These copies provide Read/Write access for your employees while you're custom policies.

4. "Create Custom Policies" on page 53

You've made your plan. Now draft your policies!

## Learn Device Control Concepts and Policy Features

Before you begin planning your policies, review the core ideas behind Device Control. Understanding these ideas helps you create a comprehensive plan.

### Device Control Concepts

Before planning your policies, you should understand some of the larger concepts behind Device Control.

- "Device Control Policies" on the next page
- "Device Classes" on the next page

- "Device Collections" on the next page
- "The Default-Deny Principle" on page 28

### Device Control Policies

The purpose of Device Control is to allow your users to access devices needed to do their job, while blocking use of devices that present unnecessary security risk.

These goals are accomplished by using Device Control Policies, which are sets of rules that determine:

- Which specific devices a user can access (or cannot access)
- When users can access a device
- What permissions the user has on a device (read access, write access, etc.)
- The physical ports that can be used to connect a device
- The object used to assign a Device Control Policy (users or endpoints)

There are four types of Device Control Policies:

- Device Class Policies
- Device Collection Policies
- Media Collection Policies
- Port Control Policies

For more information on these, see "Policy Types" on page 29.

### Device Classes

Device classes are categories created by Microsoft to sort similar hardware devices into logical groups. Device Control uses these categories to block or permit device use.

Within Endpoint Security, hardware devices are classified into Device Classes. When a device is connected to a Windows endpoint, that device registers itself with Windows as one or more device classes.

Some examples of device classes include:

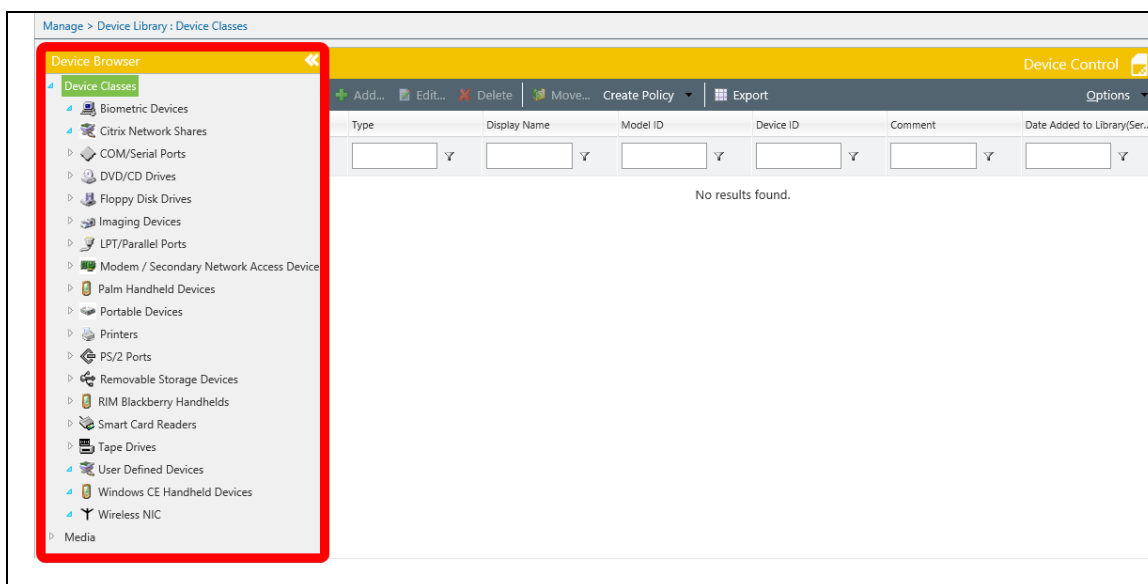
- Biometric Devices
- DVD/CD Drives
- Printers
- Removable Storage Devices



For a list of all Device Classes supported, see "Supported Device Classes" on page 80.

---

You can view device classes in Endpoint Security by selecting **Manage > Device Library**. View them in the **Device Browser**.



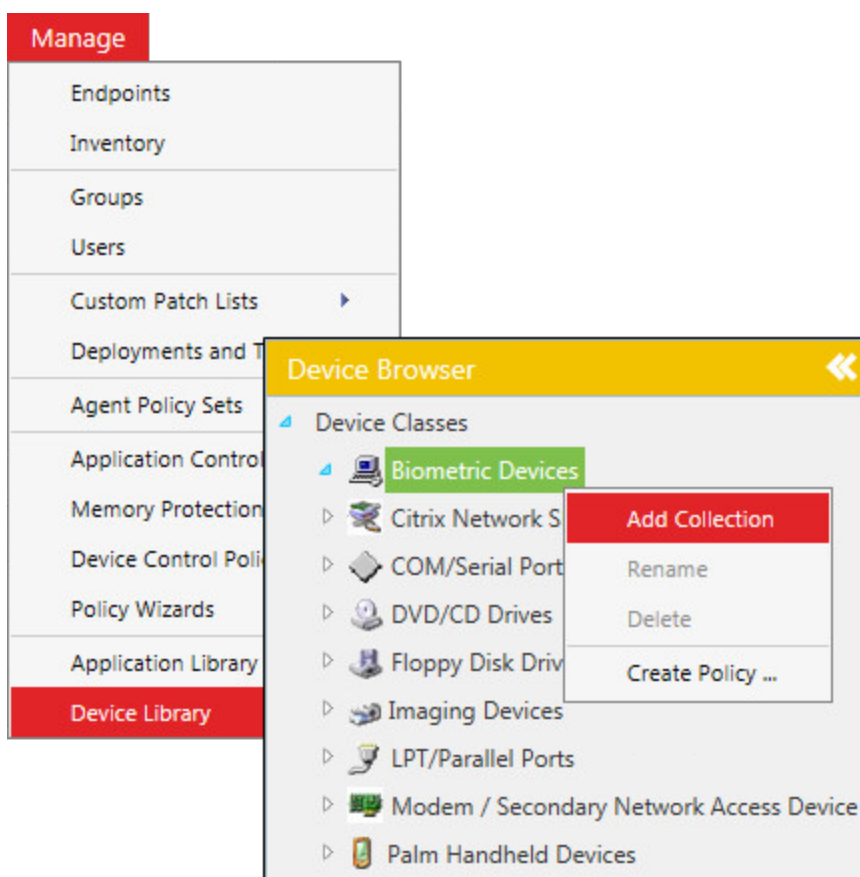
## Device Collections

Some device classes, such as Removable Storage Devices, are so diverse that they are difficult to organize. For example, the Removable Storage Device class can include:

- Internal secondary hard drives
- External hard drives
- USB flash drives

Because of these large categories, Device Control includes Device Collections, which are smaller groups that you can create within the Device Library.

You can create Device Collections by right-clicking an existing Device Class.



### The Default-Deny Principle

While enforcement mode is enabled, Device Control operates on a default-deny principle. This principle dictates that if no policy for a device exists, that device is blocked from use.

Some implications of this principle are:

- You, the administrator, must create a policy for each device that your end users need to complete their work. End users can only use devices that you explicitly approve.
- Any device that you have no policy for is blocked. The default-deny principle protects your organization from unknown devices.

### Device Control Policy Types and Options

When planning your policies, it's important to understand the different policy types at your disposal, along with the options they offer.

- "Policy Types" on the next page
- "Policy Options" on page 33

### **Policy Types**

Device Control allows you to create four different policy types. Review this section to understand each policy type and how they fit into your organization security policy.

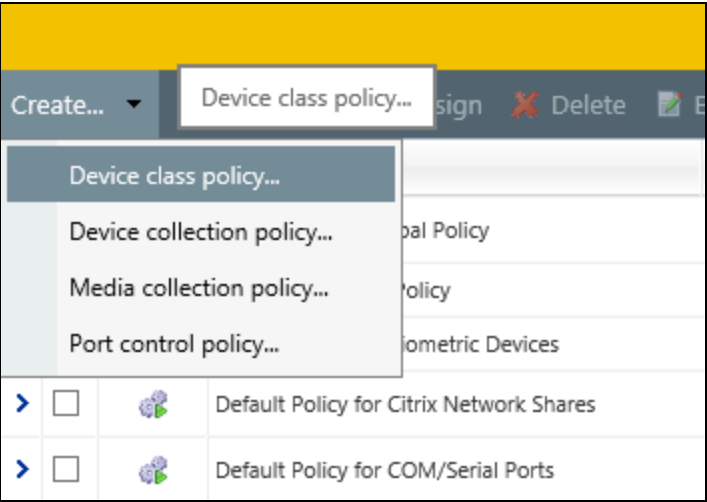
The policy types are:

- "Device Class Policies" on the next page
- "Device Collection Policies" on page 32
- "Media Collection and Port Control Policies" on page 33

**Device Class Policies**

Device Class Policies are policies based on "Device Classes" on page 26. These policies control user access to a generic type of endpoint hardware. This is the main type of policy you'll be creating.

Create Device class policies by selecting **Manage > Device Control Policies** and then selecting **Create > Device class policy** from the toolbar.



**Default Device Class Policies**

Device Control comes pre-configured with a default Device Class Policy for each Windows Device Class. View these policies from **Manage > Device Control Policies**.

>	<input type="checkbox"/>		Default Policy for Citrix Network Shares
>	<input type="checkbox"/>		Default Policy for COM/Serial Ports
>	<input type="checkbox"/>		Default Policy for DVD/CD Drives
>	<input type="checkbox"/>		Default Policy for Floppy Disk Drives
>	<input type="checkbox"/>		Default Policy for Imaging Devices
>	<input type="checkbox"/>		Default Policy for LPT/Parallel Ports
>	<input type="checkbox"/>		Default Policy for Network Access Devices
>	<input type="checkbox"/>		Default Policy for Palm Handheld Devices

After transitioning from **Audit** mode to **Policy enforcement** mode (which will happen later in "Enable Enforcement" on page 57), these default policies are in effect. They are configured to be minimally intrusive. Their default settings assign full Read/Write permissions to all users.

We've provided these policies so that you can deploy your own policies individually. The default policy remains in effect until you disable it in favor of your custom policy.



We *do not* recommend editing the default policies. We recommend leaving the default settings in place so that if you have to troubleshoot custom Device Control policies, you have the default policies to fall back on while you troubleshoot.

---

### **Device Collection Policies**

This policy type is similar to a Device Class Policy. However, instead of targeting an entire class, it targets "Device Collections" on page 27 that you've created.

This policy type is useful when a Device Class Policy would be ineffective due to variety within the class.

Let's simulate a scenario where you want to create a policy for the Removable Storage Devices class. This class includes many different devices, including internal hard drives, USB flash drives, and external hard drives. However, you want to treat each of these devices differently:

- Internal Hard Drives: You want to allow all users unlimited access.
- USB Flash Drives: You want to allow all users read-only access.
- External Hard Drives: You want to limit user copying to less than a gigabyte a day.

For cases like the one above, instead of creating a single Device Class Policy, you would instead create three Device Collections, and then create three Device Collection Policies. These policies allow more flexibility within a given Device Class.



### **Media Collection and Port Control Policies**

The remaining policy types are media collection policies and port control policies. These policy types are used less than device policies.

- **Media Collection Policies**

Use these policies to control access to data on CDs and DVDs.

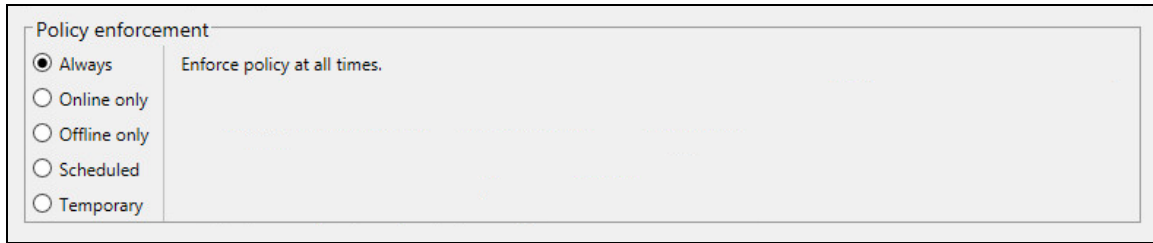
- **Port Control Policies**

Use these policies to control access to endpoint physical ports, such as USB ports, FireWire, Bluetooth, and so on.

### **Policy Options**

Regardless of policy type, policies are created by completing a wizard. This wizard contains common options. You can review what those options are here.

