



Device Control 8.6

User Guide



Endpoint Security

powered by HEAT

Notices

Version Information

Ivanti Endpoint Security: Device Control User Guide - Ivanti Endpoint Security: Device Control Version 8.6 -

Published: Dec 2020

Document Number: 02_219_8.6_171281100

Copyright Information

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

For the most current product information, please visit www.ivanti.com.

Copyright© 2020, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <https://www.ivanti.com/patents>.

Table of Contents

Chapter 1: Ivanti Device Control Overview.....	9
Major Features of Ivanti Device Control.....	9
Supported Device Types in Ivanti Device Control.....	11
Chapter 2: Device Control Encryption Methodology.....	15
Encrypting Removable Storage Devices.....	15
Easy Exchange Encryption.....	15
Encrypting Media.....	16
Decentralized Encryption.....	16
Chapter 3: Getting Started with Device Control.....	19
Device Control at a glance.....	19
The Ivanti Device Control Workflow.....	20
Step 1: Install the Device Control Module Server Component.....	21
Step 2: Add the Device Control Module to Endpoints.....	22
Step 3: Create a Device Event Log Query.....	23
Step 4: Create Device and Media Collections.....	26
Step 5: Add Devices and Media to Collections.....	27
Step 6: Create Device Control Policies.....	29
Step 7: Edit a Policy.....	49
Step 8: Generate Ivanti Device Control Reports.....	51
Chapter 4: Using the Ivanti Endpoint Security Console.....	53
Common Functions.....	53
Common Conventions.....	54
The Navigation Menu.....	55
The Page Banner.....	62
List Pages.....	62
Toolbars.....	63
The Options Menu.....	63
Filters.....	64
Group By.....	68
Expanding and Collapsing Structures.....	69
Advancing Through Pages.....	70
Help.....	70
Exporting Data.....	71
The Home Page.....	71
The Dashboard.....	72
Dashboard Setting and Behavior Icons.....	90
Previewing and Printing the Dashboard.....	91
Editing the Dashboard.....	91
The System Alert Pane.....	92
License Expiration.....	94

Chapter 5: Managing Devices with the Device Library.....	97
Granting Access to the Device Library.....	97
The Device Library Page.....	100
The Device Browser.....	100
The Device Library Page Toolbar.....	102
The Device Library Page List.....	103
Working with the Device Library.....	104
Creating a Device Collection.....	104
Creating a Media Collection.....	105
Adding a Device to a Collection.....	105
Adding a Network Printer to a Collection.....	107
Adding a Device Model to a Collection.....	108
Adding Media to a Collection.....	109
Editing a Collection.....	110
Moving Items Between Collections.....	111
Removing an Item From a Collection.....	111
Renaming a Collection.....	112
Deleting a Collection.....	112
Exporting a Collection.....	113
Chapter 6: Using Device Control Policies.....	115
Granting Access to the Device Control Policies Module.....	116
The Device Control Policies Page.....	119
The Policies Page Toolbar.....	119
The Policies Page List.....	120
Viewing the Device Control Policies Page.....	121
Policy Permissions.....	122
Permission Settings for a Policy.....	122
Priority Options when Defining Permissions.....	124
File Type Filtering.....	125
File Type Filtering Permissions.....	126
Available File Type Filters.....	127
File Shadowing.....	129
Supported Device Classes for File Shadowing.....	130
Supported Formats when Shadowing.....	130
Printed Content Shadowing.....	131
Viewing a shadowed print file.....	132
Working with Device Control Policies.....	133
The Global Device Policies Page.....	134
Setting Global Device Policy.....	135
Creating a Device Class Policy.....	139
Creating a Device Collection Policy.....	149
Creating a Media Collection Policy.....	157
Creating a Port Control Policy.....	160
Assigning a Policy.....	163
Assigning a Device Control Policy on an Endpoint.....	164
Unassigning a Single Policy.....	164
Unassigning Multiple Policies.....	165
Editing a Policy.....	166
Enabling Policies.....	167

Disabling Policies.....	167
Deleting a Policy.....	168
Exporting Policies.....	169
Creating Policies for a Group.....	169
Creating Policies for Users.....	170
Chapter 7: Using Device Event Logs.....	171
Granting Access to Device Event Logs.....	171
The Device Event Log Queries Page.....	174
The Device Event Logs Page Toolbar.....	174
The Device Event Log Queries Page List.....	175
Working with Device Event Log Queries.....	175
Viewing Device Event Logs.....	176
Creating a Device Event Log Query.....	176
Editing a Device Event Log Query.....	178
Copying a Scheduled Device Event Log Query.....	181
Rerunning a Completed Device Event Log Query.....	182
Viewing the Result of a Device Event Log Query.....	182
Deleting a Device Event Log Query.....	185
Exporting Device Event Log Queries.....	185
Adding a Device to the Device Library from the Query Results Page.....	186
Chapter 8: Using the Tools Module.....	187
Granting Access to Device Control Tools.....	187
The Ivanti Device Control Options Page.....	189
Working with Ivanti Device Control Tools and Options.....	193
Viewing Ivanti Device Control Options.....	193
Configuring Ivanti Device Control Options.....	194
Temporary Access Permissions.....	194
Crypto Password Recovery.....	199
Chapter 9: Using the Reports Module.....	209
Generating Ivanti Device Control Reports.....	209
Available Ivanti Device Control Reports.....	210
Device and Media Collections Report.....	210
Device Control Options Report.....	212
Device Permissions Report.....	214
Endpoint Permissions Report.....	216
User Permissions Report.....	218
Chapter 10: Managing Individual Users.....	221
The Directory Sync Schedule Page.....	222
About Active Directory Synchronization.....	223
Viewing the Directory Sync Schedule Page.....	223
The Directory Sync Schedule Page Toolbar.....	224
The Directory Sync Schedule Page List.....	224
Working with Active Directory Synchronizations.....	225
Creating Directory Syncs.....	226
Editing Directory Syncs.....	228
Deleting Directory Syncs.....	230
Syncing Directories Immediately.....	231
Disabling Directory Syncs.....	231

Enabling Disabled Directory Syncs.....	231
Exporting Directory Sync Information.....	232
The Users Page.....	232
The User Browser Directory Tree.....	232
The Users Page Toolbar.....	233
The Users Page List.....	238
Working with Network Users.....	244
Adding an Individual User to a Policy.....	244
Removing an Individual User from the User Browser.....	245
Unassigning Policies from Users.....	246
Exporting User Data.....	246
Chapter 11: Using the Device Control Client.....	247
Device Control Client Menu.....	247
About Encrypting Devices.....	247
Encrypting CD/DVDs for Multiple Users.....	248
Managing Device Passwords.....	253
Manage Device.....	254
Unlocking Media.....	255
Opening Portable Media.....	256
Decrypting Media.....	256
Using the Encrypt Medium Utility.....	257
Portable Device Encryption Permission.....	259
Nonportable Device Encryption Permission.....	265
Portable and Nonportable Device Encryption Permission.....	272
My Computer Page.....	277
Select Access Method Page.....	278
User Access to Device Page.....	279
Add User Page.....	280
User List Page.....	281
Data Integrity Page.....	282
Secure Unused Space Page.....	283
Start Encryption Page.....	284
Transferring Encryption Keys.....	284
Export an Encryption Key.....	284
Import Encryption Key.....	286

Chapter 1

Ivanti Device Control Overview

In this chapter:

- Major Features of Ivanti Device Control
- Supported Device Types in Ivanti Device Control

Ivanti Device Control is a module for the Ivanti Endpoint Security that enables you to control end user access to devices in your network.

By limiting user access to devices, Device Control helps minimize the risks associated with the theft of company data and other intellectual property. Device Control also assists in preventing the abuse of network resources.

Using Device Control results in increased productivity through the prevention of unauthorized user access to devices. Thereby, you can avoid unnecessary costs incurred to remove unlicensed software and defend against malicious code introduced by unsecured devices in a network.

Major Features of Ivanti Device Control

Ivanti Device Control allows administrators to set access rights for various device types. Permissions can be temporary, permanent, or applicable only at designated times.

Here are some of the features offered:

Manage device access from a central location	The primary function of Device Control is to allow centralized management of access to devices and device types between users, endpoints, user groups, and endpoint groups.
Various device types supported	Device Control supports a wide variety of device types, in addition to supporting device types, such as FireWire, USB, SCSI, ATA/IDE, and Bluetooth, PCMCIA (Cardbus) and IrDA buses. For a complete list of supported device types, see Supported Device Types in Ivanti Device Control on page 11.
Easy-to-use interface	An Access Control List is responsible for helping with the management of device permissions. With the Access Control List, you can control access to devices at various levels: user groups, endpoint groups, device classes, device collections, or individual devices.

Define devices as read-only	With Device Control, it is possible to deny write permissions for specific devices or device types. These include CD/DVD writers, floppy drives, USB drives, and so on. You may also restrict other permissions such as encrypting, writing, decrypting, importing data, and exporting data to devices.
Define copy limits	You can prevent users from misusing their writing permissions by limiting the amount of data that can be written to external storage devices.
Grant temporary access	Certain situations call for giving a user, endpoint, or a group access to a device for a limited period. Device Control allows you to grant temporary access. You can grant temporary access for a predetermined time frame and the access is automatically terminated when the specified time expires.
Schedule permissions	With Device Control, you can create policies that allow or prevent access to a device during a certain period. For example, you can permit access to DVD drives from 9 A.M. to 5 P.M, Monday to Friday.
Create context-sensitive permissions	Device Control supports the creation of sophisticated policies that are applicable to specific devices based on their context or connection status. This allows you to create permissions for devices that differ based on the device's network connection status. For example, laptop Wi-Fi cards may be disabled when company laptops are connected to the organization's network and they may be enabled once disconnected from the network.
Enable file shadowing	Device Control incorporates shadow technology that allows administrators to enable copying of data to or from removable media such as CD/DVD, floppy disks, storage devices, and PCMCIA drives. Copies of data written to parallel and serial ports can also be obtained. For devices that support partial shadowing, only the file name is copied. Shadowing can be enabled on a per-group basis.
Manage user-defined devices	In addition to default device classes, Device Control allows you to manage those devices not defined in the default installation. These devices may be added as user-defined devices. Their permissions are applied in the same way as those for default devices.
Create permissions on a per-device basis	Controlling access to sensitive data is sometimes not possible by controlling access to an entire device type. It may require controlling access to a particular device model or even individual devices of a model. For example, you may grant access to only a few devices of a company-approved model and restrict access to devices of the same class that contain sensitive data.

Control access to serially-identified removable devices	Besides granting permissions for devices belonging to a particular class, and devices of a specific model, Device Control allows you to grant permissions for unique devices, based on their serial numbers.
Encrypt individual devices	Unauthorized users and systems can be prevented from accessing sensitive data on removable devices while still using the device. Device Control allows specific data on a device to be encrypted and access to it restricted to authorized persons.
Filter file types for copying	Device Control enables you to determine copying permission granted to and from removable devices for each file type.
Log device actions	Device Control has a device logging feature that you can enable if you want to keep track of specific actions performed on devices. For example, you can choose to log whenever a device is connected to an endpoint.
Maintain a library of devices in your network	The Device Library in Device Control gives you a centralized location from where you can add and control various network devices. You can also create device groups and define access permissions in this module.

Supported Device Types in Ivanti Device Control

Ivanti Device Control (Device Control) supports defining access permissions for most standard device types such as removable storage devices, and biometric devices. You can also grant permissions at device type level and restrict them to a particular bus type, such as FireWire, USB, ATA/IDE, PCMCIA, Bluetooth, SCSI, and IrDA buses.

Actual creation of permissions depends on the type of device and not the mode of connection. For example, a DVD-ROM drive connected to a PC through its USB port is controlled by the same settings and mechanism as the computer's internal DVD-ROM drive. Device Control can also recognize Plug and Play devices and subject them to the same access permissions as those granted fixed devices of the same type.

Note: For Plug and Play devices in Windows operating systems, Device Control applies permissions based on the device class to which Windows registers the device. For example, if Windows registers a camera under the Removable Storage Devices class, access is granted based on the permissions applied for the remote storage device class.

Device Control manages most of the commonly used device types, including:

Table 1: Supported Device Types

Device Type	Description
Biometric devices	This device type includes fingerprint readers and password managers. Connection to the computer is via the USB port.

Device Type	Description
COM/serial ports	<p>This category includes serial ports and devices using COM device drivers, such as terminal adaptors and certain modem types. PDA cradles that are connected through a USB port may also use the serial port.</p> <p>Note: Some devices will work only if access permission to the COM port is enabled. For example, a Bluetooth printer configured to use a COM port provided by a Bluetooth adaptor will require access to be enabled for both the adaptor and the COM port.</p>
CD/DVD drives	Device Control allows varied access management for CD/DVD-ROM drives. You can lock or unlock drives completely, or allow access only to drives that are authorized by the company.
Floppy Disk Drives	Access to floppy disk drives can be managed as read-only or completely unlocked/locked. These include regular diskette drives and high-capacity drives like the LS-120.
Imaging Devices	<p>Scanners and webcams are examples of SCSI or USB devices used for imaging purposes. Device Control can manage access to these device types.</p> <p>Note: For all-in-one models that comprise a scanner, a printer, and a memory card reader, there are situations where access to the scanner functionality is denied if Device Control disables the Printer functionality.</p>
LPT/Parallel Ports	Device Control allows access management for dongles, parallel printer ports, and variants like ECB.
Modems/Secondary Network Access Devices	<p>Network devices that are not connected directly using normal channels are referred to as secondary network access devices. Device Control enables access to these internal or external devices.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Modems belonging to different brands operate differently. Based on the brand, you may need to permit access to the modem port, COM port, or both. Determine the best option for you by experimenting with the settings. 2. Users who connect through dialup will require a permission rule to be set up for the modem's Local System account. 3. The Secondary network access devices/modems type also includes FireWire (IEEE 1394) net adapters. New permissions are applied following a reboot.
Palm Handheld Devices	Use Device Control to control access to this type of device.
Portable Devices	This type includes removable media like digital cameras, MP3 players, portable storage devices, mobile phones, and so forth.

Device Type	Description
Printers	<p>You can permit or deny access to all print devices with drivers that use the Windows Print Spooler service.</p> <p>Note: For all-in-one models that comprise a scanner, a printer, and a memory card reader, there are situations where access to the scanner functionality is denied if the Printer functionality is disabled.</p>
PS/2 Ports	Traditional keyboards are connected to the computer through PS/2 ports but nowadays most keyboards rely on USB connections. Blocking all PS/2 ports is an option for an organization that uses only USB mice and USB keyboards. It reduces the risk of attack by PS/2 keyloggers (hardware devices that record keyboard movements and capture typed data, including passwords).
Removable Storage Devices	<p>Removable storage devices are all those devices that are not categorized as floppy or CD/DVD-ROM drive-based devices. Device Control allows access management for this device type, which includes PCMCIA hard drives and USB memory devices such as MP3 players, digital cameras, memory sticks, and so forth.</p> <p>Note: Removable storage devices also include secondary hard disk drives. If you specify whether a policy is intended for a hard drive or non hard drive, it allows you to choose between secondary hard disk drives and memory keys. In addition, you can restrict access through connection modes like SCSI, PCMCIA, or USB.</p>
RIM Blackberry Handhelds	RIM (Research in Motion) Blackberry devices are mobile phones or handheld computers that are usually connected to a computer through the USB port. With Device Control, you can manage access to these GSM or PDA devices.
Smart Card Readers	Device Control allows access permissions for fingerprint readers and smart card readers, such as eToken.
Tape Drives	<p>You can manage access to internal and external tape drives of any capacity with Device Control.</p> <p>Note: Device Control cannot control certain backup units that do not use Microsoft-supplied drivers.</p>
User-defined Devices	Some devices, such as web cams, OTEC, HTC, and PDAs (non-Compaq IPAQ USB, non-Palm handheld USB) do not fit into conventional device categories. Device Control allows you to manage access to them by labeling them as user-defined devices.
Windows CE Handheld Devices	Handheld Windows CE devices such as HP iPAQ or XDA (running Windows Pocket PC 2002/2003 OS) connect to the computer through a USB port. Access to these devices can be managed with Device Control.

Device Type	Description
Wireless Network Interface Cards	During installation of the Device Control agent, you can decide if you want to allow access to a wireless LAN adaptor.
	Note: Wireless card access is permitted only for those cards that do not require administrator installation privileges or a manufacturer-specific driver.

Chapter 2

Device Control Encryption Methodology

In this chapter:

- Encrypting Removable Storage Devices

Device Control uses a combination of encryption algorithms to protect data communications between the product components and to protect data transferred to removable storage devices and CD/DVD media. Encryption methods are combined with user access control to enforce device permission usage policies.

Encrypting Removable Storage Devices

Device Control creates encrypted files in virtual memory, and then writes the files to physical media available in various formats, such as removable storage devices and CD/DVDs. Decentralized encryption enables users to encrypt removable media using the client.

Device Control supports decentralized encryption methods from the client for ciphering data copied to removable storage media and CD/DVD media. *Easy Exchange* encryption encrypts devices for portable use, which means that a user can use the encrypted device with a password and the encryption key without having to connect to the network through a computer running the client.

Tip: Ensure auto-enrollment is enabled in the Microsoft Management Console (MMC), otherwise the domain administrator will need to approve each enrollment request before a certificate can be retrieved and installed.

Important: Only default user certificate templates are supported.

Easy Exchange Encryption

Easy Exchange encryption is volume-based. The entire volume of the removable storage media is used for ciphering existing data and all sectors on the volume and installing the Secure Volume Browser (SVolBro.exe) deciphering program.

Devices encrypted using the *Easy Exchange* method do not require a password or encryption key when attached to a computer running the client. These encrypted devices are deciphered when users attach the device to a computer running the client, and there is a Microsoft® Certificate Authority (CA) available from the network for authentication.

Important: When there is no Microsoft Enterprise CA installed in the network, users can only access encrypted data using a password and a public encryption key.

When a user is working outside your network, they must use the installed Secure Volume Browser to access encrypted data. The Secure Volume Browser does not require local administrative rights, however a password and a public encryption key are required. The Secure Volume Browser program is automatically copied on to the media when it is encrypted.

The administrator also has an option during encryption to export the public key to the media or to an external file, depending on enterprise network security policies and procedures.

Important: If the encryption key is not exported to the encrypted media, then an administrator must send the key in a separate file to the user before the decryption process can start.

The *Easy Exchange* encryption method is used for decentralized encryption because this method uses the Secure Volume Browser to unlock a medium for user access.

Encrypting Media

Encrypting media from the client is performed using the **Encrypt Medium** utility. The rules governing the behavior of the encryption options depend upon the **Export** permissions assigned by the administrator for user access.

Standard User Options Rules

The default behavior for the **Encrypt Medium** utility options are governed by the following rules:

For the list of users granted access:

- When a user does not have valid certificate, the user name is displayed in red and disabled.
- When a user is added, the domain and account name are displayed to distinguish between users having similar names in different contexts.
- The user can add any number of **Passphrase users**.
- The user can add any number of **Windows users**.

Encryption options for **Easy Exchange** are:

- Enabled when the device size is less than 128GB.

Decentralized Encryption

Decentralized encryption enables a user to perform device encryption at a computer workstation without requiring network administrator rights. The user is forced to cipher and administer their removable storage devices, based on user access and device permissions established centrally by the network administrator.

Decentralized encryption is defined by an administrator using a central rule that establishes which users have access to removable storage devices, whether a user is forced to encrypt their removable storage devices, and whether they are allowed to access unencrypted devices. Depending upon the rule, a user may be able to:

- Read and/or write data to a removable storage device.
- Encrypt a device.
- Format a device.

Users encrypt their devices using the Easy Exchange method, where all existing data is erased and the remaining storage volume is encrypted. Removable storage devices encrypted using decentralized encryption can also be used outside the enterprise network, when necessary.

When a user has the necessary permissions formats or modifies an encrypted removable storage device, the Security Identification (SID) changes. The new SID is not recognized by the server because there is no matching record in the database. Therefore, access to the new device is restricted. This ensures that no data, encrypted or not, can leave the enterprise network using unauthorized removable storage devices. As an additional security measure when a removable storage device is used outside the network, an administrator can choose to export the public key to an external file that can be sent separately to the user, instead of storing the public key on the removable storage device.

Encryption from the client provides several options:

- Passphrase users can use encrypted media with an encryption key stored on the device at the time of encryption.
- Passphrase users can use encrypted media with an encryption key accessed from a file that is stored separately from the media at the time of encryption.
- Windows Active Directory users can use encrypted media with an encryption key protected by a Certificate Authority.

Chapter

3

Getting Started with Device Control

In this chapter:

- Device Control at a glance
- The Ivanti Device Control Workflow

Learn the initial tasks you need to perform to start enforcing usage policies for removable devices, removable media, and data in your environment to limit data leakage and its impact.

You will continue to perform these tasks, plus many others. Ivanti Endpoint Security contains many features and functions, and by learning the environment, you can secure your network quickly and efficiently.

Important: Before you roll out Device Control to endpoints in an environment, it is recommended that you work with your end users and other stakeholders, together with any IT security personnel, to start formulating a business policy regarding the usage of peripheral devices. Having a clear idea of what is to be achieved from the start will help shape the future steps you take with this product.

Device Control at a glance

Learn the basic concepts, functions, and terminology you require to be proficient in the use of Ivanti Device Control.

Benefits

- Protect valuable organization and customer data from loss or theft via removable devices/media.
- Require end users to encrypt data being copied to removable devices / media in compliance with policy and regulation.
- Monitor all files being transferred onto / off your network by file metadata or the patented bi-directional full file shadowing capability.
- Add another layer to your defense-in-depth strategy to protect against USB-borne malware introduction / propagation.

Key terms

device class	A group of physical devices or device drivers that have similar characteristics and that can be managed in a similar manner.
device collection	A group of target devices that can be managed in a similar manner.
file shadowing	A feature that tracks the data read, written to, or written from a device. Depending on the configuration, either copies of the files are created or only filenames are recorded.
portable encryption	The encoding of data on a portable device or media into a form in which meaning cannot be assigned without the use of a confidential process or key.

The Ivanti Device Control Workflow

Learn the sequence of specific tasks you need to perform to implement your first device control policy.

Important: While Ivanti Device Control has been designed to minimize the administrative burden of device control, it is important to invest adequate time during its deployment to ensure a successful implementation. Work with your end users and their representatives, together with any IT security personnel, to formulate a business policy regarding the usage of peripheral devices.

Install the Device Control module server component. This component is installed after the initial Ivanti Endpoint Security installation.

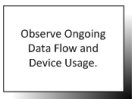


Note: If you purchased an Device Control license during your initial Ivanti Endpoint Security purchase, Device Control is installed during the initial Ivanti Endpoint Security installation by default.

For more information, see [Step 1: Install the Device Control Module Server Component](#) on page 21.



Add the Device Control module endpoint component to agents you want to support Device Control functions. Each agent you add the endpoint component to consumes an Device Control license. For more information, see [Step 2: Add the Device Control Module to Endpoints](#) on page 22.



Observe ongoing data flow and device usage. By default, the module runs in an "Audit Mode" which enables endpoint users to operate devices but records device connections and other events related to those devices. Discuss valid device uses with key end user representatives. For more information, see [Step 3: Create a Device Event Log Query](#) on page 23.



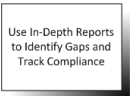
Organize the various devices and media in your network into collections to make them more manageable. For more information, see [Step 4: Create Device and Media Collections](#) on page 26 and [Step 5: Add Devices and Media to Collections](#) on page 27.



Define device usage and data flow policies. Assign permissions to users, endpoints, and groups to use only the types you allow. For more information, see [Step 6: Create Device Control Policies](#) on page 29.



Maintain your Device Control policies by actively monitoring device events in your network and updating policies for device classes and collections accordingly. For more information, see [Step 7: Edit a Policy](#) on page 49.



Use in-depth Device Control reports module to identify gaps and track compliance in the areas of Device and Media Collections, Device Control Options, Device Permissions, Endpoint Permissions, and User Permissions. For more information, see [Step 8: Generate Ivanti Device Control Reports](#) on page 51.

Step 1: Install the Device Control Module Server Component

After logging in to Ivanti Endpoint Security, the first step in implementing Device Control features and functions is to install the server module

Prerequisites:

You must be licensed for Ivanti Device Control.

Install the Device Control module server component using the Ivanti Installation Manager.

Tip: For additional information on using Ivanti Installation Manager, refer to [Ivanti Endpoint Security User Guide \(https://help.ivanti.com/\)](https://help.ivanti.com/).

1. Select **Tools > Launch Installation Manager**.

Step Result: Installation Manager opens to the **New/Update Components** tab.

2. Select the **Device Control** check box for your version number of Ivanti Endpoint Security.

3. Click **Install**.

Step Result: The **Install/Update Components** dialog opens.

4. Click **Install**.

Step Result: A dialog opens, notifying you that installing the module may cause logged-in users to lose their work.

5. Click **OK**.

Step Result: The installation begins.

6. Click Finish.

Tip: Select the **Launch Ivanti Endpoint Security** check box to relaunch Ivanti Endpoint Security after clicking **Finish**.

Result: The Device Control module server component is installed. To begin using the module, reopen the Ivanti Endpoint Security.

After Completing This Task:

Continue to [Step 2: Add the Device Control Module to Endpoints](#) on page 22.

Step 2: Add the Device Control Module to Endpoints

After installing the Device Control server module, add the Device Control module to your managed network endpoints.

Prerequisites:

- Complete [Step 1: Install the Device Control Module Server Component](#) on page 21
 - The Ivanti Endpoint Security Agent is installed on target endpoints.
-

1. Select Manage > Endpoints.

Step Result: The **Endpoints** page opens to the **All** tab.

2. From the list, select the endpoints to which you want to add the Device Control module endpoint component to.**3. Click Manage Modules.**

Step Result: The **Add/Remove Modules** dialog opens.

4. Select the Device Control check box for all endpoints you want to install the component on.**5. Click OK.**

Result: The Device Control module endpoint component begins installing, as denoted by the **DCInstalled** column **pending** status. The process is completed when the status changes to **Yes**.

After Completing This Task:

- Reboot target endpoints to complete the installation. For additional information on how to perform the reboot using agent policy sets, refer to the Reboot Behavior Defaults option, described under "Creating an Agent Policy Set" in the [Ivanti Endpoint Security User Guide](https://help.ivanti.com/) (<https://help.ivanti.com/>).
 - Continue to [Step 6: Create Device Control Policies](#) on page 29.
-

Step 3: Create a Device Event Log Query

Schedule a query that records specific device-related actions in your network. This includes queries for granted and blocked actions.

Prerequisites:

Complete [Step 2: Add the Device Control Module to Endpoints](#) on page 22.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.
3. Click **Create**.

Step Result: The **Device Event Log Query** wizard opens.

Figure 1: Device Event Log Query Wizard

4. Type the **Query name**.
5. Select the **Type**.
6. Select the desired scheduling option. You can choose from the following options:

Option	Description
Immediate	The query will run immediately after creation.
Once	The query will run once at a specified time.

Option	Description
Daily	The query will run every day at the selected time.
Weekly	The query will run every week at the selected time.

Depending on the option you choose, additional settings are available in the right-side box.

Note: The start and end dates are the date range for which you want the query results. If you choose **Immediate** or **Once**, specify the start and end dates in the **Date range** fields.

7. [Optional] Select the **Notify me via email when query is complete** check box.
Ensure that you provide a valid email address in the associated field.
8. Click **Next**.

Step Result: The **Select endpoints/users/groups** page opens.

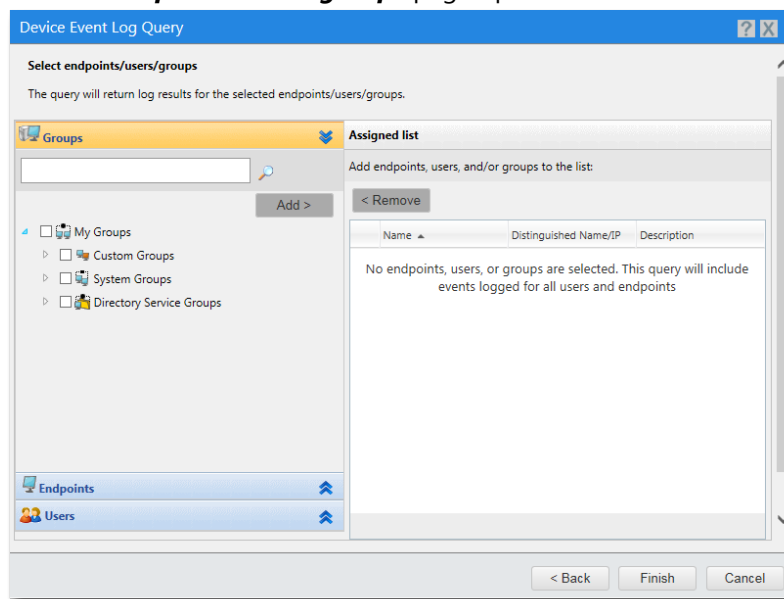


Figure 2: Select Endpoints/Users/Groups

9. Select the groups, endpoints, or users the policy will apply to. Use any of the following methods:

Note: The built-in user groups Administrators, Everyone, Power Users, and Users and Active Directory groups are not supported in log queries and will be removed from the query.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Add.
	Note: Active Directory groups are not supported in log queries.
To add individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Add.
	Note: The Built-in Users and Groups Administrators, Everyone, Power Users, and Users are not supported in log queries.
To remove groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Remove.
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

10. Click **Finish**.

Step Result: The **Device Event Log Query** wizard closes.

Result: A new query is created and runs. When the query completes, its summary is displayed in the **Completed** tab.

After Completing This Task:

Continue to [Step 4: Create Device and Media Collections](#) on page 26.

Step 4: Create Device and Media Collections

Create collections of devices and media through the **Device Library** page.

Prerequisites:

Complete [Step 3: Create a Device Event Log Query](#) on page 23.

Creating a Device Collection

The **Device Library** page allows you to create a collection of devices. Use the right-click menu or **Add Collection Icon** in the **Device Browser** to create the collection for the desired device class.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select a device class in the **Device Browser**.

Step Result: The **Add Collection Icon** becomes active.

3. Click the **Add Collection** icon.

Step Result: A **New Device Collection** entry is added to the device class.

4. Type a name for the device collection.

Result: A device collection is created for the selected device class.

Creating a Media Collection

The **Device Library** page allows you to create a collection of media such as CDs and DVDs. Use the right-click menu or **Add Collection Icon** in the **Device Browser** to create the collection for the desired media type.

Prerequisites:

To add CDs and DVDs to collections, you first need to install the MediaHasher control. This will allow Ivanti Device Control to calculate the unique hash ID of each CD and DVD you are adding.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select a media type in the **Device Browser**.

Step Result: The **Add Collection Icon** becomes active.

3. Click the **Add Collection** icon.

Step Result: A **New Collection** entry is added to the media type.

4. Type a name for the media collection.

Result: A media collection is created for the selected media type.

After Completing This Task:

Continue to [Step 5: Add Devices and Media to Collections](#) on page 27.

Step 5: Add Devices and Media to Collections

Add specific devices and media to collections so they are in manageable groups.

Prerequisites:

Complete [Step 4: Create Device and Media Collections](#) on page 26.

Adding a Device to a Collection

Device collections in the **Device Browser** allow you to organize your devices into manageable groups. Once a collection is created, you can add specific devices to it.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection to which you want to add the device.

- a) Expand the device class.
- b) Click the desired collection.

Step Result: A list of devices already in the collection are displayed in the **Device Control** section.

3. Click **Add**.

Step Result: The **Add Devices** dialog opens.

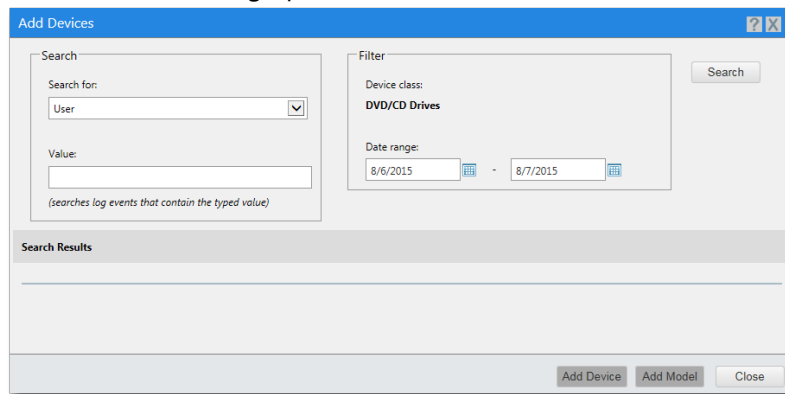


Figure 3: Add Devices Dialog

4. Search for the device you want to add to the collection.

- a) Select a search criteria from the **Search For** drop-down list.

You can select from **User**, **Endpoint IP Address**, **Endpoint Name**, **Device Model**, and **Device Unique Id**.

- b) [Optional] Type a search term in the **Value** field.

- c) [Optional] Select a beginning and end date from the calendar icons in the **Date Range** fields.

- d) Click **Search**.

Step Result: A list of devices corresponding to the search criteria appear in the **Search Results** field.

5. Select the device you want to add to the collection.

6. Click **Add Device**.

Step Result: A pop-up message appears stating all selected items are now in the device collection.

7. Click **OK**.

Step Result: The pop-up message closes.

8. Click **Close**.

Step Result: The **Add Devices** dialog closes.

Result: The selected device appears in the list of devices of the collection. The **Type** column entry for that device is **Instance**.

Adding Media to a Collection

Media collections in the **Device Browser** allow you to organize your media for better control over access rights. Once a collection is created, you can add specific media to it.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection to which you want to add the medium.

- a) Expand the media type.

- b) Click the desired collection.

Step Result: A list of media already in the collection are displayed in the **Device Control** section.

3. Click **Add**.

Step Result: The **Add CD/DVD** dialog opens.

4. Select the medium you want to add to the collection.

- a) Select a drive from the **Drive** drop-down list.

- b) Type a unique name in the **Display name** field.
- c) [Optional] Type any comments in the **Comment** field.

5. Click **OK**.

Step Result: The **Add CD/DVD** dialog closes.

After Completing This Task:

Continue to [Step 6: Create Device Control Policies](#) on page 29.

Step 6: Create Device Control Policies

Use policies to administer control over device classes, device collections, and media collections in your network.

Prerequisites:

Complete [Step 5: Add Devices and Media to Collections](#) on page 27.

Creating a Device Class Policy

Device class policies are policies that apply to an entire device class. You can create a device class policy if you have **Manage Global Device Control Policies** access rights.

Prerequisites:

You must have **Manage Global Device Control Policies** access rights.

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

Step Result: The **Device Control Policies** page opens.

Status	Policy Name	Assigned	Policy Type	Device Class	Device Collection	Last Update (Server)
<input type="checkbox"/>	Default Policy for Biometric Devices	Assigned	Device Class Policy	Biometric Devices	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Citrix Network Shares	Assigned	Device Class Policy	Citrix Network Shares	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for COM/Serial Ports	Assigned	Device Class Policy	COM/Serial Ports	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for DVD/CD Drives	Assigned	Device Class Policy	DVD/CD Drives	Any	10/1/2014 4:34:53 PM
<input type="checkbox"/>	Default Policy for Floppy Disk Drives	Assigned	Device Class Policy	Floppy Disk Drives	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Imaging Devices	Assigned	Device Class Policy	Imaging Devices	Any	12/24/2014 4:06:30 AM
<input type="checkbox"/>	Default Policy for LPT/Parallel Ports	Assigned	Device Class Policy	LPT/Parallel Ports	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Network Access Devices	Assigned	Device Class Policy	Modem / Secondary Network Ac...	Any	7/30/2014 6:17:11 AM

Figure 4: Device Control Policies Page

2. Click **Create > Create class policy**.

Step Result: The ***Device Class Policy*** wizard appears.

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

Figure 5: Device Class Policy Wizard

3. Specify the policy details.

- a) Enter the **Policy name**.
- b) Select the **Override priority**.
You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.
- c) Select the **Device class** to which the policy will apply.

4. Specify the policy rules.

Option	Description
Permission settings (Define read, write and other permissions.)	Enables the <i>Permission Settings</i> panel later in the wizard, where you can define which permissions users will have based on this policy.

Option	Description
Shadow settings (Store a copy of data written to or read from devices.)	<p>Enables the Shadow Settings panel later in the wizard. File shadowing lets you to track the data that is being read, written to, or written from a device. It can be enabled for:</p> <ul style="list-style-type: none"> • COM/Serial Ports • DVD/CD Drives • Floppy Disk Drives • LPT/Parallel Ports • Modem / Secondary Network Access Device • Portable Devices • Printers • Removable Storage Devices <p>For Printers specifically, shadowing involves storing a copy of all information sent to a printer during a print job governed by this policy. This information can later be viewed administratively via log queries by sending the same content to the same printer or another printer of the same model.</p> <p>See File Shadowing on page 129 for more information.</p>
Daily copy limit	<p>Sets the amount of data (in MB) per day that a user can copy.</p> <ul style="list-style-type: none"> • Floppy Disk Drives • Portable Devices • Removable Storage Devices <p>Note: Only one copy limit setting per device class will be enforced. For example, copy limits configured for removable storage devices apply to hard drives and non-hard drives. To avoid ambiguity, it is recommended that you do not combine copy limit policies and permissions policies.</p>

5. Select the desired policy enforcement option.

Option	Description
Always	The policy applies at all times.
Online only	The policy applies only when the endpoint/user/group is connected to the server.
Offline only	The policy applies only when the endpoint/user/group is disconnected from the server.
Scheduled	The policy applies only during a set schedule.

Option	Description
Temporary	The policy allows one-time access for a specified period.

Depending on the option you choose, additional settings are available in the right-side box.

6. Select whether you want the policy to be applicable immediately.

Option	Description
Enable	Activates the policy immediately when you finish configuring it. (default)
Disable	Lets you to delay when the policy takes effect. You can activate the policy later on the Manage > Device Control Policies page by selecting it and clicking Enable .

7. Click **Next**.

Step Result: If you selected **Permission settings** on the **Policy Details** panel, the **Permission Settings** panel displays.

Device Class Policy ?

Permission Settings

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:

Block all access on All connections for hard and non hard drives with self contained encryption,unencrypted/unknown encryption type.

< Back Next > Cancel

Figure 6: Permission Settings

8. [Optional] Specify the permission users will have based on this policy.