- "Policy Enforcement: When and Where to Enforce Policies" on the next page
- "Policy Permission Settings: What Permissions to Give Users on What Devices" on page 36
- "Policy Assignment: Who (Or What) to Assign the Policy to" on page 37

**Policy Enforcement: When and Where to Enforce Policies**A screenshot of a software interface titled "Policy enforcement". It features a list of five radio button options: "Always", "Online only", "Offline only", "Scheduled", and "Temporary". The "Always" option is selected, indicated by a filled circle. To the right of the "Always" option, the text "Enforce policy at all times." is displayed. The other options are unselected, shown with empty circles.

When planning your policies, consider when and where you want them enforced. During policy creation, Device Control offers the following policy enforcement options:

- **Always**

This simple, straightforward option enforces the policy at all times once applied. This is the mostly commonly chosen option, but the policy is applied without regard to context.

- **Online Only**

Online policies are enforced when the endpoint is within your organization's network and can contact the Endpoint Security Server.

- **Offline Only**

Offline policies are enforced when the endpoint is disconnected from your organization's network. This policy is best applied to users and endpoints that are mobile; field workers who carry laptops for example.

Online and Offline policy enforcement is best used in tandem, applying them to the same users and groups. This enforcement plan allows you to apply a restrictive policy when the endpoint is off site, preventing field workers from copying data off their endpoints when at customer sites.

- **Scheduled**

Scheduled policies are enforced during days and times that you choose. This policy enforcement option restricts device use during office hours.

- **Temporary**

This enforcement option temporarily assigns a user special permissions for a short time before revoking them.

Normally this enforcement option isn't used during initial deployment of Device Control, and is best-used for daily administration—for example, when allowing access to a USB flash drive from a conference room computer.

However, organizations with high employee turnover may prefer **Temporary** policies rather than **Always** policies. For example, you might:

- Assign users permissions six months to a year.
- Either extend or revoke the policy when the initial period ends.

## Policy Permission Settings: What Permissions to Give Users on What Devices

The screenshot shows the 'Device Class Policy' configuration window. The 'Permission Settings' section is active, with the instruction 'Define which permissions users will have based on this policy.' Below this, the 'Permissions' section has two options: 'Block all access' (unselected) and 'Allow the following permissions:' (selected). Under 'Allow the following permissions:', there are checkboxes for Read, Write, File filters, Encrypt, Decrypt, Export to file, Export to media, and Import. Read, Write, and Import are checked. The 'Apply permissions to:' section has a 'Connections' subsection with radio buttons for All (selected), USB, FireWire, ATA/IDE, SCSI, PCMCIA, Bluetooth, and IrDA. The 'Drives' subsection has radio buttons for Both drive types (selected), Hard drives only, and Non hard drives only. The 'Encryption' subsection has checkboxes for Self contained encryption and Unencrypted/Unknown encryption type, both of which are checked. At the bottom, the 'Rule definition:' text box contains the text: 'Allow Read Write Import on All connections for hard and non hard drives with self contained encryption unencrypted/unknown encryption type'. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

Regardless of the policy types that you create, they all include Permission Settings. These settings let you choose different access rights for users and endpoints that are assigned the policy. The permissions that are available change according to device class, but the most important settings are:

- **Permissions** for users (or endpoints) assigned this policy, including standard Windows permissions like read and write access, and more specialized access like the ability to encrypt devices.
  - Need help with creating policies that include encryption permissions? See "Encryption Scenarios" on page 87.
  - The permissions available vary according to policy type and device class. See "Policy Permission Settings: What Permissions to Give Users on What Devices" above for more information.
- **Connections** (and other settings), which specify that the permissions that you've selected apply to *only devices that have connected over a specific type of physical port*. For example, you can create a policy for secondary storage devices that are connected internally using a SCSI port.



There may be additional options for specifying what devices that the permissions apply to, such as [Encryption](#).

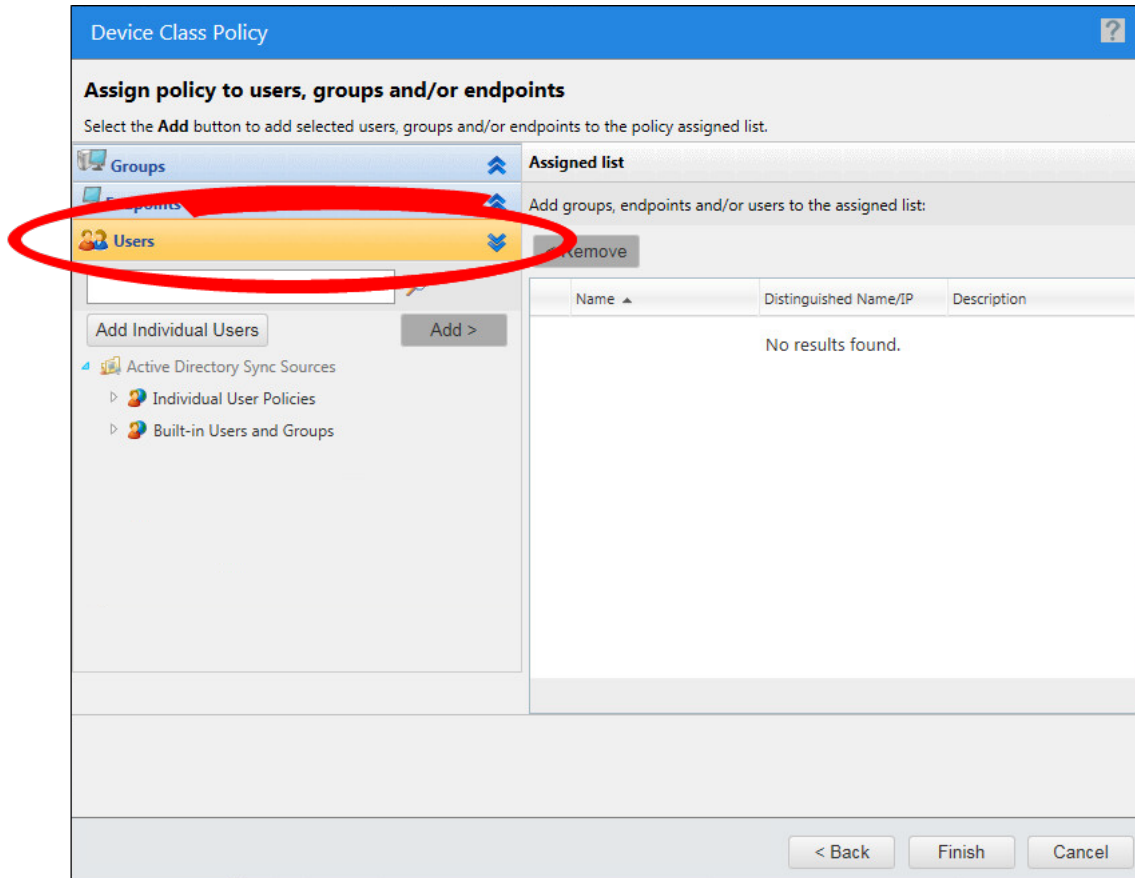
### **Policy Assignment: Who (Or What) to Assign the Policy to**

Before creating your policies, determine how you're going to assign them to your organization. Earlier in this best practice guide we demonstrated how to [synchronize Endpoint Security with your Active Directory](#). You can now use your active directory objects to assign Device Control policies. You can assign policies using one of two methods:

- "Assignment by Users " on the next page
- "Assignment by Endpoint" on page 40

## Assignment by Users

Typically, Device Control policies are centered around people, not machines. Therefore, we recommend assigning Device Control policies by user groups rather than endpoints. Assignment by user groups improves policy distribution and enforcement efficiency.



This method of assignment can be a shift in thinking, especially for IT organizations that usually manage other functions by endpoint, such as patching or antivirus. However, assignment by user ultimately reduces your administrative workload.

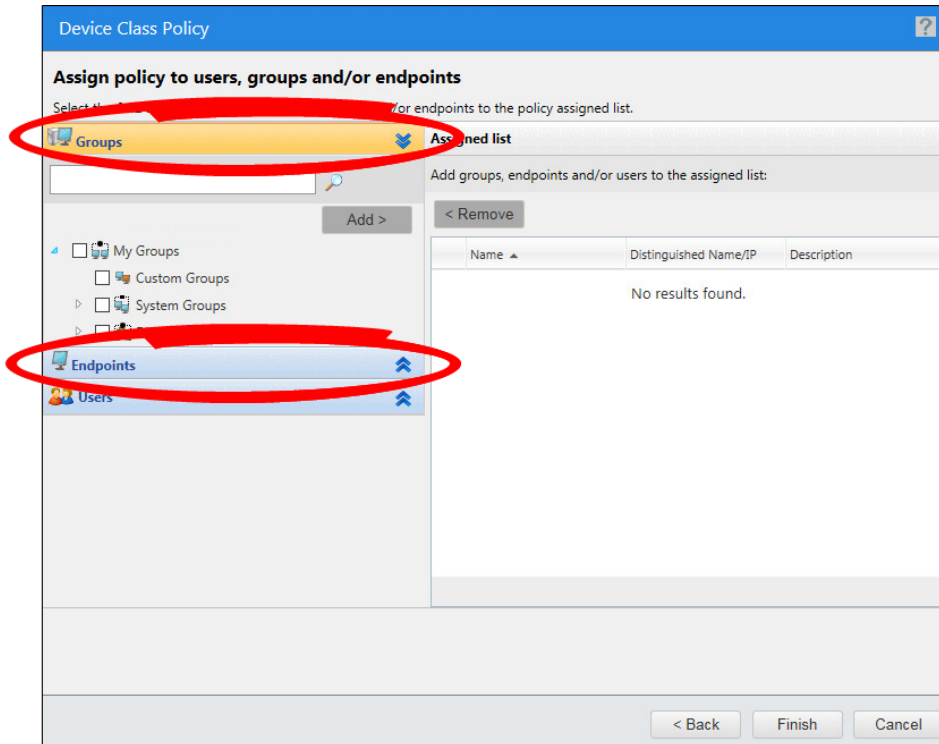
## Why Should I Apply Policies to Users and Not Endpoints?

- When a policy is applied only to a user or user group, it applies to those users on *all* endpoints they use. In contrast, when a policy is applied only to an Organizational Unit, endpoint, or endpoint group, it applies to all users on those specific endpoints.
- When a policy is applied to a combination of users and endpoints, it applies only to those users when they are logged onto those endpoints.

- A policy that's assigned to users is identical on every endpoint. Therefore, it can be distributed as a single policy. In contrast, policies assigned to endpoints are unique; a policy file per policy must be distributed. When assigning a policy directly to a large number of endpoints, many policy files are created and transmitted, resulting in increased network traffic.
- Assigning by user ensures you won't have to reassign policies when hardware is upgraded, replaced, or moved.

## Assignment by Endpoint

Although we typically recommend assigning policies by user and user group, you can also assign policies to endpoints and endpoints groups. We recommend assigning Device Control policies by endpoint instead of users only in specific circumstances.



## When Should I Apply Policies by Endpoint?

Examples of when you should apply a Device Control policy to an endpoint/endpoint group instead of a user include:

- Apply policies directly to endpoints such as a lobby kiosk that only has guests using it.
- Apply policies directly to servers that have a specialized piece of hardware not used with other servers.



## Create Policy Goals

Before creating your first Device Control policies, you should develop goals for those policies. Device Control is very flexible and can help you meet those goals regardless of what they are.

When shaping your policy goals, divide planning into two parts:

1. Review Organizational Data

Before you create policies, you need to gather information that will help you shape them.

2. Use that Data to Shape Your Policies

After reviewing your data, you should have a bigger picture of who is using what devices in your organization, and with what purpose. Now you should know what policies are needed.



Use the "Policy Planning Worksheet" on page 93 as a template for creating your policies.

---

If your organization already has a written security policy, determining your Device Control policy goals should be straightforward. Simply identify the authorized use cases in the policy and make a list of them. You can then create a Device Control policy for each case. If your organization does not have a written security policy, you should develop one.

## Determine Your Security Category

Device Control is used successfully in organizations ranging from minimum to maximum IT security. Before planning your Device Control policies, determine your organization security category. Knowing this information can help you determine policy settings when you're unsure what they should be.

Organizations typically fall into one of three categories:

- **Permissive**

These organizations have few Device Control enforcement requirements. Their primary goal is usually auditing and reporting of user activity or resolving a specific issue, such as limiting USB storage devices to read-only access. The written data security policy at these organizations is usually informal or brief. External regulations and compliance concerns are minimal or non-existent.

- **Moderate**

These organizations usually have a written data security policy in place, and they want to enforce that policy without relying on voluntary user compliance. Their goal is to prevent any unauthorized usage. However, they allow exceptions in authorized cases, resulting in maximum organizational productivity. These organizations typically have external audit or compliance requirements, such as data encryption (including data transferred onto USB flash drives).

- **Stringent**

These organizations deal in confidential information, and are typically monitored either internally or externally by a third party. The goal of these organizations is to prevent device usage except for cases authorized by their data security policy. Device usage may be restricted to encrypted devices, and every file transferred to or from devices is saved and reviewed.

## Review Device Events

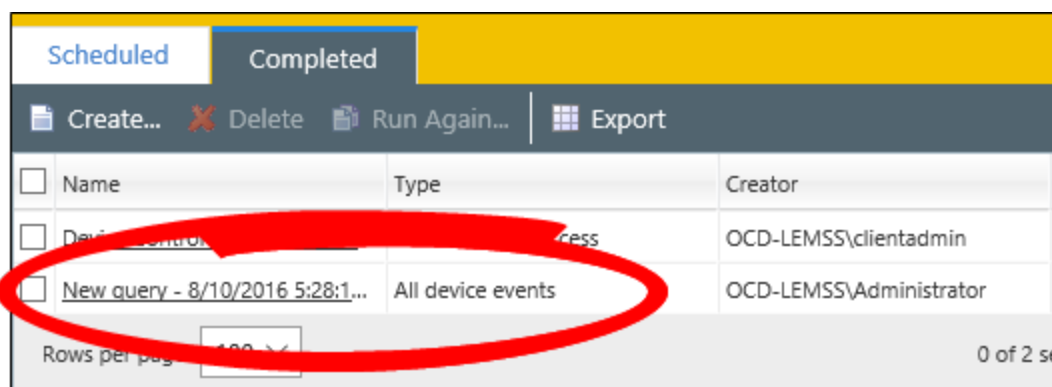
An important part of Device Control policy planning is researching how many policies you need to create. Reviewing your Device Event Log Queries provides useful information for determining this number.

### To Review Device Event Log Queries:

1. Select **Review** > **Device Event Log Queries**.



2. Select the most recent query for **All Device Events** (in the **Type** column).



- If necessary, click **Create** to make a log query. Make sure the query is configured to log all device events.
- If you've already create a query that logs all device events, you can click **Run Again** to update the results.

The latest Device Event Log Query displays.

All device events										
Lists all logged device control events for a given set of endpoints and/or users over a specified time period.										
New query - 8/10/2016 5:28:12 PM - 8/10/2016 5:29:51 PM - 10 (Server)										
<div> Add To Device Library Export Refresh Options </div>										
<input type="checkbox"/> Log Time (Agent...	Type	Logged In User	Endpoint	Class	Model ID	File Name	File Path	Process Name	Size	Reason
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	COM/Serial Ports	ACPI\VEN_PNP&...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	COM/Serial Ports	ACPI\VEN_PNP&...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:58...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	COM/Serial Ports	ACPI\PNP0501				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:58...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	COM/Serial Ports	ACPI\PNP0501				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	DVD/CD Drives	IDE\CdRomNECV...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:58...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	DVD/CD Drives	IDE\CdRomNECV...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	Floppy Disk Drives	FDC\GENERIC_FL...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:34:07...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	Floppy Disk Drives	FDC\GENERIC_FL...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	LPT/Parallel Ports	ACPI\VEN_PNP&...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	LPT/Parallel Ports	LPTENUM\Micros...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:58...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	LPT/Parallel Ports	ACPI\PNP0400				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:34:07...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	LPT/Parallel Ports	LPTENUM\Micros...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:45:01...	DEVICE-ATTACHED	mc\Administrator	EP-10EN032	PS/2 Ports	TS\NPT\TS_KBD				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:49...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	PS/2 Ports	ACPI\VEN_PNP&...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:45:01...	DEVICE-ATTACHED	mc\Administrator	EP-10EN032	PS/2 Ports	TS\NPT\TS_MOUSE				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:45:04...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	PS/2 Ports	TS\NPT\TS_KBD				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:45:04...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	PS/2 Ports	TS\NPT\TS_MOUSE				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:56...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	PS/2 Ports	ACPI\PNP0303				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/5/2016 1:42:45...	DEVICE-ATTACHED	NT AUTHORITY\...	EP-10EN032	Removable Stora...	SCSI\DiskVmware...				0	DEVICE-ATTACHED
> <input type="checkbox"/> 8/8/2016 6:33:21...	DEVICE-ATTACHED	NT AUTHORITY\...	OCD-LEM55	Removable Stora...	SCSI\DiskVmware...				0	DEVICE-ATTACHED
Rows per page: 100 0 of 20 selected Page 1 of 1 1										

### How Does This Information Help Me?

A Device Event Log Query displays all instances of a device connecting to your endpoints since you enabled **Audit** mode for your Global Device Control policy. It helps you by displaying:

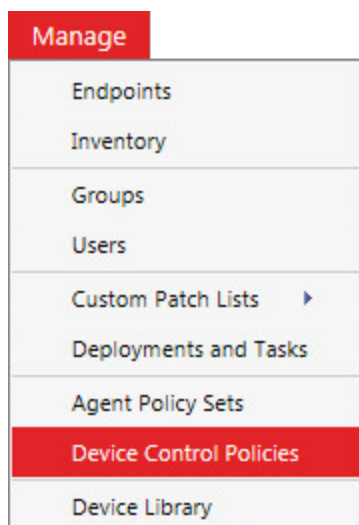
- Every type of Device Class that's operating in your network. By counting how many different class types are listed, you can make a rough estimate about the minimum number of Device Control policies you need. Notate each Device Class that your organization uses in the "Policy Planning Worksheet" on page 93.
- Every specific model of device that's been connected to your endpoints. If you find that a specific device class has many different types of models connecting, that's a good indication you need to create policies that target Device Collections, which are smaller groups of devices in a class. For example, you may determine that some devices in a Device Class are approved for company use, but others in that class are not, so you'll need two different policies. Notate Device Classes that need to be separated into Device Collections in the "Policy Planning Worksheet" on page 93.
- The Active Directory users responsible for connecting the device. This information is helpful for determining who requires what permissions when creating policies. Also, it can help you identify users who don't use devices responsibly. Use this information for determining who a policy should be to in the "Policy Planning Worksheet" on page 93.

## Review Default Policies

During planning, you can benefit from reviewing the settings configured in the default Device Class Policies.

### To Review Default Policies:

1. Select **Manage > Device Control Policies**.



- From the page list, expand a default policy to view its settings (as depicted below). Repeat this process for each default policy.

Name	Value	Description
Apply Permissions	True	Permission settings
Priority	Normal (Default)	High priority overrides Normal priority. Same priority will be merged.
Class	Biometric Devices	Device Class
Read	Allowed	Read Access
Write	Allowed	Write Access
Decrypt	Disallowed	Decrypt Access
Encrypt	Disallowed	Encrypt Access
Import	Disallowed	Allow a key file stored outside of the device to be used to unlock data on the device.
Export to media	Disallowed	Export key to a file off of the encrypted device.
Export to file	Disallowed	Export key to a file on the encrypted device.
Filtered	False	Apply File Filtering
Read Shadowing	Shadowing not applied	No shadowing
Write Shadowing	Shadowing not applied	No shadowing
Copy Limit	No limit	Limitation on bytes copied to device
Schedule	Always	Policy enforcement
Data Buses	All	Apply to connections

### How Does This Information Help Me?

- When you transition from Audit mode to Policy enforcement mode (in the upcoming phase), your endpoints will enforce the default policies until you enable your custom policies. Knowing how your users can interact with devices during this transition is helpful.
- If you're having trouble getting your custom policies to work later, you can use these default policies as a reference for troubleshooting your custom policies.



We *do not* recommend editing the default policies. We recommend leaving the default settings in place so that if you have to troubleshoot custom Device Control policies, you have the default policies to fall back on while you troubleshoot.

## Determine Policy Requirements

Determine a few things before you plan your policies:

- **What devices do I need policies for?**

- a. Find out what devices are used in your organization. You need a policy for each device class that's used. See "Review Device Events" on page 43 to find information that helps you determine how many policies you need.
- b. After getting a general idea of how many policies you'll need, learn the different "Policy Types" on page 29. This info should help you further refine the number of policies you need.

- **When and where should the policy be active?**

You can configure each of your policies to be active on certain dates and times. Review "Policy Enforcement: When and Where to Enforce Policies" on page 34 and then plan your policies to keep unnecessary device use to a minimum.

- **What permissions do my users need?**

Different users require different access rights. Review "Policy Permission Settings: What Permissions to Give Users on What Devices" on page 36 for more information on assigning user access permissions to each of your policies.

- **How should I assign my policies?**

You can assign policies by user or endpoint. Review "Policy Assignment: Who (Or What) to Assign the Policy to" on page 37 to figure out which method is best for you: users, endpoints, or a combination of both.

## Policy Planning Pitfalls

There are some common mishaps that occur during policy planning. Don't let them happen to you!

### Device Class Policies: Secondary Hard Drives

If your organization has endpoints that use secondary internal hard drives, you need to have a policy that allows access to those secondary hard drives.

The most common endpoint configuration designates:

- The C: drive as the primary operating system (OS) drive
- Any other drives as user and/or application data drives

Windows operating systems classify secondary hard drives in the Removable Storage Device class. Windows does not clearly communicate this classification (for example, Windows displays the secondary drives in **My Computer**). However, both Windows and Device Control consider secondary drives removable storage devices. Access to these drives is blocked unless allowed by policy.

To restrict the applicability of a policy to these drives, you have some choices:

- One option is to add all models of secondary hard drives into a Device Collection, and then create a Device Collection policy that allows the *Everyone* user read and write access to those drives, not just an AD user. This option is the most restrictive, but requires the connection of these drives to a managed endpoint to log the device-attached event so the device model can be added to a collection.
- Another option is to create a Device Class policy for the **Removable Storage Device** class. On the second page of the policy wizard, allow **read and write** permissions. Do not allow **Encrypt** permissions in order to prevent accidental encryption of this drive. In the **Connections** group, select **ATA/IDE**, and in the **Drives** group, select **Hard drives** only. Assign this policy to **Everyone**. This policy requires less effort, but is not quite as restrictive. The OS has no way of differentiating between IDE and EIDE connected drives. They are actually the same bus, but the connector is on the outside of the case instead of the inside. A user could connect an EIDE drive and have access to that drive. Also, if you have SCSI connected drives, you must create a second policy, identical to this example except for the bus connection setting.

#### **All Policy Types: Encryption Policy**

The encryption options available when creating policy are a little confusing, so we have more detail for you here.

Need instructions on how to set to set encryption permissions? See "Encryption Scenarios" on page 87.

#### **Permission Encryption Options vs. Encryption Options**

- **Permission Encryption Options**

These options (**Encrypt** and **Decrypt**) determine whether a user has permission to Encrypt or



Decrypt devices.

The screenshot shows the 'Device Class Policy' configuration window. The 'Permissions' section is selected, and the 'Allow the following permissions' option is chosen. A red circle highlights the 'Encrypt' and 'Decrypt' checkboxes, which are both checked. Other permissions like 'Read', 'Write', 'Export to file', 'Export to media', and 'Import' are also visible. The 'Connections' section shows 'All' connections selected. The 'Drives' section shows 'Both drive types' selected. The 'Encryption' section shows 'Self contained encryption' and 'Unencrypted/Unknown encryption type' checked. The 'Rule definition' section contains the text: 'Allow Encrypt, Decrypt, Export to media on All connections for hard and non hard drives with self contained encryption, unencrypted/unknown encryption type.' The bottom of the window has '< Back', 'Next >', and 'Cancel' buttons.

Device Class Policy

Define which permissions users will have based on this policy.

Permissions

☐ Block all access

☒ Allow the following permissions

☐ Read

☐ Write

☐ File filters

☒ Encrypt

☒ Decrypt

☐ Export to file

☒ Export to media

☐ Import

Apply permissions to:

Connections

☒ All

☐ USB

☐ FireWire

☐ ATA/IDE

☐ SCSI

☐ PCMCIA

☐ Bluetooth

☐ IrDA

Drives

☒ Both drive types

☐ Hard drives only

☐ Non hard drives only

Encryption

☒ Self contained encryption

☒ Unencrypted/Unknown encryption type

Rule definition:

Allow Encrypt, Decrypt, Export to media on All connections for hard and non hard drives with self contained encryption, unencrypted/unknown encryption type.