Option	Description
Block all access	Restricts the use of all devices of this class to prevent information from getting out.
Allow the following permissions	<p>Select the types of permissions to allow. Available permissions (dependent on the type of device):</p> <ul style="list-style-type: none"> • Read • Write • FireWire • ATA/IDE • SCSI • PCMCIA • Bluetooth • IrDA <p>See Permission Settings for a Policy on page 122 for more information.</p>

9. Select the Connections to which the permissions are to apply.

Dependent on the type of device class policy you are creating, the available connections are:

- All
- USB
- FireWire
- ATA/IDE
- SCSI
- PCMCIA
- Bluetooth
- IrDA

10. If you are creating a Removable Storage Devices device class policy, select the type of Drives to which the permissions are to apply.

Option	Description
Both drive types	Permissions are applied to both hard drives and non-hard drives.
Hard drives only	Permissions are only applied to hard disk drive (HDD) drives.
Non hard drives only	Permissions are only applied to non hard disk drives, for example solid-state drives (SSD).

11.[Optional] If you are creating a Removeable Storage Devices or DVD/CD Drives device class policy, select the type of Encryption to which the permissions are to apply.

Option	Description
Self contained encryption	Encryption is self-contained on the device, allowing only those with an encryption key to access the information.
Unencrypted/Unknown encryption type	Information is either unencrypted or encrypted with an unknown type of encryption.

12.Review the phrase in the **Rule definition** section to ensure you have selected the permissions and connections you want.

13.Click **Next**.

Step Result: If you selected **File Filters** on the *Policy Details* panel, the *File Filters* panel displays.

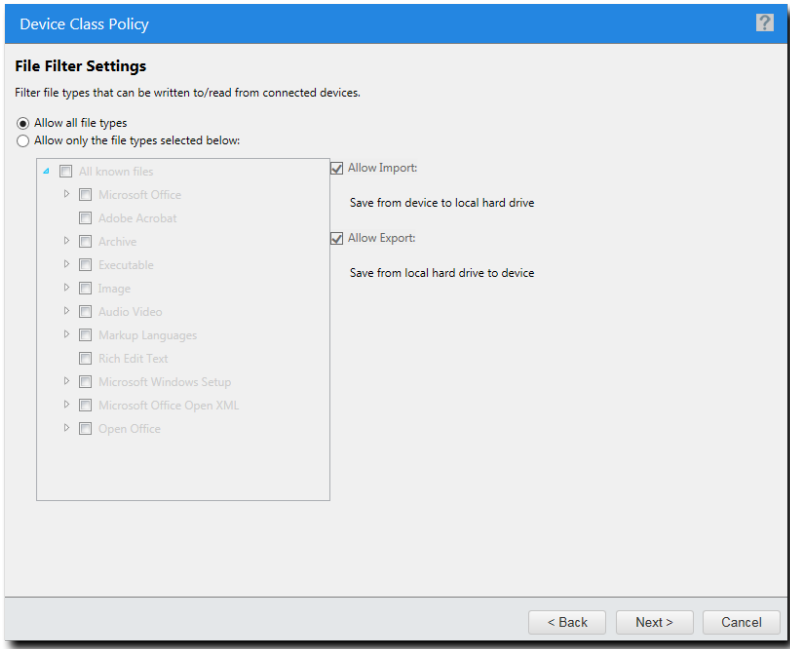


Figure 7: File Filters

14.Specify the file filtering options.

Option	Description
Allow all file types	All files types can be accessed.

Option	Description
Allow only the file types selected below	Only file types you select from a list can be accessed.
Allow Import	User can copy files from the external device to the local hard drive.
Allow Export	User can copy files from the local hard drive to the external device.

For more information on file filters, see [File Type Filtering](#) on page 125.

15.Click **Next**.

Step Result: If you selected **Shadow settings** on the **Policy Details** panel, the **Shadow Settings** panel displays.

16.Specify the shadow settings.

Shadow files are stored in <install_dir>\DeviceControl\Shadow.

Device Class Policy Type	Options	
<ul style="list-style-type: none">• COM/Serial Ports• DVD/CD Drives• Floppy Disk Drives• LPT/Parallel Ports• Modem / Secondary Network Access Device• Portable Devices• Removable Storage Devices	For both the Read and Write sections:	
	Do not shadow	No content is shadowed.
	Full file content	Saves a copy of the entire file.
	File name only	Records only the file name.
Printers	Do not shadow printed content	This setting can be used to prevent shadowing for specific assignment targets. For example, if you shadow printed content for a specific AD Group you can prevent shadowing for a specific user within that group by selecting this setting and assigning the policy to that user.
	Shadow printed content	This setting is used to store a copy of all information sent to a printer during a print job governed by this policy. This information



17. Review the phrase in the **Rule definition** section to ensure you have selected the shadow settings you want.
18. Click **Next**.

Step Result: The **Assign policy** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

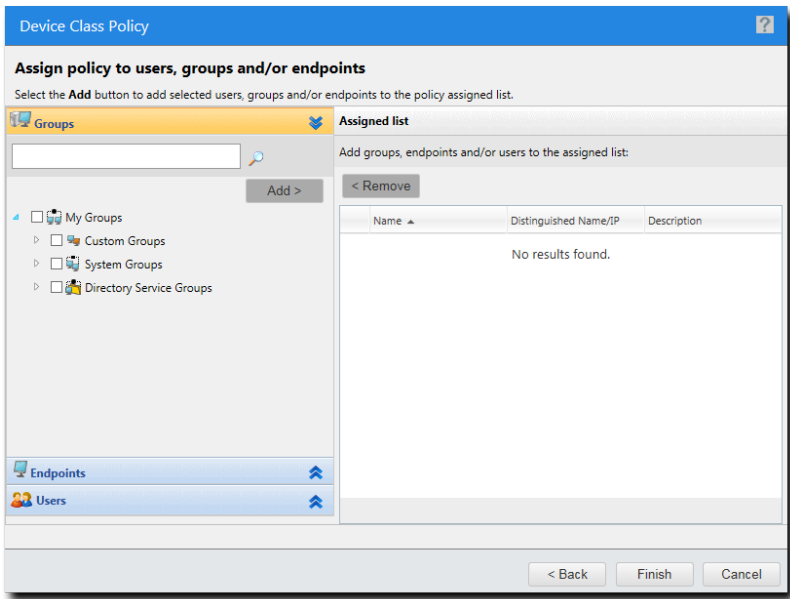


Figure 8: Assign Policy

19. Select the group, endpoint, or user to which the policy applies.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Add.
To add individual endpoints	<ol style="list-style-type: none">1. Select an endpoint or endpoints from the Endpoints list.2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none">1. Select users or usergroups from the Users list.2. Click Add.
To remove groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Remove.

Option	Description
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

20. Click **Finish**.

Step Result: The **Device Class Policy** wizard closes.

Result: A new policy is created for the selected device class. The policy is displayed in the **Device Control Policies** page.

Creating a Device Collection Policy

Device collection policies allow you to define access rights for specific devices rather than an entire device class. Use the **Device Collection Policy** wizard to create policies for device collections.

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

Step Result: The **Device Control Policies** page opens.

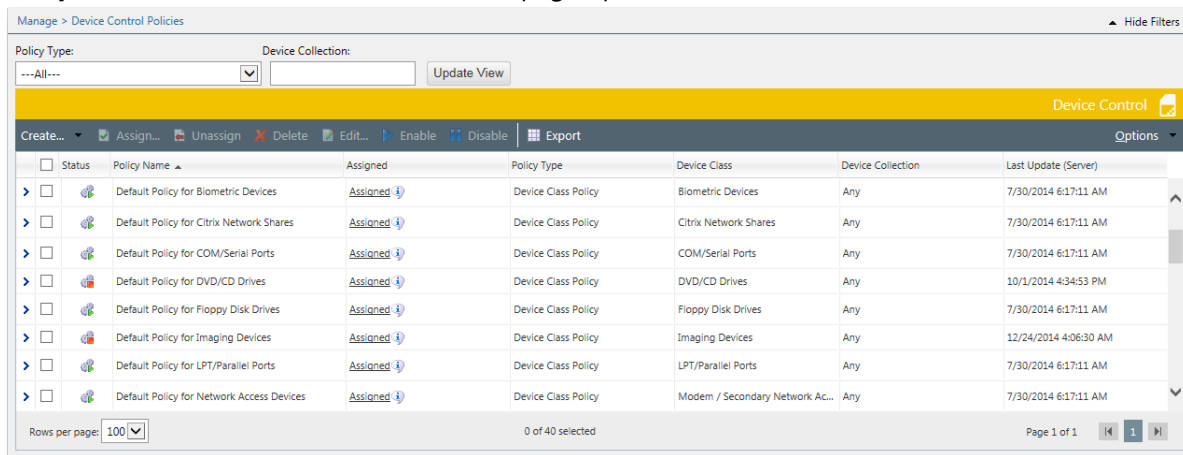


Figure 9: Device Control Policies Page

2. Click **Create > Device collection policy**.

Step Result: The **Device Collection Policy** wizard appears.

Figure 10: Device Collection Policy Wizard

3. Type a name for the policy in the **Policy Name** field.

4. Select the class to which the policy will apply from the **Device class** drop-down list.

Step Result: The device collection section becomes active.

Note: You can either add an existing collection or create a new one.

5. [Optional] To add an existing collection:

- a) Click **Add**.

Step Result: The **Add Collections from Library** dialog opens.

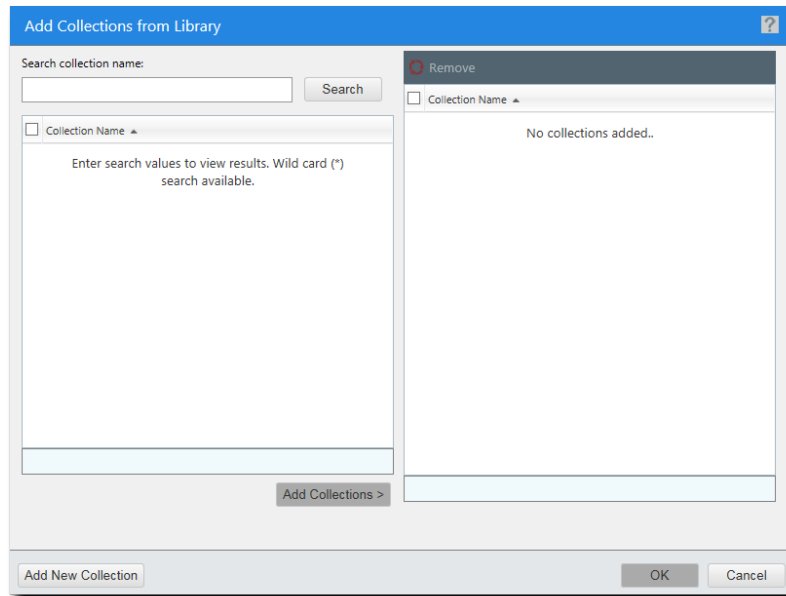


Figure 11: Add Collections from Library

- b) Type a collection name in the **Search collection name** field and click **Search**.

Step Result: A list of collections is displayed.

- c) Select the collection you want to add.
d) Click **Add Collections**.
e) Click **OK**.

Step Result: The **Add Collections from Library** dialog closes.

- f) [Optional] Select the **Disable** option to delay the activation of the policy.
By default, the **Enable** option is selected, which activates the policy immediately upon completing the creation process.

6. [Optional] To create a new collection:

- a) Click **Add New Collection**.

Step Result: The **New Collection** dialog displays.

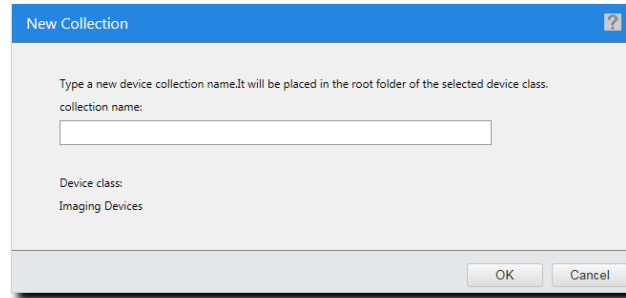


Figure 12: New Collection

- b) Type the name of the collection in the **Collection name** field.

- c) Click **OK**.

Step Result: The **New Collection** dialog and the collection appears in the collections list.

7. Click **Next**.

Step Result: The **Device Collection Policy** dialog opens.

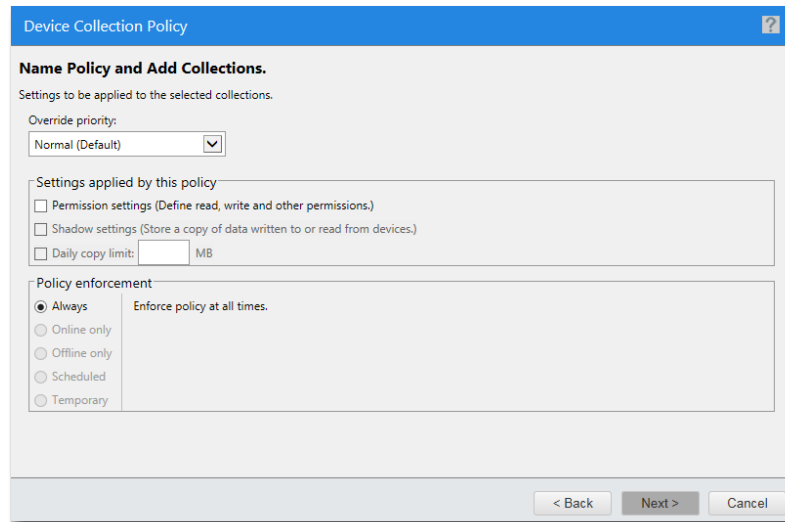


Figure 13: Policy Rules

8. [Optional] Select the **Permission settings** check box to define read, write, and other permissions.

9. [Optional] Select the **Shadow settings** check box to define read, write, and other permissions. Shadow settings can only be enabled for the COM/Serial Ports, CD/DVD Drives, Floppy Disk Drives, LPT/Parallel Ports, and Removable Storage Devices classes.
- 10.[Optional] Select the **Daily copy limit** check box. Specify a copy limit value in the text box.
- 11.Select the desired policy enforcement option. You can choose from the following options:

Option	Description
Always	The policy will apply at all times.
Online only	The policy will apply only when the endpoint/user/group is connected to the server.
Offline only	The policy will apply only when the endpoint/user/group is disconnected from the server.
Scheduled	<p>The policy will apply only during a set schedule. To set the schedule:</p> <ol style="list-style-type: none"> 1. Enter the start time in the From field. 2. Enter the end time in the To field. 3. Select the checkboxes for the days of the week in which the policy will be applied.
Temporary	<p>The policy will give one-time access for a specified period. To specify the enforcement period:</p> <ol style="list-style-type: none"> 1. Select the Immediately option to begin enforcing the policy upon completion of the policy creation process. 2. Select the date and time option and enter a date (mm/dd/yyyy format) and a time (hh:mm AM/PM format) to designate an enforcement start time in the future. 3. Enter a date (mm/dd/yyyy format) and a time (hh:mm AM/PM format) to designate an enforcement end time in the future.

Note: You can click on the clock icon to view and select a list of times in half hour increments and the calendar icon to view and select dates using a calendar.

12. Click Next.

Step Result: The **Permission Settings** page opens.

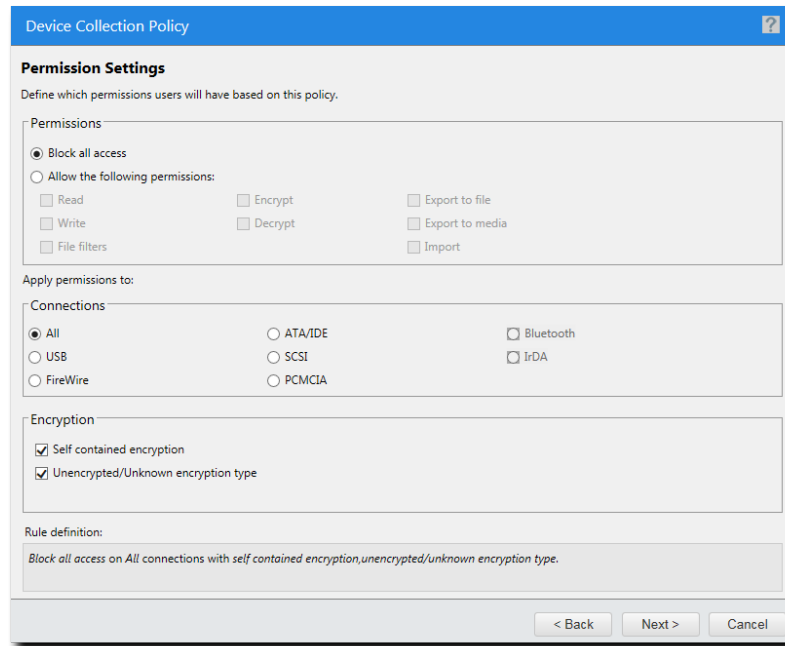


Figure 14: Permission Settings

13. Specify the permission details.

For more information on setting permissions, refer to [Permission Settings for a Policy](#) on page 122.

- Select the **Allow access with following** radio button and then select the desired permissions check boxes. The available permissions vary according to device class.
- Select the connections you want to apply the permissions to in the **Connections** group box. The available connections vary according to device class.
- Select the applicable drives in the **Drives** group box. The availability of drives varies according to device class.
- [Optional] Specify the type of encryption in the **Encryption** group box. The availability of encryption options varies according to device class.

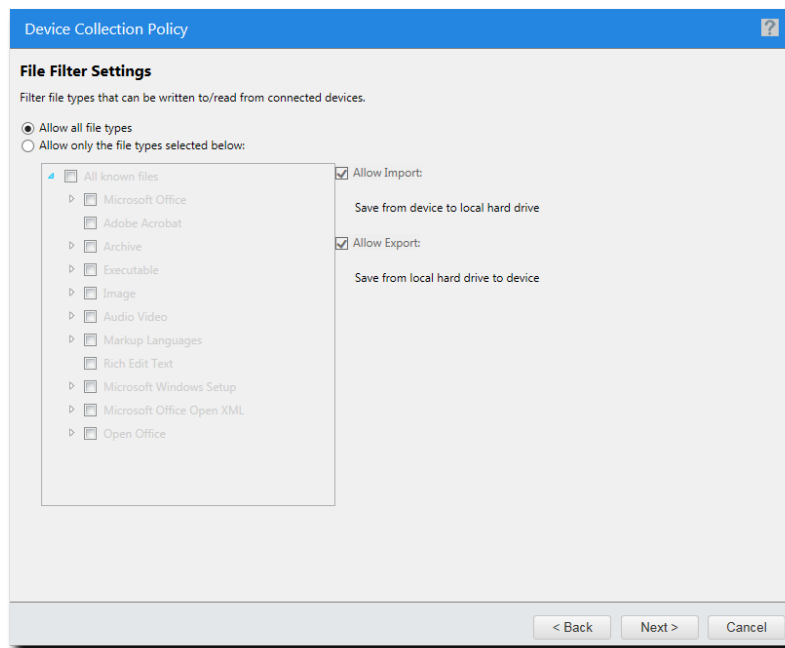
14. Click Next.**Step Result:** The **File Filters** page opens.**Note:** This page will only appear if you select **File Filters** in the **Permission Settings** page.

Figure 15: File Filters

15. Specify the file filtering options.For more information on file filters, see [File Type Filtering](#) on page 125.**16. Click Next.****Step Result:** The **Shadow Settings** page opens.**Note:** This page will only appear if you select **Shadow settings** in the **Policy details** page.

17.Specify the shadow settings.

Shadow files are stored in <install_dir>\DeviceControl\Shadow.

Device Class Policy Type	Options	
<ul style="list-style-type: none">• COM/Serial Ports• DVD/CD Drives• Floppy Disk Drives• LPT/Parallel Ports• Modem / Secondary Network Access Device• Portable Devices• Removable Storage Devices	For both the Read and Write sections:	
	Do not shadow	No content is shadowed.
	Full file content	Saves a copy of the entire file.
	File name only	Records only the file name.
Printers	Do not shadow printed content	This setting can be used to prevent shadowing for specific assignment targets. For example, if you shadow printed content for a specific AD Group you can prevent shadowing for a specific user within that group by selecting this setting and assigning the policy to that user.
	Shadow printed content	This setting is used to store a copy of all information sent to a printer during a print job governed by this policy. This information

18. Click Next.

Step Result: The **Assign policy** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

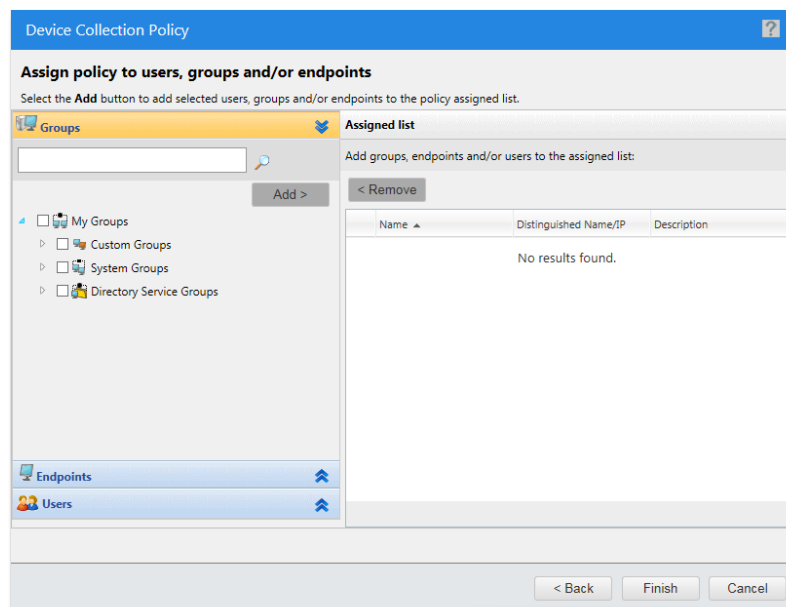


Figure 16: Assign Policy

19. Select the group, endpoint, or user the policy will apply to.**20. Click Finish.**

Step Result: The **Device Collection Policy** wizard closes.

Result: A new policy is created for the selected device collection. The policy is displayed in the **Device Control Policies** page.

Creating a Media Collection Policy

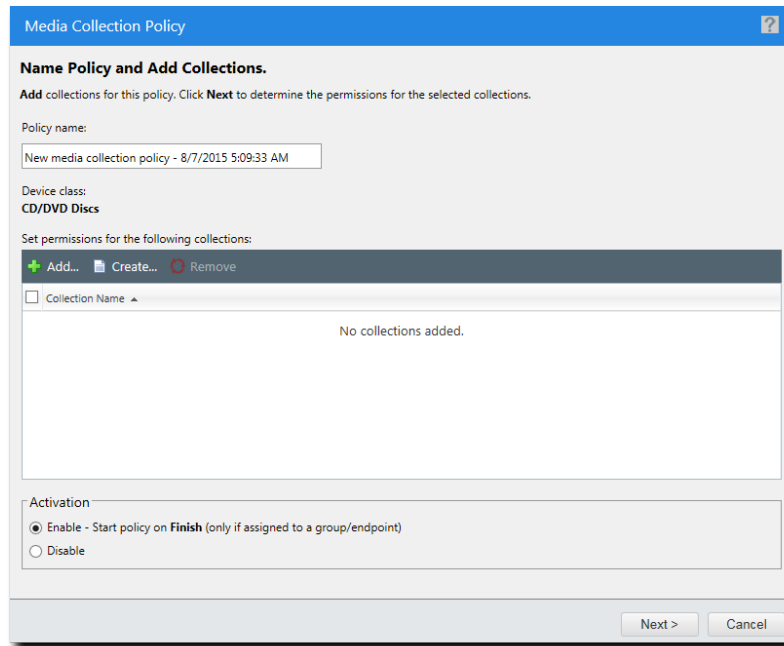
Media collection policies are policies created to grant permissions to media collections in the Device Library.

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

Step Result: The **Device Control Policies** page opens.

2. Click **Create > Create media collection policy.**

Step Result: The **Media Collection Policy** wizard appears.



The screenshot shows the 'Media Collection Policy' wizard window. The title bar is blue with a question mark icon. The main content area is titled 'Name Policy and Add Collections.' and contains the following elements:

- A sub-header: 'Add collections for this policy. Click **Next** to determine the permissions for the selected collections.'
- A 'Policy name:' label followed by a text input field containing 'New media collection policy - 8/7/2015 5:09:33 AM'.
- A 'Device class:' label followed by the text 'CD/DVD Discs'.
- A label 'Set permissions for the following collections:' followed by a toolbar with three buttons: 'Add...' (green plus icon), 'Create...' (blue document icon), and 'Remove' (red minus icon).
- A list box with a 'Collection Name' header and a 'No collections added.' message.
- An 'Activation' section with two radio buttons: 'Enable - Start policy on **Finish** (only if assigned to a group/endpoint)' (selected) and 'Disable'.
- At the bottom right, there are 'Next >' and 'Cancel' buttons.

Figure 17: Media Collection Policy Wizard

3. Type the **Policy name.**

4. To add an existing collection, click **Add**.

Step Result: The **Add Collections from Library** dialog opens.

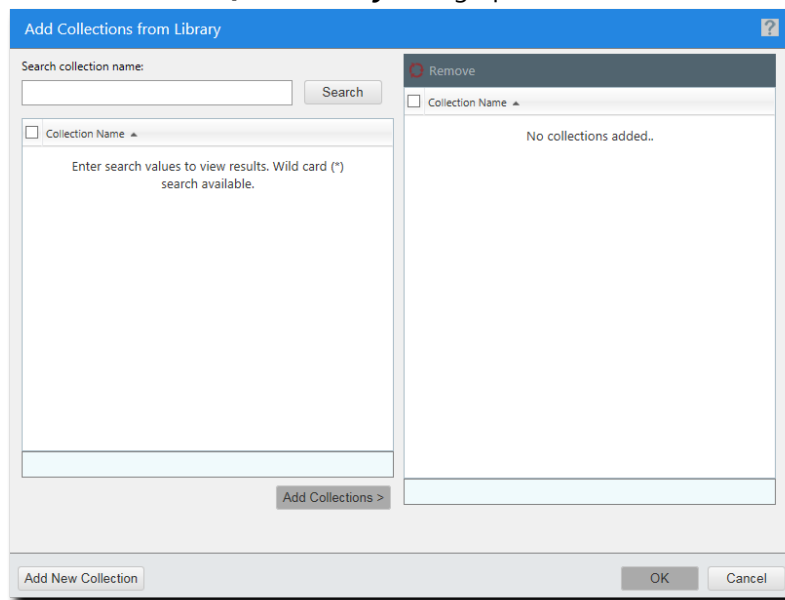


Figure 18: Add Collections from Library

5. Type a collection name in the **Search collection name** field.

6. Click **Search**.

Step Result: A list of collections is displayed.

7. Select the collection you want to add.

8. Click **Add Collections**.

Step Result: The selected collection is added to the right side of the dialog.

9. Click **OK**.

Step Result: The **Add Collections from Library** dialog closes.

10. Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default. If you do not want the policy to be auto-enabled, select **Disable**.

Note: You must manually select enable before the policy will be applicable.

11. Click Next.

Step Result: The **Assign policy** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

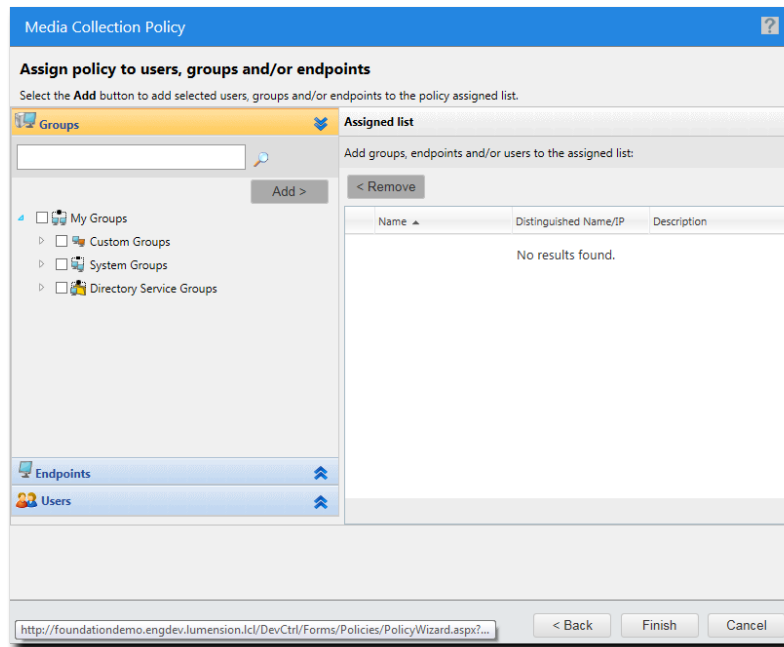


Figure 19: Assign Policy

12. Select the group, endpoint, or user the policy will apply to.**13. Click Finish.**

Result: A new policy is created for the selected media collection. The policy is displayed in the **Device Control Policies** page.

Step 7: Edit a Policy

Edit a policy as desired. While editing a policy, you can define permissions, specify shadowing and logging options, change assigned users and endpoints.

Prerequisites:

Complete [Step 6: Create Device Control Policies](#) on page 29.

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

Step Result: The **Device Control Policies** page opens.

Status	Policy Name	Assigned	Policy Type	Device Class	Device Collection	Last Update (Server)
<input type="checkbox"/>	Default Policy for Biometric Devices	Assigned	Device Class Policy	Biometric Devices	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Citrix Network Shares	Assigned	Device Class Policy	Citrix Network Shares	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for COM/Serial Ports	Assigned	Device Class Policy	COM/Serial Ports	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for DVD/CD Drives	Assigned	Device Class Policy	DVD/CD Drives	Any	10/1/2014 4:34:53 PM
<input type="checkbox"/>	Default Policy for Floppy Disk Drives	Assigned	Device Class Policy	Floppy Disk Drives	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Imaging Devices	Assigned	Device Class Policy	Imaging Devices	Any	12/24/2014 4:06:30 AM
<input type="checkbox"/>	Default Policy for LPT/Parallel Ports	Assigned	Device Class Policy	LPT/Parallel Ports	Any	7/30/2014 6:17:11 AM
<input type="checkbox"/>	Default Policy for Network Access Devices	Assigned	Device Class Policy	Modem / Secondary Network Ac...	Any	7/30/2014 6:17:11 AM

Figure 20: Device Control Policies

2. Select the policy you want to edit.

Tip: Filter the **Policy Name** and **Device Class** or **Device Collection** columns to locate the policies.

3. Click **Edit**.

Step Result: The **Policy Wizard** dialog opens.

Note: The policy wizard that opens will depend on the type of policy you are editing.

4. Edit the policy details as desired.

5. Click **Finish**.

Step Result: The **Policy Wizard** dialog closes.

Result: The selected policy is edited.

After Completing This Task:

Continue to [Step 8: Generate Ivanti Device Control Reports](#) on page 51.

Step 8: Generate Ivanti Device Control Reports

All Ivanti Device Control reports are accessible from the **Reports** menu. Select from the available report templates to view the details of that report.

Prerequisites:

- Complete [Step 7: Edit a Policy](#) on page 49.
 - Review the [Available Ivanti Device Control Reports](#) on page 210.
-

1. Select **Reports > Device Control**.

Step Result: The **Reports** page opens.

2. From the display list, select the report you want to generate.
3. Filter the report by selecting user or endpoint groups.

Note: Not all reports will provide you with filtering options. Some reports do not have selection parameters.

4. Click **Generate Report**.

Result: The selected report opens in a new window.

Chapter 4

Using the Ivanti Endpoint Security Console

In this chapter:

- Common Functions
- The Home Page

Within the Ivanti Endpoint Security console, you can use a number of common functions to navigate and operate the system. After you log in, Ivanti Endpoint Security opens to the **Home Page**.

Ivanti Endpoint Security performs the following functions:

- Endpoint Detection
- Agent Installation
- Endpoint Management
- Endpoint Grouping
- Agent Policy Set Creation
- User and Role Creation and Management
- Server Module Management
- Report Generation

Ivanti Endpoint Security consists of a browser-based management console, which provides access to system management, configuration, reporting, and deployment options.

Common Functions

Ivanti Endpoint Security uses standard Web browser conventions and unique conventions. Familiarize yourself with these conventions to facilitate efficient product use.

From the **Navigation Menu** and system pages, you can access all features and functions you are authorized for.

Common Conventions

The Web console supports user interface conventions common to most Web applications.

Table 2: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Depending on text, type data into these fields to either: <ul style="list-style-type: none">Retrieve matching criteriaEnter new information
Drop-Down Menus	Display a list of selectable values when clicked.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to: <ul style="list-style-type: none">Enable or disable a featureInitiate functions for list items Some lists include a Select All check box for selecting all items, including overflow items.
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by clicking column headers. Columns can be sort in the following orders: <ul style="list-style-type: none">Ascending (default)Descending
Mouseovers	Move your mouse over an item to display a text description.
Auto Refresh	Some pages feature an Auto Refresh check box. Select the check box to automatically refresh the page every 15 seconds.
Scrollbars	Drag scrollbars to see additional data.
Tabs	Select different tabs to display hidden information.
Bread Crumb	Displays the path to the page you are viewing. The breadcrumb lists: <ul style="list-style-type: none">The page you are viewingIts parent page (if applicable)The Navigation Menu item used to open the page If the breadcrumb contains a link, you can click it to retrace your steps.

Tip: Most pages support right-click.

The Navigation Menu

This menu appears on all Ivanti Endpoint Security pages. Use this menu to navigate through the console.

This menu organizes product features based on functionality. When you select a menu item, a new page, dialog, wizard, or window opens. You can access all system features from this menu (that your access rights authorize).

Note: The menu items available change based on modules you install.

Home

Discover

Review

Manage

Reports

Tools

Help

TechPubs Admin | Log Out

Figure 21: Navigation Menu

Table 3: Navigation Menus

Menu	Description
Home	Opens the <i>Home</i> page. This link contains no menu items.
Discover	Contains menu items related to running discovery scan jobs and virus and malware scans.
Review	Contains menu items related to reviewing security content, application event logs, virus and malware events, and discovery scan jobs.
Manage	Contains menu items related to managing system features.
Reports	Contains menu items related to creating reports.
Tools	Contains menu items related to system administration.
Help	Contains menu items related to help systems.

Mobile Device Management adds new **Navigation Menu** items.

Most navigation menus contain items. The following table lists each menu item in the **Discover** menu and the actions that occur when they are selected.

Table 4: Discover Menu Items

Menu Item	Description
Assets...	The <i>Discover Assets</i> dialog.
Assets and Install Agents...	The <i>Install Agents</i> dialog.
Assets and Uninstall Agents...	The <i>Uninstall Agents</i> dialog.

Menu Item	Description
Scan Now - Virus and Malware Scan	The <i>Virus and Malware Scan</i> dialog.

The following table lists each menu item in the **Review** menu and the actions that occur when they are selected.

Table 5: Review Menu Items

Menu Item	Description
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.
	Create Custom Patch List The <i>Create Custom Patch List</i> dialog.
	Custom Patch List The Custom Patch Lists sub-menu lists the last five custom patch lists that you have edited.
	All Lists If you have created more than five custom patch lists, the navigation menu lists an All Lists item, which will open the <i>Patch Content</i> page with all custom patch lists displayed.
My Default View	The <i>All Content</i> page with your saved filters.
Vulnerabilities	Opens a sub-menu. The sub-menu contains the following items:
	All The <i>Patch Content</i> page, filtered to show only critical vulnerabilities.
	Critical Vulnerabilities The <i>Patch Content</i> page, filtered to show only critical vulnerabilities that are not superseded.
	New Vulnerabilities The <i>Patch Content</i> page, filtered to show only critical but not superseded vulnerabilities released in the last 30 days.
	Top Vulnerabilities The <i>Patch Content</i> page, filtered to show only critical but not superseded vulnerabilities sorted by the greatest number of applicable endpoints that are not patched.



Menu Item	Description
Software	Opens a sub-menu. The sub-menu contains the following items:
	All The Patch Content page, filtered to show all software.
	Service Packs The Patch Content page, filtered to show only service packs.
	Software Installers The Patch Content page, filtered to show only software installers.
	Updates The Patch Content page, filtered to show only software updates.
Other	Opens a sub-menu. The sub-menu contains the following items:
	All The Patch Content page, filtered to show all non-critical content.
	Detection Only The Patch Content page, filtered to display Detection Only content.
	Informational The Patch Content page, filtered to display only Information content.
	Packages The Patch Content page, filtered to display only Packages content.
	Policies The Patch Content page, filtered to display only Policies content.
	Recommended The Patch Content page, filtered to display only Recommended content.
	System Management The Patch Content page, filtered to display only System Management content.
	Tasks The Patch Content page, filtered to display only Task content.
	Virus Removal The Patch Content page, filtered to display only Virus Removal content.
Asset Discovery Job Results	Opens the Job Results page, which is filtered to display discovery job results.
Agent Management Job Results	Opens the Job Results page, which is filtered to display Agent Management Job results.

Menu Item	Description
Virus and Malware Event Alerts	Opens the <i>Virus and Malware Event Alerts</i> page.
Application Control Log Queries	Opens the <i>Application Control Log Queries</i> page, which allows users to create log queries that extract information on application activity.
Device Event Log Queries (Device Control only)	Opens the <i>Device Event Log Queries</i> page, which you can use to create, edit, or review device event log queries.

The following table lists each menu item in the **Manage** menu and the actions that occur when they are selected.

Table 6: Manage Menu Items

Menu Item	Description
Endpoints	Opens the <i>Endpoints</i> page.
Mobile Endpoints	Opens the <i>Mobile Endpoints</i> page.
Inventory	Opens the <i>Inventory</i> page.
Groups	Opens the <i>Groups</i> page.
Users	Opens the <i>Users</i> page.
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.
	Create Custom Patch List The <i>Create Custom Patch List</i> dialog.
	Custom Patch List The <i>Custom Patch Lists</i> sub-menu lists the last five custom patch lists that you have edited.
	All Lists If you have created more than five custom patch lists, the navigation menu lists an <i>All Lists</i> item, which will open the <i>Patch Content</i> page with all custom patch lists displayed.
Deployments and Tasks	Opens the <i>Deployments and Tasks</i> page.
Agent Policy Sets	Opens the <i>Agent Policy Sets</i> page.
Mobile Policies	Opens the <i>Mobile Policies</i> page.
Antivirus Policies	Opens the <i>Antivirus Policies</i> page.

Menu Item	Description						
Application Control Policies	<p>Opens the Application Control Policies page, which contains the following tabs:</p> <table> <tr> <td>Managed Policies</td><td>Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/Auditor Policy. This tab is selected by default.</td></tr> <tr> <td>Trusted Change</td><td>Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.</td></tr> <tr> <td>Memory Injection Policies</td><td>Memory Injection Policies.</td></tr> </table>	Managed Policies	Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/Auditor Policy. This tab is selected by default.	Trusted Change	Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.	Memory Injection Policies	Memory Injection Policies.
Managed Policies	Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/Auditor Policy. This tab is selected by default.						
Trusted Change	Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.						
Memory Injection Policies	Memory Injection Policies.						
Device Control: Policies (Device Control only)	Opens the Device Control Policies page, which you use to create, edit, or review Device Control policies.						
Policy Wizards	<p>Opens a sub-menu. The sub-menu contains the following items:</p> <table> <tr> <td>Easy Auditor...</td><td>The Easy Auditor wizard.</td></tr> <tr> <td>Easy Lockdown...</td><td>The Easy Lockdown wizard.</td></tr> </table>	Easy Auditor...	The Easy Auditor wizard.	Easy Lockdown...	The Easy Lockdown wizard.		
Easy Auditor...	The Easy Auditor wizard.						
Easy Lockdown...	The Easy Lockdown wizard.						
Application Library (Application Control only)	Opens the Application Library page, which lists the applications and files on your network endpoints.						
Device Library (Device Control only)	Opens the Device Library page, which lists all devices on your network endpoints.						

The following table lists each menu item in the **Reports** menu and the actions that occur when they are selected.

Table 7: Reports Menu Items

Menu Item	Description
All Reports	Opens the All Reports page.
AntiVirus	Opens the All Reports page with antivirus reports expanded.
Configuration	Opens the All Reports page with configuration reports expanded.
Deployments	Opens the All Reports page with deployments reports expanded.

Menu Item	Description
Device Control (Device Control only)	Opens the All Reports page with Device Control reports expanded.
Inventory	Opens the All Reports page with inventory reports expanded.
Management/Status	Opens the All Reports page with management/status reports expanded.
Policy and Compliance	Opens the All Reports page with policy and compliance reports expanded.
Power Management (Power Management only)	Opens the All Reports page with Power Management reports expanded.
Risks	Opens the All Reports page with risks reports expanded.
Vulnerabilities/Patch Content	Opens the All Reports page with vulnerabilities/patch content reports expanded.
Enhanced Reports	Opens a custom, user-defined URL. This URL is usually used to open a third-party reporting Web page.

The following table lists each menu item in the **Tools** menu and the actions that occur when they are selected.

Table 8: Tools Menu Items

Menu Item	Description
Users and Roles	Opens the Users and Roles page.
Change My Password...	Opens the Change My Password dialog.
Download Agent Installer...	Opens the Download Agent Installer dialog opens over the currently selected page.
Wake on LAN	Opens the Wake on LAN page.
Power Management (Power Management only)	Opens the Power Management page.
Directory Sync Schedule	Opens the Directory Sync Schedule page.

Menu Item	Description				
Device Control Device Control only)	Opens the Device Control submenu. The submenu includes the following items: <table> <tr> <td>Recover Password</td><td>Opens the Recover Password dialog, which you can use to help network users recover forgotten passwords for encrypted devices.</td></tr> <tr> <td>Grant Temporary Permissions</td><td>Opens the Grant Temporary Permissions dialog, which you can use to extend network users temporary access to certain network devices.</td></tr> </table>	Recover Password	Opens the Recover Password dialog, which you can use to help network users recover forgotten passwords for encrypted devices.	Grant Temporary Permissions	Opens the Grant Temporary Permissions dialog, which you can use to extend network users temporary access to certain network devices.
Recover Password	Opens the Recover Password dialog, which you can use to help network users recover forgotten passwords for encrypted devices.				
Grant Temporary Permissions	Opens the Grant Temporary Permissions dialog, which you can use to extend network users temporary access to certain network devices.				
Launch Installation Manager...	Opens the Installation Manager in a new window.				
Subscription Updates	Opens the Subscription Updates page.				
Mobile Management Setup	Opens the Mobile Management Setup page.				
Mobile Endpoint Registration	Opens the Mobile Endpoint Registration dialog.				
Email Notifications	Opens the Email Notifications page.				
Options	Opens the Options page.				

The following table lists each menu item in the **Help** menu and the actions that occur when they are selected.

Table 9: Help Menu Items

Menu Item	Description
Help Topics...	Opens the Help page.
Knowledge Base...	Opens the Ivanti knowledge base.
New Users Start Here...	Opens the New Users Start Here page.
Technical Support	Opens the Technical Support page.
Product Licensing	Opens the Product Licensing page.

Menu Item	Description
About...	Opens the About dialog.

Note: Any unavailable or absent menus, menu items, or sub-menu items are due to restricted access rights or unavailable modules. Contact your network administrator if you require access to unavailable features.

The Page Banner

A page banner displays when the page is added for a new module. Use this banner to identify the module that the page belongs to.



Figure 22: Page Banner

For example, pages for Ivanti Patch and Remediation display a Patch and Remediation page banner. Page banners are color-coded by module.

List Pages

Most pages feature lists of selectable items. These items represent different product features that can be edited using menus and buttons.

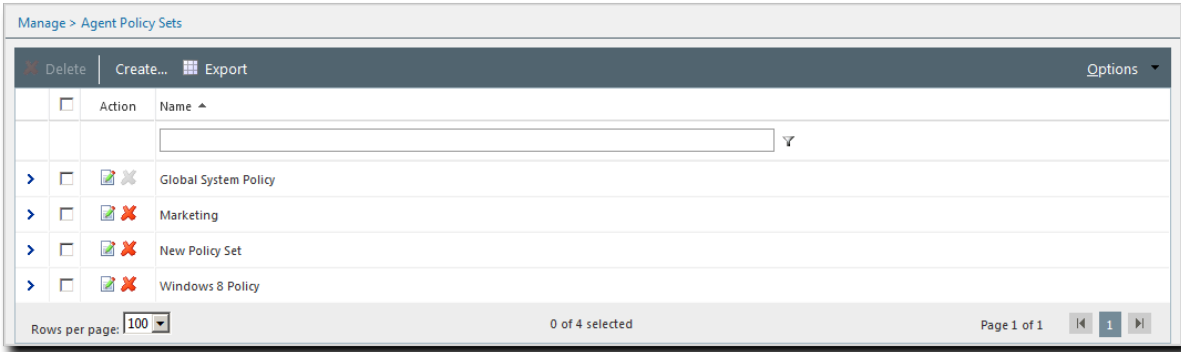


Figure 23: List Page

To select a single list item:

- Select a check box.
- Click a list row.

To select multiple list items:

- Select the **Select All** check box.
- Select multiple, concurrent items by using **SHIFT+Click** and mousing over list rows.

Toolbars

Toolbars appear on most Web console pages. They contain menus and buttons you can use to initiate page features.

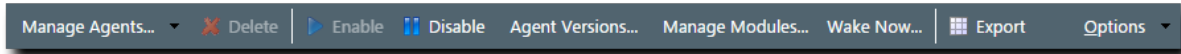


Figure 24: Toolbar

- The menus and buttons displayed vary according to page.
- Click the available menus and buttons to use them.
- User roles determine which buttons are available.

The Options Menu

Toolbars feature an **Options** menu. You can use these options to change how the page displays information.

Table 10: Options Menu Items

Option	Description
Show results on page load	Toggles automatic page results on and off. <ul style="list-style-type: none">• When enabled, the page list automatically populates with results.• When disabled, you must define page filters and click Update View before results populate. For more information, see Filters on page 64.
Save as default view	Saves the current page settings as the default view.
Clear default view	Resets the saved view to the system default.
Show Filter Row ¹	Toggles the Filter Row on and off. For additional information, refer to Using Filter Rows on page 66
Show Group By Row ²	Toggles the Show Group By Row on and off. For additional information, refer to Group By on page 68.
Enable Copy to Clipboard ³	Toggles the ability to select text for clipboard copy.
1. This option title changes to Hide Filter Row when toggled. 2. This option title changes to Hide Group By Row when toggled. 3. Selecting this option disables other features, such as right-click context menus and list item dragging.	

Filters

Filters appear on most list pages. You can use them to search pages for specific data.

Depending on which page you are viewing, you can filter pages using one of the following features. Only one feature appears per page.

- Filters
- Filter Row

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

Name:

Scheduled date:

Last Status:

Type:

Last 30 days ▾

All ▾

Discovery ▾

Update View

Figure 25: Filters

You can save frequently used filter settings as your default view. To save your settings, select **Options > Save as default view** from the toolbar. The toolbar **Options** menu contains the following options for filtering.

Table 11: Filter Options

Option	Function
Show results on page load	Automatically retrieves and displays results when selected.
Save as default view	<div>Saves the active filter and sort criteria as the default view for the page.</div> <ul style="list-style-type: none">• The default view displays each time the page is accessed, including the following events:<ul style="list-style-type: none">• Browsing to a different page.• Logging out of the Web console.• The default view is saved until you save a new one or you clear it.
Clear default view	Resets a saved default view to the system default view.

Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column.

Type	Display Name	Model ID	Device ID
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 26: Filter Row

- Filters are not case sensitive.
- Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.

Supported Wildcards

When searching for or filtering vulnerabilities, you can use wildcards to make search results more specific and efficient.

Wildcards can be used anywhere within the search string. The following table lists the supported operators and wildcards in Ivanti Endpoint Security. Type any wildcards that you intend to use in the **Name or CVE-ID** field.

Table 12: Supported Wildcards

Wildcard	Description	Example
%	Any string. The string can be empty or contain any number of characters.	Typing <i>Microsoft%Server</i> in the Name or CVE-ID field returns any vulnerability with the words <i>Microsoft</i> and <i>Server</i> in any part of the name, such as: <ul style="list-style-type: none">• MS12-043 Security Update for Microsoft Office SharePoint Server 2007 32-Bit Edition (KB2687497)• The 2007 Microsoft Office Servers Service Pack 3 (SP3), 32-bit Edition (KB2526299)
_ (underscore)	An underscore can be used as a Wildcard placeholder for any single character.	Typing <i>_itrix</i> or <i>Citri_</i> in the Name or CVE-ID field returns any vulnerabilities with <i>Citrix</i> in the name.
[]	Any single character within the brackets. You can also type a range ([a-f]) or set ([acegik]).	Typing <i>[m]ic</i> in the Name or CVE-ID field returns vulnerabilities with the string <i>mic</i> within the name (<i>Microsoft</i> and <i>Dynamic</i>). Typing <i>200[78]</i> in the Name or CVE-ID field returns vulnerabilities with 2007 or 2008 within the name.

Wildcard	Description	Example
[^]	Any single character not specified within the brackets. You can also type a range ([^a-f]) or set ([^acegik]).	Typing M[^i]cro in the Name or CVE-ID field returns results that: <ul style="list-style-type: none">• Replace <i>i</i> with all remaining alphanumeric and symbolic characters (a, \$, and so on).• Include all other characters remaining in the string (m, c, r, o). Results would include Macro, Mecro, M\$cro, and so on. If a vulnerability contains Micro and a valid combination like Macro in its name (e.g. MS99-999 Microsoft Word 2010 Vulnerability Could Enable Macros to Run Automatically), it will be returned in the results.

Using Filters

When list pages are overpopulated with items, use filters to search for specific list items. Use this feature to filter list pages by criteria specific to the page.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to [List Pages](#) on page 62.
2. Ensure filters are displayed.
If filters are not displayed, click **Show Filters**.
3. Define filter criteria.

Note: Available filters differ by page.

- In filter fields, type the desired criteria.
- From filter lists, select the desired list item.

4. If applicable, select the **Include sub-groups** check box.

Note: This check box only appears on list pages related to groups.

5. Click **Update View**.

Step Result: The list is filtered according to the filter criteria.

6. [Optional] Save the filter criteria by selecting **Options > Save as default view** from the toolbar.

Using Filter Rows

Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results. Filter column results to search for specific list items.

These rows appear on several list pages.



1. Select a page featuring the filter row.
2. Ensure the filter row is displayed.
 - a) If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.
3. Type criteria in a filter row field.
4. Apply a filter type.
 - a) Click the **Filter** icon.

Step Result: A menu opens.

- b) Select a filter type.

The following table describes each filter type.

Table 13: Data Filtering Types

Type	Description
NoFilter	Removes previously applied filtering.
Contains	Returns results that contain the value applied to the filter.
DoesNotContain	Returns results that do not contain the value applied to the filter.
StartsWith	Returns results that start with the value applied to the filter.
EndsWith	Returns results that end with the value applied to the filter.
EqualTo	Returns results equal to the value applied to the filter.
NotEqualTo	Returns results that are not equal to the value applied to the filter.
Greater Than	Returns results that are greater than the value applied to the filter.
Less Than	Returns results that are less than the value applied to the filter.
GreaterThanOrEqualTo	Returns results that are greater than or equal to the value applied to the filter.
LessThanOrEqualTo	Returns results that are less than or equal to the value applied to the filter.
Between	Returns results that are between two values. Place a space between the two values.
NotBetween	Returns results that are not between two values. Place a space between the values.
IsEmpty	Returns results that are empty.
NotIsEmpty	Returns results that are not empty.
IsNull	Returns results that have no value.

Type	Description
NotNull	Returns results that have a value.
Note: <ul style="list-style-type: none">Filters are not case sensitive.Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.The availability of filtering options depends on the type of data displayed in the column. For example, filtering options that can only apply to numeric data are available in columns that contain text data.	

Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

Using a Custom Date Range Filter

Use the Custom Date Range filter on Virus and Malware Event pages and tabs to display events that have occurred over a specific time period.

Prerequisites:

You must have launched the **Custom Date Range** dialog from the **Last Date Detected** filter field of a Virus and Malware Event page or tab.

1. Enter Start and End dates and times that cover the period you want to view alerts for, then click **OK**. Calendar and Time View popups can be opened to facilitate the entry of dates and times. Times that can be selected are provided in 30-minute intervals.

Note: Your Start date should be less than 90 days from the current date, as event alerts raised outside that range are removed from view.

2. Click **Update View** to display the filtered results.

Result: The list is filtered according to the custom date range criteria you entered. Last Detected Dates are always displayed using server time.

Tip: As Malware and Virus Event alerts can be removed from view, the results list may not display all alerts that occurred within your custom date range. However, removed alerts are not deleted from the database and can therefore be viewed by [generating an appropriate report](#).

Group By

The **Group By** row lets you sort list items into groups based on column headers. Use this feature to see which list items share similarities.

To use the **Group By** row, ensure **Options > Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.



To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options > Hide Group By Row**.

Discover...	Delete	Copy...	View...	Log...	Merge...	Export	Options
Drag a column header and drop it here to group by that column							
<input type="checkbox"/>	Name	Creator	Scheduled Time	Frequency	Last Status	Last Status Time	Type
<input type="checkbox"/>	Weekly Discovery Job - 7/27/2015 10:45:06 AM	FOUNDATION\TechPubs Admin (Windows)	8/3/2015 11:00:00 AM	Weekly	Finished	8/3/2015 11:00:52 AM	Discovery
<input type="checkbox"/>	New Discovery Job - 7/27/2015 11:14:20 AM	FOUNDATION\TechPubs Admin (Windows)	7/27/2015 11:14:50 AM	Immediate	Finished	7/27/2015 11:15:00 AM	Discovery
<input type="checkbox"/>	Daily Discovery Job - 7/27/2015 10:44:43 AM	FOUNDATION\TechPubs Admin (Windows)	7/27/2015 11:00:00 AM	Once	Finished	7/27/2015 11:00:55 AM	Discovery

Figure 27: Group By Row

Expanding and Collapsing Structures

Certain structures in the Web console are expandable and collapsible. Expand structures to view additional information or options. Collapse them to conserve screen space. Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.

☐

Action

Name ▲

☒

Global System Policy

Name	Value	Description
Policy Name	Global System Policy	Indicates the unique name of the policy set
Type	System	Indicates the type of policy (System or User Defined)
Description	The settings defined within the Global System Policy are us...	Indicates the description of the policy
Created By	System	Indicates the name of the user that created the policy
Created Date		Indicates the date that the policy was created

Policy Set Details

Policy set name *

Global System Policy

Policy set description

The settings defined within the Global System Policy are used to populate those policy values that are not defined through an agent's group memberships.

Figure 28: Expandable Structure Examples

Advancing Through Pages





When a list page contains an overflow of items, pagination links are created to manage the overflow. Click these links to advance through list items.

The number of list items and the page you are viewing determines the number of pagination links.



Figure 29: Pagination Feature

Table 14: Pagination Feature Functions

Icon or Link	Title	Function
	Final Page Link	Advances to the final page of list items.
	First Page Link	Returns to the first page of list items.
	Next Ten/Previous Ten Pages Link	Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages.
	Pagination Links	Advances or returns to the selected pagination link.

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

Help

Ivanti Endpoint Security contains context-sensitive HTML help that includes feature explanations, step-by-step procedures, and reference materials.

Accessing Help differs according to context.

- From a page, select **Help > Help Topics**.
- From a dialog, click the **Question Mark** icon (?).

Use the following features to navigate through Help:

- From the **Content** tab, expand the bookmarks and click links to display Help topics.
- From the **Search** tab, type criteria in the **Keywords** field and click **Search** to display Help topics related to your search.

Exporting Data

On many system pages, you can export the listed data to a comma-separated value file (.csv) available for use outside of the Web console. Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of pages.

Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Open a system page or dialog that you can export information from.
2. [Optional] Use the page filters to refine the items listed.
3. Click **Export**.

Step Result: The **File Download** dialog opens.

4. Use the browser controls to complete the data export.

Result: The data is exported. All data results export, including data on overflow pages.

The Home Page

The entry point to Ivanti Endpoint Security is the **Home Page**. From this page you can view the dashboard, which features drag-gable widgets that display information about Ivanti Endpoint Security and agent-managed endpoints.

Some widgets display general information about the system, others provide links to documentation, and still others summarize activity for Ivanti Endpoint Security modules you are licensed for.

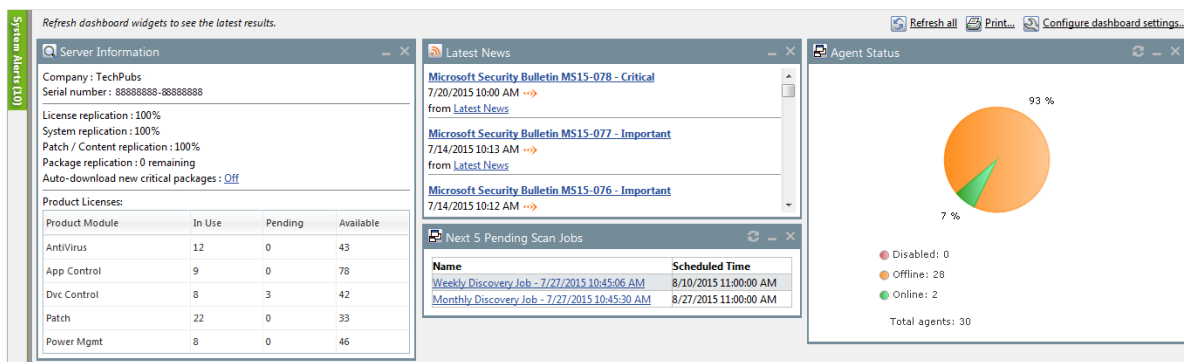


Figure 30: The Home Page

The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located on the **Home** page, the dashboard provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following ***Dashboard*** widgets are available:

- [The Agent Module Installation Status Widget](#) on page 73
- [The Agent Status Widget](#) on page 73
- [The Applicable Content Updates Widget](#) on page 73
- [The Discovery Scan Results: Agents Widget](#) on page 77
- [The Critical Patch Status by Endpoint Widget](#) on page 76
- [The Endpoints with Unresolved Updates Widget](#) on page 77
- [The Incomplete Deployments Widget](#) on page 78
- [The Last 5 Completed Scan Jobs Widget](#) on page 78
- [The Latest News Widget](#) on page 79
- [The Mobile Endpoint Last Check In Widget](#) on page 79
- [The Mobile Endpoint Status Widget](#) on page 80
- [The Mobile Endpoints with Policy Widget](#) on page 80
- [The Mandatory Baseline Compliance Widget](#) on page 79
- [The Next 5 Pending Scan Jobs Widget](#) on page 81
- [The Offline Patch Endpoints Widget](#) on page 81
- [The Patch Agent Module Status Widget](#) on page 82
- [The Scheduled Deployments Widget](#) on page 82
- [The Server Information Widget](#) on page 83
- [The Time Since Last DAU Scan Widget](#) on page 84
- [The Un-remediated Critical Vulnerabilities Widget](#) on page 84
- [The Endpoints with Unresolved AV Alerts Widget](#) on page 85
- [The Top 10 Infected Endpoints Widget](#) on page 86
- [The Top 10 Virus/Malware Threats Widget](#) on page 87
- [The Estimated Energy Savings: Daily Widget](#) on page 87
- [The Estimated Energy Savings: Weekly Widget](#) on page 88
- [The Estimated Energy Savings: Monthly Widget](#) on page 89
- [The Device Control Denied Actions Widget](#) on page 89
- [The Devices Connected to Endpoints Widget](#) on page 90

The Agent Module Installation Status Widget

This widget displays the installation and licensing stats of each agent module.

A graph bar displays for each installed module. The following table describes the widget graph.

Table 15: Graph Bar Color Descriptions

Bar Color	Description
Blue	The number of endpoints with the module pending install or uninstall.
Green	The number of endpoints with the module installed.
Red	The number of endpoints without the module installed.

Tip: Click the graph to open the **Endpoints** page.

Note: Endpoints with an agent version that does not support a module are not counted.

The Agent Status Widget

This widget displays all agents grouped by agent status.

Table 16: Agent Status Widget Fields

Field	Description
Online	The number of agents that are online.
Offline	The number of agents that are offline.
	Tip: Offline status is determined by the amount of time since the agent last communicated as determined on the Options page.
Disabled	The number of agents that are disabled.
Total Agents	The total number of agents in your environment.
Tip: Click the graph to open the Endpoints page. The page is filtered to display all agents.	

The Applicable Content Updates Widget

This widget displays applicable content updates grouped by content type. View this widget when determining what content is applicable to endpoints in your network.

Table 17: Applicable Content Updates Widget Graph Bars

Bar	Description
Critical	The number of critical content items that are applicable to the your endpoints.

Bar	Description
Recommended	The number of recommended content items that are applicable to your endpoints.
Optional	The number of optional software, informational, and virus removal content items that are applicable to your endpoints.
Tip: Click the widget graph to open the Content page, which is filtered to display all applicable non-patched content.	

Table 18: Applicable Content Updates Widget Fields

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.
Endpoints	The total number of endpoints with applicable updates.

Note:

- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.
- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.



The Critical Patch Status by Endpoint Widget

This widget depicts the patch status of all managed endpoints. Each bar indicates the number of managed endpoints with applicable vulnerabilities within a given release date range.

The following table describes the **Critical Patch Status By Endpoint** widget. Green bars indicate endpoints that are patched for critical vulnerabilities, while red bars indicate endpoints that are not patched for critical vulnerabilities.

Table 20: Critical Patch Status By Endpoint Bars

Graph Bar	Description
<30 days	The number of endpoints with applicable critical vulnerabilities fewer than 30 days old.
30 - 120 days	The number of endpoints with applicable critical vulnerabilities between 30 to 120 days old.
>120 days	The number of endpoints with applicable critical vulnerabilities greater than 120 days old.

The following table describes the widget fields.

Table 21: Critical Patch Status By Endpoint Fields

Field	Description
Endpoints	The total number of endpoints with applicable critical vulnerabilities.
Critical vulnerabilities	The total number of critical vulnerabilities applicable to your environment.

Tip: Click the graph to open the **Critical Vulnerabilities** content page.

Note:

- If an endpoint is marked as *Do Not Patch* for a critical vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved critical vulnerabilities.
- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the **Critical vulnerabilities** count.



The Discovery Scan Results: Agents Widget

This widget displays the number of endpoints capable of hosting agents discovered in the latest Discovery Scan Job. The endpoints are classified in to two groups: endpoints with agents and endpoints without agents.

Table 22: Discovery Scan Results: Agents Widget Fields

Field	Description
As of	The name of the Discovery Scan Job used to generate the widget graph and statistics. This job is the job most recently run.
Endpoints with agents	The number of agent-compatible endpoints discovered that have agents installed.
Endpoints without agents	The number of agent-compatible endpoints discovered that have no agents installed.
Endpoints	The total number of agent-compatible endpoints discovered.

Tip: Click the widget to open the **Results** page for the most recently run Discovery Scan Job.

The Endpoints with Unresolved Updates Widget

This widget displays all endpoints with unapplied applicable content updates, grouped by content type. View this widget when determining if an endpoint requires deployment.

An unresolved update is an occurrence of an endpoint that has not had an applicable content item installed.

Bar	Description
Critical	The number of endpoints that have unresolved critical content updates.
Recommended	The number of endpoints that have unresolved recommended content updates.
Optional	The number of endpoints that have unresolved software, informational, and virus removal content updates.

Tip: Click a widget graph bar to open the **Content** page, which is filtered to display all unapplied applicable content.

Field	Description
Endpoints	The number of endpoints with applicable updates within your network.

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.

Note:

- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved updates.
- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.

The Incomplete Deployments Widget

This widget displays all deployments with elapsed start dates and a status of *not started* or *in progress*.

Table 23: Incomplete Deployment Widget Fields

Field	Description
<25%	The number of deployments that are less than 25 percent complete. This field includes deployments that have not started.
25% - 49%	The number of deployments that are 25 to 49 percent complete.
50% - 69%	The number of deployments that are 50 to 69 percent complete.
70% - 79%	The number of deployments that are 70 to 79 percent complete.
80% - 89%	The number of deployments that are 80 to 89 percent complete.
>90%	The number of deployments that are more than 90 percent complete.
Total	The total number of deployments that have a status of <i>in progress</i> or <i>not started</i> with an elapsed start time.
Total affected endpoints	The total number of endpoints receiving pending or in-progress deployments.

The Last 5 Completed Scan Jobs Widget

This widget contains information about the last five completed discovery scan jobs. Each job name is a link to the associated **Result** page.

Table 24: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the Results page for the job.

Column	Description
Completed Date	The date and time the job completed on the server.
Status	The status of the completed job.

The Latest News Widget

This widget displays important announcements and other information in Ivanti Endpoint Security. Click a link to view additional details about an announcement.

The Mandatory Baseline Compliance Widget

This widget displays the Mandatory Baseline status for all endpoints that have the Patch and Remediation module installed.

Table 25: Mandatory Baseline Compliance Widget Fields

Field	Description
Compliant	The number of endpoints with all Mandatory Baseline content installed.
	Note: Endpoints that don't have Mandatory Baseline content installed that's marked <i>Do Not Patch</i> are considered compliant.
In process	The number of endpoints currently downloading Mandatory Baseline content.
No baseline	The number of endpoints with no content assigned to their Mandatory Baselines.
Non compliant	The number of endpoints that do not have all content in their Mandatory Baselines installed.
Total number of endpoints	The number of endpoints with an agent installed.

The Mobile Endpoint Last Check In Widget

This widget displays your mobile endpoints, which are grouped by the duration or their last check in.

The total number of mobile endpoints is grouped into six different time categories. Click the graph to open the **Mobile Endpoints** page, which will be sorted by date with the oldest endpoints listed on top.

Graph Bar	Description
1 day (Green)	The number of mobile endpoints that last checked in one day ago.
2 days (Light Green)	The number of mobile endpoints that last checked in two days ago.
3 days (Blue)	The number of mobile endpoints that last checked in three days ago.
4-7 days (Yellow)	The number of mobile endpoints that last checked in four to seven days ago.

Graph Bar	Description
8-14 days (Orange)	The number of mobile endpoints that last checked in 8 to 14 days ago.
14+ days (Red)	The number of mobile endpoints that last checked in 14 days ago or more.

The Mobile Endpoint Status Widget

This widget shows the last known status of all registered mobile endpoints. A pie chart displays the percentage of endpoints in each status.

Status	Description
Online	The number of endpoints that have checked in within the set communication interval without issue.
Online Jailbroken	The number of jailbroken iOS endpoints that have checked in within the set communication interval.
Online Rooted	The number of rooted Android endpoints that have checked in within the set communication interval.
Offline	The number of endpoints that have not checked in within the set communication interval.
Disabled	The number of disabled mobile endpoints.
Unmanaged	The number of mobile endpoints that have their profile removed or the app uninstalled.
Expired	The number of endpoints issued an expired license.
Wiped	The number of endpoints that have been sent a command to revert to factory settings.
Total mobile endpoints	The total number of mobile endpoints registered with Ivanti Endpoint Security.

Tip: Click an endpoint status to open the **Mobile Endpoints** page, which is filtered to display the clicked endpoint status.

The Mobile Endpoints with Policy Widget

This chart displays all mobile endpoints and their policy assignment status.

This table describes each widget bar.

Bar	Description
No Policy	The number of mobile endpoints that have no policy assignments.

Bar	Description
Blocked	The number of mobile endpoints that have policy assignments that are not being enforced because the endpoint has a status of Unmanaged , Offline , or Expired .
Pending	The number of mobile endpoints that have had a policy assignment that has not yet been applied.
Applied	The number of mobile endpoints that have a policy assignment applied successfully.

The Next 5 Pending Scan Jobs Widget

This widget displays information about the next five pending discovery scan jobs.

Table 26: Next 5 Pending Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the link to view the Discovery Scan Jobs page Scheduled tab.
Scheduled Time	The date and time the job is scheduled for on the server.

Tip: Click a job name link to view the **Discovery Scan Jobs** page **Scheduled** tab.

The Offline Patch Endpoints Widget

This widget displays all offline Patch and Remediation endpoints. These endpoints are grouped by time ranges since they last checked in.

Table 27: Offline Agents Widget Fields

Field	Description
< 48 hours	The number of Patch and Remediation endpoints offline fewer than 48 hours.
48 - 72 hours	The number of Patch and Remediation endpoints offline 48 to 72 hours.
> 72	The number of Patch and Remediation endpoints offline greater than 72 hours.
Total number of offline agents	The number of Patch and Remediation endpoints that are offline (since their last scheduled Discover Applicable Updates task).

Tip: Clicking the **Offline Patch Endpoints** widget pie chart opens the **Endpoints** page **Patch and Remediation** tab, which is filtered to display offline patch endpoints.

The Patch Agent Module Status Widget

This widget displays all endpoints with the Patch and Remediation module installed, which are grouped by Patch and Remediation status.

Table 28: Patch Agent Module Status Widget Fields

Field	Description
Working	The number of Patch and Remediation endpoints that are working on a deployment task.
Idle	The number of Patch and Remediation endpoints that are idle.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Sleeping	The number of Patch and Remediation endpoints that are sleeping.
Offline	The number of Patch and Remediation endpoints that are offline.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Agents with PR module installed.	The number of endpoints with the Patch and Remediation module installed.
Total Agents	The total number of Patch and Remediation endpoints in your network.

Tip: Click the graph to open the *Endpoints* page *Ivanti Patch and Remediation* tab.

The Scheduled Deployments Widget

This widget displays endpoints that have not-yet installed applicable content. These endpoints are divided in to two categories: endpoints with deployments scheduled and endpoints with deployments not scheduled. These categories are further divided into three categories: endpoints with not-yet applied critical content, endpoints with not-yet applied recommended content, and endpoints with not-yet applied optional content.

Orange graph bars indicate endpoints that are not scheduled to receive applicable content, while blue graph bars indicate endpoints that are scheduled to receive applicable content.

Table 29: Scheduled Deployments Widget Graph Bars

Graph Bar	Description
Critical	The number of endpoints scheduled or not scheduled to receive deployments for critical content.
Recommended	The number of endpoints scheduled or not scheduled to receive deployments for recommended content.



Graph Bar	Description
Optional	The number of endpoints scheduled or not scheduled to receive deployments for optional content.

Tip: Clicking the **Scheduled Deployments** widget opens the **Deployments and Tasks** page, which is filtered to display scheduled deployments.

Table 30: Scheduled Deployments Widget Field

Field	Description
Endpoint with unresolved updates	The number of endpoints with unresolved updates.

The Server Information Widget

This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

Table 31: Server Information Widget Fields

Field Name	Description
Company	The company your server is registered to as defined during installation.
Serial Number	The license number (serial number) assigned to your server.
License Replication	The subscription status between your server and the Global Subscription Service (GSS).
System Replication	The system replication status between your server and the GSS.
Patch / Content Replication	The replication status between your server and the GSS.
Package Replication	The number of packages remaining for replication.
Auto-download New Critical Packages	The indication of whether your automatically downloads packages for critical vulnerabilities. Click the link to open the Subscription Service Configuration dialog. For additional information refer to Configuring the Service Tab .

Table 32: Product Licenses Table Columns

Column	Description
Product Module	The module for which you purchased licenses.
In Use	The number of module licenses in use.

Column	Description
Pending	The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion.
Available	The number of licenses available.

Note: A license expiration notice displays if all available licenses are expired.

The Time Since Last DAU Scan Widget

This widget displays all active agents (not including *disabled* or *offline*) grouped by the amount of time since their last Discover Applicable Updates task.

Table 33: Time Since Last Agent Scan Widget Fields

Field	Description
< 24 hours	The number of agents that last performed a Discover Applicable Updates (DAU) task and checked in fewer than 24 hours ago.
24 - 47 hours	The number of agents that last performed a DAU task and checked in 24 to 47 hours ago.
48 - 72 hours	The number of agents that last performed a DAU task and checked in 48 to 72 hours ago.
> 72 hours	The number of agents that performed a DAU task and last checked in greater than 72 hours ago.
Never checked in	The number of agents that have registered yet have not completed a DAU task.
Total active agents	The total number of active agents.

Tip: Click the **Time Since Last Agent Scan** widget graph to open the **Endpoints** page, which is filtered to display enabled endpoints.

The Un-remediated Critical Vulnerabilities Widget

This widget displays the total number of unremediated critical vulnerabilities that are applicable to your environment grouped by age.

Table 34: Un-remediated Critical Vulnerabilities Widget Graph

Graph Bar	Description
<30 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network fewer than 30 days old.

Graph Bar	Description
30 - 120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network that are 30 to 120 days old.
>120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network greater than 120 days old.

Tip: Click the graph to open the **Vulnerabilities** page, which is filtered to display critical but not superseded applicable vulnerabilities.

Table 35: Un-remediated Critical Vulnerabilities Widget Fields

Field	Description
Critical Vulnerabilities	The number of critical but not superseded vulnerabilities applicable in your network.
Endpoints	The number of endpoints with critical but not superseded applicable vulnerabilities.

Note:

- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Critical vulnerabilities** count.
- If an endpoint is marked as *Do Not Patch* for an applicable vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Endpoints with Unresolved AV Alerts Widget

This widget displays the number of endpoints with unresolved antivirus event alerts.

There are two types of unresolved antivirus event alerts, *not cleaned* and *quarantined*. If an endpoint has multiple not cleaned event alerts, it is counted only once in the **Not Cleaned** column. Likewise, if it has multiple quarantined event alerts, it is counted only once in the **Quarantined** column. However,

if an endpoint has both not cleaned and quarantined event alerts, it is counted twice (once in each column).

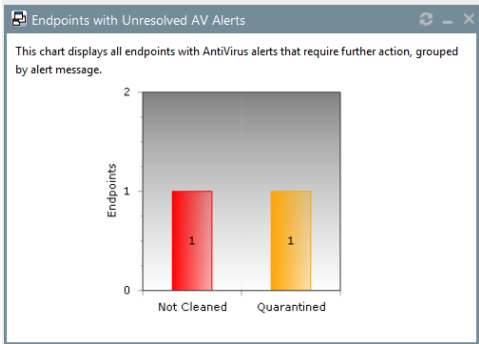


Figure 32: Endpoints with Unresolved AV Alerts Widget

The following table describes each graph bar.

Bar	Description
Not Cleaned	The number of endpoints with not cleaned event alerts.
Quarantined	The number of endpoints with quarantined event alerts.
Tip: Clicking a widget graph bar opens the <i>Virus and Malware Event Alerts</i> page, which is filtered on the endpoint name.	

The Top 10 Infected Endpoints Widget

This widget displays the 10 endpoints which have received the most event alerts in the last 10 days, and a breakdown of each endpoint's alert status.

The widget lists all event alert types, including cleaned, not cleaned, deleted, and quarantined.

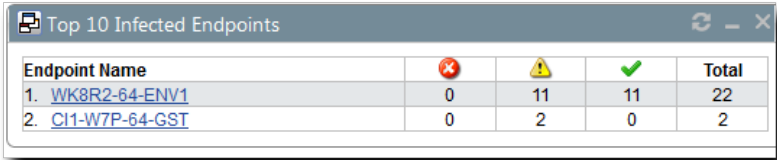


Figure 33: Top 10 Infected Endpoints Widget

The following table describes each column in the widget.

Column	Description
Endpoint Name	The name of the endpoint, with a link to its <i>Details</i> page.
Not Cleaned	The number of alerts on the endpoint where it was not possible to clean a suspect file.



Column	Description
Quarantined	The number of alerts on the endpoint where the file was moved to quarantine.
Cleaned	The number of alerts on the endpoint where a file was successfully cleaned.
Deleted	The number of alerts on the endpoint where a suspect file was deleted.
Total	The total number of all alerts on the endpoint. This is the number on which the ranking of the list is based.

The Top 10 Virus/Malware Threats Widget

This widget displays the 10 types of virus or malware that have generated the most event alerts in the last 10 days.

The malware types are listed from the top down in descending order of frequency, and the number of endpoints affected is displayed along the bottom of the widget.

Note: The display is based on the number of event alerts generated by each virus/malware type, regardless of how the event was handled (cleaned, not cleaned, deleted, or quarantined).

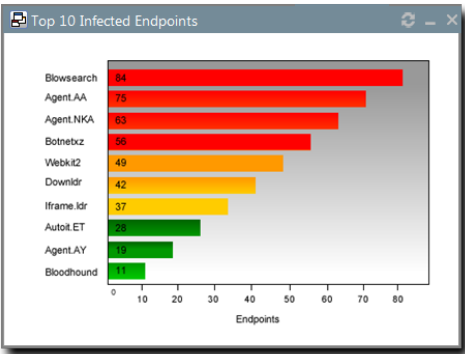


Figure 34: Top 10 Virus/Malware Threats

Clicking on any virus/malware bar will bring you to its **Virus/Malware Details** page.

The Estimated Energy Savings: Daily Widget

This widget displays the energy savings for the previous day. This calculation is based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 36: Estimated Energy Savings: Daily Widget Fields

Field	Description
Results for the day of	The date for which the widget displays the results.
Desktop count	The number of monitored desktops.