< Back Next > Cancel

## • Encryption Options

These options determine how the user can interact with a device that is:

- **Self contained encryption**, a device that has encryption contained to the individual device. Only users with a password can access encrypted information on the device.
- **Unencrypted/Unknown encryption type**, a device that does not have encryption or has an encryption type unrecognized by Device Control control.

**Device Class Policy**

Define which permissions users will have based on this policy.

**Permissions**

☐ Block all access

☒ Allow the following permissions:

☐ Read ☒ Encrypt ☐ Export to file

☐ Write ☒ Decrypt ☒ Export to media

☐ File filters ☐ Import

**Apply permissions to:**

**Connections**

☒ All ☐ ATA/IDE ☐ Bluetooth

☐ USB ☐ SCSI ☐ IrDA

☐ FireWire ☐ PCMCIA

**Drives**

☒ Both drive types

☐ Hard drives only

☐ Non hard drives only

**Encryption**

☒ Self contained encryption

☒ Unencrypted/Unknown encryption type

**Rule definition:**

*Allow Encrypt, Decrypt, Export to media on All connections for hard and non hard drives with self contained encryption, unencrypted/unknown encryption type.*

< Back Next > Cancel

## Copy Default Policies

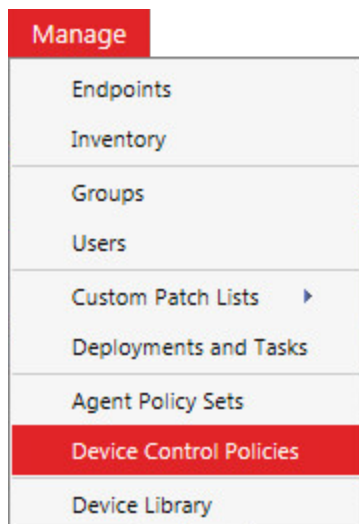
By default, Device Control includes a policy for each Device Class. These default policies allow read and write access. These policies are intended to function as a fallback if any custom policy that you create doesn't function as intended.

However, in a production environment, you should test your custom policies on an endpoint group dedicated to testing. This testing requires a set of policies identical to the default Device Policies.

We'll have more information about setting up test groups later in "Test Device Control Policies" on page 58.

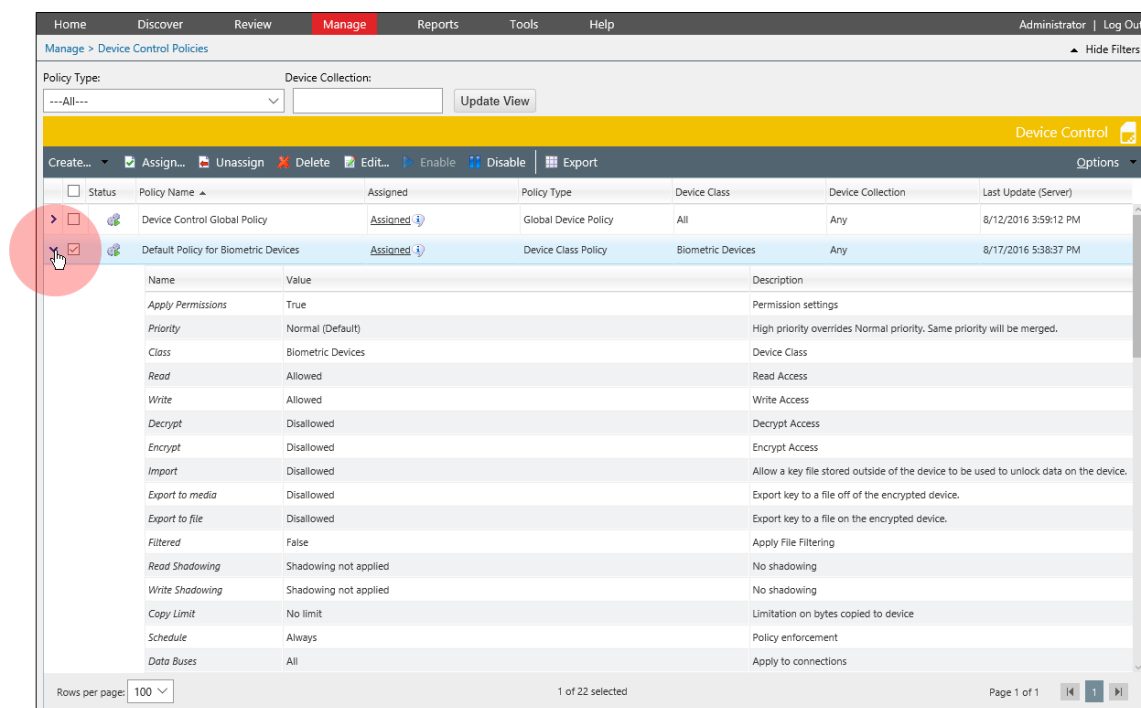
**To Copy Default Policies:**

1. From the Endpoint Security Console, select **Manage > Device Control Policies**.



2. Expand one of the default policies. Each default policy is named **Default Policy for Device Class**.

In this example, we're starting with the **Default Policy for Biometric Devices**.



3. From the toolbar, select **Create > Device class policy**.

4. Complete the Policy Wizard, duplicating each setting that's listed in the expanded policy. Name the policy something like **Copy of Default Policy of Device Class**.

In this example, we're naming the policy **Copy of Default Policy for Biometric Devices** and duplicating the original policy's settings.

Name	Value
Apply Permissions	True
Priority	Normal (Default)
Class	Biometric Devices
Read	Allowed
Write	Allowed
Decrypt	Disallowed
Encrypt	Disallowed
Import	Disallowed
Export to media	Disallowed
Export to file	Disallowed
Filtered	False
Read Shadowing	Shadowing not applied
Write Shadowing	Shadowing not applied
Copy Limit	No limit
Schedule	Always
Data Buses	All
Device Collections	Any
Users	Everyone
Endpoint	None
Groups	None

Device Class Policy

**Policy Details**

Create a policy that applies to an entire device class.

Policy name:  Override priority:

Device class:

Settings applied by this policy

☒ Permission settings (Define read, write and other permissions.)

☐ Shadow settings (Store a copy of data written to or read from devices.)

☐ Daily copy limit:  MB

Policy enforcement

☒ Always Enforce policy at all times.

☐ Online only

☐ Offline only

☐ Scheduled

☐ Temporary

Activation

☒ Enable - Start policy on **Finish** (only if assigned to a group/endpoint)

☐ Disable

Next > Cancel

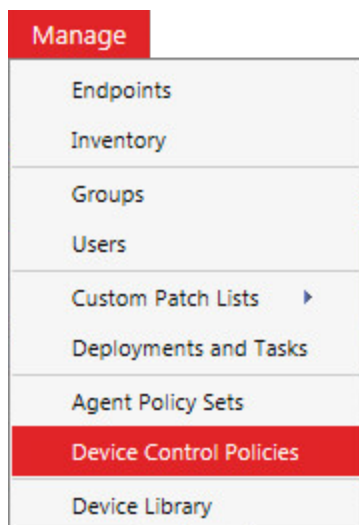
5. Repeat steps 2 through 4 until you have a copy of each default Device Class Policy.

## Create Custom Policies

You've completed the hard part of planning your policies. Now you just need to create them.

### To Create Custom Device Control Policies:

1. From the Endpoint Security Console, select **Manage > Device Control Policies**.



2. Complete the Policy Wizard, using the settings that you've determined you need during planning for a device class (or collection).

**Device Class Policy**

**Policy Details**  
Create a policy that applies to an entire device class.

Policy name:  Override priority:

Device class:

**Settings applied by this policy**

- ☐ Permission settings (Define read, write and other permissions.)
- ☐ Shadow settings (Store a copy of data written to or read from devices.)
- ☐ Daily copy limit:  MB

**Policy enforcement**

☒ Always Enforce policy at all times.

☐ Online only

☐ Offline only

☐ Scheduled

☐ Temporary

**Activation**

☒ Enable - Start policy on **Finish** (only if assigned to a group/endpoint)

☐ Disable

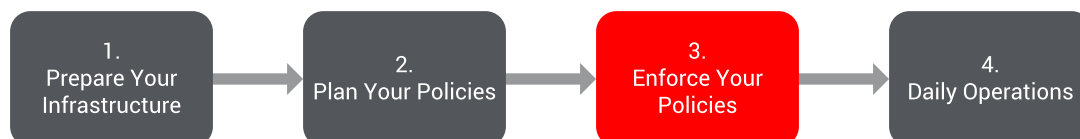
Next > Cancel



We do not recommend changing the **Override priority** option from **Normal** to **High**. This edit can lead to odd results when two or more policies are applied to an endpoint group. These odd results can make troubleshooting difficult. If you need to achieve a specific outcome when applying multiple policies to the same group, we recommend reviewing "Default Policy/ Custom Policy Conflict Resolution" on page 84.

3. Repeat the first two steps, creating a policy for each device class or device collection that you've planned for.

## Phase 3: Enforce Policies



Now that you've created your Device Control Policies, you can begin deploying them to your organization. This section of the guide describes each step in a smooth deployment.

In this phase, you will:

1. "Plan Deployment Informational Campaign" on the next page  
Inform your end users that you're deploying your policies. They need to know how Device Control affects them.
2. "Enable Enforcement" on page 57  
Switch from **Audit** mode to **Policy enforcement** mode to begin enforcing the default Device Control Policies.
3. "Test Device Control Policies" on page 58  
Before deploying your custom Device Control Policies to your production endpoints, test them on a small group of endpoints to confirm they're working correctly.
4. "Confirm Policy Functionality" on page 62  
Finally, review device event logs to make sure that your policies are functioning correctly. If they aren't, edit your policies to correct them.
5. "Deploy Device Control Policies" on page 65  
After testing your custom policies, deploy them to your production endpoints. When you're done deploying, circle back to "Confirm Policy Functionality" on page 62 to reconfirm that your policies are working properly.

## Plan Deployment Informational Campaign

A crucial step for Device Control deployment is communicating the product's roll-out to your organization. Inform your employees that you are changing how they can interact with their devices.

### Why Do I Need an Informational Campaign?

Your users are probably accustomed to unlimited access to their personal devices while using their endpoints—they likely connect their smart phones and USB flash drives without considering security. Although this use isn't malicious, it does introduce security risk. If you plan on blocking device access that users are accustomed to, an information campaign targeting your employees will help your Device Control deployment succeed.

### What Info Should the Campaign Include?

At a minimum, we recommend including the following information in this campaign:

- Clearly state your security policy. Inform users of the rules that are being enforced.
- State why the security policy is being introduced. Examples might be:
  - Protecting the organization from malware introduced by unapproved devices.
  - Protecting lost or stolen data using a device encryption policy.
  - Protecting the organization from regulatory fines and lawsuits.
- Inform users how to request permissions for special circumstances.
- Encourage users to ask questions.

Your organization may have its own specific reasons for introducing the security policy. Be sure that your information campaign includes them.

### How Should I Communicate This Info?

Use a variety of different mediums, such as:

- Emails
- Company newsletters
- Posters in common areas

We recommend sending follow-up messages that communicate progress about the Device Control deployment. Let your employees know how the project is progressing. If you are open with your communications, employees are less likely to see your security policy as restrictive.

We also recommend recruiting an executive sponsor to support the deployment. If company employees see that leadership is endorsing the project, they are more likely to embrace it.



## Enable Enforcement

The first step in moving to enforcement is to switch the Global Device Control policy from **Audit** mode to **Enforcement** mode.

After you enable **Enforcement** mode, all Device Control policies are calculated, combined, and deployed to your endpoints. The endpoints continue logging events as they did in **Audit** mode, but they begin enforcing the policies they receive.

Each device class has its own default policy. If you leave these policies intact, enabling enforcement is minimally disruptive. These default policies:

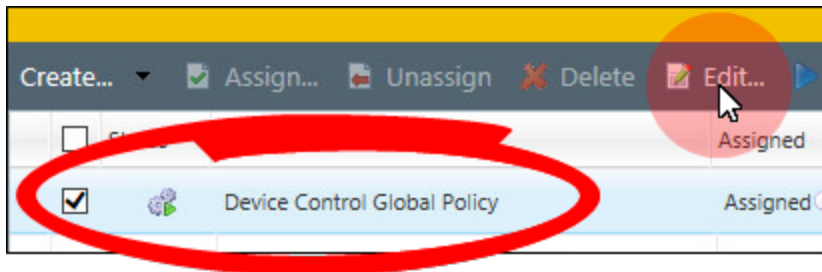
- Allow read and write permission for its device class
- Are assigned to the highest level user:

*Everyone*

Read and write permissions take priority over read only permissions and no permissions. Therefore, users assigned default policies have read and write access when default policies are in place. The only exceptions are policies configured to explicitly block all access. These policies override the default policies.