Field	Description
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Weekly Widget

This widget displays the energy savings of the past seven days based on your endpoints' actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 37: Estimated Energy Savings: Weekly Widget Fields

Field	Description
Results for the week from	The dates for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Monthly Widget

This widget displays the energy savings of the past 30 days based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

The following table describes the fields in the **Estimated Energy Savings: Monthly** widget.

Table 38: Estimated Energy Savings: Monthly Widget Fields

Field	Description
Results for the month from	The month for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Device Control Denied Actions Widget

This widget displays the users with the highest number of actions blocked by device control policies. View this widget when determining the lists of users for whom action block occurred due to the device control policies.

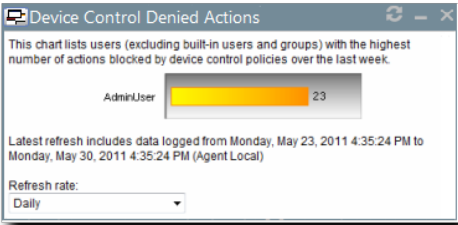


Figure 35: Device Control Denied Actions Widget

The chart displays the users with the highest number of actions blocked by device control policies. The widget can displays five users with the highest number of actions blocked by device control policies. The count on the bar displays the number of times the user actions were blocked by the device control policies.

The Devices Connected to Endpoints Widget

This widget displays the number of peripheral device classes that were connected to endpoints. View this widget when determining which devices were connected to endpoints over the last week.

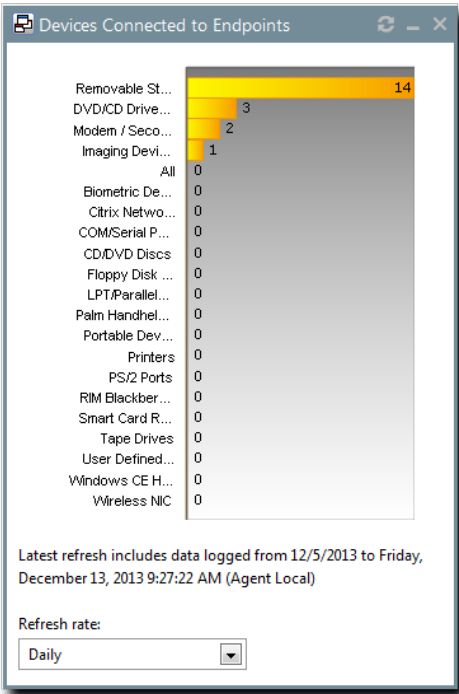


Figure 36: Devices Connected to Endpoints Widget



The chart displays the number of devices in each device class connected to the endpoints. The count on the bar displays the number of devices in a particular device class that were connected to the endpoints.





Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 39: Widget Setting and Behavior Icons

Icon	Action
	Opens the Dashboard Settings dialog.
	Opens the dashboard in print preview mode.

Icon	Action
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.
	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing. This reformat omits the Web site header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

1. From the **Navigation Menu**, select **Home**.
2. Click .

Step Result: The dashboard print preview opens in a new Web browser window.

3. [Optional] Use your Web browser controls to print the dashboard.



Editing the Dashboard

You can customize how widgets are arranged and prioritized. Edit the dashboard to display only the widgets useful in your environment.

Edit the dashboard from the **Dashboard Settings** dialog.



1. From the **Navigation Menu**, select **Home**.
2. Click .

Step Result: The **Dashboard Settings** dialog opens.



3. Choose which widgets you want to display on the dashboard.
 - Select widget check boxes to display them.
 - Clear widget check boxes to hide them.
4. Prioritize the widgets in the desired order.
 - Click  to increase a widget priority.
 - Click  to decrease a widget priority.

Highly prioritized widgets are more prominently placed.

5. Display or hide widget descriptions.

- Click  to display descriptions.
- Click  to hide descriptions.

6. Choose a widget layout.

- Click  to display widgets in two columns.
- Click  to display widgets in three columns.

7. Click **OK**.

Result: Your dashboard settings are saved. The **Home** page displays the selected widgets in the priority you defined.

The System Alert Pane

The **System Alert** pane displays information about changing conditions in your environment. This pane alerts you to required actions and links to related help topics.

The **System Alert** pane displays in the dashboard and shows the number of alerts that require your attention.

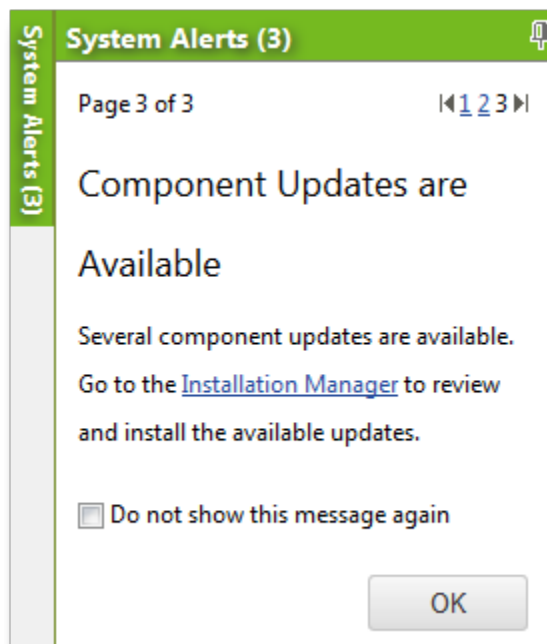


Figure 37: The System Alert Pane

The following functions can be found in the **System Alert** pane.

Table 40: Options Menu Items

Option	Description
Pin (icon)	Docks the System Alert pane. Clicking this icon again collapses it.
Pagination Links	Allows you to navigate between alerts. For more information, see Advancing Through Pages on page 70.
Action Link	Opens the appropriate application page, external Web page, or context-sensitive help topic, depending on the action specified in the alert.
Don't show this again (check box)	Collapses the System Alert pane. The alert shown in the System Alert pane when this check box is selected will no longer be shown.
OK (button)	Collapses the System Alert pane.

Note:

- Dismissing a notification only dismisses the notification for logged in user. The notification still displays for others.
- The system automatically dismisses alerts as you complete their related actions, regardless of whether you dismiss the alerts.

License Expiration

When licensing for a module expires, the module behavior changes. All functionality is restored when the licensing is renewed.

Note: When a subscription expires, the module history and configuration is retained. No work is lost when the module is renewed.

Table 41: License Expiration Scenario and Events

Scenario	Event(s)
Server Module Expiration	<ul style="list-style-type: none">Endpoint module functionality is partially disabled.The module cannot be installed on additional endpoints.The Endpoints page list the module status as <code>Expired</code>.The Home page lists the Available license count as <code>Expired</code>.
Endpoint Module Expiration	<ul style="list-style-type: none">Endpoint module functionality is partially disabled.The module cannot be installed on additional endpoints.The Endpoints page list the module status as <code>Expired</code>.The Home page lists the Available license count as <code>Expired</code>.The Patch and Remediation endpoint module component continues to inventory its host, but no longer enforces Patch and Remediation policies or downloads deployments.The AntiVirus endpoint module continues enforcing policies and completing scans, but no longer downloads new virus definitions.The Application Control endpoint component stops enforcing all policies, no longer blocking or logging applications.The Device Control endpoint component allows all actions and stop logging activity.

Table 42: License Expiration Scenario and Events for Mobile Endpoints

Scenario	Event
Mobile Endpoint Module Expiration	<ul style="list-style-type: none">The Mobile Endpoints page list the module status as <code>Expired</code>.<ul style="list-style-type: none">Endpoints with the oldest check ins expire first.Endpoints that attempt to register when your license count is depleted are listed with a status of <code>Expired</code>.Endpoints cannot be issued commands with the exception of Delete.Any push notifications available on expired endpoints are removed.Any policy events queued or issued to expired endpoints have display a status of <code>Expired</code>.Endpoints cease communications with the server and the cloud.The Home page lists the available license count as <code>0</code>.
	Note: Endpoints in an <code>Offline</code> or <code>Wiped</code> status hold their license until deleted.



To reactivate your licenses following renewal, open the ***Subscription Updates*** page and click **Update Now**. Your server replicates updated subscription information. The page refreshes when the update completes, and all previous module functionality is restored.

Note: For more information about renewing or adding licenses, contact [Ivanti Sales Support](#) (sales@ivanti.com) .

Chapter

5

Managing Devices with the Device Library

In this chapter:

- Granting Access to the Device Library
- The Device Library Page
- Working with the Device Library

The Device Library allows you to view and organize the various devices in your network as well as create policies for both device classes and device collections.

The Device Control Device Library module allows you to assign permissions to users, endpoints, and groups to use any kind of I/O devices available in your network. In addition, you can also use the Device Library to setup and maintain device types.

Granting Access to the Device Library

Users can access the Device Library only if they have the requisite permissions to do so. You can grant access permissions through the **Users and Roles** option in the **Tools** menu.

1. Select **Tools > Users and Roles**.

Step Result: The ***Users and Roles*** page opens.

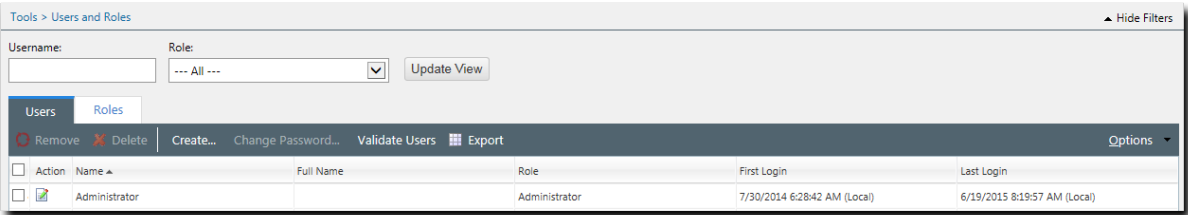


Figure 38: Users and Roles Page

2. Select the **Roles** tab.

Step Result: The **Roles** tab displays.

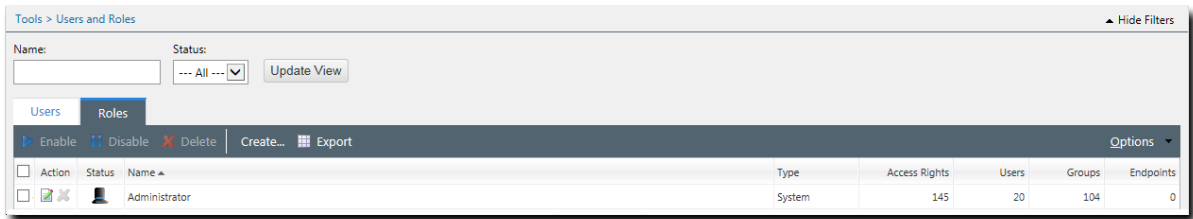


Figure 39: Roles Page

3. Click the **Edit Role** icon for the user to whom you want to grant permission.

Step Result: The **Edit Role** dialog opens.

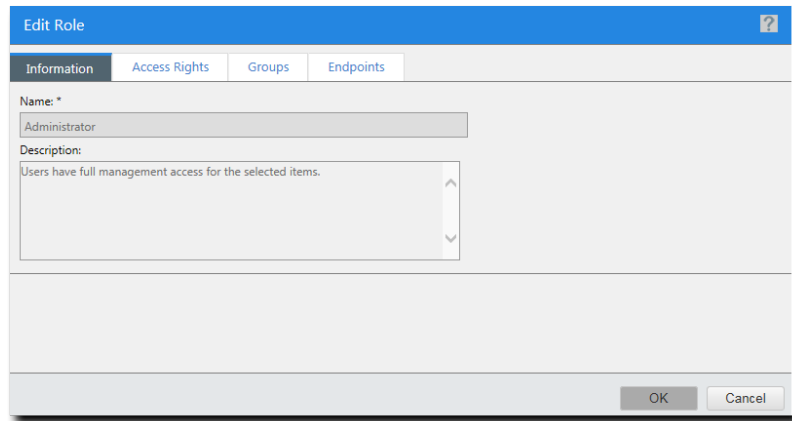


Figure 40: Edit Role Dialog

4. Select the **Access Rights** tab.

Step Result: The **Access Rights** page opens.

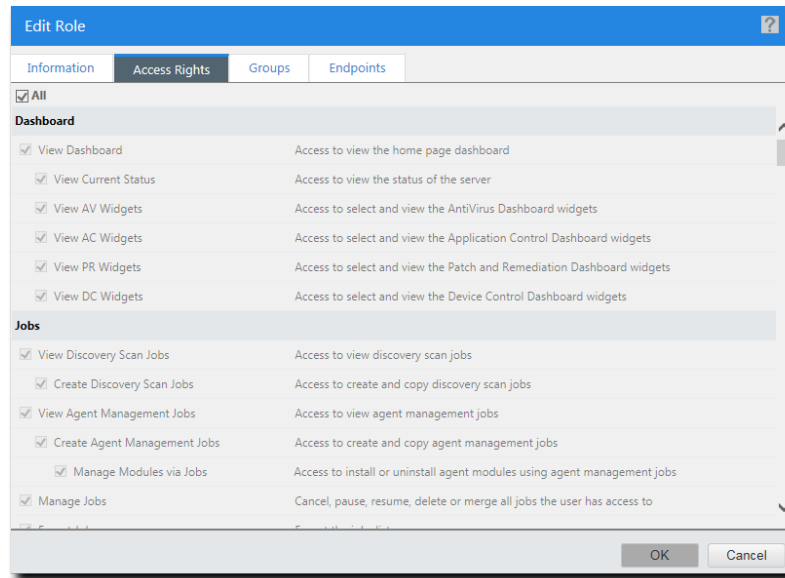


Figure 41: Access Rights

5. Select the appropriate Device Library rights.

- a) In the **Device Library** section, select the **View DC Library** check box.

Step Result: The **Manage DC Library** and **Export DC Library** check boxes become active.

- b) [Optional] Select the **Manage DC Library** check box.

Step Result: The user has access to add and edit Device Library content.

- c) [Optional] Select the **Export DC Library** check box.

Step Result: The user can export Device Library content.

6. Click **OK**.

Step Result: The **Edit Role** dialog closes.

Result: The user is granted permission to access the Device Library.

The Device Library Page

The **Device Library** page contains a list of all the device classes and collections under which the devices in your network are grouped. The page is divided into two panes, the **Device Browser** pane and **Device Control** pane. You can create and edit collections through the **Device Library** page.

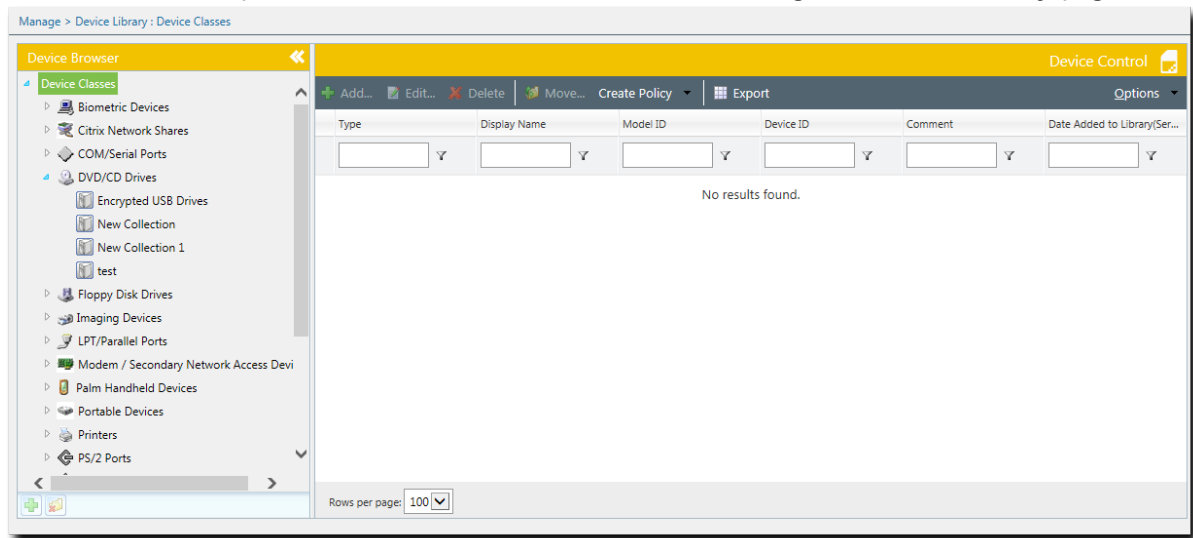


Figure 42: Device Library Page

The Device Browser

Use the **Device Browser** located on the left side of the **Device Library** page to select predefined and user-defined containers for viewing and managing device classes and collections in the Device Library. The contents of the selected container are displayed in a list on the right side of the **Device Library** page.

The **Device Browser** has the following elements:

Device Classes	The Device Browser has a list of predefined device classes. You cannot rename or delete a device class.
Device Collections	You can create, rename, and delete user-defined device collections within a selected device class.

Tip: The **Device Browser** can be collapsed into a narrow vertical strip by clicking the arrow in its top right corner. This provides more screen area to view the right side of the **Device Library** page. Clicking the arrow again expands the browser to its original size.

The **Device Browser** allows the user to perform actions on its device classes and device collections as follows:

Table 43: Device Browser Actions








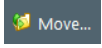

Field	Description
Right-clicking a device class or collection	Opens a contextual menu with the following options:
	<div><div>Add Custom Device Collection</div><div>Allows you to create a device collection for the selected device class. A collections cannot be created within an existing device collection.</div></div>
	<div><div>Rename</div><div>Renames the container. Device classes cannot be renamed.</div></div>
	<div><div>Delete</div><div>Deletes the container. Device classes cannot be deleted.</div></div>
	<div><div>Create Policy</div><div>Opens the policy creation wizard. The wizard type that opens depends on the type of policy you are creating, that is, for a device class or a device collection.</div></div>
Selecting a container	Displays the container's files.
Expanding a device class	Clicking the small triangle beside a device class expands it to reveal the collections inside.
Using the buttons at the bottom of the Device Browser	Adds or deletes device collections at the selected level.
	<div><div>Add</div><div>Adds a collection to the selected device class.</div></div>
	<div><div>Delete</div><div>Deletes the selected device collection.</div></div>



The Device Library Page Toolbar

This toolbar contains buttons that let you create and manage device collections.

The following table describes the **Device Library** page options and their functions:

Table 44: Device Library Page Options

Icon	Option	Description
	Device Browser	Collapsible navigation feature on the left of the page, which provides both predefined and user-defined views of the contents of the Device Library. For more information, see The Device Browser on page 100.
	Add Collection	Creates a new collection in the selected device class or media type. Note: This icon becomes active only if you select a device class or media type in the Device Browser .
	Delete Collection	Deletes the selected collection. Note: This icon becomes active only if you select a collection in the Device Browser .
	Device Control Pane	Area of the Device Library page that allows you to create and edit collections, as well as create policies. Note: A user should have Manage Device Library access rights to use the controls in this part of the page.
	Add	Opens the Add Devices or Add CD/DVD dialog. Note: This button is active only if a collection is selected in the Device Browser .
	Edit	Opens the respective Edit dialog. Note: This button is active only if a collection is selected in the Device Browser and one item selected in the grid of items.
	Delete	Deletes items from the selected collection.
	Move	Opens the Move Items dialog.
	Create Policy	Shows a drop-down list from which you can choose the type of policy to create.

Icon	Option	Description
	Export	Generates a .csv file containing information about the Device Library access rights.
		Note: This button is active only if the user has Export Device Library access rights.
	Options	Shows a drop-down list with Device Library options.

The Device Library Page List

A record of each device and device class resides in the **Device Library** page list.

The **Device Control** list has the following columns:

Table 45: Device Control List Columns

Field	Description
Type	The type of device in the collection.
Model	The device model associated with the device.
Device ID	The unique identifiable serial number of the device.
	Note: If the row represents a unique CD/DVD, this column will display the hash of that disc's contents.
Comments	Displays any comments associated with the device.
Date Added to Library (Server)	The date the current device or model was last added to the Device Library, in the time of the Ivanti Endpoint Security Server.

Working with the Device Library

There are several procedures associated with organizing your devices and media into collections. You can perform the following tasks from the **Device Library** page:

- [Creating a Device Collection](#) on page 104
- [Creating a Media Collection](#) on page 105
- [Adding a Device to a Collection](#) on page 105
- [Adding a Device Model to a Collection](#) on page 108
- [Adding Media to a Collection](#) on page 109
- [Editing a Collection](#) on page 110
- [Moving Items Between Collections](#) on page 111
- [Removing an Item From a Collection](#) on page 111
- [Renaming a Collection](#) on page 112
- [Deleting a Collection](#) on page 112
- [Exporting a Collection](#) on page 113

Creating a Device Collection

The **Device Library** page allows you to create a collection of devices. Use the right-click menu or **Add Collection Icon** in the **Device Browser** to create the collection for the desired device class.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select a device class in the **Device Browser**.

Step Result: The **Add Collection Icon** becomes active.

3. Click the **Add Collection** icon.

Step Result: A **New Device Collection** entry is added to the device class.

4. Type a name for the device collection.

Result: A device collection is created for the selected device class.

After Completing This Task:

After creating a device collection, you can add devices to it. For more information, see [Adding a Device to a Collection](#) on page 105.

Creating a Media Collection

The **Device Library** page allows you to create a collection of media such as CDs and DVDs. Use the right-click menu or **Add Collection Icon** in the **Device Browser** to create the collection for the desired media type.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select a media type in the **Device Browser**.

Step Result: The **Add Collection Icon** becomes active.

3. Click the **Add Collection** icon.

Step Result: A **New Collection** entry is added to the media type.

4. Type a name for the media collection.

Result: A media collection is created for the selected media type.

After Completing This Task:

After creating a media collection, you can add media to it. For more information, see [Adding Media to a Collection](#) on page 109.

Adding a Device to a Collection

Device collections in the **Device Browser** allow you to organize your devices into manageable groups. Once a collection is created, you can add specific devices to it.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection to which you want to add the device.

- a) Expand the device class.
- b) Click the desired collection.

Step Result: A list of devices already in the collection are displayed in the **Device Control** section.

3. Click **Add**.

Step Result: The **Add Devices** dialog opens.

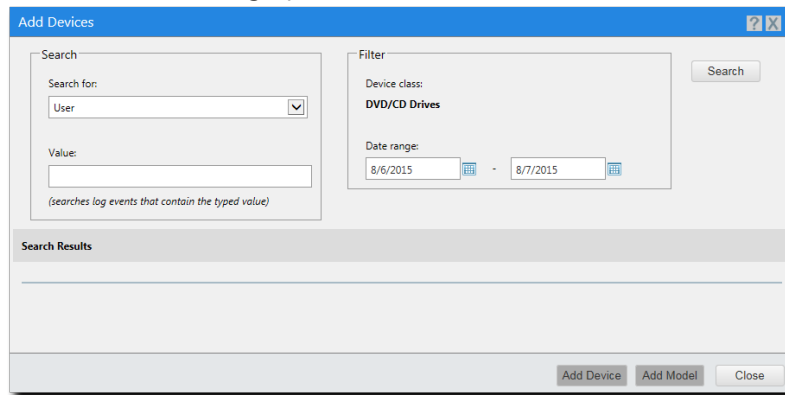


Figure 43: Add Devices Dialog

4. Search for the device you want to add to the collection.

a) Select a search criteria from the **Search For** drop-down list.

You can select from **User**, **Endpoint IP Address**, **Endpoint Name**, **Device Model**, and **Device Unique Id**.

b) [Optional] Type a search term in the **Value** field.

c) [Optional] Select a beginning and end date from the calendar icons in the **Date Range** fields.

d) Click **Search**.

Step Result: A list of devices corresponding to the search criteria appear in the **Search Results** field.

5. Select the device you want to add to the collection.

6. Click **Add Device**.

Step Result: A pop-up message appears stating all selected items are now in the device collection.

7. Click **OK**.

Step Result: The pop-up message closes.

8. Click **Close**.

Step Result: The **Add Devices** dialog closes.

Result: The selected device appears in the list of devices of the collection. The **Type** column entry for that device is **Instance**.

Adding a Network Printer to a Collection

As network printers do not have unique ID, you must add them to a new or existing Device Collection through the **Device Event Log Query Results** page for a query that fetches denied device access events.

Prerequisites:

- Permissions for the Printers device class must be set to None.
 - You must have attempted to print to the network printer to create a WRITE_DENIED action.
 - You must have the appropriate permissions to access Device Event Log Queries. For more information, see [Granting Access to Device Event Logs](#) on page 171.
-

1. Create a Device Event Log Query that fetches recent WRITE-DENIED events:

- a) Select **Review > Device Event Log Queries**. The Device Event Log Queries page opens.
- b) Click **Create**. The **Device Event Log Query** wizard opens.
- c) Type the **Query name**. For example: `Network Printer`
- d) From the **Type** drop-down, select **Denied device access**.
- e) In the **Scheduling**, select **Immediate**.
- f) In the Date range section, select a range that encompasses the date when the print attempt occurred.
- g) Click **Next**. The **Select endpoints/users/groups** page opens.
- h) Select the endpoints from which the print attempt took place.
- i) Click **Finish**.

Step Result: A new query is created and runs. When the query completes, its summary is displayed in the **Completed** tab.

2. View the results of the Device Event Log Query:

- a) Select the **Completed** tab.
- b) Sort the list to find the query you want to view.
- c) Click the name of the query you want to view in the **Name** column.

Step Result: The **Device Event Log Query Results** page opens, displaying the detailed results of the query.

3. Add the Network Printer to a Device Collection in the Device Library:

- a) Locate the WRITE-DENIED event associated with the Network Printer.
- b) Select the check box for the event.
- c) Click the **Add to Device Library** button. The **Add To Device Library** dialog opens.
- d) Select **Selected device models**.
- e) Add the Network Printer to an existing collection (select from the drop-down) or type the name of a new collection (for example, `Network Printers`).

- f) Click **OK**.

Result: The Network Printer is added to the specified Device Collection.

After Completing This Task:

You can now assign permissions to the network printer's device collection. For more information, see [Creating a Device Collection Policy](#) on page 149

Adding a Device Model to a Collection

You can add a specific device model to a device collection. Once a device model is added, all devices with the same model number are automatically added to the collection.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection to which you want to add the device model.

- a) Expand the device class.
- b) Click the desired collection.

Step Result: A list of devices already in the collection are displayed in the **Device Control** section.

3. Click **Add**.

Step Result: The **Add Devices** dialog opens.

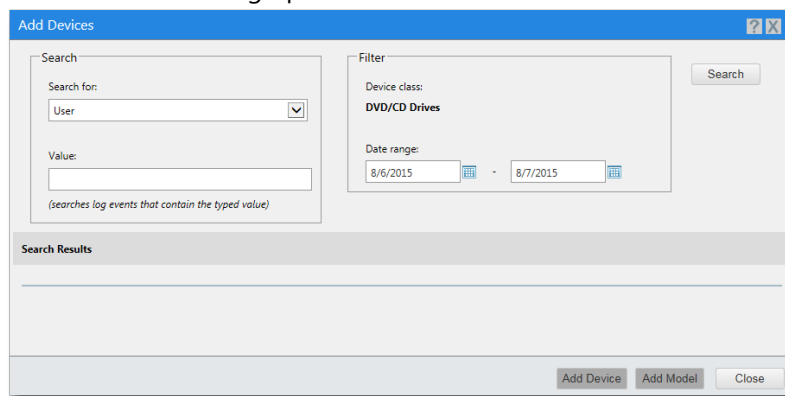


Figure 44: Add Devices Dialog

4. Search for the device model you want to add to the collection.

- a) Select a search criteria from the **Search For** drop-down list.

You can select from **User**, **Endpoint IP Address**, **Endpoint Name**, **Device Model**, and **Device Unique Id**.

- b) [Optional] Type a search term in the **Value** field.

- c) [Optional] Select a beginning and end date from the calendar icons in the **Date Range** fields.
- d) Click **Search**.

Step Result: A list of devices corresponding to the search criteria appear in the **Search Results** field.

5. Select the device you want to add to the collection.

6. Click **Add Model**.

Step Result: A pop-up message appears stating that the device models were added to the device collection.

7. Click **OK**.

Step Result: The pop-up message closes.

8. Click **Close**.

Step Result: The **Add Devices** dialog closes.

Result: The selected device model appears in the list of devices of the collection. The **Type** column entry for that device is **Model**.

Adding Media to a Collection

Media collections in the **Device Browser** allow you to organize your media for better control over access rights. Once a collection is created, you can add specific media to it.

Prerequisites:

To add CDs and DVDs to collections, you first need to install the MediaHasher control. This will allow Ivanti Device Control to calculate the unique hash ID of each CD and DVD you are adding.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection to which you want to add the medium.

- a) Expand the media type.
- b) Click the desired collection.

Step Result: A list of media already in the collection are displayed in the **Device Control** section.

3. Click **Add**.

Step Result: The **Add CD/DVD** dialog opens.

4. Select the medium you want to add to the collection.

- a) Select a drive from the **Drive** drop-down list.

- b) Type a unique name in the **Display name** field.
- c) [Optional] Type any comments in the **Comment** field.

5. Click **OK**.

Step Result: The **Add CD/DVD** dialog closes.

Result: The selected medium appears in the list of media of the collection.

Editing a Collection

The **Edit** button in the **Device Library** page allows you to add and edit comments for items in a collection. The **Edit** button is active only if a collection is selected in the **Device Browser**.

1. Select **Manage > Device Library**.

Step Result: The **Device Library** page opens.

2. Select the collection that contains the item you want to edit.

- a) Expand the parent group.
- b) Click the desired collection.

Step Result: A list of items already in the collection are displayed in the **Device Control** section.

3. Select the item you want to edit.

Step Result: The **Edit** button becomes active.

4. Click **Edit**.

Step Result: The **Edit** dialog opens.

Note: The dialog that opens will depend on the type of collection item selected such as device, device model, or CD/DVD.

5. Edit the entry as desired.

- a) Type a comment in the **Comments** field.
Comments can have a maximum length of 200 characters.
- b) If you are editing a CD/DVD, you can type a **Display name**.

Note: The **Display name** must be unique among all the CDs and DVDs in the Device Library. If the **Display name** is not unique, an error message will be displayed.

6. Click **OK**.

Step Result: The **Edit** dialog closes.

Result: The collection item is edited and the Device Library list is refreshed to show the edited information.

Moving Items Between Collections

You can move items between two collections as long as both collections are part of the same parent group.

1. Select **Manage > Device Library**.

Step Result: The *Device Library* page opens.

2. Select the collection that contains the item you want to move.

- a) Expand the parent group.
- b) Click the desired collection.

Step Result: A list of items already in the collection are displayed in the *Device Control* section.

3. Select the item you want to move.

Step Result: The **Move** button becomes active.

4. Click **Move**.

Step Result: The *Move items* dialog opens.

5. Select a collection from the drop-down list.

You can also type the name of the collection.

6. Click **OK**.

Step Result: The *Move items* dialog closes.

Result: The selected items are moved to the target collection.

Removing an Item From a Collection

Once a collection is created, you can remove items from it. This is useful when you have items in the collection whose access priority changes over time.

1. Select **Manage > Device Library**.

Step Result: The *Device Library* page opens.

2. Select the collection that contains the item you want to edit.

- a) Expand the parent group.
- b) Click the desired collection.

Step Result: A list of items already in the collection are displayed in the *Device Control* section.

3. Select the item you want to edit.

Step Result: The **Delete** button becomes active.

4. Click *Delete*.

Step Result: A confirmation message appears.

5. Click *OK*.

Step Result: The confirmation message closes.

Result: The selected item is removed from the collection and the device library. The **Device Library** list is refreshed to show the remaining items in the collection.

Renaming a Collection

Ivanti Device Control allows you to rename existing collections as and when required. You can rename a collection as long as you specify a name that is unique among all the other collections in the parent group.

1. Select *Manage* > *Device Library*.

Step Result: The **Device Library** page opens.

2. Right-click the collection you want to rename.**3. Select *Rename*.****4. Type the new name of the collection.**

Result: The selected collection is renamed successfully.

Deleting a Collection

You can delete a collection in the Device Library based on whether the collection already has a policy associated with it. Ivanti Device Control does not allow a collection to be deleted if a policy is currently associated with it.

1. Select *Manage* > *Device Library*.

Step Result: The **Device Library** page opens.

2. Right-click the collection you want to delete.**3. Select *Delete*.**

Note: If you try to delete a collection with an associated policy, an error message appears.

Step Result: A confirmation message appears.

4. Click *OK*.

Step Result: The confirmation message closes.

Result: The selected collection is deleted from the Device Library.

Exporting a Collection

You can export information about a collection by using the **Export** button. The exported data is contained in a comma-separated values (.csv) file.

1. Select **Manage > Device Library**.

Step Result: The *Device Library* page opens.

2. Select the collection you want to export.

Step Result: A list of items already in the collection are displayed in the *Device Control* section.

3. Click **Export**.

Result: A .csv file containing information about the collection is generated. Save the file to the desired location.

Chapter 6

Using Device Control Policies

In this chapter:

- Granting Access to the Device Control Policies Module
- The Device Control Policies Page
- Policy Permissions
- File Type Filtering
- File Shadowing
- Working with Device Control Policies

The **Device Control Policies** page allows you create and edit policies for device classes and device collections. The **Device Control Policies** page is accessible only if the user has the requisite permissions for the module.

When you install Ivanti Device Control, a standard list of supported device classes is provided in the Device Library. You can define a general policy for all devices based on the device classes that appear by default in the device list. If a particular device is not recognized in one of the types listed in the device list or if it belongs to a type for which the user has no access defined then the user can still access the device.

If you want to define permissions more precisely, you can set rules for certain models of devices or specific ones in some cases (removable devices). In this case, and only in this case, it is your responsibility to set up and manage the different models and specific devices for which you want to define permissions. You do not need to do that for all possible devices plugged to your network.

Granting Access to the Device Control Policies Module

When Ivanti Endpoint Security is installed, the administrator is automatically assigned rights to access all Device Control modules. Administrators can then assign rights to specific users through the **Tools** menu.

- 1. Select **Tools > Users and Roles**.

Step Result: The *Users and Roles* page opens.

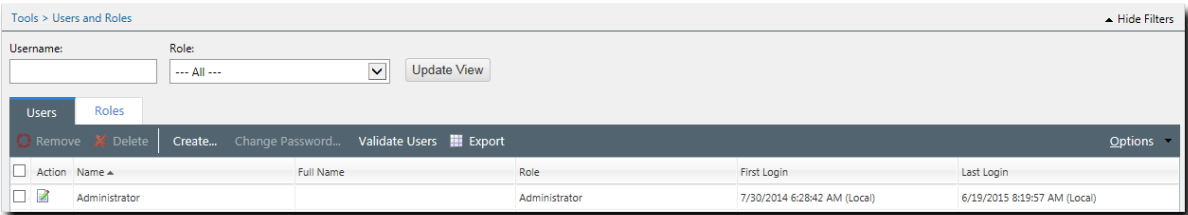


Figure 45: Users and Roles Page

- 2. Select the **Roles** tab.

Step Result: The *Roles* tab displays.

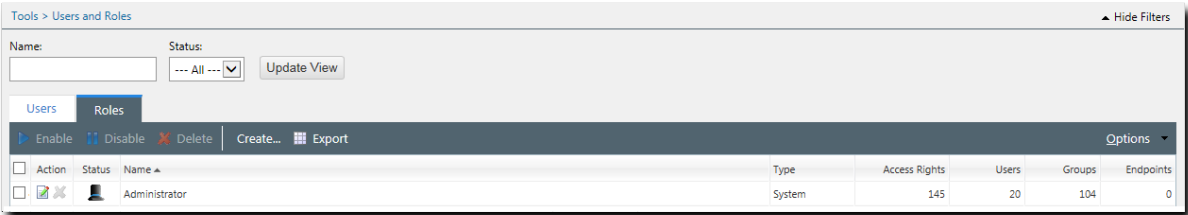


Figure 46: Roles Page

- 3. Select the role to which you want to give access rights.

- Click the **Edit Role** icon for the user to whom you want to grant permission.

Step Result: The **Edit Role** dialog opens.

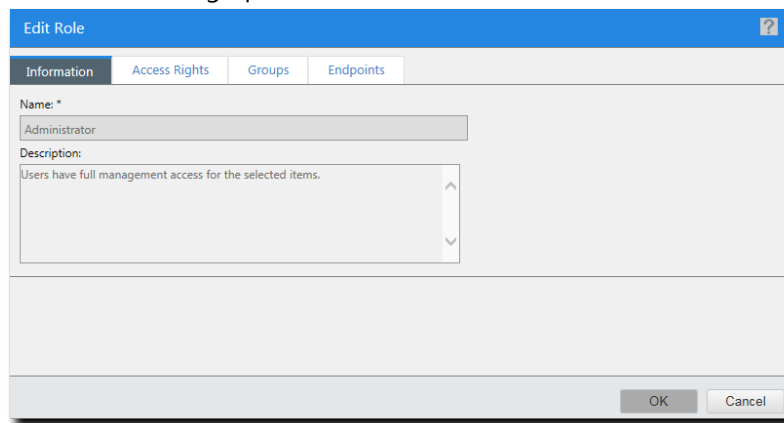


Figure 47: Edit Role Dialog

- Select the **Access Rights** tab.

Step Result: The **Access Rights** tab displays.

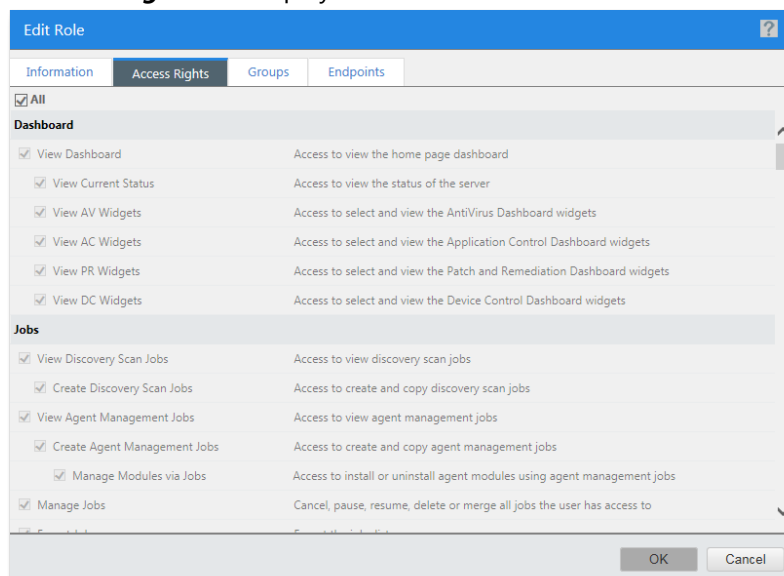


Figure 48: Access Rights

6. Select the Device Control policy access rights that you want to apply to the role.

- a) In the **Device Control Policies** section, select the **View Group/Endpoint/User DC Policies** check box.

Step Result: The **Manage Group/Endpoint/User DC Policies**, **Assign Group/Endpoint/User DC Policies**, and **Export Group/Endpoint/User DC Policies** check boxes become active.

- b) [Optional] Select the **Manage Group/Endpoint/User DC Policies** check box.

Step Result: The user can create Device Control policies in the context of groups, endpoints, and users.

- c) [Optional] Select the **Assign Group/Endpoint/User DC Policies** check box.

Step Result: The user can assign and unassign Device Control policies in the context of groups, endpoints and users.

- d) [Optional] Select the **Export Group/Endpoint/User DC Policies** check box.

Step Result: The user can export Device Control policy lists in the context of groups, endpoints, and users .

- e) [Optional] Select the **View Centralized DC Policies** check box.

Step Result: The **Manage Centralized DC Policies**, **Assign Centralized DC Policies**, and **Export Centralized DC Policies** check boxes become active.

- f) [Optional] Select the **Manage Centralized DC Policies** check box.

Step Result: The user can create, edit, enable, disable, and delete Device Control policies in **Manage > Device Control Policies**.

- g) [Optional] Select the **Assign Centralized DC Policies** check box.

Step Result: The user can assign and unassign Device Control policies in **Manage > Device Control Policies**.

- h) [Optional] Select the **Export Centralized DC Policies** check box.

Step Result: The user can export the Device Control list in **Manage > Device Control Policies**.

7. Click **OK**.

Step Result: The **Edit Role** dialog closes.

Result: The user is granted the specified access to the Device Control Policies module.

The Device Control Policies Page

The **Device Control Policies** page displays a centralized list of policies applicable for different devices in your network. You can also manage policies using this page.

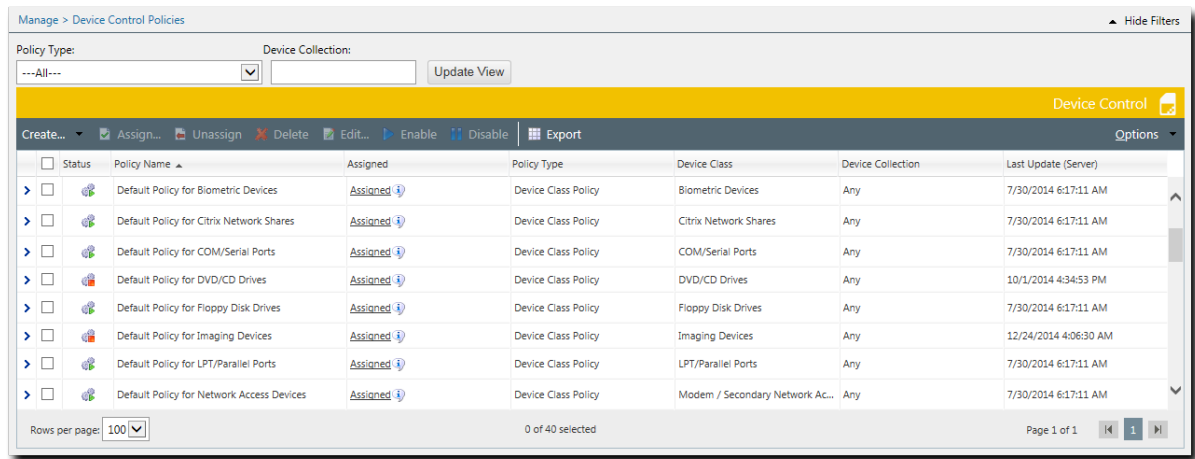


Figure 49: Device Control Policies

The Policies Page Toolbar

This toolbar contains buttons that let you create, assign, and manage policies.

The following table describes the **Device Control Policies** page options and their functions:

Table 46: Device Control Policies Page Options

Option	Description
Create	Displays a drop-down menu that allows you to select the type of policy to create.
	Note: A user should have Manage Centralized DC Policies access rights to access this functionality.
Assign	Opens the Assigned Users and Endpoints dialog for the selected policy.
	Note: This button is enabled only if the user has Assign Centralized DC Policies access rights and a policy is selected from the list.

Option	Description
Unassign	Allows you to unassign the selected policy.
	Note: This button is enabled only if the user has Assign Centralized DC Policies access rights and an assigned policy is selected from the list.
Delete	Allows you delete the selected policy.
	Note: This button is enabled only if the user has Manage Centralized DC Policies access rights.
Edit	Opens the respective policy wizard with the policy details.
	Note: This button is enabled only if the user has Manage Centralized DC Policies access rights.
Enable	Allows you enable a policy that is currently disabled.
Disable	Allows you disable a policy that is currently enabled.
Export	Generates a .csv file containing information about the selected Device Control policies.
	Note: This button is active only if the user has Export access rights.
Options	Displays a list with Device Control Policies page options.

The Policies Page List

A record of each policy that you have created resides in the **Policies** page list.

The **Device Control Policies** list has the following options:

Table 47: Device Control Policies List Columns

Field	Description
Status	The enabled or disabled status of the policy.
Policy Name	The name of the policy.
Assigned	The assigned or unassigned status of the policy.
Device Class	The device class to which the policy applies.
Device Collection	The device collection to which the policy applies.
Last Update (Server)	The date the policy was modified last.

Viewing the Device Control Policies Page

The **Device Control Policies** page displays the policies created for device classes and collections. It also allows you to perform various actions related to policies.

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

Step Result: The **Device Control Policies** page displays.

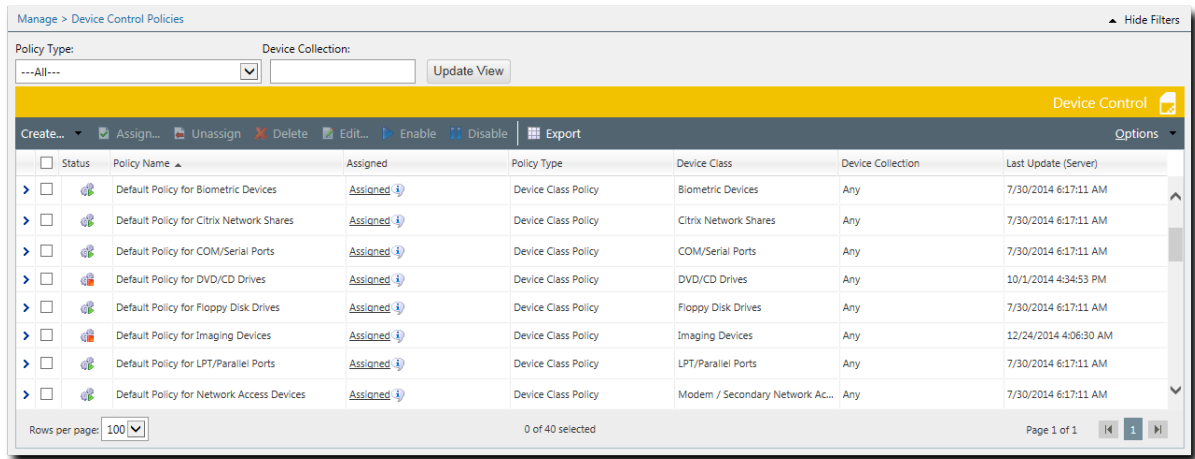


Figure 50: Device Control Policies Page

- 2. Click the applicable rotating chevron (>) to view policy details.

Policy Permissions

Policy permissions allow you to configure which of the device's connections can be used to access the device's hard drives. Configuring policy permissions is an optional part of the process of creating a device class policy.

Permission Settings for a Policy

The **Permission Settings** page in the **Device Class Policy Wizard** lets you define access permissions for a policy.

Device Class Policy

Permission Settings

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:

Block all access on All connections for hard and non hard drives with self contained encryption,unencrypted/unknown encryption type.

< Back

Next >

Cancel

Figure 51: Permission Settings

The following table describes the **Permission Settings** page options.

Table 48: Permission Settings Page Options

Field	Description
Block all access	Lets you create a deny-access policy.
	Note: If you select this option, all other options in this section are disabled.
Allow access with following	Lets you specify the access permissions.



Field	Description
Read	Displays whether read access is permitted.
Write	Displays whether write access is permitted.
Encrypt	Displays whether device encryption is allowed.
Decrypt	Displays whether device decryption is allowed.
Export to file	Displays whether the key used to encrypt a device can be exported to a file.
Export to media	<p>Displays whether the key used to encrypt a device can be exported to the medium itself.</p> <p>Note: Choosing this option allows the device to be decrypted directly, eliminating the need for an external key.</p>
Import	Displays whether data can be imported from an external encryption key.
File Filters	<p>Displays whether access is restricted to specific file types.</p> <p>Note: Selecting this check box will let you access the File Filters page in the policy wizard.</p>
Connections	<p>Displays the available interface standards for the device type and allows you to specify if permissions should be applied only to specific interfaces.</p> <p>Note: Bus Connection options are available depending on the device type selected.</p>
Drives	<p>Allows you to enable permissions for hard drive-based devices, non-hard drive-based devices, or both.</p> <p>Note: This field is valid only for removable storage devices.</p>
Encryption	Displays the encryption status of the devices for whom the policy has been created. This field is valid only for some device types.

Priority Options when Defining Permissions

When you create a policy, you can assign a priority to it. This determines the level of access for a device collection assigned to that policy.

The following table explains the resulting access when permissions are defined between protecting a general device type (class) and a specific device from that class:

Table 49: Resulting Access for Different Permissions

Device Level where Permission is Defined	Permission Set	Priority	Resultant Permission for Selected Device
Type	None	High	None
Model	Read-Write	Normal	
Type	None	Normal	Read-Write
Model	Read-Write	High	
Type	Read-Write	High	None
Model	None	High	
Type	None	Normal	None
Model	Read-Write	Normal	
Type	Read	High	Read-Write
Model	Read-Write	Normal	
Type	Read	Normal	Read-Write
Model	Read-Write	High	
Type	Read-Write	High	Read-Write
Model	Read	High	
Type	Read	Normal	Read-Write
Model	Read-Write	Normal	
Type	None	High	None
Model	Read	High	
Type	None	Normal	None
Model	Read	High	

Permission settings go from high to low in the order None, Read-Write, and Read.

File Type Filtering

You can configure File type filters for the Removable Storage Devices, Floppy Disk Drives, and DVD/CD Drives device class policies that limit access to certain file types.

After setting **Read** or **Read and Write** on the Permission Settings page of the **Device Class Policy** wizard, the **File Filters** option becomes available. Selecting it provides access to the **File Filter Settings** page, on which you can configure the file types that can be written to/read from connected devices.

On the **File Filter Settings** page you can:

- Allow all files types to be accessed.
- Allow only certain file types to be accessed, selectable from a list.

You can also specify the ways all or selected files can be copied.

Allow Import	User can copy files from the external device to the local hard drive.
Allow Export	User can copy files from the local hard drive to the external device.

If no filter is defined or the import/export options of the filter dialog are not activated, then even if some files are selected, the profiled permission applies to all type of files.

Warning: File type filtering rules cannot be combined with encrypt, decrypt, and bus-specific permissions inside the same rule. One permission cannot have both file type filtering defined and encrypt/decrypt/bus-specific options selected, but separate permissions can, and will be properly enforced.

If you combine the access settings, file filtering works as follows:

Table 50: File Filter Settings and Permission Relation

Permission Type	Example
Device access set to None	You are unable to define any file filter settings.
Device access set to Read	If you select MPEG Audio Stream Layer III in the File Type Filtering dialog then read access is allowed for .mp3 files.
Device acces set to Read Write	If you select Microsoft Word in the File Type Filtering dialog then read-write access is allowed for .doc files.

Note: When defining file filters, you cannot open files directly from the external device. You must first copy them to your system (or another authorized hard disk drive).

File Type Filtering Permissions

You can define different file filters for read or read-write permissions.

When applying file filters to a policy, you can use the following file type filtering options:

Table 51: File Type Filtering Options

Permission Setting	Import-Export Settings	Result
Read	Allow Import	Allow file copy from device to the local HDD.
	Allow Export	Allow file copy from the local HDD to the device.
Read-Write	None	Filters are not enforced. The end result is like not defining filters at all.

If no filter is defined or the import/export options of the filter dialog are not activated, then even if some files are selected, the profiled permission applies to all type of files.

Warning: File type filtering rules cannot be combined with encrypt, decrypt, and bus-specific permissions inside the same rule. One permission cannot have both file type filtering defined and encrypt/decrypt/bus-specific options selected, but separate permissions can, and will be properly enforced.

If you combine the access settings, file filtering works as follows:

Table 52: File Filter Settings and Permission Relation

Permission Type	Example
Device access set to None	You are unable to define any file filter settings.
Device access set to Read	If you select MPEG Audio Stream Layer III in the File Type Filtering dialog then read access is allowed for .mp3 files.
Device acces set to Read Write	If you select Microsoft Word in the File Type Filtering dialog then read-write access is allowed for .doc files.

Note: When defining file filters, you cannot open files directly from the external device. You must first copy them to your system (or another authorized hard disk drive).



Available File Type Filters

The **File Filters** page in the **Policy Wizard** dialog allows you to select which file types can be read and transferred to or from a device.

The following table provides a full listing of the file types available in the **File Filters** page.

Table 53: File Types for Filtering

File Type Family	File Type	
Microsoft Office	Microsoft Word	<ul style="list-style-type: none"> Microsoft Word Document Microsoft Word Document Template Microsoft Word Wizard
	Microsoft Excel	<ul style="list-style-type: none"> Microsoft Excel Worksheet Microsoft Excel Add-in Microsoft Excel Template
	Microsoft Visio	<ul style="list-style-type: none"> Microsoft Visio Drawing Microsoft Visio Stencil Microsoft Visio Template
	Microsoft PowerPoint	<ul style="list-style-type: none"> Microsoft PowerPoint Slideshow Microsoft PowerPoint Presentation Microsoft PowerPoint Template Microsoft PowerPoint Add-in
	Microsoft Graph	Microsoft Graph Chart
	Microsoft Project	Microsoft Project File
	Microsoft Access Database	
Microsoft Office Open XML	Microsoft Office Open XML Word	Microsoft Office Open XML Word Document
	Microsoft Office Open XML Excel	Microsoft Office Open XML Excel Work Book
	Microsoft Office Open XML PowerPoint	Microsoft Office Open XML Presentation
Open Office	OpenOffice Writer	<ul style="list-style-type: none"> OpenOffice Text Document OpenOffice Text Template
	OpenOffice Math	<ul style="list-style-type: none"> OpenOffice Formula OpenOffice Formula Template

File Type Family	File Type	
	OpenOffice Base	OpenOffice Data Base
	OpenOffice Calc	<ul style="list-style-type: none"> • OpenOffice Spreadsheet • OpenOffice Spreadsheet Template
	OpenOffice Draw	<ul style="list-style-type: none"> • OpenOffice.org Graphics • OpenOffice.org Graphics Template
	OpenOffice Impress	<ul style="list-style-type: none"> • OpenOffice Presentation • OpenOffice Presentation Template
Adobe Acrobat	Adobe Illustrator Vector Graphic	
	Adobe Acrobat Portable Document Format	
Archive	Zip Compressed Archive	
	Protected Zip Compressed Archive	
	PRIM'X ZED Compressed Archive	
Executable	Executable	
	Dynamic Link Library	
Images	Microsoft Windows OS/2 Bitmap Graphics	
	Joint Photographic Experts Group	
	Graphics Interchange Format	
	Tagged Image File Format	
	Microsoft Windows Metafile	
	Microsoft Windows Icon	
	Microsoft Windows Cursor	
	Enhanced Microsoft Windows Metafile Format	

File Type Family	File Type	
	Portable Network Graphic	
Audio Video	Moving Picture and Associated Audio/Video for digital storage media	<ul style="list-style-type: none"> • Moving Picture Experts Group • MPEG Audio Stream Layer II • MPEG Audio Stream Layer III
	Resource Interchange File Format	<ul style="list-style-type: none"> • Windows Animated Cursor • Audio Video Interleave • Downloadable Sounds • Musical Instrument Digital Interface • DirectMusic Style • WAVEform audio format • Corel Vector Graphic Drawing
	Advanced Streaming Format Files	<ul style="list-style-type: none"> • Microsoft Windows Media File • Advanced Streaming Format • Microsoft Windows Media Audio
	Standard MIDI File	Musical Instrument Digital Interface
	RealNetworks	<ul style="list-style-type: none"> • RealMedia Streaming Media • RealAudio Streaming Media
Markup Languages	Extensible Markup Language	
Rich Edit Text	Rich Text Format	
Microsoft Windows Setup	Microsoft Windows Installer File	
	Microsoft Windows Installer Patch	
	Microsoft Windows SDK Setup Transform Script	

File Shadowing

File shadowing enables you to track the data that is being read, written to, or written from a device. When you enable file shadowing for a device, Ivanti Device Control either creates copies of the files or the filenames that have been read, written to, or written from the device, depending on the file shadowing configuration. Tracking data that is written or read from a device allows you to take prompt action against users, systems, or groups if you discover data transfer violations. File shadowing also allows you to closely monitor specific users or systems.

Note: File shadowing data collected while a user is disconnected from the network is transferred to the server as soon as the user has reconnected.

File shadowing is a powerful feature that requires careful use. Creating copies of transferred data can be a data-intensive task, which can require a hard disk drive with the capacity to hold hundreds of megabytes or gigabytes of copied data. In addition, transferring large amounts of copied data at one time can cause network saturation for slower network connections. Weigh these considerations carefully when deciding whether to shadow files for all the devices in your network or specific device classes or systems in your network.

Note: Removable devices include secondary hard disks. Applying a file shadowing policy to the entire Removable Storage Device device class may consume a large amount of storage space.

When editing a file previously copied to a shadowed device (in the same user’s session), no read shadow data is created since Windows saves the file in its cache and, therefore there is no new read operation request. This does not apply if the file initially resides in the device or in a new user session (the cache is empty).

When defining shadowing permissions, there may sometimes be priority conflicts, if the priorities are not clearly defined.

Note: Lower priority policies with shadowing enabled retain the shadowing function even when a higher priority policy is applied with shadowing disabled.

Supported Device Classes for File Shadowing

A subset of the device classes available in Device Control support file shadowing.

Device Control supports file shadowing for the following device types:

- COM/Serial ports (full)
- LPT/Parallel ports (full)
- CD/DVD drives (file name only)
- Printers (full)
- Modems/Secondary network access devices (full)
- Removable storage devices (file name only)
- Floppy disk drives (file name only)

Supported Formats when Shadowing

Current CD recording standards allow for a bewildering array of formats, ranging from plain user data in a simplified ISO file system to a UDF/ISO+Joliet bridge DVD with interleaving, extended attributes, security descriptors, and associated files.

Common recording software uses only a small subset of those combinations, and Ivanti Device Control concentrates on those; the following table offers an overview of what is and what is not supported in each of the two possible shadow modes.

Table 54: Supported formats for the full shadow or file name only shadow modes

Format	Full shadow mode	File name only shadow mode
Audio tracked (not interpretable)	○	✕



Format	Full shadow mode	File name only shadow mode
Scrambled tracks (not interpretable)	○	×
Raw-mode data (not interpretable)	○	×
Packet writing, Mount Rainier	○	×
ISO, ISO/Joliet	●	●
UDF	○	×
UDF+ISO/Joliet bridge	◐	◐
ISO+El Torito bootable CDs	◐	◐
ISO+Rock Ridge extensions	◐	◐
High Sierra Group format	○	×
Apple HFS	◐	◐
Legend:		
×	Not supported, writing blocked	
●	Shadowed and fully supported; individual files are extracted and made available	
◐	Shadowed, partially supported; individual files are extracted and made available	
○	Shadowed, but individual files are not extracted	

Printed Content Shadowing

You can shadow content printed from all local and network printers in your environment that use the Microsoft Windows Print Spooler service.

Printers often handle sensitive documents and information, outputting them in a hard copy format that can be impossible to control. They can be left in a printer tray for anyone to see or intentionally carried out of the organization. You can monitor if endpoint users are printing unauthorised or undesirable documents and create an audit trail for compliance purposes by selecting the **Shadow settings** option when creating a Printer Device Class Policy or Device Collection Policy.

A Printer policy with shadowing enabled captures the `PRN` file sent to the printer. When a user prints a file, a Shadow copy is stored on the endpoint in `C:\Windows\sxdata\shadow` folder and renamed with the extension `.dat.final`. The file is then moved to `C:\ProgramData\Lumension\LEMSSAgent\logs` and uploaded to the Ivanti Endpoint Security Server to the location set in **Tools > Options > Device Control > Server shadow directory**.

You can view the contents of a `PRN` file by reprinting it or opening it in a print spooler file viewer application.

Viewing a shadowed print file

You can view a shadowed file sent from an endpoint to a printer by re-printing it or opening it in a utility for viewing print spooler files in formats appropriate for your printer.

Prerequisites:

You have selected a file from `<install_dir>\DeviceControl\Shadow`.

When shadowing is enabled for a printer, the `PRN` file used by the printer to generate the printout is saved and logged on the endpoint. Shadowing also provides enforcement for printing operations using the Print Spooler API, both for local and remote printers

Important: Only print jobs sent to printers that use the Microsoft Windows Print Spooler service are shadowed.

Option	Description
Printing a shadowed print file on a physical printer	<div><div><div>1. Open a command prompt.</div><div>2. Enter: <code>copy <filename.prn> /B \\<printer-server> \<printer-share-name></code></div></div><div><div>Note:</div><div><ul style="list-style-type: none"><printer-server> must be the name or address of the computer to which the printer is physically connected.You must print to the printer that shadowed the file, or a same model of printer, as the <code>PRN</code> file format is printer dependent.</div></div></div>
Opening a shadowed print file using a utility for viewing print spooler files in formats appropriate for your printer.	As the <code>PRN</code> file contains both the printout content and commands necessary to control the specific printer used, an external viewer is required. Download and install a viewer, then associate it with the <code>PRN</code> file extension.

Result: The contents of the shadowed print file are displayed and can be reviewed.



Working with Device Control Policies

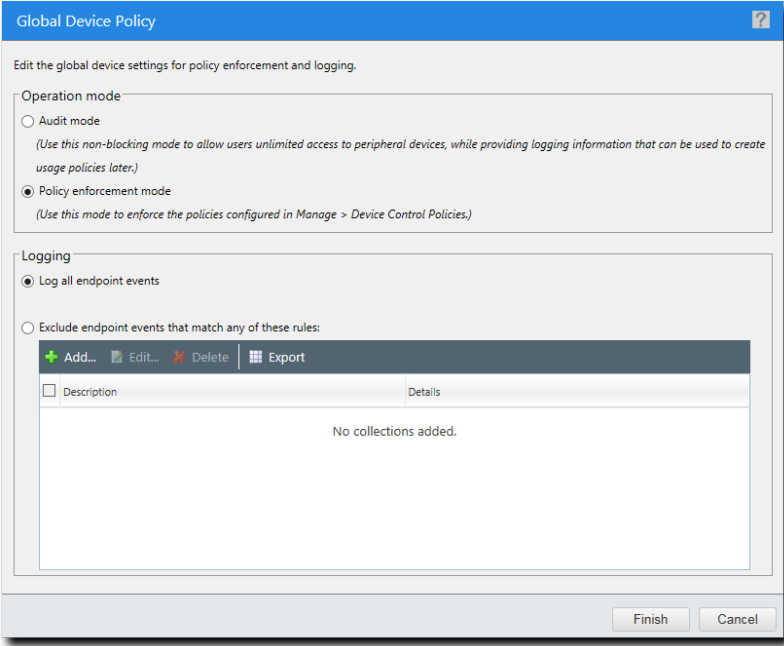
There are several procedures associated with creating and assigning policies to users and groups.

You can perform the following tasks from the **Device Control Policies** page:

- [Setting Global Device Policy](#) on page 135
- [Creating a Device Class Policy](#) on page 139
- [Creating a Device Collection Policy](#) on page 149
- [Creating a Media Collection Policy](#) on page 157
- [Creating a Port Control Policy](#) on page 160
- [Assigning a Policy](#) on page 163
- [Unassigning a Single Policy](#) on page 164
- [Unassigning Multiple Policies](#) on page 165
- [Editing a Policy](#) on page 166
- [Enabling Policies](#) on page 167
- [Disabling Policies](#) on page 167
- [Exporting Policies](#) on page 169
- [Creating Policies for a Group](#) on page 169
- [Creating Policies for Users](#) on page 170

The Global Device Policies Page

The **Global Device Policies** page enables you to manage the global device setting for policy enforcement and logging of all the devices connected to your network.



The screenshot shows a window titled "Global Device Policy" with a blue header bar. Below the header, there is a subtitle "Edit the global device settings for policy enforcement and logging." The window is divided into two main sections: "Operation mode" and "Logging".

Operation mode

- ☐ Audit mode
(Use this non-blocking mode to allow users unlimited access to peripheral devices, while providing logging information that can be used to create usage policies later.)
- ☒ Policy enforcement mode
(Use this mode to enforce the policies configured in Manage > Device Control Policies.)

Logging

- ☒ Log all endpoint events
- ☐ Exclude endpoint events that match any of these rules:

Below the "Exclude endpoint events" option, there is a toolbar with four buttons: "Add..." (green plus icon), "Edit..." (green pencil icon), "Delete" (red X icon), and "Export" (blue grid icon). Below the toolbar is a table with two columns: "Description" and "Details". The table is currently empty, and the text "No collections added." is displayed in the center.

At the bottom right of the window, there are two buttons: "Finish" and "Cancel".

Figure 52: Global Device Policy Page

Setting Global Device Policy

The global device policy applies to all the devices on your network.

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

Step Result: The *Device Control Policies* page opens.

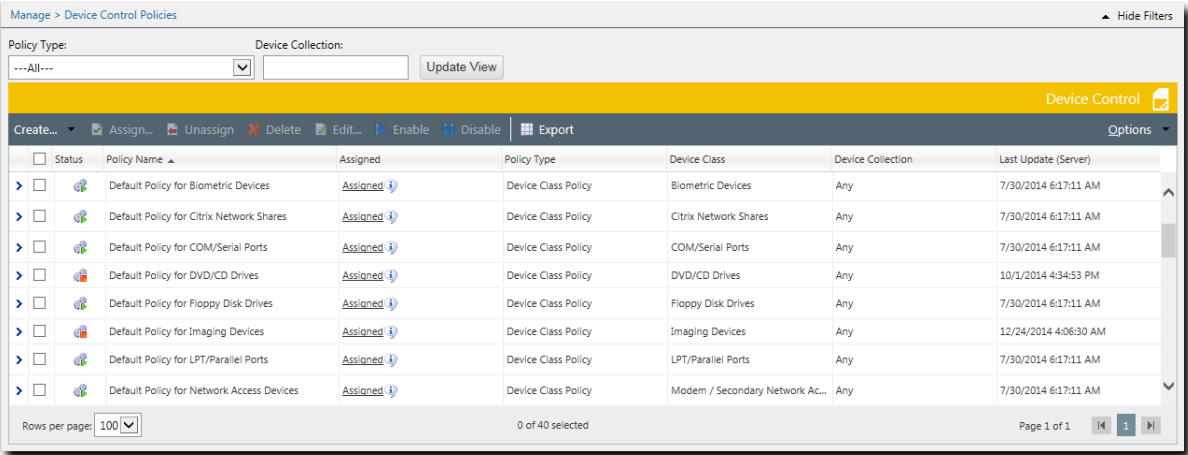


Figure 53: Device Control Policies

- 2. Select the **Device Control Global Policy**.

3. Click **Edit**.

Step Result: The **Global Device Policy** dialog opens.

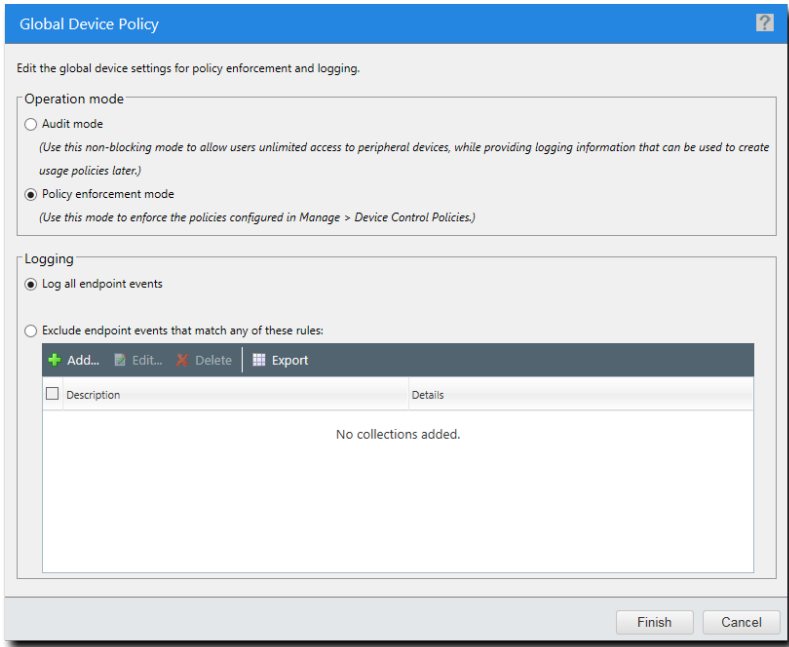


Figure 54: Global Device Policy

4. Set the Operation Mode:

Option	Description
Audit mode	Non-blocking mode that allows users unlimited access to peripheral devices, while providing logging information that can be used to create usage policies later.
Policy enforcement mode	Enforces the policies configured in Manage > Device Control Policies .

5. Set the Logging:

Option	Description
Log all endpoint events	Every event is logged and can be viewed using a Device Event Log Query. For more information, see Working with Device Event Log Queries on page 175.

Option	Description
Exclude endpoint events that match any of these rules.	Add edit rules for filtering out events that match specific criteria. For more information about how to create rules, see Device Event Filtering Rules on page 137.

6. On the **Global Device Policy** dialog, click **OK**.

Result: The new Global Device Policy settings are saved and effective immediately.

Device Event Filtering Rules

When creating or editing a Global Device Policy, you can configure the policy to exclude certain endpoint events so that the logs don't consume excessive disk space.

Purpose and Best Practices

By default, Global Device Policies records all Device Control events to a log. These logs can consume excessive server disk space if left unattended. To prevent log overconsumption, you can exclude trivial events using *Device Event Filtering Rules*. These rules identify different Device Control events that contain data and values that you define. These events are not recorded in the future. Disk space consumption is reduced and Device Event Log Queries are truncated.

Generally, you should filter events from a Global Device Policy when they occur repeatedly. Remember, when reviewing log queries, you're looking for exceptional events, not common ones. If you see a common pattern, filter it out.

Note:

- **Device Event Filtering Rules** can only be added to the **Device Control Global Policy**; you cannot add these exclusions to any other policy.
- After configuring **Device Event Filtering Rules**, they are not applied to **Device Event Log Queries** retroactively.

Rule Descriptions and Buttons

While working with Device Event Filtering Rules, you can add as many filters as you'd like to reduce the amount of data that the Global Device Policy captures.

- When you begin creating a Device Event Filtering Rule, type a **Rule description**. This is the text you'll use to identify the rule from the **Global Device Policy** dialog.
- To add a new filter, click **Add**, and then select from the drop-down lists to define [rule filter criteria](#).
- To remove an old filter, select it and click **Delete**.
- When you're done adding or deleting filters, click **OK** to accept changes and close the dialog.

Rule Filter Criteria

Column	Description
Field ¹	<p>The types of data available for use in filter rules. Field drop-downs include:</p> <ul style="list-style-type: none"> • File Name: Excludes Device Control events based on their file name. • Event Type: Excludes events based on their type. • Device Name: Excludes events based on the device name. • Device Type: Excludes events based on a device class. • File Size: Excludes Device Control events that impact files of a defined size. • Log Entry (Agent Local): Excludes events based on the time that it occurred on the endpoint. • Endpoint Name: Excludes events based on the endpoint name. • Message: Excludes events based on attached custom messages. • Model ID: Excludes events based on a device model's ID. • NT User: Excludes events based on the user account logged in during the event. • Path: Excludes events based on a file path (which may or may not include the file itself). • Process Name: Excludes events based on process names that appear within Windows Task Manager. • Reason: Excludes events based on a reason. • Unique ID: Excludes events based on a device's unique ID. • User SID: Excludes events based on a user's Security Identifier in Windows. • Log Entry (UTC): Excludes events based on the time it occurred on the server.

Column	Description
Operator	<p>The types of operators that can be used to exclude events. Operators include:</p> <ul style="list-style-type: none"> • = : Filters the selected field to exclude the exact value defined. • ≠ : Filters the selected field to exclude any value that is <i>not</i> defined. • Contains: Filters the selected field to exclude any event containing the value that's defined. • Does Not Contain: Filters the selected field to exclude any event that does <i>not</i> contain the value that's defined. • Starts With: Filters the selected field to exclude events starting with the value that's defined. • Ends With: Filters the selected field to exclude events that end with the values that's defined. • Regular Expression Matches: Filters the selected field to exclude events that match a regular expression. • Regular Expr. Doesn't Match: Filters the selected field to exclude events that do <i>not</i> match a regular expression.
Value ¹	A numerical value or character string to be used with the field and operator.

Tip:

1. To see examples of filter **Field** text or **Value** syntax, see **Review > Device Event Log Queries** and then view a **Completed** query.

Creating a Device Class Policy

Device class policies are policies that apply to an entire device class.

Prerequisites:

You must have **Manage Global Device Control Policies** access rights.

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

Step Result: The *Device Control Policies* page opens.

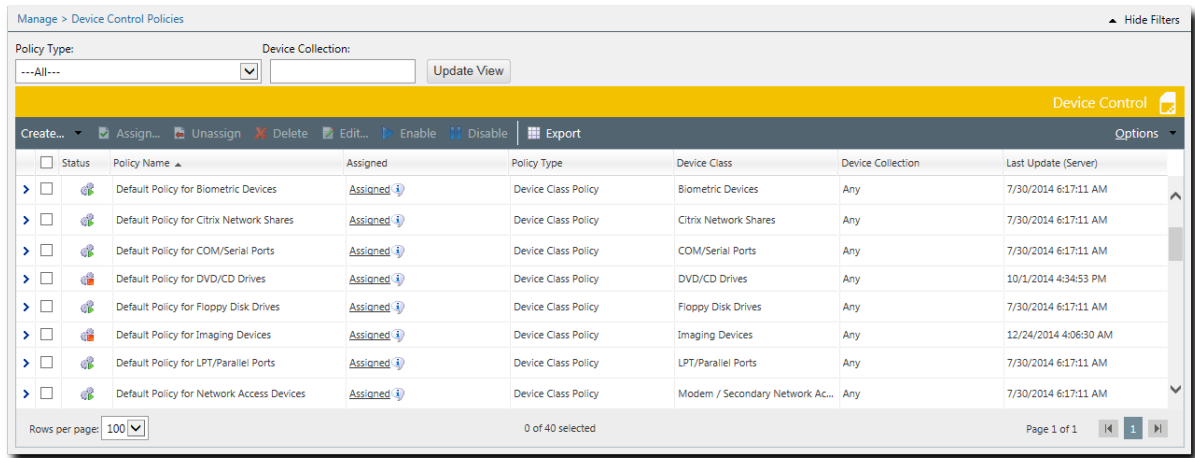


Figure 55: Device Control Policies Page

2. Click **Create > Create class policy**.

Step Result: The *Device Class Policy* wizard appears.

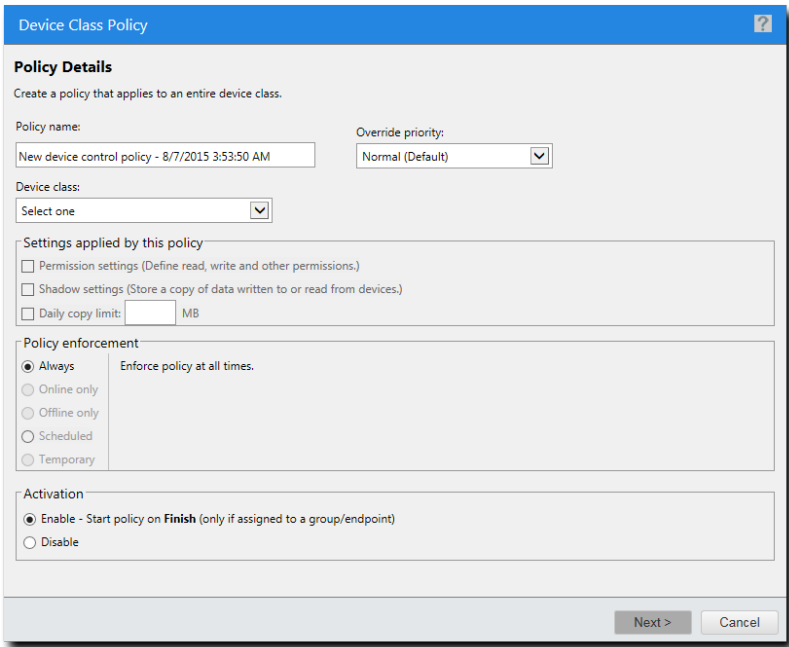


Figure 56: Device Class Policy Wizard

3. Specify the policy details.

- a) Enter the **Policy name**.
- b) Select the **Override priority**.

You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.

- c) Select the **Device class** to which the policy will apply.

4. Specify the policy rules.

Option	Description
Permission settings (Define read, write and other permissions.)	Enables the Permission Settings panel later in the wizard, where you can define which permissions users will have based on this policy.
Shadow settings (Store a copy of data written to or read from devices.)	<p>Enables the Shadow Settings panel later in the wizard.</p> <p>File shadowing lets you to track the data that is being read, written to, or written from a device. It can be enabled for:</p> <ul style="list-style-type: none"> • COM/Serial Ports • DVD/CD Drives • Floppy Disk Drives • LPT/Parallel Ports • Modem / Secondary Network Access Device • Portable Devices • Printers • Removable Storage Devices <p>For Printers specifically, shadowing involves storing a copy of all information sent to a printer during a print job governed by this policy. This information can later be viewed administratively via log queries by sending the same content to the same printer or another printer of the same model.</p> <p>See File Shadowing on page 129 for more information.</p>
Daily copy limit	<p>Sets the amount of data (in MB) per day that a user can copy.</p> <ul style="list-style-type: none"> • Floppy Disk Drives • Portable Devices • Removable Storage Devices <p>Note: Only one copy limit setting per device class will be enforced. For example, copy limits configured for removable storage devices apply to hard drives and non-hard drives. To avoid ambiguity, it is recommended that you do not combine copy limit policies and permissions policies.</p>

5. Select the desired policy enforcement option.

Option	Description
Always	The policy applies at all times.
Online only	The policy applies only when the endpoint/user/group is connected to the server.
Offline only	The policy applies only when the endpoint/user/group is disconnected from the server.
Scheduled	The policy applies only during a set schedule.
Temporary	The policy allows one-time access for a specified period.