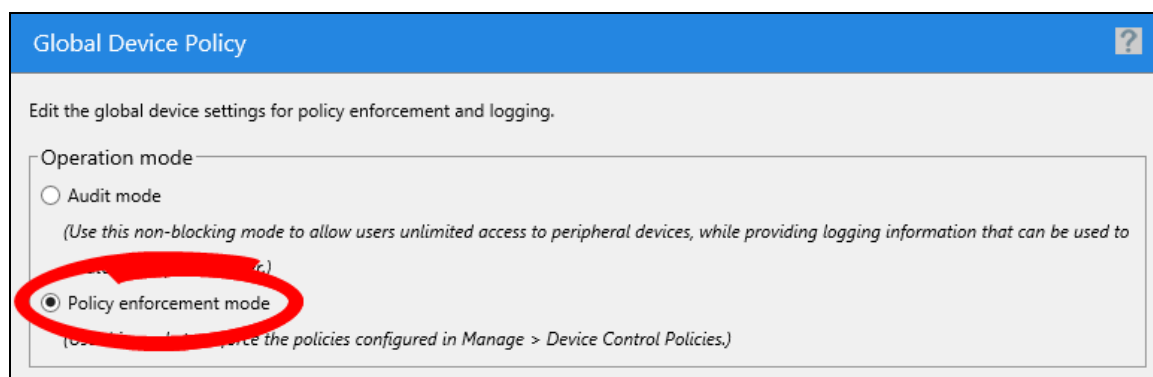
### To Enable Enforcement:

1. Select **Manage > Device Control Policies**.
2. Select the **Device Control Global Policy** and click **Edit**.



The **Global Device Policy** dialog opens.

3. Make sure that the Global Device Policy is in **Policy enforcement mode**.



4. After you select **Policy enforcement mode**, click **Finish**.
- Device Control begins enforcing policies. At this point, only the default policies are active, so users will still have relatively full access.
  - On the endpoints:
    - Monitor the system tray for the notification **Settings have changed**.
    - Or watch the Status dialog available from the system tray icon. This dialog shows what permissions the endpoint is enforcing, which may change based on policies you have configured in your environment. View this dialog to confirm that your policies are being enforced.

## Test Device Control Policies

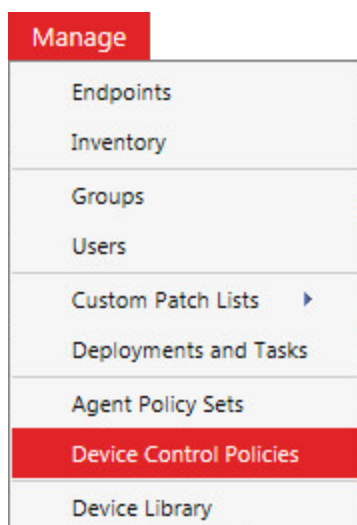
Before you deploy your policies to the entire organization, we recommend first deploying your policies to a test group. This test deployment helps reveal issues that may emerge during deployment.

### To Test Device Control Policies:

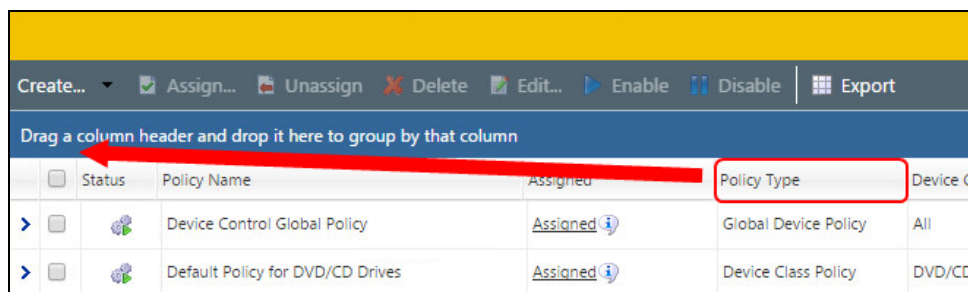
Before you begin testing your custom policies, create an endpoint group and populate it with endpoints containing a small, diverse collection of endpoints that represents different system configurations common in your organizations: desktops, laptops, and servers from different departments.

To create an endpoint group, select **Manage > Groups**, select the **Group Membership** view, and click **Create**.

1. From the Endpoint Security Console, select **Manage > Device Control Policies**.



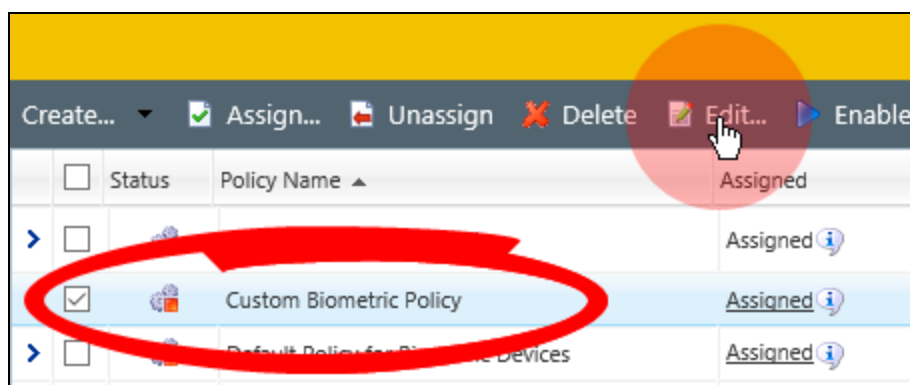
Once viewing the Device Control Policies page, you can easily sort your policies by policy type. From the toolbar, select **Options > Show Group by Row**. Then drag the **Device Class** column header into the **Group by Row...**



...to sort the policies by Device Class.

Device Class ^					
<input type="checkbox"/>	Status	Policy Name	Assigned	Policy Type	De
▼ - All					
<input type="checkbox"/>		Device Control Global Policy	Assigned	Global Device Policy	All
▼ - Biometric Devices					
<input type="checkbox"/>		Default Policy for Biometric Devices	Assigned	Device Class Policy	Bi
<input type="checkbox"/>		Copy of Default Policy for Biometric Devices	Assigned	Device Class Policy	Bi
<input type="checkbox"/>		Custom Policy for Biometric Devices	Assigned	Device Class Policy	Bi
▼ - CD/DVD Discs					
<input type="checkbox"/>		New media collection policy - 8/9/2016 4:52:16 ...	Assigned	Device Collection Policy	CD

- From the page list, select the custom policy that you want to test. From the toolbar, click **Edit**.  
In our example, we're editing a custom policy for biometric devices that we created earlier.



The **Policy Details** dialog opens for the policy.

- From the dialog, click **Next** until you get to the **Assign policy to users, groups and/or endpoints** page.

4. Assign the policy to a test group that you've created and click **Finish**.



Don't assign the policy to any other groups, endpoints, or users.

**Device Class Policy**

**Assign policy to users, groups and/or endpoints**

Select the **Add** button to add selected users, groups and/or endpoints to the policy assigned list.

**Groups**

- My Groups
- Custom Groups
  - Test Group**
- System Groups
- Directory Service Groups

**Assigned list**

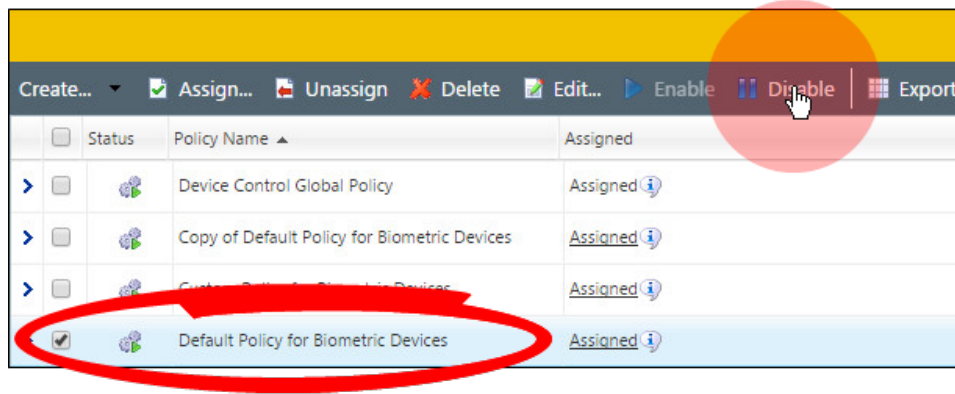
Add groups, endpoints and/or users to the assigned list:

<input type="checkbox"/>	Name ▲	Distinguished Name/IP	Description
<input type="checkbox"/>	Test Group	OU=Test Group,OU=Cus...	

0 of 1 selected Page 1 of 1

5. From the **Device Control Policies** page list, disable the default policy related to the custom Device Control Policy that you just assigned to the test group.

Since we're testing a custom policy for biometric devices, we're disabling the **Default Policy for Biometric Devices** in our example.



Don't be alarmed that you're disabling the default policy. Remember, you created a copy of each default policy earlier in "Copy Default Policies" on page 50, and that policy will continue to be enforced for all other endpoints.

6. Repeat steps 2 through 4 for each custom policy that you want to test.

Your policies are applied to the test group. Now you need to make sure those policies are functioning as intended. Proceed to "Confirm Policy Functionality" below.

## Confirm Policy Functionality

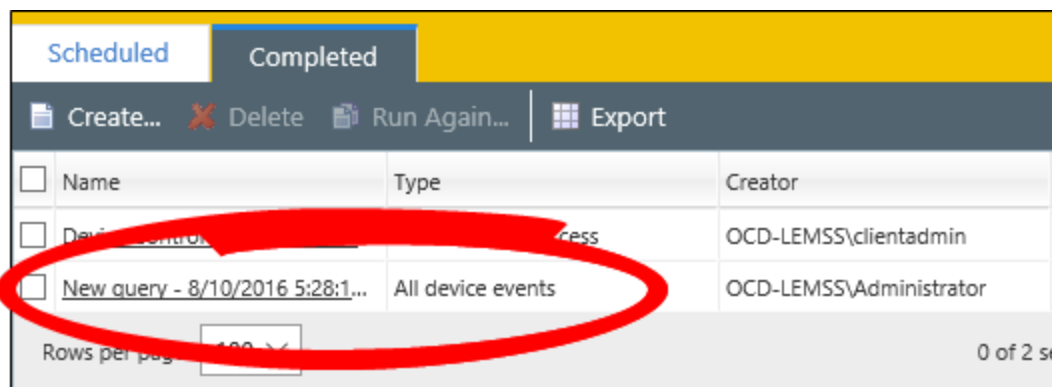
After you've applied your custom policies to your test group, review the Device Event logs to confirm that they're functioning as intended.

**To Confirm Policy Functionality:**

1. Select **Review** > **Device Event Log Queries**.



2. Select the most recent query for **All Device Events** (in the **Type** column).



- If necessary, click **Create** to make a log query. Make sure the query is configured to log all device events.
- If you've already create a query that logs all device events, you can click **Run Again** to update the results.

3. Review each device event that occurred. Make sure that each device event is either approved or blocked as you intended when you created your custom policies. If your custom policies are not functioning as intended, edit them.
  - If an event is being handled incorrectly, deactivate the offending policy and reactivate the default policy for the device class until you can correct the offending policy.
  - If you're having trouble achieving a desired result, two or more policies may be conflicting. Review "Default Policy/ Custom Policy Conflict Resolution" on page 84 for help achieving your desired outcome.