Depending on the option you choose, additional settings are available in the right-side box.

6. Select whether you want the policy to be applicable immediately.

Option	Description
Enable	Activates the policy immediately when you finish configuring it. (default)
Disable	Lets you to delay when the policy takes effect. You can activate the policy later on the Manage > Device Control Policies page by selecting it and clicking Enable .

7. Click **Next**.

Step Result: If you selected **Permission settings** on the **Policy Details** panel, the **Permission Settings** panel displays.

Device Class Policy

Permission Settings

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:

Block all access on All connections for hard and non hard drives with self contained encryption,unencrypted/unknown encryption type.

< Back

Next >

Cancel

Figure 57: Permission Settings

8. [Optional] Specify the permission users will have based on this policy.

Option	Description
Block all access	Restricts the use of all devices of this class to prevent information from getting out.

Option	Description
Allow the following permissions	<p>Select the types of permissions to allow. Available permissions (dependent on the type of device):</p> <ul style="list-style-type: none"> • Read • Write • FireWire • ATA/IDE • SCSI • PCMCIA • Bluetooth • IrDA <p>See Permission Settings for a Policy on page 122 for more information.</p>

9. Select the Connections to which the permissions are to apply.

Dependent on the type of device class policy you are creating, the available connections are:

- All
- USB
- FireWire
- ATA/IDE
- SCSI
- PCMCIA
- Bluetooth
- IrDA

10. If you are creating a Removable Storage Devices device class policy, select the type of Drives to which the permissions are to apply.

Option	Description
Both drive types	Permissions are applied to both hard drives and non-hard drives.
Hard drives only	Permissions are only applied to hard disk drive (HDD) drives.
Non hard drives only	Permissions are only applied to non hard disk drives, for example solid-state drives (SSD).

- 11.[Optional] If you are creating a Removeable Storage Devices or DVD/CD Drives device class policy, select the type of Encryption to which the permissions are to apply.

Option	Description
Self contained encryption	Encryption is self-contained on the device, allowing only those with an encryption key to access the information.
Unencrypted/Unknown encryption type	Information is either unencrypted or encrypted with an unknown type of encryption.

- 12.Review the phrase in the **Rule definition** section to ensure you have selected the permissions and connections you want.

- 13.Click **Next**.

Step Result: If you selected **File Filters** on the **Policy Details** panel, the **File Filters** panel displays.

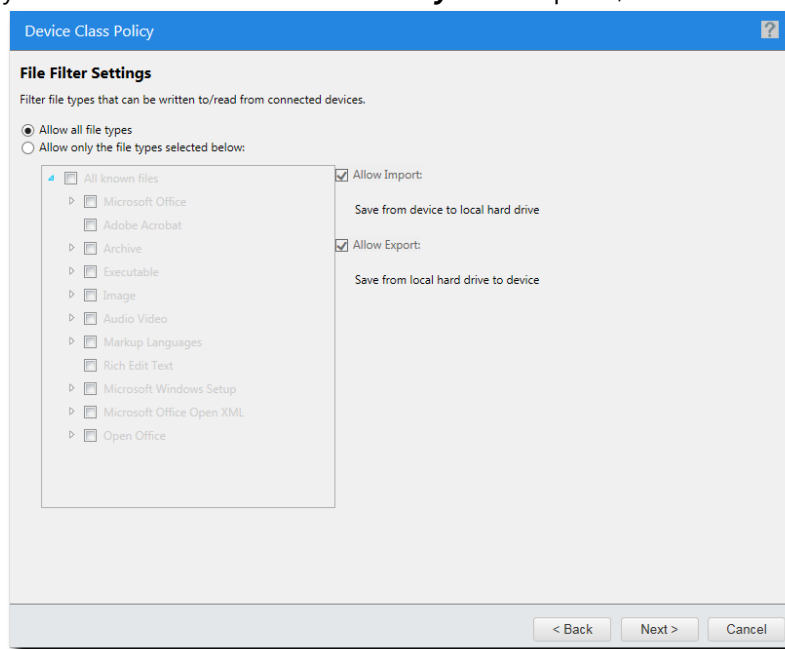


Figure 58: File Filters

- 14.Specify the file filtering options.

Option	Description
Allow all file types	All files types can be accessed.

Option	Description
Allow only the file types selected below	Only file types you select from a list can be accessed.
Allow Import	User can copy files from the external device to the local hard drive.
Allow Export	User can copy files from the local hard drive to the external device.

For more information on file filters, see [File Type Filtering](#) on page 125.

15. Click **Next**.

Step Result: If you selected **Shadow settings** on the **Policy Details** panel, the **Shadow Settings** panel displays.

16.Specify the shadow settings.

Shadow files are stored in <install_dir>\DeviceControl\Shadow.

Device Class Policy Type	Options	
<ul style="list-style-type: none">• COM/Serial Ports• DVD/CD Drives• Floppy Disk Drives• LPT/Parallel Ports• Modem / Secondary Network Access Device• Portable Devices• Removable Storage Devices	For both the Read and Write sections:	
	Do not shadow	No content is shadowed.
	Full file content	Saves a copy of the entire file.
	File name only	Records only the file name.
Printers	Do not shadow printed content	This setting can be used to prevent shadowing for specific assignment targets. For example, if you shadow printed content for a specific AD Group you can prevent shadowing for a specific user within that group by selecting this setting and assigning the policy to that user.
	Shadow printed content	This setting is used to store a copy of all information sent to a printer during a print job governed by this policy. This information

- 17.Review the phrase in the **Rule definition** section to ensure you have selected the shadow settings you want.
- 18.Click **Next**.

Step Result: The ***Assign policy*** page opens.

Note: This page is skipped when the wizard is launched from the ***Groups, Endpoints, or Users*** page of the **Manage** menu.

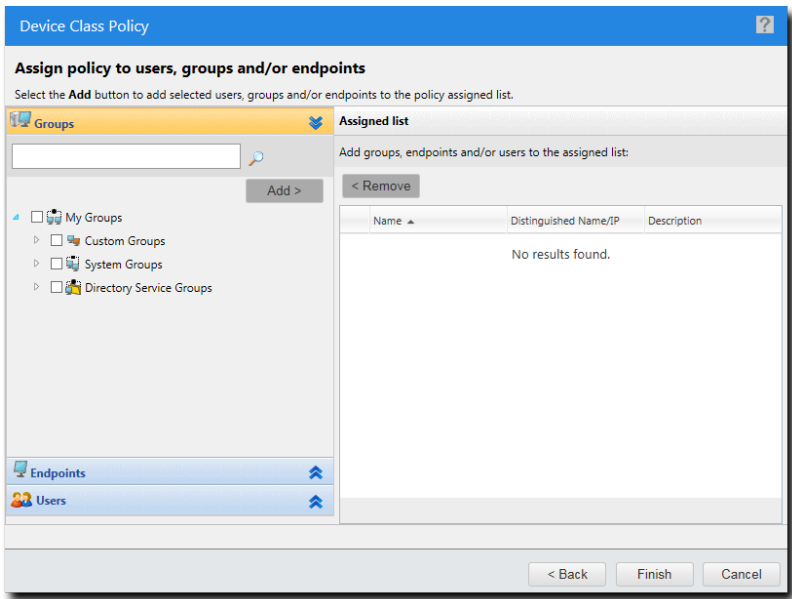


Figure 59: Assign Policy

- 19.Select the group, endpoint, or user to which the policy applies.

Option	Description
To add groups of endpoints	<div>1. Select a group or groups from the Groups list.</div> <div>2. Click Add.</div>
To add individual endpoints	<div>1. Select an endpoint or endpoints from the Endpoints list.</div> <div>2. Click Add.</div>
To add individual users or user groups	<div>1. Select users or usergroups from the Users list.</div> <div>2. Click Add.</div>
To remove groups of endpoints	<div>1. Select a group or groups from the Groups list.</div> <div>2. Click Remove.</div>

Option	Description
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

20. Click **Finish**.

Step Result: The **Device Class Policy** wizard closes.

Result: A new policy is created for the selected device class. The policy is displayed in the **Device Control Policies** page.

Creating a Device Collection Policy

Device collection policies allow you to define access rights for specific devices rather than an entire device class. Use the **Device Collection Policy** wizard to create policies for device collections.

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

Step Result: The **Device Control Policies** page opens.

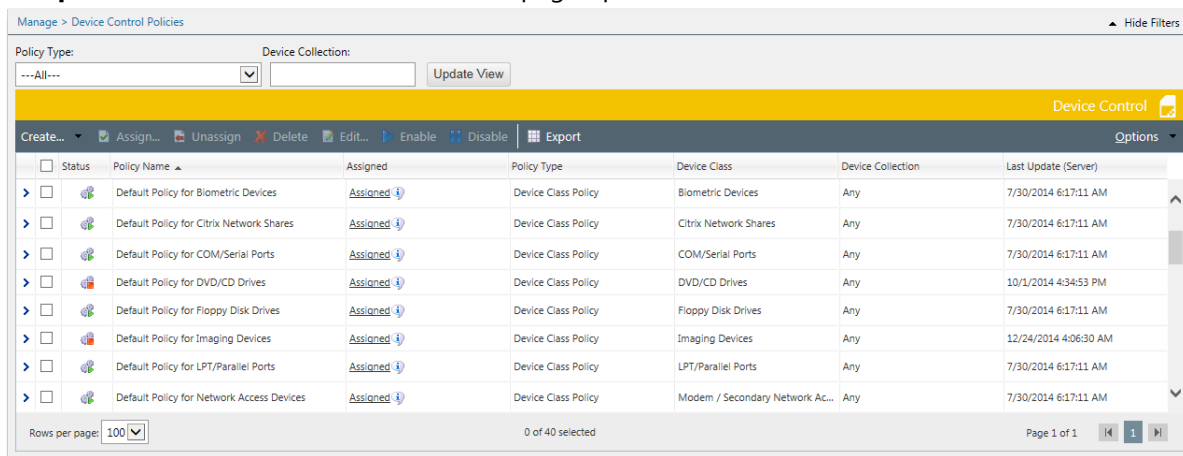
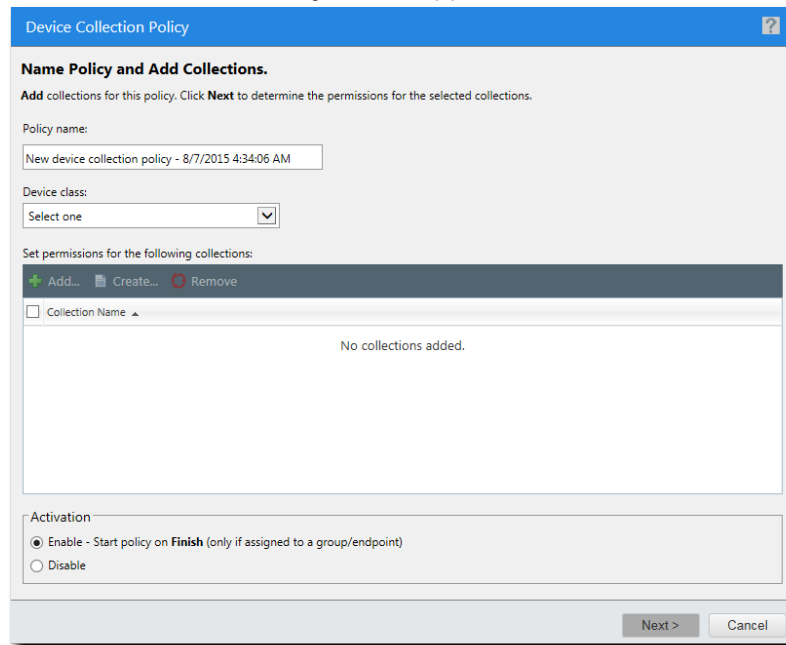


Figure 60: Device Control Policies Page

2. Click **Create > Device collection policy**.

Step Result: The **Device Collection Policy** wizard appears.



The screenshot shows the 'Device Collection Policy' wizard window. The title bar is blue with a question mark icon. The main content area is titled 'Name Policy and Add Collections.' and contains the following elements:

- A sub-header: 'Add collections for this policy. Click **Next** to determine the permissions for the selected collections.'
- A 'Policy name:' label followed by a text input field containing 'New device collection policy - 8/7/2015 4:34:06 AM'.
- A 'Device class:' label followed by a dropdown menu showing 'Select one'.
- A section titled 'Set permissions for the following collections:' with three buttons: '+ Add...', 'Create...', and 'Remove'.
- A table with one column header 'Collection Name' and a sub-header 'Collection Name'. The table is currently empty, displaying 'No collections added.'
- An 'Activation' section with two radio buttons: 'Enable - Start policy on **Finish** (only if assigned to a group/endpoint)' (which is selected) and 'Disable'.
- At the bottom right, there are 'Next >' and 'Cancel' buttons.

Figure 61: Device Collection Policy Wizard

3. Type a name for the policy in the **Policy Name** field.

4. Select the class to which the policy will apply from the **Device class** drop-down list.

Step Result: The device collection section becomes active.

Note: You can either add an existing collection or create a new one.

5. [Optional] To add an existing collection:

- a) Click **Add**.

Step Result: The **Add Collections from Library** dialog opens.

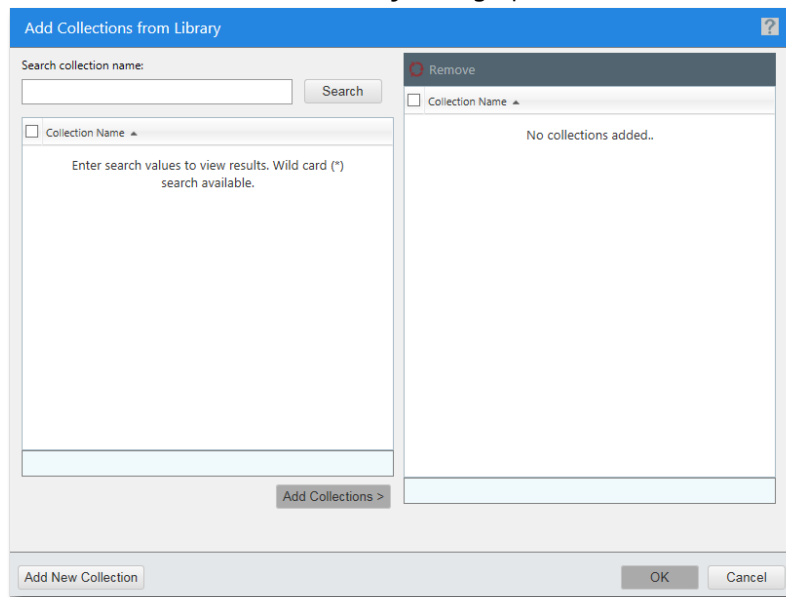


Figure 62: Add Collections from Library

- b) Type a collection name in the **Search collection name** field and click **Search**.

Step Result: A list of collections is displayed.

- c) Select the collection you want to add.
 d) Click **Add Collections**.
 e) Click **OK**.

Step Result: The **Add Collections from Library** dialog closes.

- f) [Optional] Select the **Disable** option to delay the activation of the policy.
 By default, the **Enable** option is selected, which activates the policy immediately upon completing the creation process.

6. [Optional] To create a new collection:

- a) Click **Add New Collection**.

Step Result: The **New Collection** dialog displays.

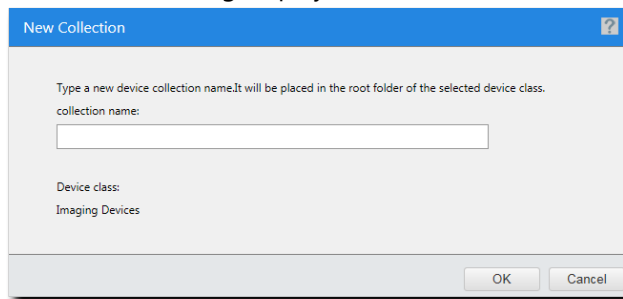


Figure 63: New Collection

- b) Type the name of the collection in the **Collection name** field.

- c) Click **OK**.

Step Result: The **New Collection** dialog and the collection appears in the collections list.

7. Click **Next**.

Step Result: The **Device Collection Policy** dialog opens.

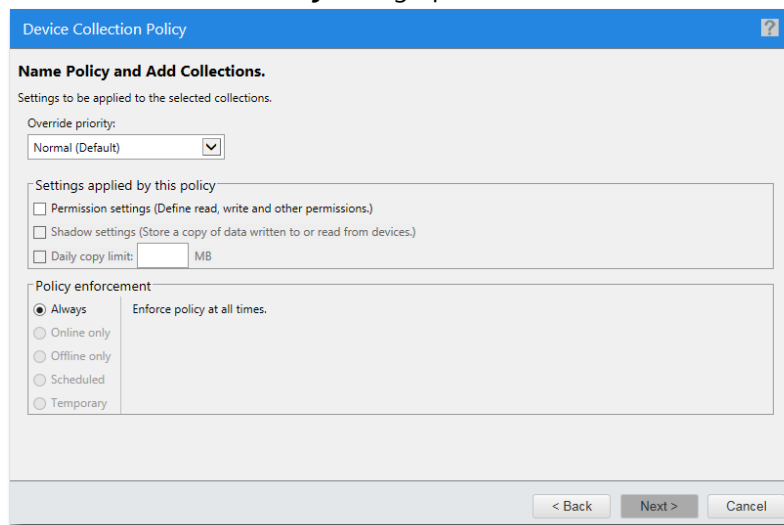


Figure 64: Policy Rules

8. [Optional] Select the **Permission settings** check box to define read, write, and other permissions.

9. [Optional] Select the **Shadow settings** check box to define read, write, and other permissions. Shadow settings can only be enabled for the COM/Serial Ports, CD/DVD Drives, Floppy Disk Drives, LPT/Parallel Ports, and Removable Storage Devices classes.
- 10.[Optional] Select the **Daily copy limit** check box. Specify a copy limit value in the text box.
- 11.Select the desired policy enforcement option. You can choose from the following options:

Option	Description
Always	The policy will apply at all times.
Online only	The policy will apply only when the endpoint/user/group is connected to the server.
Offline only	The policy will apply only when the endpoint/user/group is disconnected from the server.
Scheduled	<p>The policy will apply only during a set schedule. To set the schedule:</p> <ol style="list-style-type: none"> 1. Enter the start time in the From field. 2. Enter the end time in the To field. 3. Select the checkboxes for the days of the week in which the policy will be applied.
Temporary	<p>The policy will give one-time access for a specified period. To specify the enforcement period:</p> <ol style="list-style-type: none"> 1. Select the Immediately option to begin enforcing the policy upon completion of the policy creation process. 2. Select the date and time option and enter a date (mm/dd/yyyy format) and a time (hh:mm AM/PM format) to designate an enforcement start time in the future. 3. Enter a date (mm/dd/yyyy format) and a time (hh:mm AM/PM format) to designate an enforcement end time in the future.

Note: You can click on the clock icon to view and select a list of times in half hour increments and the calendar icon to view and select dates using a calendar.

12. Click Next.

Step Result: The **Permission Settings** page opens.

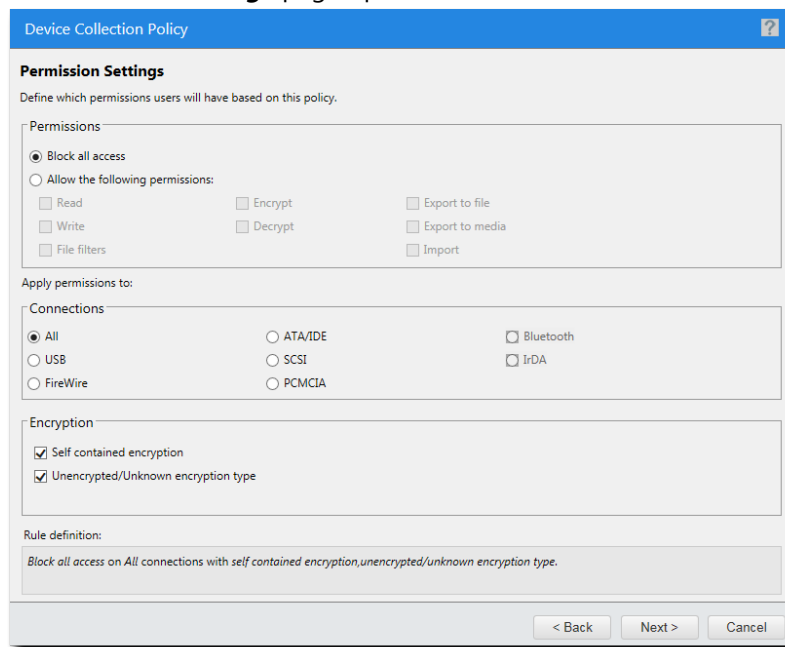


Figure 65: Permission Settings

13. Specify the permission details.

For more information on setting permissions, refer to [Permission Settings for a Policy](#) on page 122.

- Select the **Allow access with following** radio button and then select the desired permissions check boxes. The available permissions vary according to device class.
- Select the connections you want to apply the permissions to in the **Connections** group box. The available connections vary according to device class.
- Select the applicable drives in the **Drives** group box. The availability of drives varies according to device class.
- [Optional] Specify the type of encryption in the **Encryption** group box. The availability of encryption options varies according to device class.

14. Click **Next**.

Step Result: The **File Filters** page opens.

Note: This page will only appear if you select **File Filters** in the **Permission Settings** page.

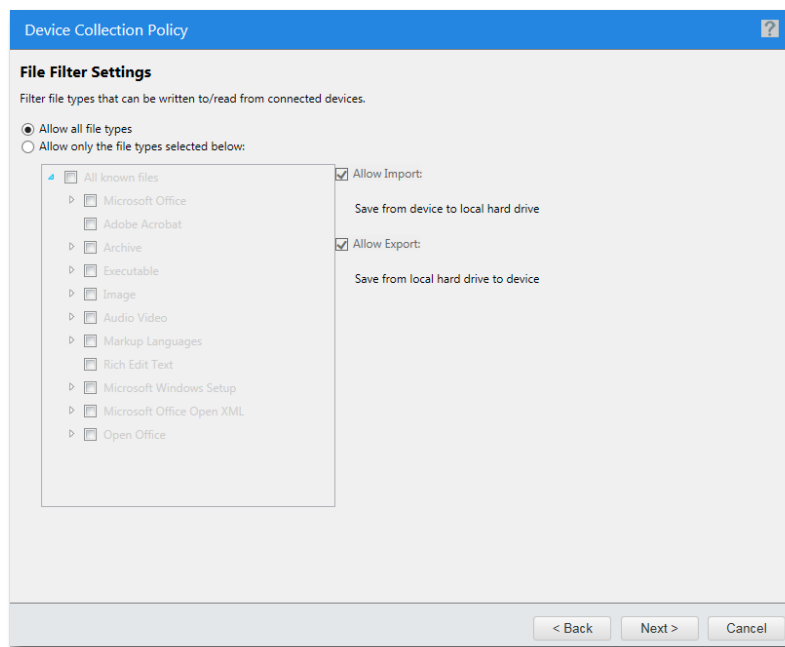


Figure 66: File Filters

15. Specify the file filtering options.

For more information on file filters, see [File Type Filtering](#) on page 125.

16. Click **Next**.

Step Result: The **Shadow Settings** page opens.

Note: This page will only appear if you select **Shadow settings** in the **Policy details** page.

17.Specify the shadow settings.

Shadow files are stored in <install_dir>\DeviceControl\Shadow.

Device Class Policy Type	Options	
<ul style="list-style-type: none">COM/Serial PortsDVD/CD DrivesFloppy Disk DrivesLPT/Parallel PortsModem / Secondary Network Access DevicePortable DevicesRemovable Storage Devices	For both the Read and Write sections:	
	Do not shadow	No content is shadowed.
	Full file content	Saves a copy of the entire file.
	File name only	Records only the file name.
Printers	Do not shadow printed content	This setting can be used to prevent shadowing for specific assignment targets. For example, if you shadow printed content for a specific AD Group you can prevent shadowing for a specific user within that group by selecting this setting and assigning the policy to that user.
	Shadow printed content	This setting is used to store a copy of all information sent to a printer during a print job governed by this policy. This information



18. Click **Next**.

Step Result: The **Assign policy** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

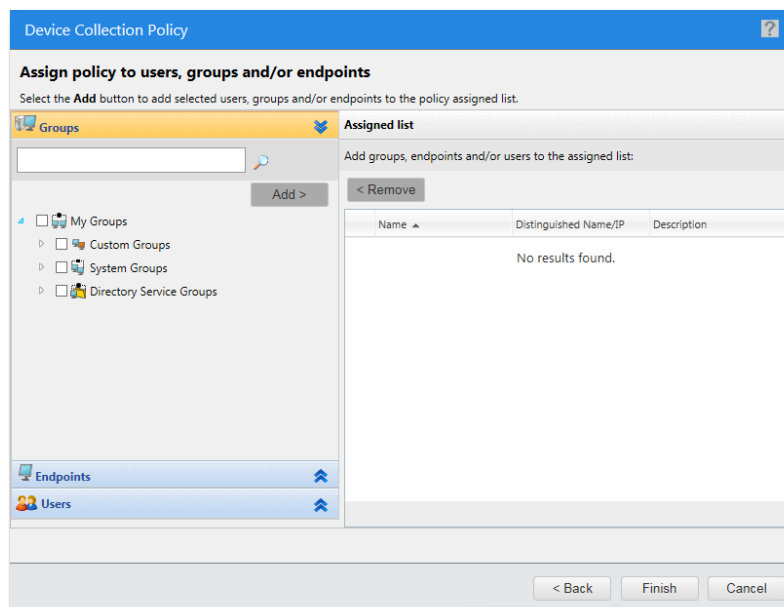


Figure 67: Assign Policy

19. Select the group, endpoint, or user the policy will apply to.

20. Click **Finish**.

Step Result: The **Device Collection Policy** wizard closes.

Result: A new policy is created for the selected device collection. The policy is displayed in the **Device Control Policies** page.

Creating a Media Collection Policy

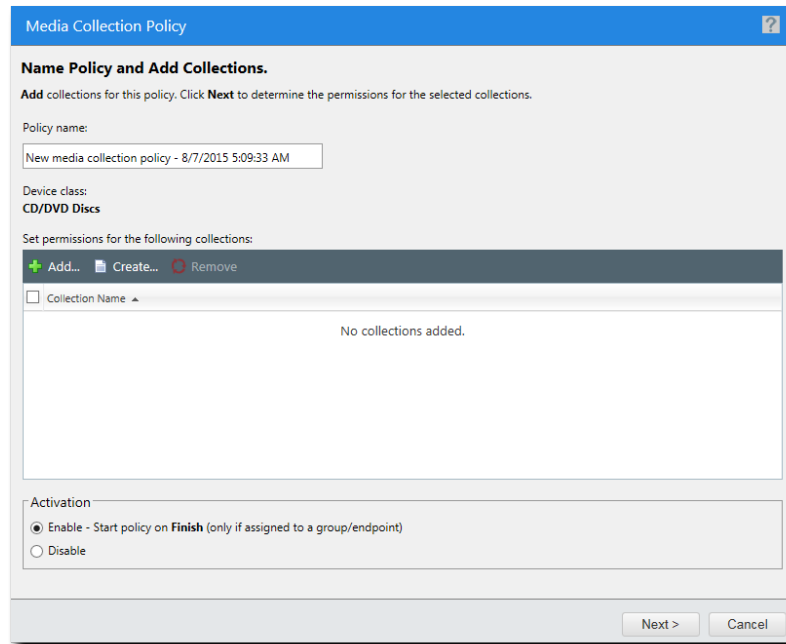
Media collection policies are policies created to grant permissions to media collections in the Device Library.

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

Step Result: The **Device Control Policies** page opens.

2. Click **Create > Create media collection policy**.

Step Result: The **Media Collection Policy** wizard appears.



The screenshot shows the 'Media Collection Policy' wizard window. The title bar is blue with a question mark icon. The main content area is titled 'Name Policy and Add Collections.' and contains the following elements:

- A sub-header: 'Add collections for this policy. Click **Next** to determine the permissions for the selected collections.'
- A 'Policy name:' label followed by a text box containing 'New media collection policy - 8/7/2015 5:09:33 AM'.
- A 'Device class:' label followed by the text 'CD/DVD Discs'.
- A label 'Set permissions for the following collections:' followed by a toolbar with three buttons: 'Add...' (green plus icon), 'Create...' (blue document icon), and 'Remove' (red minus icon).
- A table with one column header 'Collection Name' and a sub-header 'Collection Name ▲'. The table body is empty, displaying the text 'No collections added.'
- An 'Activation' section with two radio buttons: 'Enable - Start policy on **Finish** (only if assigned to a group/endpoint)' (selected) and 'Disable'.
- At the bottom right, there are 'Next >' and 'Cancel' buttons.

Figure 68: Media Collection Policy Wizard

3. Type the **Policy name**.

4. To add an existing collection, click **Add**.

Step Result: The **Add Collections from Library** dialog opens.

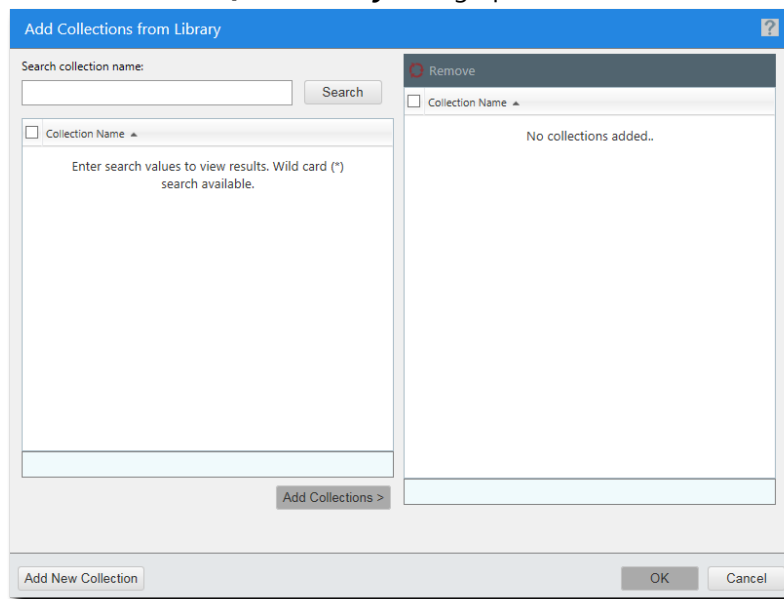


Figure 69: Add Collections from Library

5. Type a collection name in the **Search collection name** field.

6. Click **Search**.

Step Result: A list of collections is displayed.

7. Select the collection you want to add.

8. Click **Add Collections**.

Step Result: The selected collection is added to the right side of the dialog.

9. Click **OK**.

Step Result: The **Add Collections from Library** dialog closes.

10. Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default. If you do not want the policy to be auto-enabled, select **Disable**.

Note: You must manually select enable before the policy will be applicable.

11. Click Next.

Step Result: The **Assign policy** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

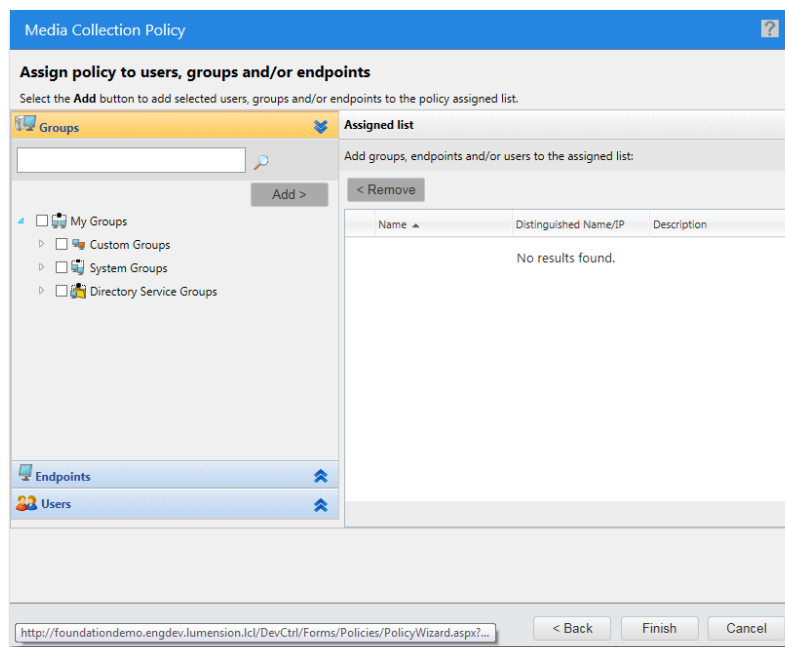


Figure 70: Assign Policy

12. Select the group, endpoint, or user the policy will apply to.**13. Click Finish.**

Result: A new policy is created for the selected media collection. The policy is displayed in the **Device Control Policies** page.

Creating a Port Control Policy

Define permissions for all or specific port connections, such as USB, FireWire, and Bluetooth, which are enforced at all times.

1. Select Manage > Device Control Policies.

Step Result: The **Device Control Policies** page opens.

2. Click **Create > Port control policy**.

Step Result: The **Port control policy** wizard appears.

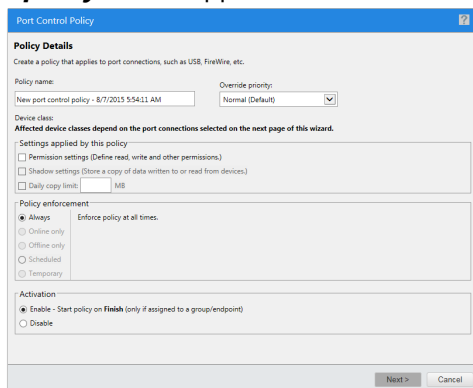


Figure 71: Port Control Policy Wizard

3. Type the **Policy name**.

Use a name that reflects the organizational or functional need the policy fulfills (for example, Users with USB restrictions)

4. Select the **Override priority**.

You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.

5. Select the **Permission settings** check box.

6. Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default. If you want to delay when the policy will begin working, select **Disable**.

7. Click **Next**.

Step Result: The **Permission Settings** page opens.

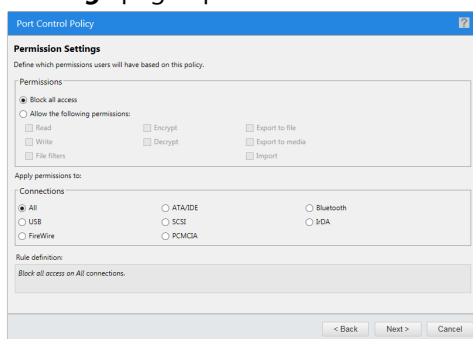


Figure 72: Port Control Policy Wizard

8. In the **Permissions** section, select the permissions you want to associate with the policy:
- Block all access
 - Allow the following permissions: select **Read** and **Write**
9. In the **Apply Permissions to** section, select the connections you want to associate with the permissions:
- All
 - USB
 - FireWire
 - ATA/IDE
 - SCSI
 - PCMCIA
 - Bluetooth
 - IrDA
10. Click **Next**.

Step Result: The **Assign policy to users, groups and/or endpoints** page opens.

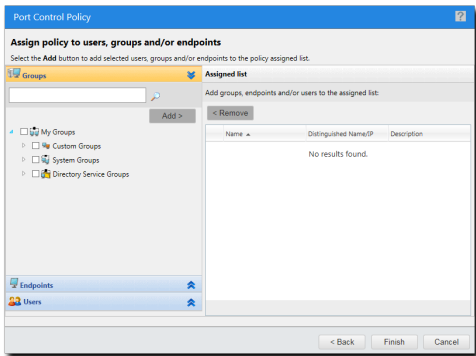


Figure 73: Port Control Policy Wizard

11. Select the group, endpoint, or user to which the policy applies.

Option	Description
To add groups of endpoints:	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Add.
To add individual endpoints:	<ol style="list-style-type: none">1. Select an endpoint or endpoints from the Endpoints list.2. Click Add.
To add individual users or user groups:	<ol style="list-style-type: none">1. Select users or usergroups from the Users list.2. Click Add.

Option	Description
To remove groups of endpoints:	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Remove.
To remove individual endpoints:	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups:	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

12. Click **Finish**.

Step Result: The **Port Control Policy** wizard closes.

Result: A new policy is created for the selected ports. The policy is displayed in the **Device Control Policies** page.

Assigning a Policy

The **Assign Policy** page of the policy creation wizard allows you to assign the policies to one or more users, user groups, endpoints, or endpoint groups. If the policy is launched from the **Groups**, **Endpoints**, or **Users** pages, it is assigned automatically.

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

Step Result: The **Device Control Policies** page opens.

2. Select the policy you want to assign.

3. Click **Assign**.

Step Result: The **Assign policy** dialog for the selected policy type opens.

4. Click the tab corresponding to the parent category of the user or endpoint you want to assign. You can choose from the following options:

- **Groups**
- **Endpoints**
- **Users**

Step Result: The selected parent category expands.

5. Select the desired individual or group.

6. Click **Add**.

Step Result: The selected item appears in the **Assigned list**.

7. [Optional] Remove any previously assigned items.
 - a) Select the item you want to remove from the **Assigned list**.
 - b) Click **Remove**.

Step Result: The item is removed from the **Assigned list**.

8. Click **OK**.

Step Result: The **Assign policy** dialog closes.

Result: The policy is assigned to the selected group, user, or endpoint. The **Device Control Policies** page is automatically refreshed to show the updated assignment status.

Assigning a Device Control Policy on an Endpoint

You can assign one or more Device Control policies on an endpoint's **Details** page.

1. Select **Manage > Endpoints**.
2. Click the hyperlinked name of the desired endpoint.

Step Result: The endpoint's **Details** page opens to the Information tab.

3. Click the **Device Control Policies** tab.

Step Result: The **Device Control Policies** tab opens, displaying any policies that are currently assigned to the endpoint.

4. Click **Assign**.

Step Result: The **Assign Policy** dialog opens.