## Deploy Device Control Policies

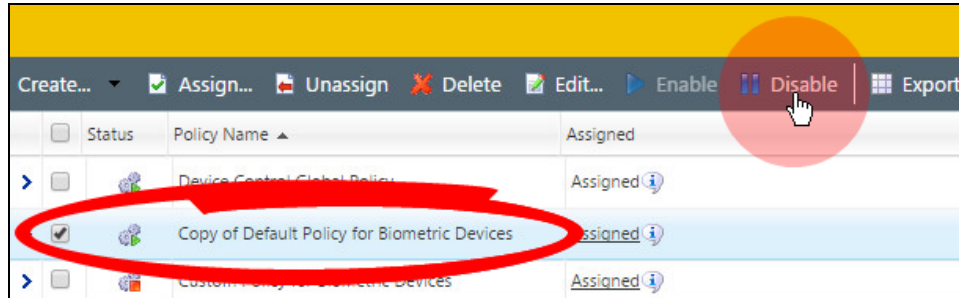
Your next step is to begin deploying your Device Control policies. We recommend the following tips when deploying your policies to avoid troubleshooting scenarios:

- Use a phased deployment approach. Take a step, verify the result, and then take another step. This deployment method helps avoid chaotic troubleshooting in environments that have many factors contributing simultaneously.
- We recommend starting the organizational deployment by enabling policies for your smallest groups of users first. Once those policies are working as intended, repeat the process with progressively larger groups.
- When applying policies to a group, only apply policies for one device class at a time. This practice leaves only the policies you created for that class in place. Check with users to confirm that policy enforcement is functioning as intended. Also check the Device Event Logs for those endpoints to validate that read or write-denied logs are functioning as intended. Users will not be aware of some device access, especially by built-in user accounts such as *LocalSystem*, or may not yet be aware of any issues that are present. If there are read- or write-denied events that should have been allowed, adjust your policies to allow them.
- Once the first device class policy is working properly, continue the process with the remaining device classes policies. Disable any Default Policies for that class (including default policy copies), confirm operation, check the logs, adjust policy as needed, and proceed to the next class. When complete, the Default Policies will all be disabled, and only your policies will be enforced.

**To Deploy Device Control Policies:**

1. Select **Manage > Device Control Policies**.
2. Disable the copy of the default policy related to custom policy that:
  - You tested in "Test Device Control Policies" on page 58.
  - Are now ready to deploy.

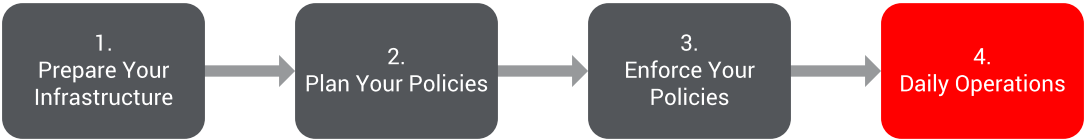
In our example we are deploying a custom policy for Biometric Devices, so we are disabling the copy we made earlier, **Copy of Default Policy for Biometric Devices**.



Disabling both the default policy and the copy of the default policy implicitly deploys your custom policy, even though you've done nothing to explicitly activate it. This implicit deployment occurs because the default policy settings of Read/Write take priority over your custom policy's settings. See "Default Policy/ Custom Policy Conflict Resolution" on page 84 for more information.

3. Repeat step 2 for each custom policy that you've tested and now want to activate. Disable any default policies related to the custom policies that you want to deploy.
4. Validate that the policy you enabled is functioning correctly. Circle back to "Confirm Policy Functionality" on page 62 and check the logs to validate policy function. Make any policy edits as needed.

# Phase 4: Daily Operation



After enforcing your policies, you still need to perform daily maintenance to keep Device Control functioning as intended. This chapter contains instructions for completing routine maintenance.

**In This Chapter:**

Dashboard Widgets .....	68
File Shadowing .....	69
Temporary Permissions .....	72
Temporary Policy .....	73
Password Recovery .....	74
Policy Maintenance .....	75
Adding Individual Users .....	76
Adding New Devices .....	78

## Dashboard Widgets

After the Device Control Server module is installed, two new widgets are available to display on the Endpoint Security Dashboard:

- "Devices Connected to Endpoints Widget" below
- "Device Control Denied Actions Widget" below

Both of these widgets display information from your Device Event Log Queries. You can view these queries from **Review > Device Event Log Query**.



These widgets omit built-in users and group data so that only actual user data is displayed (instead of unused system accounts).

---

### Devices Connected to Endpoints Widget

This widget displays the number of devices that have connected to your endpoints over the last week, organized by device class. The number of devices displayed in this widget stays relatively consistent.

If you notice the number of devices fluctuating quickly, you should investigate. For example, if you usually have no previous records of an external hard drive connecting to your endpoints, and then this widget suddenly displays that an external hard drive is being connected, you should investigate.

Click the graph bars to view data that shaped the total, including endpoint and user name.

### Device Control Denied Actions Widget

This widget totals:

- The number of read-denied events logged.
- The number of write-denied events logged.
- The users with the highest event totals.

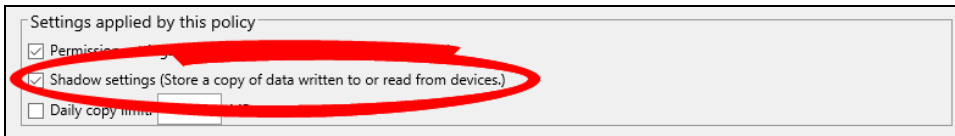
This information alerts you that either a user is trying to legitimately use devices and a policy adjustment should be made, or that a user is attempting to connect prohibited devices and warrants further investigation.

## File Shadowing

File Shadowing is a Device Control feature that creates a copy of any file that a user interacts with on a device. This interaction includes reading a file on a device, saving a file to a device, or saving a file from a device. This copied file is then uploaded to the Endpoint Security Server.

You can enable File Shadowing while creating:

- Device class policies
- Device collection policies
- Port control policies



After creating a policy that shadows files, you can view those files by creating a Device Event Log Query.

### To Create A File Shadow Device Event Log Query:

1. From the **Navigation Menu**, select **Review > Device Event Log Queries**.
2. Click **Create**.

The Device Event Log Query wizard opens.

- Complete the wizard. While completing the wizard, select **Shadowing events** from the **Type** drop-down. Click **Finish** when you're done.

**Device Event Log Query**

Create device log query

Query device activity logs immediately or schedule a recurring job.

Query name:

Type: **Shadowing events**

**Scheduling**

☒ Immediate

☐ Once

☐ Daily

☐ Weekly

Date range:  -

Email notification:

☐ Notify me via email when query is complete:

#### To View A File Shadow Device Event Log Query

- From the **Navigation Menu**, select **Review > Device Event Log Queries**. Make sure the Completed tab is selected.
- Click the Device Event Log Query containing **Shadowing events**.

Scheduled

Completed

Create...

Delete

Run Again...


Export

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	<u>New query - 8/15/2016 3:57:54 PM</u>	Shadowing events
<input type="checkbox"/>	<u>New query - 8/15/2016 3:48:18 PM</u>	Shadowing events
<input type="checkbox"/>	<u>New query - 8/15/2016 11:08:23 AM</u>	All device events

The Shadow files are displayed with the following metadata:

- The names of files transferred to and from devices (depending on how your policy is configured)
- User name

- Endpoint name
- Time of the transfer

If you enabled **Full File Shadowing**, you can view the file itself. Expand the row for an event and click the  icon. You have three options for viewing the file:

- **View using Hex Viewer**

This option is the safest, but least informative (depending on the file). The file content displays in hexadecimal format, alongside an ASCII representation of the data. This option is safest because the file is not sent to your browser. It remains in the shadow storage location and is not executed.

- **Download the file to your computer through your browser**

This option lets you choose the best option for examining the file.

- **Open the file in the browser using the browser's default action for that file type**

This option is the fastest way of viewing the file, but introduces risk as the file may contain malware or have other unexpected content.

## Temporary Permissions

This feature allows you to grant temporary permissions to users who cannot connect to the Endpoint Security Server to receive an updated policy. If a user is in the field and has an unanticipated need for device access, this feature allows you to grant specific permissions.

This process involves a challenge/response between the user and you to confirm that the request is valid. The user selects Request Temporary Access Offline from the system tray icon and completes a wizard. When the user completes the wizard, it provides them with a client key. The user then reads that key to you.

You, the administrator, can access this feature by using the Grant Temporary Permissions wizard (**Tools > Device Control > Grant Temporary Permissions**). While you complete the wizard, use the same exact settings that the end user used, including:

- Device class
- Permissions requested
- Duration of the permissions
- User the permissions are for



The end user can only select their own account or the Everyone account. You, the administrator, can choose other accounts. However, since your settings and the user's settings must be identical, you must select either the end user account or the Everyone account to grant the permissions.

---

The user reads you the client key, and you enter it in the Endpoint Security console. You then generate an unlock code and read it to the user, who enters it on the client. The user is then granted the specified permissions.



## Temporary Policy

Temporary Policies are different than "Temporary Permissions" on the previous page. Temporary policies are actual policies configured in the Endpoint Security Console and delivered to connected endpoints.

Temporary Policies are typically used for a single permission exception. They temporarily expand on a user's permissions, and then they are revoked after a set deadline expires. Temporary policies are useful for situations like:

- Providing access to devices a common area computer, such as in a conference room.
- Providing after-hours access for a team working to meet a deadline.

## Password Recovery

If you use device encryption in your organization, your users will sometimes need help recovering forgotten passwords. The **Secure Volume Browser** on encrypted devices provides a link for users to initiate password recoveries in such instances.

Password recovery requires a challenge/response. You, the administrator, must authenticate that the user is valid.

When the user clicks the **Recover Password** link, an **Encrypted Medium ID and Security Code** displays. You, the administrator, can access the password recovery by selecting **Tools > Device Control > Recover Password** from the **Navigation Menu**.

The user reads the codes to you, and you enter them into the console. You then generate another code, which you read to the user, who enters it into the **Secure Volume Browser**. The user can then set a new password for the device.

## Policy Maintenance

Policy maintenance should be minimal. If you assign the majority of your policies to the highest hierarchical level (Device Class, User Group) and plan for exceptions, then policies require no maintenance—even when new devices are added to the market or new endpoints or users are added to your organization. Policy changes are only needed when your business needs change.



If you find that you frequently need to make changes to policies, there is likely a better strategy for your policy design.

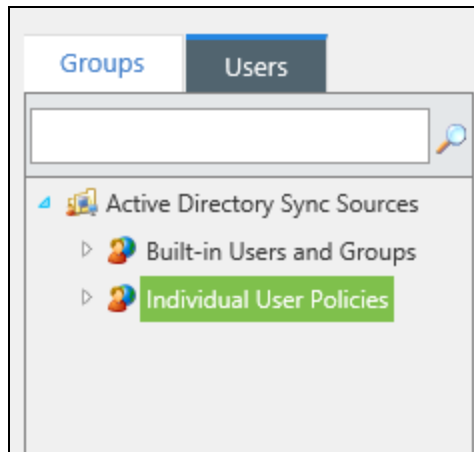
---

## Adding Individual Users

You may need to add individual users to Endpoint Security if a specific user needs a unique policy. This addition should only be done as an exception. *Do not* add all of your users Endpoint Security individually—it's too much work!

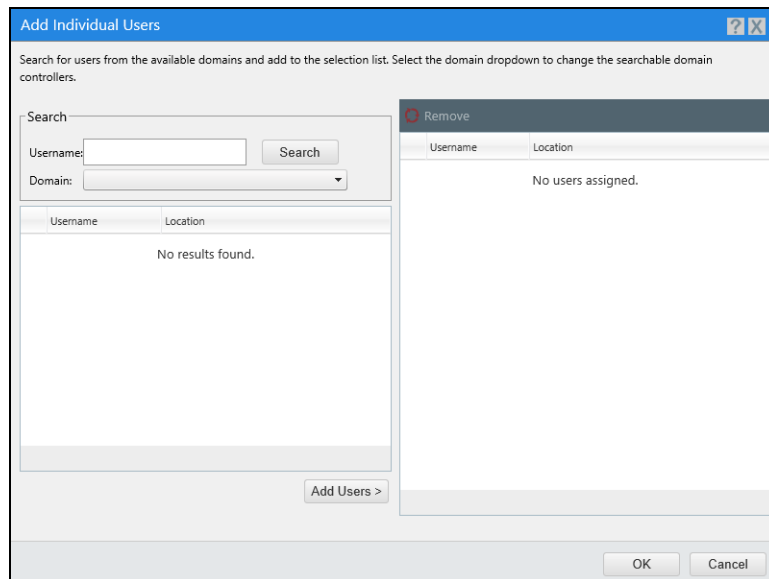
### To Add An Individual User:

1. From the **Navigation Menu**, select **Manage > Users**.
2. From the **User Browser**, select **Individual User Policies**.

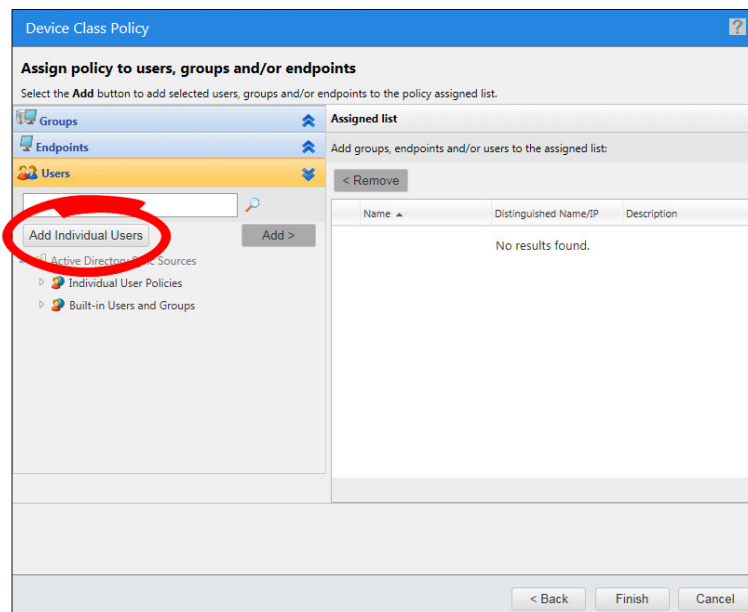


3. Click **Add**.

The Add Individual Users dialog opens.



You can also open this dialog while assigning users to a policy by clicking **Add Individual Users**.



4. Use the dialog to add a user to the system. Click **OK** when you're done.

- The user is added to the system.
- The user is available for selection in the policy wizards.

## Adding New Devices

Over time you will need to add more devices into device collections to manage their access. You can do this using either of the methods described in "Device Collection Policies" on page 32.

When you add a device to a collection, any policies that are related to that collection are updated with the new device information, and the Device Collection policies for that collection are automatically updated on the endpoints. Typically, you don't need to alter your policies or create new ones. Simply add the device to a collection that is assigned the appropriate permissions and assigned to the appropriate users.

# Appendix: References

This appendix contains reference tables about settings mentioned earlier in the document.

**In This Appendix:**

Supported Device Classes .....	80
Supported Permission Types .....	81
Default Policy/ Custom Policy Conflict Resolution .....	84
Configuration Options .....	85
Encryption Scenarios .....	87
FAQ .....	90
Policy Planning Worksheet .....	93

## Supported Device Classes

Device Control manages the following device classes:

Physical Interfaces USB	Wireless Interfaces	Device Types
<ul style="list-style-type: none"> <li>• Firewire</li> <li>• PCMCIA</li> <li>• ATA / IDE</li> <li>• SCSI</li> <li>• LPT / Parallel</li> <li>• COM / Serial</li> <li>• PS/2</li> </ul>	<ul style="list-style-type: none"> <li>• Wi-Fi</li> <li>• Bluetooth</li> <li>• IrDA</li> <li>• Wireless NICs</li> </ul>	<ul style="list-style-type: none"> <li>• Removable Storage Devices</li> <li>• External Hard Drives</li> <li>• CD / DVD Drives</li> <li>• Floppy Drives</li> <li>• Tape Drives</li> <li>• Printers</li> <li>• Modems / Secondary Network Access Devices</li> <li>• PDAs and other handhelds</li> <li>• Imaging Devices (Scanners)</li> <li>• Biometric Devices</li> <li>• Windows Portable Devices</li> <li>• Smart Card Readers</li> <li>• PS/2 Keyboards</li> <li>• User-Defined Devices</li> </ul>


Each class offers different capabilities. For example:


- Some classes can be set to allow or block all access.
- Other classes can be configured as no access, read only, or read and write access.
- Commonly used classes such as CD/DVD drives (readers/burners) and Removable Storage Devices can be further configured to:
  - Use encryption
  - Limit the types of files that are transferable to/from the device



## Supported Permission Types

There are several levels of permission that can be enforced with Device Control. While not all permission levels are supported by all classes, the most common classes are the most flexible. Here are the permissions that you can enforce, by device class.

Permission Type	Description	Device Classes Supported
<b>Block All Access</b>	Both read and write access to the device is blocked.	<p>All device classes.</p> <hr/> <p> Human Interface Devices (HID) and the primary hard drive are never blocked. Keyboards are the one exception—they can be configured to be blocked when a keylogger is detected.</p> <hr/>
<b>Read Only</b>	Data may be transferred from the device to the endpoint.	<ul style="list-style-type: none"> <li>• Citrix Network Shares</li> <li>• CD/DVD Drives</li> <li>• Floppy Disk Drives</li> <li>• LPT/Parallel Ports</li> <li>• Removable Storage Devices</li> </ul>
<b>Read+Write</b>	Data may be written from the endpoint to the device, and read from the device to the endpoint. Read permission is required to grant write permission.	All device classes.
<b>Encrypt</b>	<p>The user may encrypt devices or media. You can configure:</p> <ul style="list-style-type: none"> <li>• Encryption methods</li> <li>• Access methods</li> </ul> <p>These configuration settings are discussed later in this paper.</p>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>

Permission Type	Description	Device Classes Supported
<b>Export to Media (encryption key)</b>	<p>This permission allows end users to place the encryption key on the device itself. The key is password protected.</p> <p>Access to the encrypted data requires:</p> <ul style="list-style-type: none"> <li>• The device</li> <li>• The encryption password</li> </ul>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>
<b>Export to File (encryption key)</b>	<p>This permission allows end users to place an encryption key on a separate file during the encryption process. This file is password protected.</p> <p>Access to the encrypted data requires:</p> <ul style="list-style-type: none"> <li>• The device</li> <li>• The encryption key file</li> <li>• The encryption password</li> </ul>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>
<b>Import from File (encryption key)</b>	<p>This permission allows the user to use an exported encryption key file to unlock an encrypted device.</p>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>
<b>Decrypt</b>	<p>This permission allows end users to destroy the data on an encrypted device. This action formats the device as a new, unencrypted volume. Data on the device is lost.</p> <hr/> <p> Decrypt should not be confused with unlocking an encrypted device to access the data on the device.</p> <hr/>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>

Permission Type	Description	Device Classes Supported
<b>Copy Limit</b>	This permission limits the amount of data that a user can copy to external devices in a 24-hour period. Setting reasonable copy limits can reduce data loss.	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Removable Storage Devices</li> </ul>
<b>Shadowing (filename only)</b>	This permission records the name of files that are transferred to or from devices. All details (such as the machine name, user name, and timestamp) are also recorded. The shadowed copy can be accessed from the Endpoint Security Console.	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Floppy Disk Drives</li> <li>• Removable Storage Devices</li> </ul>
<b>Shadowing (full file)</b>	This permission retains a copy of every file transferred to or from devices. The shadowed copy can be accessed from the Endpoint Security Console.	<ul style="list-style-type: none"> <li>• COM/Serial Ports<sup>1</sup></li> <li>• CD/DVD Drives</li> <li>• Floppy Disk Drives</li> <li>• LPT/Parallel Ports<sup>1</sup></li> <li>• Modem/Secondary NIC<sup>1</sup></li> <li>• Removable Storage Devices</li> </ul> <p><sup>1</sup>Write Only</p>
<b>File Type Filtering</b>	<p>This permission allows you to control the specific file types that can be copied to or from devices. The file content is inspected. The file extension (which can be altered) is not used for enforcement.</p> <p>You can control the import and export of file types separately. For example, you may allow the reading of Microsoft Office documents but only allow the writing of PDF files.</p>	<ul style="list-style-type: none"> <li>• CD/DVD Drives</li> <li>• Floppy Disk Drives</li> <li>• Removable Storage Devices</li> </ul>

# Default Policy/ Custom Policy Conflict Resolution

As mentioned in "Device Class Policies" on page 30, Device Control includes a default policy for each device class. You should not edit these policies because they are intended for use when troubleshooting your custom policies. However, it's important to know how these default policies interact with custom policies when they are both applied simultaneously.

Here's what you need to know:

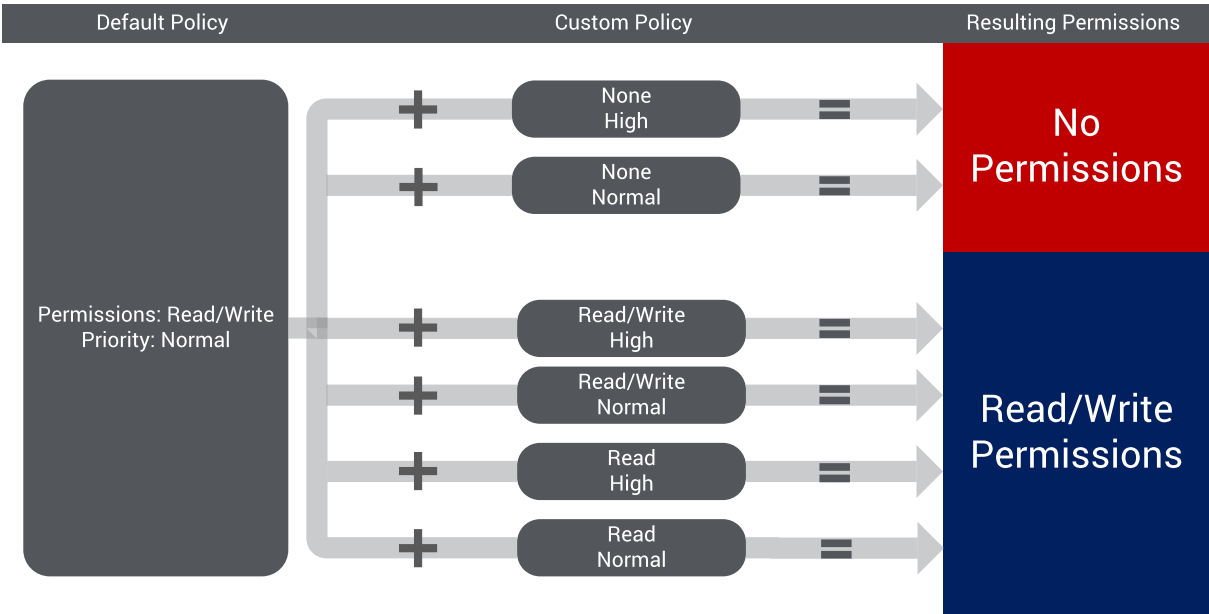
- By default, all default policies are configured to allow read and write permissions. These lenient settings allow your users to use their devices freely while you set up more stringent policies.
- If you enforce your custom policies and default policies simultaneously, the Read/Write permissions set in the default policies will almost always take priority over the permissions set in the custom policies. Read/Write permissions always take priority over read permissions.

See the [graphic](#) below to see how different permissions are resolved when there are conflicting settings.

**i** This priority resolution is the reason you need to disable default policies (and their copies) when deploying custom policies to your organization.


- The only exception to Read/Write permissions as the priority permission is when you explicitly configure your custom policy to remove all user permissions.



## Device Control Policy Conflict Resolution



## Configuration Options

You can configure default settings for Device Control from the **Tools > Options** page.