5. Select one or more policies to assign to the endpoint.

6. Click **OK**.

Step Result: The dialog closes and the policy is added to the list on the **Device Control Policies** tab.

Result: One or more Device Control policies have been assigned to the endpoint.

Unassigning a Single Policy

Unassigning policies require users to have **Assign Global Device Control Policies** access rights. You can unassign a policy only if it has been previously assigned to a group, user, or endpoint.

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

Step Result: The **Device Control Policies** page opens.

2. Select the policy you want to unassign.
Verify that the selected policy assignment status is **Assigned**.

Step Result: The **Unassign** button becomes active.

3. Click **Unassign**.

Step Result: The **Unassign Policy** dialog opens.

4. Click **OK**.

Step Result: The **Unassign Policy** dialog closes.

Result: The selected policy is unassigned. The **Device Control Policies** page is automatically refreshed to show the updated policy assignment status.

Unassigning Multiple Policies

Unassigning multiple policies allows you to simultaneously dissociate policies from their assigned users, endpoints, or group. Policies that are unassigned can subsequently be assigned to other users, endpoints, or groups.

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

Step Result: The **Device Control Policies** page opens.

2. Select the policies you want to unassign.
Verify that the assignment status for the selected policies is **Assigned**.

Step Result: The **Unassign** button becomes active.

3. Click **Unassign**.

Step Result: The **Unassign Policy** dialog opens.

Tip: Click the arrow next to a policy name in the dialog, to view more details about that policy.

4. Click **Yes**.

Step Result: The **Unassign Policy** dialog closes.

Result: The selected policies are unassigned. The **Device Control Policies** page is automatically refreshed to show the updated policy assignment status.

Editing a Policy

You can edit a policy as desired. While editing a policy, you can define permissions, specify shadowing and logging options, change assigned users and endpoints, and so on.

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

Step Result: The ***Device Control Policies*** page opens.

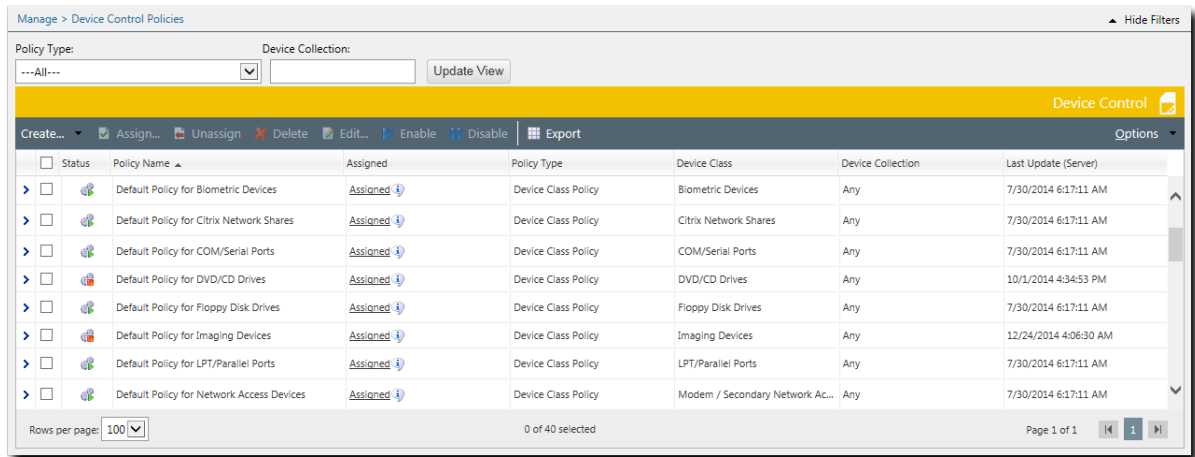


Figure 74: Device Control Policies

2. Select the policy you want to edit.

Tip: Filter the **Policy Name** and **Device Class** or **Device Collection** columns to locate the policies.

3. Click **Edit**.

Step Result: The ***Policy Wizard*** dialog opens.

Note: The policy wizard that opens will depend on the type of policy you are editing.

4. Edit the policy details as desired.

5. Click **Finish**.

Step Result: The ***Policy Wizard*** dialog closes.

Result: The selected policy is edited.

Enabling Policies

You can enable policies that are currently disabled. You can only enable those policies that are already assigned to users, endpoints, or groups.

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

Step Result: The ***Device Control Policies*** page opens.

2. Select the policy or policies you want to enable.

Tip: Filter the **Policy Name** and **Device Class** or **Device Collection** columns to locate the policies.

3. Click **Enable**.

Step Result: The ***Enable Policy*** dialog opens.

4. Click **Yes**.

Step Result: The ***Enable Policy*** dialog closes.

Result: The selected policies are enabled.

Disabling Policies

You can disable policies without deleting them. This allows you to retain policy details if you want to enable policies again.

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

Step Result: The ***Device Control Policies*** page opens.

2. Select the policy or policies you want to disable.

Tip: Filter the **Policy Name** and **Device Class** or **Device Collection** columns to locate the policies.

3. Click **Disable**.

Step Result: The ***Disable Policy*** dialog opens.

4. Click **Yes**.

Step Result: The ***Disable Policy*** dialog closes.

Result: The selected policies are disabled.

Deleting a Policy

You can delete a policy if you no longer require it. Any previously-created policy can be deleted as long as it is not assigned to an endpoint, user, or group.

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

Step Result: The **Device Control Policies** page opens.

2. Select the policy you want to delete.

Note: Ensure that the policy you are deleting is in an **Unassigned** state. If you try to delete an assigned policy, you will receive an error message.

3. Click **Delete**.

Step Result: The **Delete Policy** dialog opens.

4. Click **Yes** to confirm the deletion.

Step Result: The **Delete Policy** dialog closes.

Result: The selected policy is deleted.

Exporting Policies

You can export information about Ivanti Device Control policies to a `.csv` (comma separated value) file. Exported policy information includes policy name, policy status, assignment status, device class, device collection, and the date of the last policy update.

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

Step Result: The **Device Control Policies** page opens.

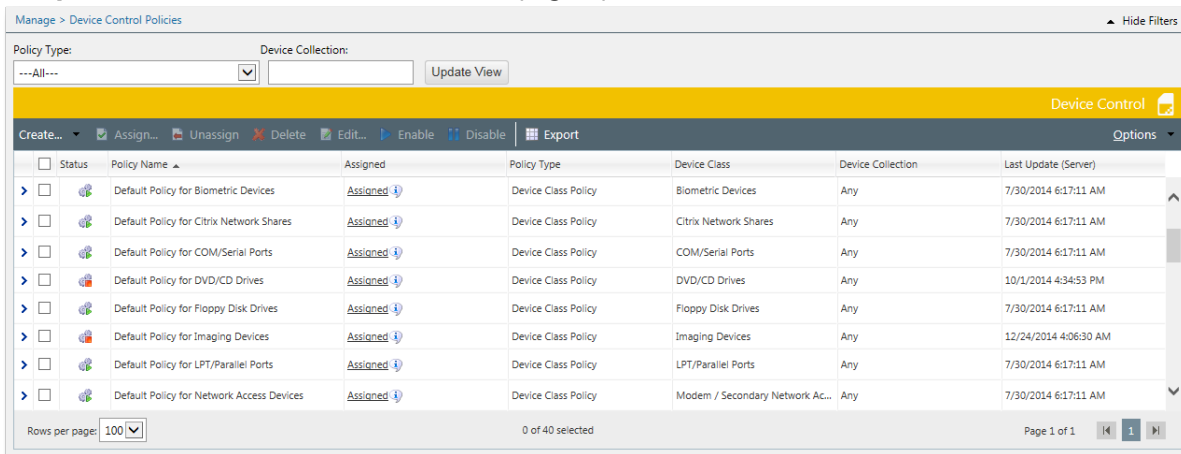


Figure 75: Device Control Policies

2. Select the policy you want to export.

Tip: Filter the **Policy Name** and **Device Class** or **Device Collection** columns to locate the policies.

3. Click **Export**.

Result: The policy details are exported to a `.csv` file.

Creating Policies for a Group

You can create and administer permissions for a group of endpoints directly in the **Groups** page.

1. Select **Manage > Groups**.

Step Result: The **Groups** page opens.

2. Select **Device Control Policies** from the **View** drop-down list.

3. Select the group for which you want to create the policy.

4. Click **Create**.

Step Result: A drop-down list appears.

5. Select the type of policy you want to create.

You can choose among device class, device collection, and media policies.

Result: The policy wizard for the selected policy type opens.

Creating Policies for Users

You can create and administer permissions for a group of users directly in the **Users** page.

1. Select **Manage > Users**.

Step Result: The **Users** page opens.

2. Select the user group for which you want to create the policy.

3. Select **Device Control Policies** from the **View** drop-down list.

4. Click **Create**.

Step Result: A drop-down list appears.

5. Select the type of policy you want to create.

You can choose among device class, device collection, and media policies.

Result: The policy wizard for the selected policy type opens.

Chapter

7

Using Device Event Logs

In this chapter:

- Granting Access to Device Event Logs
- The Device Event Log Queries Page
- Working with Device Event Log Queries

The Ivanti Device Control **Device Event Logs** module allows you to review various events logged by endpoints regarding the use of devices in your network.

You can create queries to retrieve event logs from the database. In order for the log information to be in the database, you must have created some type of logging policy and assigned it to an endpoint. The endpoint then logs activity and passes it back to the server and database.

Granting Access to Device Event Logs

Users can create and access Device Event Logs only if they have the requisite permissions to do so. You can grant access permissions through the **Users and Roles** option in the **Tools** menu.

1. Select **Tools > Users and Roles**.

Step Result: The ***Users and Roles*** page opens.

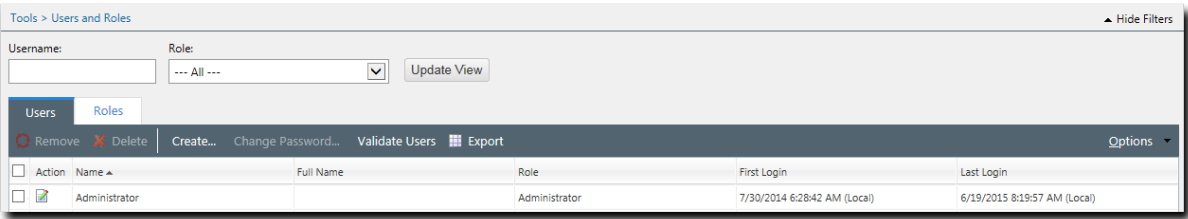


Figure 76: Users and Roles Page

2. Select the **Roles** tab.

Step Result: The **Roles** page opens.

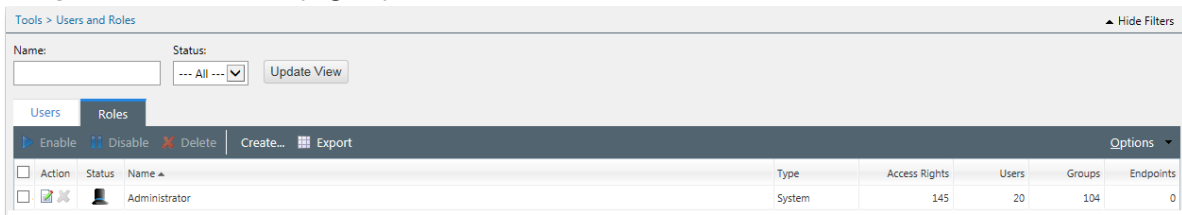


Figure 77: Roles Page

3. Click the **Edit Role** icon for the user to whom you want to grant permission.

Step Result: The **Edit Role** dialog opens.

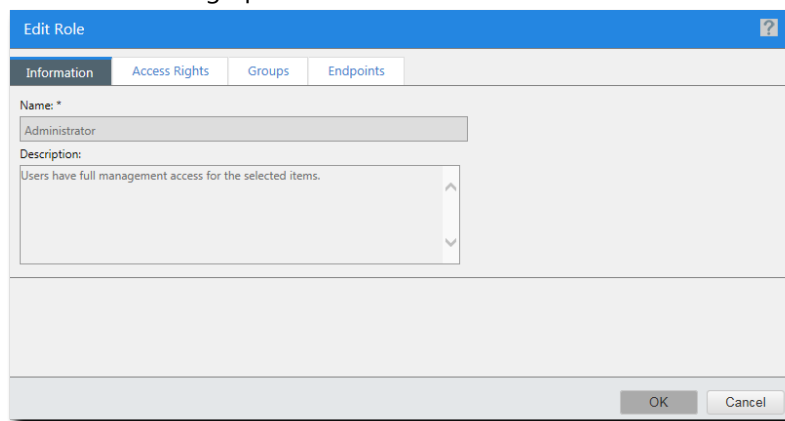


Figure 78: Edit Role Dialog

4. Select the **Access Rights** tab.

Step Result: The **Access Rights** page opens.

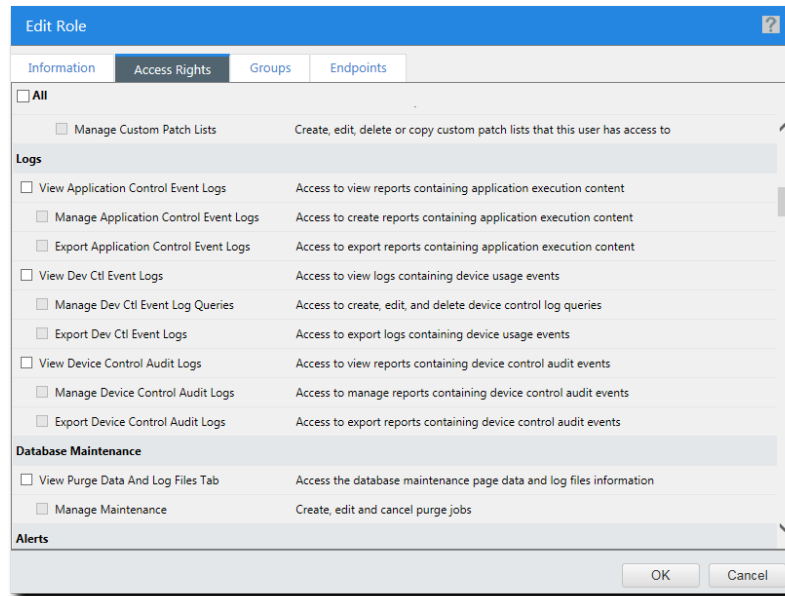


Figure 79: Access Rights

5. Select the appropriate Device Logs rights.

- a) In the **Logs** section, select the **View Device Event Logs** check box.

Step Result: The **Manage Device Event** and **Export Device Event Logs** check boxes become active.

- b) [Optional] Select the **Manage Device Event Logs** check box.

Step Result: The user has access to add and edit Device Event Log content.

- c) [Optional] Select the **Export Device Event Logs** check box.

Step Result: The user can export Device Event Log content.

6. Click **OK**.

Step Result: The **Edit Role** dialog closes.

Result: The user is granted permission to access Device Event Logs.

The Device Event Log Queries Page

The **Device Event Log Queries** page lets you create and view queries about device-related actions in your network.

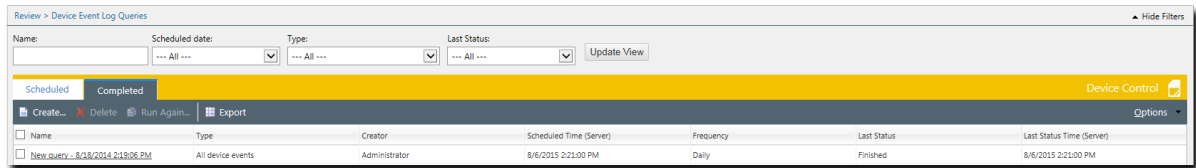


Figure 80: Device Event Log Queries Page

The **Device Event Log Queries** page contains two tabs: **Scheduled** and **Completed**. The **Scheduled** tab lists queries that have been created, but have not run yet. The **Completed** tab lists queries that have been executed.

The Device Event Logs Page Toolbar

This toolbar contains buttons that let you perform queries on device event logs.

The following table describes the **Device Event Logs** page options and their functions:

Table 55: Device Event Logs Page Options

Option	Description
Create	Opens the Device Event Log Query wizard.
Edit	Lets you edit the selected query. Note: You can edit queries only in the Scheduled tab.
Delete	Deletes the selected query.
Copy	Lets you copy an existing, scheduled log query. Note: You can copy queries only in the Scheduled tab.
Run Again	Let's you re-run a completed log query. Note: You can re-run queries only in the Completed tab.
Export	Generates a .csv file containing information about the Device Event Log queries. Note: This button is active only if the user has Export Device Event Logs access rights.
Options	Shows a drop-down list with Device Event Logs options.

The Device Event Log Queries Page List

The Device Event Log Queries page list contains details about scheduled and completed queries based on the selected tab.

The **Device Event Logs** grid list has the following columns:

Table 56: Device Event Logs List Columns

Field	Description
Name	The name of the query.
Type	The type of query.
Creator	The user who created the query.
Scheduled Time (Server)	The last scheduled time for the query.
Frequency	The frequency with which the query runs.
Last Status	The last reported status of the query.
Last Status Time (Server)	The time of the last reported status.

Working with Device Event Log Queries

There are several procedures associated with creating and managing device queries.

You can perform the following tasks from the **Device Event Log Queries** page:

- [Viewing Device Event Logs](#) on page 176
- [Creating a Device Event Log Query](#) on page 176
- [Editing a Device Event Log Query](#) on page 178
- [Viewing the Result of a Device Event Log Query](#) on page 182
- [Deleting a Device Event Log Query](#) on page 185
- [Exporting Device Event Log Queries](#) on page 185
- [Adding a Device to the Device Library from the Query Results Page](#) on page 186

Viewing Device Event Logs

The Ivanti Device Control **Device Event Log Queries** module allows you to create and modify log queries for the various endpoints in your network.

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

Note: You can access Device Event Log Queries only if you have the appropriate permissions to do so. For more information on Device Event Log Queries access, see [Granting Access to Device Event Logs](#) on page 171.

Result: The **Device Event Log Queries** page opens.

For more information on the **Device Event Log Queries** page, see [The Device Event Log Queries Page](#) on page 174.

Creating a Device Event Log Query

You can schedule queries that record specific device-related actions in your network. This includes queries for granted and blocked actions.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.
3. Click **Create**.

Step Result: The **Device Event Log Query** wizard opens.

Figure 81: Device Event Log Query Wizard

4. Type the **Query name**.
5. Select the **Type**.
6. Select the desired scheduling option. You can choose from the following options:

Option	Description
Immediate	The query will run immediately after creation.
Once	The query will run once at a specified time.
Daily	The query will run every day at the selected time.
Weekly	The query will run every week at the selected time.

Depending on the option you choose, additional settings are available in the right-side box.

Note: The start and end dates are the date range for which you want the query results. If you choose **Immediate** or **Once**, specify the start and end dates in the **Date range** fields.

7. [Optional] Select the **Notify me via email when query is complete** check box.
Ensure that you provide a valid email address in the associated field.
8. Click **Next**.

Step Result: The **Select endpoints/users/groups** page opens.

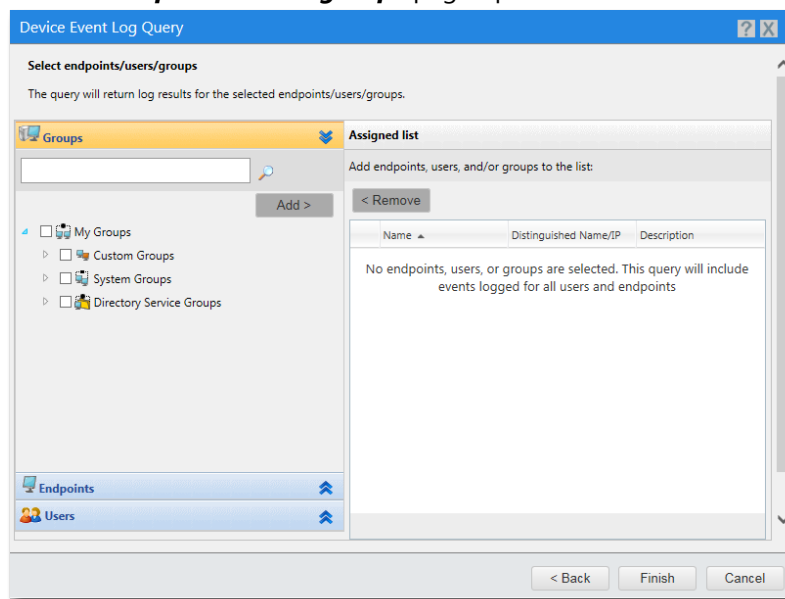


Figure 82: Select Endpoints/Users/Groups

9. Select the groups, endpoints, or users the policy will apply to. Use any of the following methods:

Note: The built-in user groups Administrators, Everyone, Power Users, and Users and Active Directory groups are not supported in log queries and will be removed from the query.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Add.
	Note: Active Directory groups are not supported in log queries.
To add individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Add.
	Note: The Built-in Users and Groups Administrators, Everyone, Power Users, and Users are not supported in log queries.
To remove groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Remove.
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

10. Click **Finish**.

Step Result: The **Device Event Log Query** wizard closes.

Result: A new query is created and runs. When the query completes, its summary is displayed in the **Completed** tab.

Editing a Device Event Log Query

You can edit scheduled queries that you have created earlier.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.

- Click the **Scheduled** tab.

Step Result: The **Scheduled** page opens.

- Select the query you want to edit.

- Click **Edit**.

Step Result: The **Device Event Log Query** wizard opens.

Device Event Log Query

Create device log query

Query device activity logs immediately or schedule a recurring job.

Query name:
Existing query - 8/7/2015 6:12:57 AM

Type:
Detected keyloggers

Scheduling

☐ Immediate Start date: Start time:

☐ Once 8/9/2015 7:00 AM

☐ Daily

☒ Weekly Run every 1 weeks on:

☐ Sunday ☒ Monday ☐ Tuesday ☐ Wednesday

☐ Thursday ☒ Friday ☒ Saturday

☐ End by:

Date range:
The last 1 week's worth of logged data at the time each recurring instance of this query runs.

Email notification:
☐ Notify me via email when query is complete:

Next > Cancel

Figure 83: Device Event Log Query Wizard

- Edit the query details.

- Type the **Query name**.
- Select the device event type from the **Type** dropdown list.

- Select the desired scheduling option. You can choose from the following options:

Option	Description
Immediate	The query will run immediately after creation.
Once	The query will run once at a specified time.
Daily	The query will run every day at the selected time.

Option	Description
Weekly	The query will run every week at the selected time.

Depending on the option you choose, additional settings are available in the right-side box.

Note: The start and end dates are the date range for which you want the query results.If you choose **Immediate** or **Once**, specify the start and end dates in the **Date range** fields.

8. [Optional] Select the **Notify me via email when query is complete** check box.
Ensure that you provide a valid email address in the associated field.

Tip: If the query results in no data found, then the subject line of the resulting email will contain the message `Report result - No Results Found`.

9. Click **Next**.

Step Result: The *Select endpoints/users/groups* page opens.

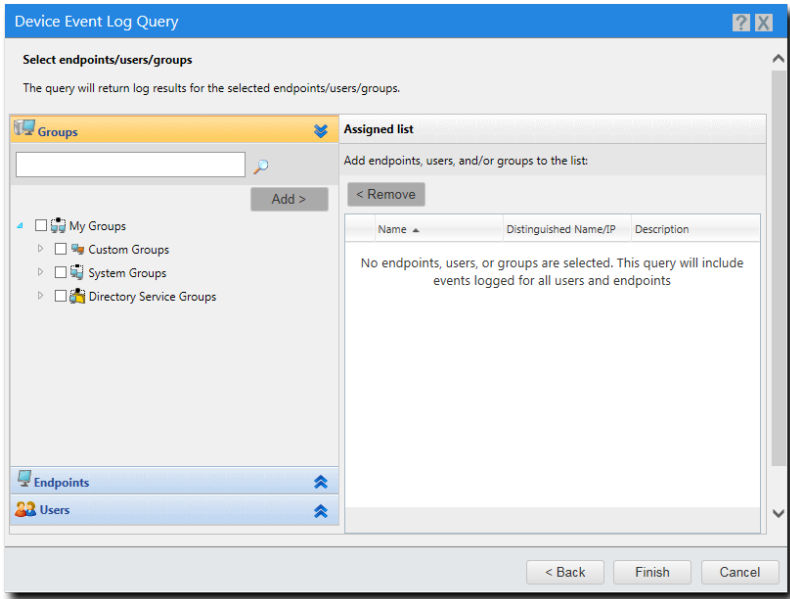


Figure 84: Select Endpoints/Users/Groups

10. Select the groups, endpoints, or users the policy will apply to. Use any of the following methods:

Option	Description
To add groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Add.

Option	Description
To add individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Add.
To remove groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Remove.
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

11. Click **Finish**.

Step Result: The **Device Event Log Query** wizard closes.

Result: The selected query is edited.

Copying a Scheduled Device Event Log Query

You can create and run a new Device Event Log Query based on an existing scheduled query.

Prerequisites:

You must be assigned the **Manage Dev Ctl Event Log Queries** access right.

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

2. Click the **Scheduled** tab.

Step Result: A list of scheduled queries is displayed.

3. If necessary, sort the list to find the query you want to copy.

4. Select the check box beside the query name. You can copy only one query at a time.

5. Click **Copy**.

Step Result: The **Create device log query** wizard opens, displaying the details of the selected query. All the settings are the same as the original query, except "Copy of" is added to the **Query name** and the **Start date** is reset (for Scheduling of type Once, Daily, and Weekly).

6. Complete the wizard to modify the query settings as required.

Tip: If you need to indicate that this query is based on an existing one, keep at least part of the original Query Name.

Result: You have created a copy of a scheduled Device Event Log Query and run it. If not run immediately, it will appear under the **Scheduled** tab on the **Device Event Log Queries** page.

Rerunning a Completed Device Event Log Query

You can create and execute a new Device Event Log Query based on a completed query.

Prerequisites:

You must be assigned the **Manage Dev Ctl Event Log Queries** access right.

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

2. Click the **Completed** tab.

Step Result: A list of completed queries is displayed.

3. If necessary, sort the list to find the query you want to rerun.
4. Select the check box beside the query name.

Note: You can select only one query to rerun at a time.

5. Click **Run Again**.

Step Result: The **Create device log query** wizard opens, displaying details of the selected query. All the settings are the same as the original query, except "Copy of" is added to the **Query name** and the **Start date** is reset (for Scheduling of type Once, Daily, and Weekly).

6. Follow the wizard and modify the query information and settings as required.

Tip: Keep at least part of the original query name so that you will know that this query has been modified.

7. Click **Finish**.

Result: You have created a copy of a completed Device Event Log Query and run it. If not run immediately, it will appear under the **Scheduled** tab on the **Device Event Log Queries** page.

Viewing the Result of a Device Event Log Query

The **Device Event Log Query Results** page is displayed when the user clicks the **Name** hyperlink of an executed query on the **Completed** tab of the **Device Event Log Queries** page.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.

3. [Optional] Sort the list to find the query you want to view.
4. Click the name of the query you want to view in the **Name** column.

Result: The **Device Event Log Query Results** page opens, displaying the detailed results of the query.

Tip: Click the arrow next to a name to view more details of the query result.

The grid list has the following columns:

Table 57: Device Event Log Query Results List Columns

Field	Description
Type	The type of event logged.
Log Time (Agent Local)	The time on the agent endpoint when the action was performed.
Endpoint	The endpoint where the action was performed.
Logged In User	The user who performed the action.
Class	The device class.
Model ID	The device model.
File Name	The name of the file accessed on the device.
File Path	The path to the file on the device.
Process Name	The description of the process used for device access.
Size	The size of the shadowed file.
Reason	Denied or Enabled.

After Completing This Task:

Now you can [refresh the completed query](#) to update the results grid with relevant events sent to the server from endpoints since the query last ran.

Refreshing a Completed Device Event Log Query

You can refresh a completed Device Event Log Query to import the latest events into the results grid list without having to recreate the query.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.
3. [Optional] Sort the list to find the query you want to view.
4. Click the name of the query you want to view in the **Name** column.

Step Result: The Device Event Log Query Results page opens, displaying the detailed results of the query.

5. Click **Refresh**.

Result: The results grid is updated with relevant events sent to the server from endpoints since the query last ran:

Scheduling	Refresh Behavior	
Immediate	Results are updated to reflect all events sent from endpoints in the last 24 hour period, from the moment Refresh is clicked.	Original Device Event Log Query is updated.
Once		
Daily		Duplicate Device Event Log Query is created.
Weekly	Results are updated to reflect all events sent from endpoints in the past 7 days from 7*24 hours before to the present moment when Refresh is clicked.	

Device Event Log Queries Open File Dialog

Safely open a file from a shadowing event on the ***Device Event Log Query Results*** page for inspection.

The dialog launches from ***All File Shadowing Event*** type ***Device Event Log Query Results*** when you click the hyperlink file path in the ***Full File Name*** field.

Caution:

- Scan the file with Ivanti AntiVirus prior to opening. If uncertain that the file was scanned by a policy-based scan on the endpoint (Real-time Monitoring Scan or Recurring Virus and Malware Scan), use the Custom Scan Now feature in the Agent Control Panel on the endpoint.
- Opening a file in an application other than the binary viewer exposes you to the vulnerabilities of that application.

Table 58: Open File Dialog

Field	Description
File	The file type, name with extension, and size.



Field	Description
Options	<ul style="list-style-type: none"> • Open in binary viewer (safest option): Displays file contents as 16 byte rows of data in Hex, ANSI, and Unicode formats, without the risk of code execution. Recommended for file types without an associated application in the browser (including those with no file extension). • Open in new browser window as the following MIME type: Displays file contents in the application the browser associates with the MIME type you select from the drop-down list: Octet Stream, HTML, Microsoft Word, PDF, Microsoft Excel, and BMP. • Open in new browser window with default browser functionality: Displays file contents using the default application the browser associates with the file extension.
Select this option by default for ...	Makes the option you select the default opening action for files with the same extension.

Deleting a Device Event Log Query

You can delete a device event log query that is scheduled to run at a later time. You cannot delete a query if it is currently running.

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

Step Result: The *Device Event Log Queries* page opens.

2. Select the **Scheduled** tab.

Step Result: The *Scheduled* page opens.

3. Select the query you want to delete.

Note: Ensure that the query you are deleting is not running. If you try to delete query that is running, you will receive an error message.

4. Click **Delete**.

Step Result: The *Delete Queries* dialog opens.

5. Click **OK** to confirm the deletion.

Step Result: The *Delete Queries* dialog closes.

Result: The selected query is deleted.

Exporting Device Event Log Queries

You can export queries and results of a query to a `.csv` (comma separated value) file.

To export data, refer to [Exporting Data](#) on page 71.

Adding a Device to the Device Library from the Query Results Page

The **Device Event Log Query Results** page lets you add devices directly to the Device Library.

1. Select **Review > Device Event Log Queries**.
2. The **Device Event Log Queries** page opens.
3. [Optional] Sort the list to find the query you want to view.
4. In the **Name** column, click the name of the query you want to view.

Step Result: The **Device Event Log Query Results** page opens, displaying the detailed results of the query.

5. Select the devices you want to add to the Device Library.
6. Click **Add To Device Library**.

Step Result: The **Add To Device Library** dialog opens.

7. Select the items to add.
 - To add the devices to the parent device class, select **Selected devices**.
 - To add the device model, select **Selected device models**.

Note: Log events prerequisites when adding devices:

- Device model: log events must have a Model ID.
- Unique device: log events must have a Model ID and a device Unique ID.

8. Type the name of a collection in the **Add to an existing collection or type the name of a new collection** or select an existing collection from the associated drop-down list.
9. Click **OK**.

Step Result: A success message is displayed.

Note: If you try to add devices that are already present in the Device Library, you will receive an error message.

Result: The selected devices are added to the Device Library.



Chapter

8

Using the Tools Module

In this chapter:

- Granting Access to Device Control Tools
- The Ivanti Device Control Options Page
- Working with Ivanti Device Control Tools and Options

The Ivanti Device Control (Device Control) Tools module allows you to access tools to perform various tasks such as recover encryption keys for encrypted devices, assign temporary permissions to offline users, and modify Device Control options.

Granting Access to Device Control Tools

Users can access the Ivanti Device Control Tools module only if they have the requisite permissions to do so. You can grant access permissions through the **Users and Roles** option in the **Tools** menu.

1. Select **Tools > Users and Roles**.

Step Result: The ***Users and Roles*** page opens.

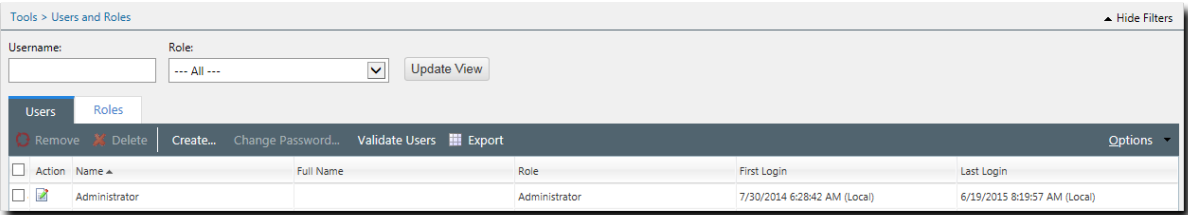


Figure 85: Users and Roles Page

2. Select the **Roles** tab.

Step Result: The **Roles** page opens.



Figure 86: Roles Page

3. Click the Edit Role icon for the user to whom you want to grant permission.

Step Result: The **Edit Role** dialog opens.

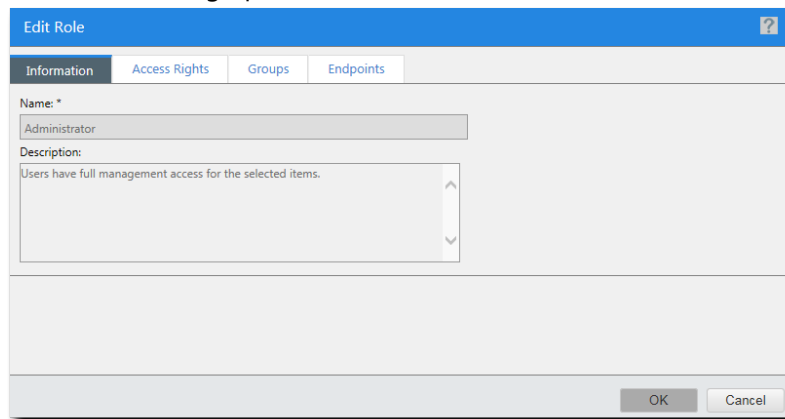


Figure 87: Edit Role Dialog

4. Select the **Access Rights** tab.

Step Result: The **Access Rights** page opens.

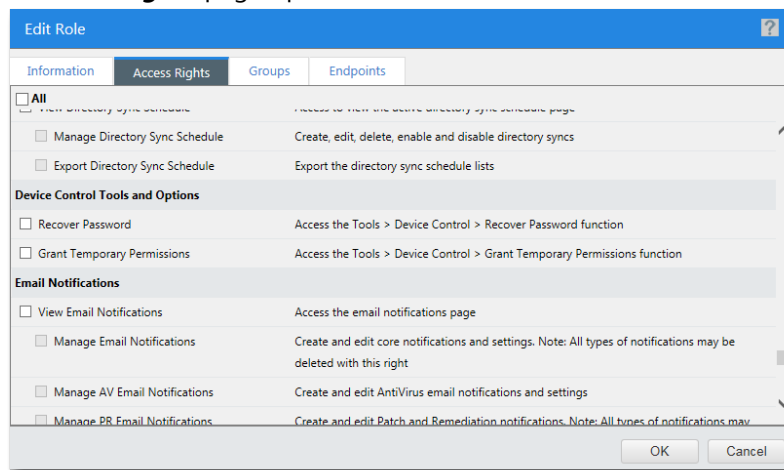


Figure 88: Access Rights

5. Select the appropriate Tools rights.

- a) In the **Options** section, select the **View Global Device Control Options** check box.

Step Result: The **Manage Global Device Control Options** check boxes become active.

- b) [Optional] Select the **Manage Global Device Control Options** check box.

Step Result: The user has access to change Ivanti Device Control options.

6. Click **OK**.

Step Result: The **Edit Role** dialog closes.

Result: The user is granted permission to access and modify Ivanti Device Control options.

The Ivanti Device Control Options Page

The Ivanti Device Control (Device Control) **Options** page lets you view global Device Control options and edit them to suit your needs.

Table 59: General settings

Option	Description
Syslog server address for endpoint events	Specify the third-party syslog server to be used. This field must contain either an IP address or a hostname, optionally followed by a port number. The field is empty by default.

Option	Description
Cryptographic compliance mode	Select <code>True</code> to force endpoints to use FIPS140-2 Level 2 encryption when encrypting devices and media.
Agent status and update notifications	Select the status changes that generate an endpoint notification.
Agent permission change notifications	Select the messages related to permission changes the agent will show endpoint users.



Option	Description
Agent action on detect USB keylogger	<p>Select the the action to be performed when an agent detects a new USB keyboard connection, which could potentially be a USB keylogger.</p> <ul style="list-style-type: none"> • Disabled • Notify user: User is notified on-screen to check for the presence of a keylogger. • Log event: A <code>Detected keyloggers</code> event is logged. • Notify user and log event: User is notified on-screen to check for the presence of a keylogger and a <code>Detected keyloggers</code> event is logged • Block keyboard and notify user: The new USB keyboard connection is blocked and the user notified on-screen to check for the presence of a keylogger. • Block keyboard and log event: The new USB keyboard connection is blocked and a <code>Detected keyloggers</code> event is logged. • Block, notify and log event: The new USB keyboard connection is blocked, user notified on-screen to check for the presence of a keylogger, and a <code>Detected keyloggers</code> event is logged. • Exclusive mode (Lock/block, notify and log event): The new USB keyboard connection is blocked, user notified on-screen to check for the presence of a keylogger, and a <code>Detected keyloggers</code> event is logged. This mode can be used to detect a USB Rubber Ducky device, which is a keyboard emulation device that can inject payloads capable of, for example, changing system settings and retrieving data.
Online state definition	<ul style="list-style-type: none"> • Server connectivity: Enforces online and/or offline permission rules for device use when the client has no connectivity with any Application Server. This is the default value. • Wired connectivity: Enforces online and/or offline permission rules for device use when the client has an active wired network interface connection.