Option	Description
<b>General Settings</b>	
<b>Agent status and update notifications</b>	This setting controls if the end user can view their current accessibility permissions in the system tray.
<b>Agent permission change notifications</b>	<p>This setting provides several options related to notifying end users of any Device Control policy updates you make.</p> <p>You can configure this notification to:</p> <ul style="list-style-type: none"> <li>• Display a message every time you update a user's Device Control policy.</li> </ul> <p>This option is useful for informing users that you've updated their permissions.</p> <ul style="list-style-type: none"> <li>• Display only when temporary permissions are assigned to the user.</li> <li>• Disable the notification.</li> </ul> <p>For example, you might use this setting to prevent your user-base from spamming you questions related to the notifications.</p>
<b>Shadowing related options</b>	
<b>Server shadow directory</b>	<p>The file path where the Endpoint Security Server stores uploaded copies of files that users transfer to and from devices. Depending on how widely you use full file shadowing, storage requirements can be demanding, so enter a file path with a safe amount of storage space.</p> <hr/> <p> Changing the storage location in the future does not move your existing shadowed files to the new location.</p> <hr/>

Option	Description
<b>When a user tries to write a CD in a format that doesn't support shadowing</b>	<p>This option determines Device Control behavior when it attempts to create a shadow file for a file copied to or from a CD or DVD.</p> <p>When burning a CD or DVD, files are not written directly to the media on a file-by-file basis. Instead, an intermediate file is created that represents the entire disc image, and that single file is used to create the disc. In some cases, Device Control cannot access the individual files stored in this image file. Therefore, Device Control cannot create individual shadow copies of the files stored on the disc.</p> <p>This option also determines what action Device Control takes when it cannot create a shadow file from a disc. Options include:</p> <ul style="list-style-type: none"> <li>• Block the write operation so no data is written without being shadowed.</li> <li>• Allow the write operation, but skip shadowing. You will have no record of what data was written to the disc.</li> <li>• Allow the write operation, and create a shadow file of the entire disc.</li> </ul> <hr/> <p> This option may consume excessive disk space if used frequently.</p> <hr/>
<b>Encryption settings</b>	
<b>Enforce Password Complexity</b>	<p>Forces users to use complex passwords when encrypting devices. Device Control uses the <a href="#">Microsoft Password Complexity Requirements</a>.</p>
<b>Microsoft CA key provider</b>	<p>This option determines if user certificates issued by a Microsoft Certificate Authority (CA) can be used to encrypt devices.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Users must enter passwords to encrypt devices and cannot associate AD users with the device.</li> <li>• <b>Enabled (Decentralized):</b> Users may add "Windows Users" to devices. When an added user connects the device, the certificate unlocks the device automatically.</li> </ul> <hr/> <p> You must have a Microsoft Certificate Authority in your environment to use this option.</p> <hr/>

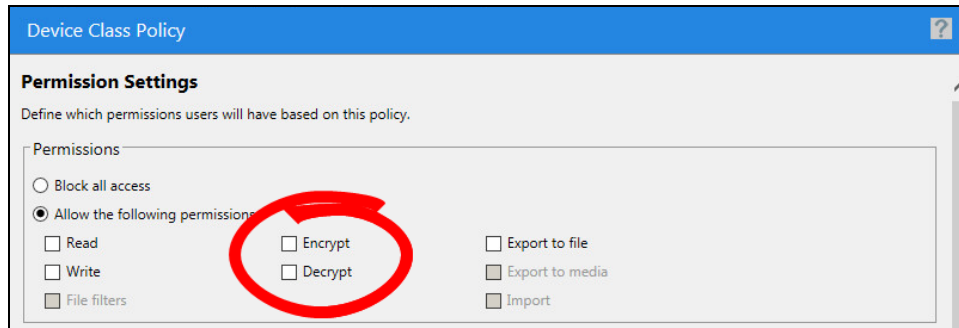
Option	Description
<b>Unencrypted device connected prompt</b>	<p>This option allows you to enter text that displays to end users if:</p> <ul style="list-style-type: none"> <li>• They connect an unencrypted device to the endpoint.</li> <li>• Their permissions allow them (but does not force them) to encrypt the device.</li> </ul> <p>Use this option to remind users who are copying files to a device that they have an encryption option available.</p> <p>For example, you can enter a message of: "Do you wish to encrypt your device now?"</p>
<b>Automatically clear unused space</b>	<ul style="list-style-type: none"> <li>• <b>True:</b> During the device encryption process, the user is forced to encrypt unused space. This option is more secure, but the encryption process takes longer.</li> <li>• <b>False:</b> During the device encryption process, the user is prompted whether they want to encrypt unused space.</li> </ul>
<b>Retain data when encrypting device</b>	<p>During the device encryption process, you can configure Device Control to:</p> <ul style="list-style-type: none"> <li>• Retain all data currently on the device and encrypt that data. Choose this option if users assume their data should be retained.</li> <li>• Erase all data currently on the device and encrypt the empty device. Choose this option if you're concerned malware exists on devices connecting to your organizational endpoints.</li> <li>• Prompt the user to choose from one of the previously mentioned options.</li> </ul>

## Encryption Scenarios

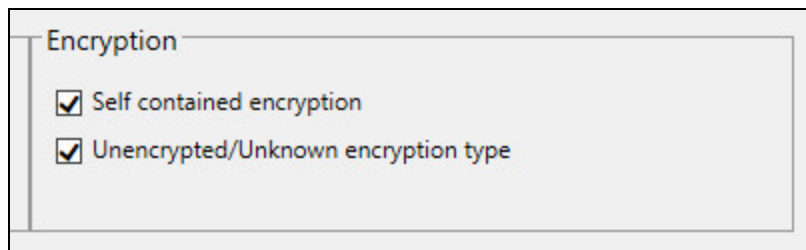
When adding encryption permissions to Device Control policies, most organizations typically divide their users into three different categories:

- **Users not approved to encrypt devices**

This category is the simplest group to address. When configuring your Device Control policies for these users, leave the Encrypt and Decrypt permission options unchecked, as depicted in the following image.

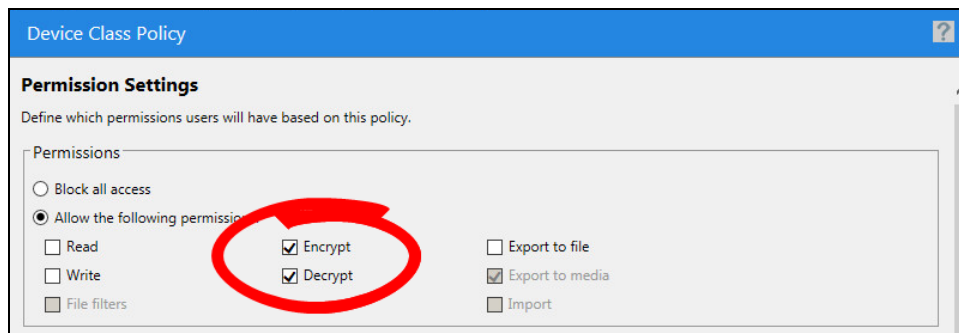


Users in this encryption category can still *access* encrypted devices, depending on the options you select when creating a policy.



- **Users permitted to encrypt devices**

This group is assigned permissions to encrypt devices, but the users assigned the policy are not forced to encryption; they have the *option* to encrypt.



- **Users required to encrypt devices**

In this case, you configure two policies: One policy for unencrypted devices, and another for encrypted devices. For more information on how to configure each policy, see [Knowledge Article 23327](#).

### Accessing Encrypted Devices

You have two options for managing how users can access encrypted devices.



- **Password based access:**

A password is chosen by the end user when the device is encrypted. The encryption key is placed on the device outside of the encryption container, and is itself encrypted with the password. To allow users to encrypt a device that is accessible with a password, they need the **Encrypt** and **Export** to media permissions in a policy that applies to them.

- **Certificate based access:**

If you have a Microsoft Certificate Authority (CA) in your organization, and you provide certificates to users that are valid for encryption, there is a second option for device access. Users can choose Windows Users who are allowed access to the device after encryption. They can add a number of users from AD, all of which will have access to the device when on a device-controlled endpoint. When the device is connected to an endpoint, Device Control compares the logged in user's encryption certificate to those added to the device. If the user is listed on the device, the device will be unlocked using the certificate. No password is required. The device cannot be unlocked in this manner on un-managed machines, or machines outside of your organization since the certificate is needed. To provide this capability, you must have a Microsoft CA in your environment, and you must set the Microsoft CA key provider option on the **Tools > Options** to **Enabled (Decentralized)**.

## FAQ

### **How do we disable the use of all USB ports?**

Universally blocking access to your USB ports usually isn't productive. A better practice is to manage devices connecting to the ports rather than the ports themselves.

However, if you still want to block access to specific ports, such as USB ports, create a Port Control policy from **Manage > Device Control Policies**. Select the **Permission** settings on the first page of the wizard. On the second page select **Block all access**, and select the desired port. On the last page of the wizard, assign the policy to **Everyone** from the **Users** panel. All access to that port, regardless of device, is blocked.

### **How do we allow our users to encrypt devices when needed?**

Refer to the "Policy Permission Settings: What Permissions to Give Users on What Devices" on page 36 section in this document for details on configuring a policy this way.

### **How do we force any data written to USB flash drives to be encrypted (users can read any USB flash drive)?**

Refer to the "Policy Permission Settings: What Permissions to Give Users on What Devices" on page 36 section in this document for details on configuring a policy this way.

### **People need to use data from our organization off site. How do I allow this practice while keeping the data safe?**

Allow for password-based access to encrypted devices. See the section "Policy Permission Settings: What Permissions to Give Users on What Devices" on page 36 for details on the settings required to allow this.

### **I need to know what users are copying to devices. How do I accomplish this?**

Use the Shadowing feature. See "File Shadowing" on page 69 for more information.

### **I need a secure solution that can't be bypassed easily. Can users with Administrative rights bypass Device Control?**

No, they can't. The Endpoint Security Agent cannot be disabled, even by users with administrative rights. The enforcement kernel driver loads before the users logs on, so protection is enabled for the entire user session.

### **I only want my employees to use company issued (or approved) devices (makes and models).**

Use Device Collections to allow the device models you want to allow. No policy or effort is required to block all other devices.

### **What considerations should I make when creating different policies for laptops, workstations, and servers?**

Consider what devices are appropriate on each of those endpoint types.

For example, Wi-Fi adapters should be allowed on laptops, but should probably be blocked on workstations and servers. Another example is tape drives—allow this device for servers, but not laptops and workstations.

Also, refer to the following sections in this document:

- "DC Install SK-NDIS Driver" on page 13
- "DC Detection Interval & DC Device Event Upload Interval" on page 13.

**How do I limit use of specific devices to specific people?**

Assign these permissions by using Device Collections. Place the permitted devices in a Device Collection, and then create a policy for that collection that is assigned to the appropriate user groups or users.

**How do I stop permission changes from displaying on user endpoints?**

These notifications can be suppressed with the Agent permission change notifications setting on the **Tools > Options**.

**I don't want to allow rogue / unmanaged devices (such as keyloggers, Wi-Fi adapters, etc.) that are prohibited in my organization. How do I account for all possibilities?**

Because Device Control denies devices by default, you need only manage the devices that you want to allow. Any other device that connects to your endpoints is denied access.

**I want to monitor use now, and then decide if we want to enforce policies later. Is that possible?**

Yes. Device Control includes an **Audit** mode, in which the system logs device activity on endpoints without enforcing any policy.

**How do I block a specific device, now!**

The device is blocked by default unless it falls within the scope of an existing policy. In that case, you can disable the policy, or search for the device in the **Device Library**, add it to a new Collection, and create a Collection Policy that specifically blocks access to that device. This explicit blocking of access takes priority over any other policies.

**We only allow specific media on these machines. How can I limit the DVDs that people can use?**

Optical media can be added to Media Collections in the same way devices can be added to device collections. You then create a Media Collection policy that allows access only to those discs.

**I want to manage my permissions with AD instead of in your console. Is that possible?**

Yes, after initial configuration of the policies, many customers manage user's permission levels through the use of AD groups. See "Synchronize With Active Directory" on page 20 for a more detailed description.

**I want to be able to define groups of machines and manage them that way. Does Device Control allow that?**

Yes, the Endpoint Security Console has flexible endpoint group creation and management. You should create groups and apply Agent Policy Sets to control reboot behavior and the installation of the NDIS driver. Servers, laptops, desktops, and unattended machines have different needs and can be handled differently.

## Policy Planning Worksheet

While planning your policies, use this worksheet to record the permissions, policy enforcement, and assignment values that you want to set for each device class policy. When you begin creating your policies, have this completed worksheet on hand so you can quickly refer to it so you can complete each policy quickly.

Device Class	Permissions <sup>1</sup>	When is the Policy Enforced? <sup>2</sup>	To Whom/What is the Policy Assigned? <sup>3</sup>
<b>Biometric Sensors</b>			Everyone / LocalSystem <sup>4</sup>
<b>Citrix Network Shares</b>			
<b>COM/Serial Ports</b>			
<b>CD/DVD Drives</b>			
<b>Floppy Disk Drives</b>			
<b>Imaging Devices</b>			
<b>LPT/Parallel Ports</b>			
<b>Modem/Secondary NICs</b>			
<b>Palm Devices</b>			
<b>Windows Portable Devices</b>			
<b>USB Printers</b>			
<b>PS/2 Ports</b>			Everyone / LocalSystem <sup>4</sup>
<b>Removable Storage Devices</b>			

Device Class	Permissions <sup>1</sup>	When is the Policy Enforced? <sup>2</sup>	To Whom/What is the Policy Assigned? <sup>3</sup>
<b>RIM Blackberry Devices</b>			
<b>Smart Card Readers</b>			Everyone / LocalSystem <sup>4</sup>
<b>Tape Drives</b>			
<b>User Defined Devices</b>			
<b>Windows CE Devices</b>			
<b>Wireless NIC</b>			Everyone / LocalSystem <sup>4</sup>

1. All possible permission values are listed in "Supported Permission Types" on page 81.
2. All possible policy enforcement values are listed in "Policy Enforcement: When and Where to Enforce Policies" on page 34.
3. All possible policy assignment values are listed in "Policy Assignment: Who (Or What) to Assign the Policy to" on page 37.
4. This device class must be assigned to one of these user accounts because the system accesses the device prior to user login.