Table 60: Shadowing related options

Option	Description
Server shadow directory	Specify the location on the server where shadowed files are to be saved. The default location is <code>%InstallDirectory%\DeviceControl\Shadow</code>

Option	Description
When user tries to write to a CD / DVD in a format that doesn't support shadowing	Select the action the agent is to perform when a user attempts to write to a CD / DVD in a format that does not support shadowing. The default action is: Deny writing to the CD / DVD (no shadowing occurs)

Table 61: Encryption settings

Option	Description
Enforce password complexity	Select <code>True</code> to enforce that all encryption passwords have at least three of the desired attributes (uppercase letters, lowercase letters, digits, non-alphanumeric symbols).
Password minimum length	Specify the minimum password length allowed when users create a password for an encrypted device on an endpoint. The default value is 6.
Agent notifies user about encryption option when connecting an un-encrypted device	Select <code>True</code> to inform the user about encrypting an unencrypted device. By default the user is not notified.
Unencrypted device connected prompt	Enter a custom text to display upon connection of an unencrypted device when an endpoint user has the option to encrypt. The text entered will be followed by: Do you want to encrypt <drive letter>?
Automatically clear unused space	Select <code>True</code> to overwrite unused space on an encrypted device, deleting any existing data.
Retain data when encrypting device	Select the action the agent is to perform on existing data on a device during encryption.
Agent encryption grace period	Specify the number of hours a non-Easy Exchange encrypted removable device is to be available after a plug-unplug operation when the endpoint has not yet sent its log to the server.
Microsoft CA key provider	<p>Select <code>Enable (Decentralized)</code> (default) for the system to employ a user's certificate to control access to an encrypted device. A user whose certificates are associated with a device will have access to it without the need to enter a password.</p> <p>Important: A Microsoft Certificate Authority must be implemented in the environment.</p>

Option	Description
Automatic certificate generation	This option becomes active when the Microsoft CA key provider option is set to <code>Enable</code> and is set to <code>Disabled</code> by default. Select <code>Enable</code> to use automatic certificate generation.
	Tip: Ensure auto-enrollment is enabled in the Microsoft Management Console (MMC), otherwise the domain administrator will need to approve each enrollment request before a certificate can be retrieved and installed.
	Important: Only default user certificate templates are supported.

Working with Ivanti Device Control Tools and Options

Ivanti Device Control tools and options include several configuration options affecting the performance and behavior of Device Control, the ability to grant temporary access permissions, and crypto password recovery.

You can perform the following tasks using Device Control tools and options:

- [Viewing Ivanti Device Control Options](#) on page 193
- [Configuring Ivanti Device Control Options](#) on page 194
- [Requesting Temporary Access Permissions](#) on page 195
- [Granting Temporary Access Permissions](#) on page 196
- [Recovering a Password When the Endpoint is Connected to the Server](#) on page 200
- [Recovering a Password When the Endpoint is Disconnected From the Server](#) on page 204

Viewing Ivanti Device Control Options

The Ivanti Device Control (Device Control) **Options** page is part of the Tools module and has options related to Device Control functions.

1. Select **Tools > Options**.

Note: You can access the **Options** page only if you have the appropriate permissions to do so. For more information on Options access, see [Granting Access to Device Control Tools](#) on page 187.

Step Result: The **Options** page opens.

2. Select the **Device Control** tab.

Result: The **Device Control** page opens.

For more information on Device Control options, see [The Ivanti Device Control Options Page](#) on page 189.

Configuring Ivanti Device Control Options

Configuring Ivanti Device Control allows you to optimize the performance and behavior of Device Control.

1. Select **Tools > Options**.

Note: You can access the **Options** page only if you have the appropriate permissions to do so. For more information on access to the **Options** page, see [Granting Access to Device Control Tools](#) on page 187.

Step Result: The **Options** page opens.

2. Select the **Device Control** tab.

Step Result: The **Device Control** options display.

The screenshot shows the 'Tools > Options' window with the 'Device Control' tab selected. The 'General settings' section includes: 'Syslog server address for endpoint events' (empty), 'Cryptographic compliance mode' (False), 'Agent status and update notifications' (Show all), 'Agent permission change notifications' (All device permission changes), 'Agent action on detect USB key logger' (Disabled), and 'Online state definition' (Server connectivity). The 'Shadowing related options' section includes: 'Server shadow directory' (C:\ProgramData\HEAT Software\DeviceControl\Shadow) and 'When user tries to write to a CD / DVD in a format that doesn't support shadowing' (Deny writing to the CD / DVD (no shadowing occurs)). The 'Encryption settings' section includes: 'Enforce password complexity' (True). At the bottom are 'Export', 'Reset', and 'Save' buttons.

Figure 89: Device Control Options Page

Temporary Access Permissions

Temporary permissions allow access to protected devices for offline users. These permissions are valid until they expire or the endpoint reconnects to the protected network.

In some cases, users need to modify their permissions while they are not connected to your network. For example, a user who has no access to the Internet may want to read a file stored on a removable storage device, or might be at an offsite meeting and needs authorization to install a customer's software application on his laptop.

To modify permissions while in an offline state, the user must contact a Ivanti Endpoint Security administrator, explain the required permissions, and quote a key code provided by the Device Control

agent. The administrator verifies the information provided by the user and generates an unlock code, which grants the required permissions.

Note: Temporary access permissions are valid until they expire or the endpoint reconnects to the Ivanti Endpoint Security Server.

Requesting Temporary Access Permissions

Users of encrypted devices must make a request to a Device Control administrator to receive temporary access permissions.

1. Right-click the Device Control agent icon in the system tray on the endpoint.
2. Select **Request temporary access offline**.

Step Result: The *Request Temporary Access Offline* wizard opens.

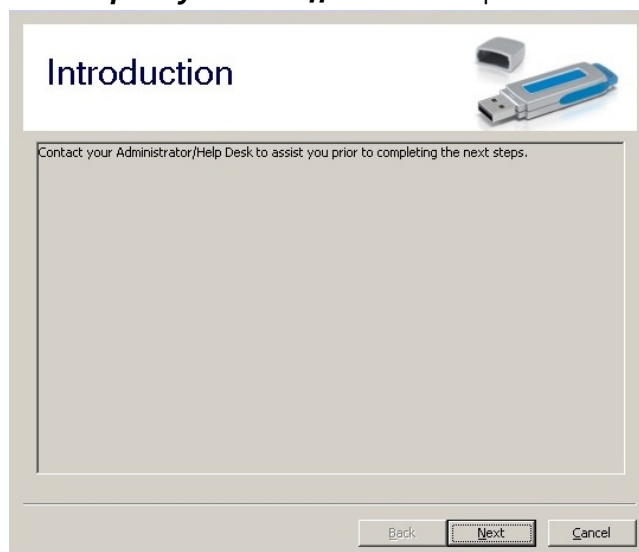


Figure 90: Request Temporary Access Offline Wizard

3. Click **Next**.

Step Result: The **Input** dialog appears.

Input

Specify the following when speaking with the Administrator.
Please confirm the information is correct before proceeding to the next page.

Device and Permissions

Device Class: Removable Storage Devices

☒ Read ☒ Encrypt ☒ Import ☒ Export (File)
☒ Write ☒ Decrypt ☒ Export (Media)

Lifetime of the permission

Day(s) : 0 Hour(s) : 1 Minute(s) : 0

For which user?

☒ For you ☐ For everyone

Back Next Cancel

Figure 91: Input

4. The user specifies the details of the permission they are requesting.
 - a) Select a device class from the **Device Class** drop-down list.
 - b) Select the check boxes corresponding to the permissions being requested.
 - c) Select how long the permissions are valid for in the **Lifetime of the permission** fields.
 - d) The user for whom the permission applies to from the **For which user?** fields.
5. The user telephones you (a Device Control administrator) and explains the problem.

Granting Temporary Access Permissions

Granting temporary access permissions allows users increased access to their encrypted device for a specified interval.

After receiving a request for temporary access permissions, confirm the circumstances and details of the request with the requesting user before granting additional permissions.

1. Select **Tools > Device Control > Grant Temporary Permissions**.

Step Result: The **Grant Temporary Permissions** wizard appears in the main window.

Tip: You can pull the comments stored in the audit log by running this query:

```
SELECT * FROM [UPCCCommon].[dbo].[vAuditLog]
WHERE OriginatingComponent = 'TemporaryPermissions'
ORDER BY AuditID DESC
```

Figure 92: Grant Temporary Permissions Wizard

2. Confirm the permission settings for the device with the user and specify them in the **Device class and permissions** fields.

The data in the **Device Class** and **Duration** fields should match that specified by the user in the **Input** page of the **Request Temporary Access Offline** wizard.

Note: The settings specified by the offline user and the administrator must be identical for the unlock key generated by the administrator to work when entered by the offline user.

- Click the **Endpoint** button to select the computer the permission is applicable for in the **Endpoint** field.
- Click the **User** button to select the user the permission will apply to in the **User** field.

Note: If the offline user has chosen the **For everyone** option, then the administrator must select the **Everyone** user.

3. The user clicks **Next**.

Step Result: The **Unlock** page appears.

Figure 93: Unlock

4. The user reads out the 27-character **Client key** to you.
5. Type the alphanumeric client key provided by the user in the **Client key** field in the wizard.
6. [Optional] Type any comments in the **Comments** field.
7. Click **Generate**.

Step Result: An **Unlock Code** dialog appears.

Figure 94: Unlock Code

Note: The unlock code will only be generated if the permission settings entered by both the administrator and the offline user match.

8. Read out the 44-character unlock code to the user.
9. The user types the alphanumeric code in the **Unlock code** field of the **Unlock** page.

10. The user clicks **Next**.

Step Result: The **Finish** page appears and a system tray message informs the that the permission status has been changed up to a certain time.

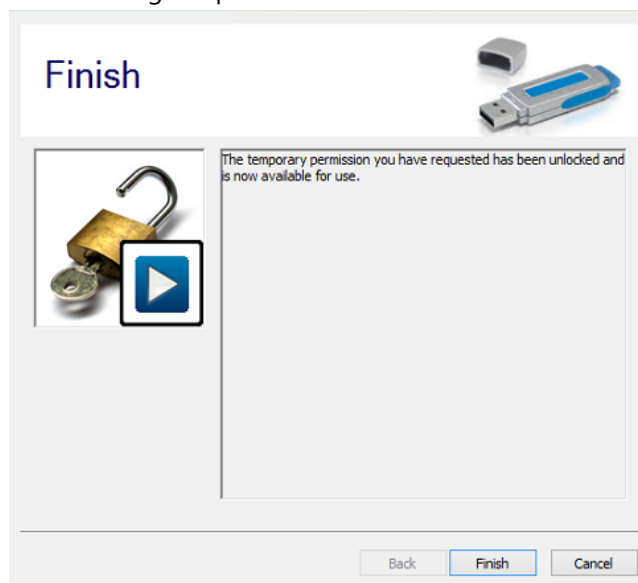


Figure 95: Finish

Note: The offline user is limited to 15 tries at entering the correct unlock code before a lockout period comes into effect. A lockout period also comes into effect if the **Request Temporary Access Offline** wizard is used to generate a client key 15 times without a valid unlock code being entered.

11. Click **Finish**.

Step Result: The **Request Temporary Access Offline** wizard closes.

Result: The offline user has temporary access to the selected device.

Crypto Password Recovery

If a user has forgotten the password associated with an encrypted device, the administrator can generate a passphrase for the user to gain access to the device using the Password Recovery tool.

Sometimes, a user forgets a password set up to access an encrypted removable storage device attached to his computer, or fails to enter this password correctly five times in a row. The user must then contact an administrator with the identity of the device and a security code. Using this information, the administrator, if the access is approved, can generate a passphrase. The device that the user needs to access is decrypted using the passphrase and re-encrypted using a new password.

Key recovery is of two types:

1. When a user is accessing the device on an endpoint with the Ivanti Device Control Agent installed. For more information, see [Recovering a Password When the Endpoint is Connected to the Server](#) on page 200.
2. When a user is accessing the device on a computer that does not have the Ivanti Device Control Agent installed. For more information, see [Recovering a Password When the Endpoint is Disconnected From the Server](#) on page 204.

Note: You cannot recover a password if the Device Log option is disabled and you have not recovered the machine's log at least once after encrypting the device.

Recovering a Password When the Endpoint is Connected to the Server

The procedure for recovering a password for an encrypted device for a user that has access to an endpoint with the Ivanti Device Control Agent installed on it involves a number of steps carried out by the user who wants to access the device as well as those carried out by the administrator authorizing the decryption and re-encryption.

1. The user attempts to access a removable storage device that is encrypted.

Step Result: The **Unlock Medium** dialog appears.

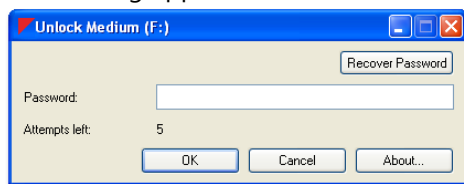


Figure 96: Unlock Medium

2. The user types the password more than the allowed number of times.

Step Result: An attempts exceeded message appears.

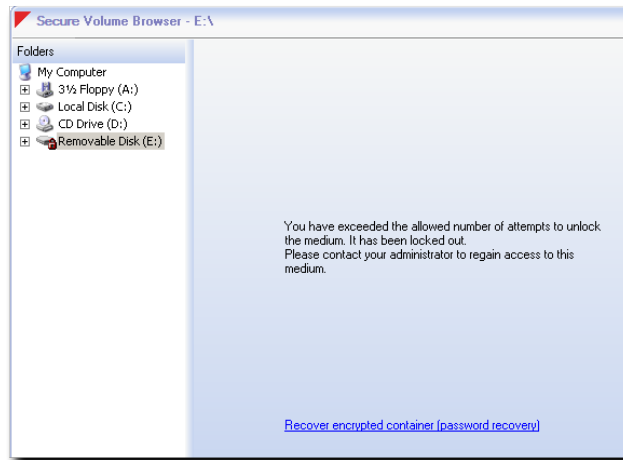


Figure 97: Attempts Exceeded

3. The user initiates password recovery in one of the following ways:

- By clicking **Recover Password** in the **Unlock Medium** dialog.

Note: Use this option if you do not want to try and guess the password.

- By clicking the **Recover encrypted container (password recovery)** link in the attempts exceeded message.

Step Result: The **Recover Password** dialog opens.

Recover Password

To recover your password, please contact your administrator or help desk and complete the following steps:

1. Provide the following information:

Encrypted Medium ID: 013BA4891413EE4B952F9B745FE60D48

Security Code: APJQW-RPJAW-RZ323-LLEA4-LSQ0C-DGUZ3-AS772-DDAAA-AAAY

2. Enter passphrase received from administrator

3. Create new password

Name: LegacyPassword

New Password

Confirm Password

OK Cancel About...

Figure 98: Recover Password

4. The user telephones you (a Ivanti Device Control administrator with Password Recovery access rights), explains the problem, and reads out the 32-character Encrypted Medium ID.
5. [Optional] Check whether the person on the telephone is allowed to access the encrypted medium.

Step Result: The user details are verified.

6. Select **Tools > Device Control > Recover Password**.

Step Result: The **Recover Password** wizard appears in the main window.

The screenshot shows a 'Recover Password' wizard dialog box with the following steps:

- Step1 - Verify user authorization**: Verify that the endpoint user is entitled to access the encrypted device they're trying to unlock, based on your organization's security policy.
- Step2 - Get medium ID and security code**: Guide the endpoint user through launching the Recover Password dialog for the device. Request the following information displayed on that dialog:
 - Encrypted Medium ID
 - Security Code
- Step3 - Enter medium ID and security code**: Enter the Encrypted Medium ID and Security Code below, as provided by the endpoint user.
 - Encrypted Medium ID: A dropdown menu.
 - Type the first three characters in the Encrypted Medium ID to show a list of available Medium ID's.
 - Security Code: A text input field.
- Step4 - Generate passphrase**: Click the Generate button below and communicate the results to the endpoint user.
 - Generate...: A button.

A 'Close' button is located at the bottom right of the dialog.

Figure 99: Recover Password Wizard

7. Select the 32-character alphanumeric string provided by the user from the **Encrypted Medium ID** drop-down field.

Note: Every time a removable device is encrypted in Ivanti Device Control, a new encrypted medium ID is generated and displayed in the **Encrypted Medium ID** drop-down field.

8. Type the 44-character alphanumeric security code received from the caller in the **Security Code** field.

9. Click **Generate**.

If the **Encrypted Medium ID** and/or the **Security Code** are incorrect, an error message is displayed explaining which one needs correcting.

Step Result: The **Password** dialog opens.

10. Read out the 52-character passphrase to the user.

11. The user types the alphanumeric passphrase in the **Enter passphrase received from administrator** field of the **Recover Password** dialog.

12. The user inputs a new password.

a) Specify the new password in the **New Password** field.

b) Retype the password in the **Confirm Password** field.

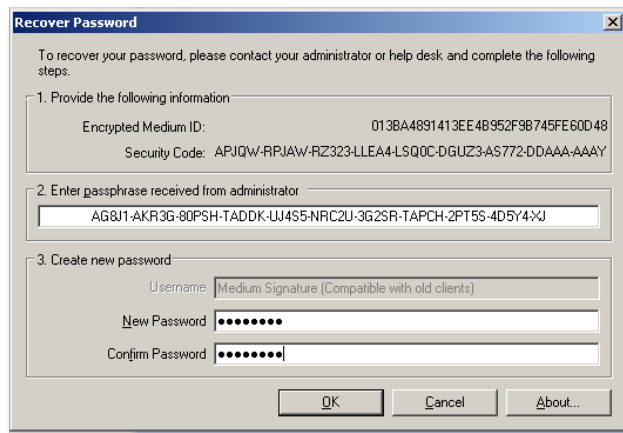


Figure 100: Recover Password

13. Click **OK**.

Step Result: A password changed message appears.



Figure 101: Password Changed

Result: The user successfully generates a new password for the encrypted device.

Recovering a Password When the Endpoint is Disconnected From the Server

A user who is trying to access an encrypted device on a computer that does not have the Ivanti Device Control Agent installed can recover the password by using the Secure Volume Browser application on the device to initiate password recovery.

Sometimes, users who are working on computers that do not have the Ivanti Device Control Agent installed on them forget their encryption passwords for encrypted devices, or they fail to enter an encryption password correctly after a specified number of attempts.

In such a case, the user needs to use Secure Volume Browser (since they do not have the Ivanti Device Control Agent) and contact a Ivanti Device Control administrator with the identity of the device and a security code. Using this information, the Administrator, if the access is approved, can generate a passphrase. The device that the user needs to access is decrypted using the passphrase and re-encrypted using a new password.

1. The user clicks **SVolBro.exe** on the encrypted removable storage device.

Step Result: The **Secure Volume Browser** window opens.

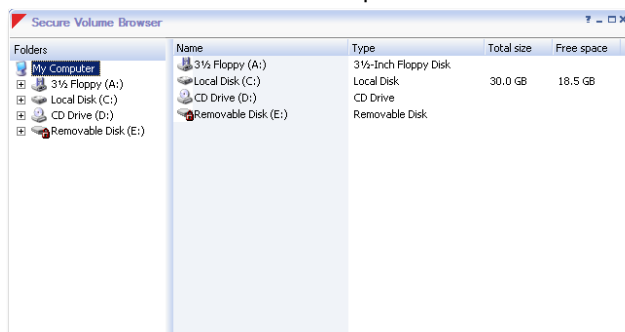


Figure 102: Secure Volume Browser

2. The user selects the encrypted medium in the **Folders** column.
An encrypted medium is identified by its lock icon.



Step Result: A password prompt appears in the **Secure Volume Browser** window.

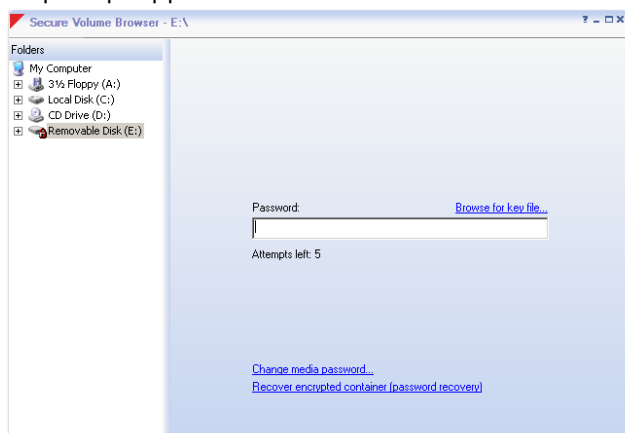


Figure 103: Secure Volume Browser

3. The user types the password more than the allowed number of times.

If the user does not know the password, he can also press the **ENTER** key more than the allowed number of times.

Step Result: An attempts exceeded message appears.

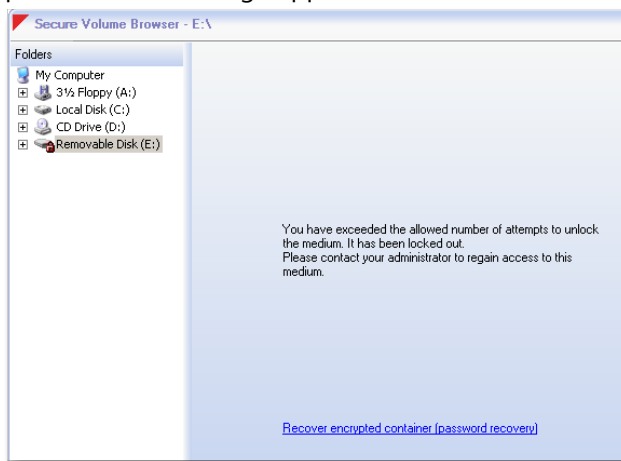


Figure 104: Attempts Exceeded

4. The user clicks the **Recover encrypted container (password recovery)** link.

Step Result: The **Recover Password** dialog opens.

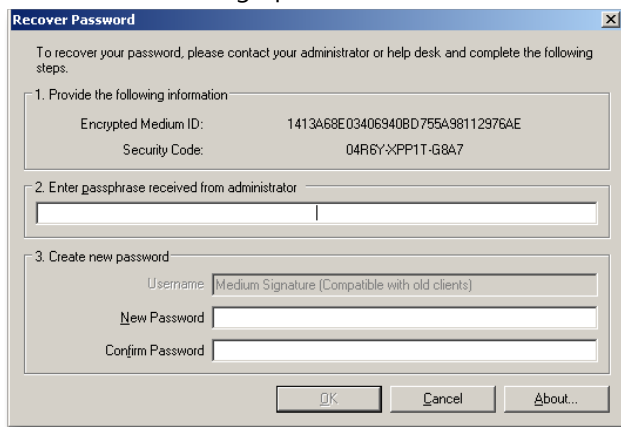


Figure 105: Recover Password

5. The user telephones you (a Ivanti Device Control administrator with Password Recovery access rights), explains the problem, and reads out the 32-character Encrypted Medium ID.
6. [Optional] Verify that the person on the telephone is allowed to access the encrypted medium.

7. Select **Tools > Device Control > Recover Password**.

Step Result: The **Recover Password** wizard appears in the main window.

The screenshot shows the 'Recover Password' wizard with the following content:

- Step1 - Verify user authorization**: Verify that the endpoint user is entitled to access the encrypted device they're trying to unlock, based on your organization's security policy.
- Step2 - Get medium ID and security code**: Guide the endpoint user through launching the Recover Password dialog for the device. Request the following information displayed on that dialog:
 - Encrypted Medium ID
 - Security Code
- Step3 - Enter medium ID and security code**: Enter the Encrypted Medium ID and Security Code below, as provided by the endpoint user.
 - Encrypted Medium ID: [Dropdown menu]
 - Type the first three characters in the Encrypted Medium ID to show a list of available Medium ID's.
 - Security Code: [Text input field]
- Step4 - Generate passphrase**: Click the Generate button below and communicate the results to the endpoint user.
 - [Generate... button]

A 'Close' button is located at the bottom right of the dialog.

Figure 106: Recover Password Wizard

8. Select the 32-character alphanumeric string provided by the user from the **Encrypted Medium ID** drop-down field.

Note: Every time a removable device is encrypted in Ivanti Device Control, a new encrypted medium ID is generated and displayed in the **Encrypted Medium ID** drop-down field.

9. Type the 44-character alphanumeric security code received from the caller in the **Security Code** field.

10. Click **Generate**.

If the **Encrypted Medium ID** and/or the **Security Code** are incorrect, an error message is displayed explaining which one needs correcting.

Step Result: The **Password** dialog opens.

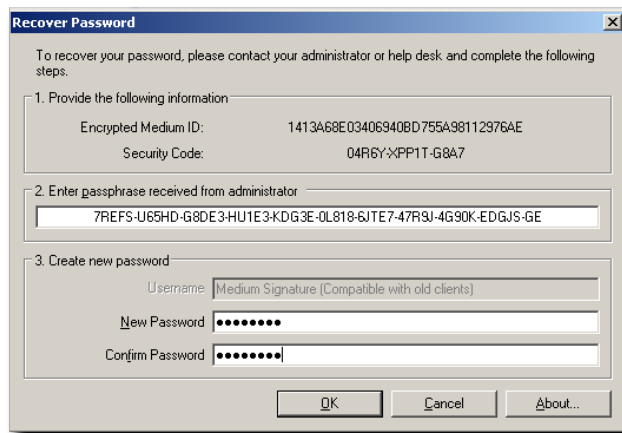
11. Read out the 52-character passphrase to the user.

12. The user types the alphanumeric passphrase in the **Enter passphrase received from administrator** field of the **Recover Password** dialog.

13. The user inputs a new password.

a) Specify the new password in the **New Password** field.

b) Retype the password in the **Confirm Password** field.



The 'Recover Password' dialog box contains the following elements:

- Title Bar:** Recover Password
- Instructions:** To recover your password, please contact your administrator or help desk and complete the following steps.
- Step 1:** Provide the following information:
 - Encrypted Medium ID: 1413A68E03406940BD755A98112976AE
 - Security Code: 04R6Y:XPP1T-G8A7
- Step 2:** Enter passphrase received from administrator:
 - Passphrase: 7REFS-U65HD-G8DE3-HU1E3-KDG3E-0L818-6JTE7-47R9J-4G90K-EDGJS-GE
- Step 3:** Create new password:
 - Username: Medium Signature (Compatible with old clients)
 - New Password: [masked]
 - Confirm Password: [masked]
- Buttons:** OK, Cancel, About...

Figure 107: Recover Password

14. Click **OK**.

Step Result: A password changed message appears.

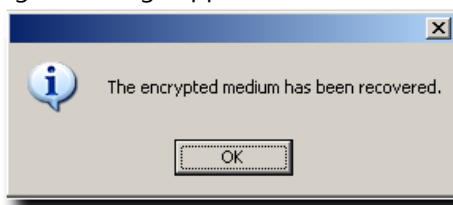


Figure 108: Password Changed

Result: The user successfully generates a new password for the encrypted device.

Chapter 9

Using the Reports Module

In this chapter:

- Generating Ivanti Device Control Reports
- Available Ivanti Device Control Reports

The **Reports** module provides predetermined report templates that allow you to generate a variety of reports about Ivanti Device Control use with information that includes permissions, shadowing, options, and media.

The generated reports are HTML files displayed in an internal window.

Note: You can change the way the date is formatted in a Ivanti Device Control report by using the **Regional and Language** options located in the Control Panel of your Windows system. Consult Windows Help for details.

Once saved, the reports can be viewed using Internet Explorer or any other Web browser defined on your system. The reports can also be printed and exported.

For more information on generating and viewing reports in the Ivanti Endpoint Security refer to [Ivanti Endpoint Security User Guide](https://help.ivanti.com/) (<https://help.ivanti.com/>) .

Generating Ivanti Device Control Reports

All Ivanti Device Control reports are accessible from the **Reports** menu. Select from the available report templates to view the details of that report.

1. Select **Reports > Device Control**.

Step Result: The **Reports** page opens.

2. From the display list, select the report you want to generate.
3. Filter the report by selecting user or endpoint groups.

Note: Not all reports will provide you with filtering options. Some reports do not have selection parameters.

4. Click **Generate Report**.

Result: The selected report opens in a new window.

Available Ivanti Device Control Reports

Ivanti Endpoint Security provides various reports that provide information about Ivanti Device Control functions.

The following reports are available within Ivanti Endpoint Security when the Ivanti Device Control module is installed.

- [Device and Media Collections Report](#) on page 210
- [Device Control Options Report](#) on page 212
- [Device Permissions Report](#) on page 214
- [Endpoint Permissions Report](#) on page 216
- [User Permissions Report](#) on page 218

Device and Media Collections Report

The **Device and Media Collections Report** lists the collections in the Device Library as well as the devices and media in those collections.

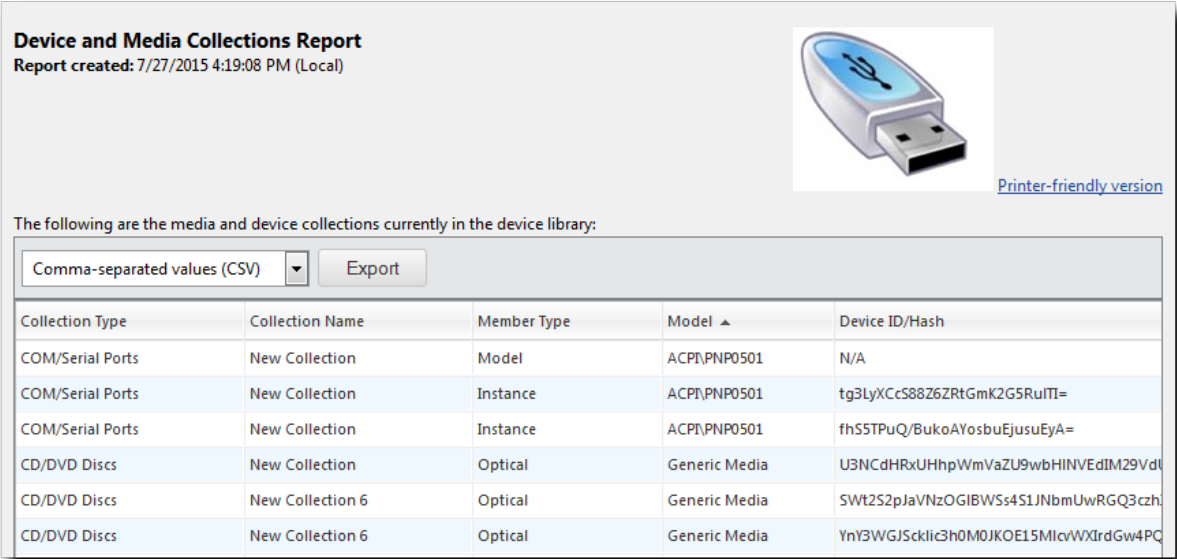


Figure 109: Device and Media Collections Report

The following table describes each report field and column:

Table 62: Device and Media Collections Report Field and Column Definitions


Option	Description
Collection Type	Indicates the device class or media type of the collection.
Collection Name	Indicates the name of the collection.
Member Type	Indicates the type of device or media in the collection.
Model	Indicates the model associated with the device in the collection.
	Note: This field will return N/A for a media collection item.
Device ID/Hash	Indicates the unique serial number of the individual device or hash value of the media in the collection.
	Note: This field will return N/A for a device model collection entry.
Volume Label	Indicates the volume label of the media in the collection.
	Note: This field will return N/A for device collection and device model collection entries.
Comments	Displays any comments associated with the entry.
Date Added to Collection	Indicates the date and time the item was added to the collection.

Device Control Options Report

The **Device Control Options Report** lists the Ivanti Device Control settings defined in the **Options** page.

Device Control Options Report

Report created: 7/27/2015 4:32:49 PM (Local)



[Printer-friendly version](#)

The following are the settings configured on the Device Control tab of the Tools > Options page:

Comma-separated values (CSV)Export

Category	Name	Value
General settings	Server shadow directory	%InstallDirectory%\DeviceControl\Shadow
General settings	Cryptographic compliance mode	False
General settings	Agent status and update notifications	Show all
General settings	Agent permission change notifications	All device permission changes
General settings	Agent action on detect USB key logger	Disabled
Encryption settings	Enforce password complexity	True
Encryption settings	Agent notifies user about encryption opti...	False
Encryption settings	Automatically clear unused space	False
Encryption settings	Retain data when encrypting device	Keep existing data by default - endpoint ...
Encryption settings	Microsoft CA key provider	Enabled (Decentralized)
Encryption settings	Automatic certificate generation	Enabled
Encryption settings	When user tries to write to a CD / DVD in ...	Deny writing to the CD / DVD (no shado...
General settings	Online state definition	Server connectivity
General settings	Syslog server address for endpoint events	
Encryption settings	Password minimum length	7
Encryption settings	Unencrypted device connected prompt	
Encryption settings	Agent encryption grace period	0

Rows per page: 1000 of 17 selectedPage 1 of 111



Figure 110 Device Control Options Report

The following table describes each report field and column:

Table 63: Device Control Options Report Field and Column Definitions

Option	Description
Category	Indicates the type of Ivanti Device Control option. Either General Settings or Encryption Settings.
Name	Indicates the name of the option.
Value	Indicates the setting assigned to the option.

Device Permissions Report

The **Device Permissions Report** lists the Ivanti Device Control policy settings in use for different devices. Entries are sorted by device class.

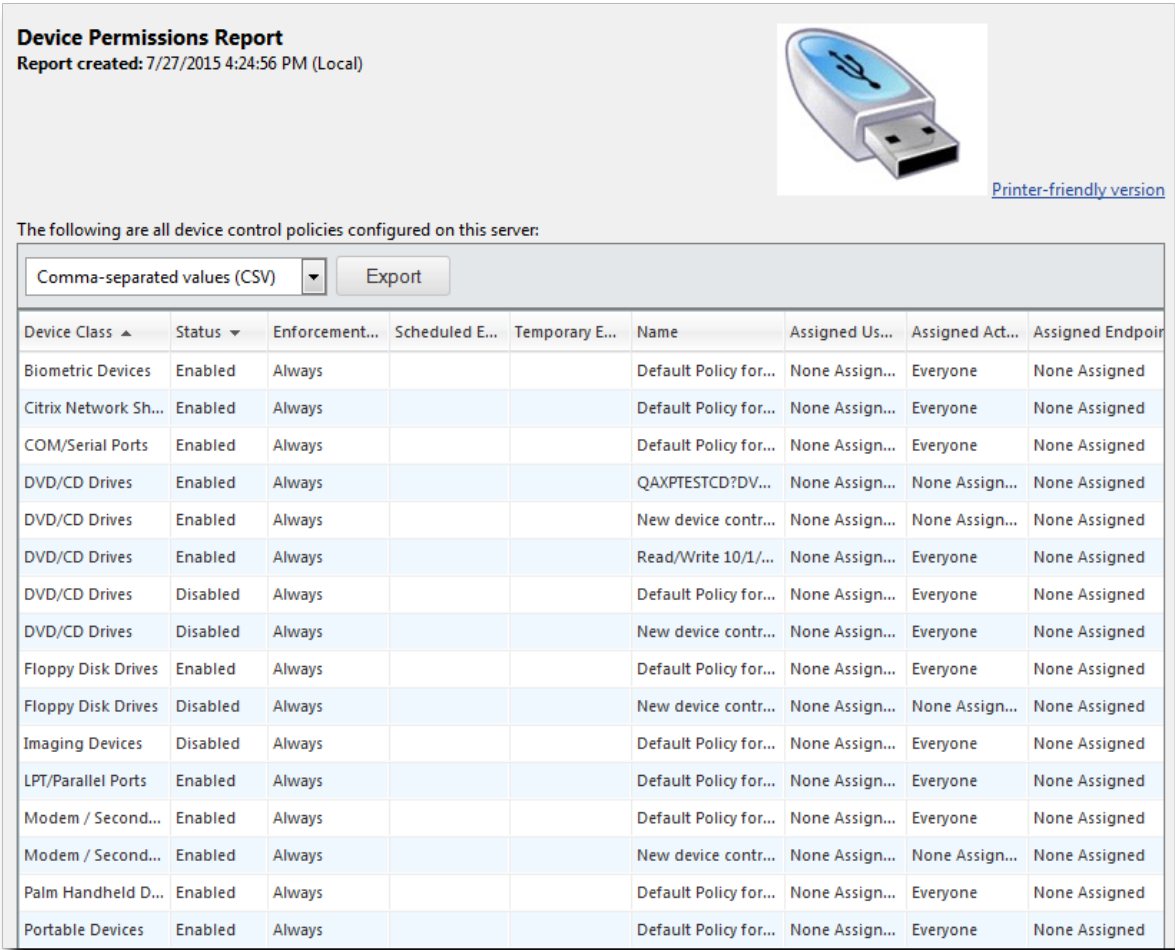


Figure 111: Device Permissions Report

The following table describes each report field and column:

Table 64: Device Permissions Report Field and Column Definitions

Option	Description
Device Class	Indicates the device class to which the policy applies.
Status	Indicates whether the policy is enabled or disabled.



Option	Description
Enforcement Times	Indicates the setting selected in the Policy enforcement option of the Device Policy Wizard .
Scheduled Enforcement	Indicates the scheduled time selected in the Policy enforcement option of the Device Policy Wizard . Note: This column will display a value only if the policy is set to run on a schedule.
Temporary Enforcement	Indicates the scheduled time for a temporary policy selected in the Policy enforcement option of the Device Policy Wizard . Note: This column will display a value only if the policy is set to run temporarily.
Name	Indicates the name of the policy.
Assigned Users	Indicates the users assigned to the policy.
Assigned Active Directory Groups	Indicates the active directory groups assigned to the policy.
Assigned Endpoints	Indicates the endpoints assigned to the policy.
Collections	Indicates the device collection associated with the policy.
Priority	Indicates the priority level of the policy as specified in the Device Policy Wizard .
Assigned Endpoint Groups	Indicates the endpoint groups assigned to the policy.
Copy Limit	Indicates the copy limit specified in the Device Policy Wizard . Note: If a copy limit has not been specified for the policy, this column will read as None .
Permissions	Indicates the access permissions defined in the Device Policy Wizard .
Permission Connections	Indicates the permission connection type selected in the Device Policy Wizard .
Permission Drive Types	Indicates the permission drive types selected in the Device Policy Wizard .
Permission Encryption	Indicates the encryption settings defined in the Device Policy Wizard .
File Filter	Indicates the file filtering settings defined in the Device Policy Wizard .

Option	Description
Read Shadowing	Indicates the shadow on read settings defined in the Device Policy Wizard .
Write Shadowing	Indicates the shadow on write settings defined in the Device Policy Wizard .
Changed By	Indicates the user who last modified the policy settings.
Last Changed	Indicates the server time when the policy was last modified.

Endpoint Permissions Report

The **Endpoint Permissions Report** lists the Ivanti Device Control permission settings that apply to a selected endpoint. Permissions include those that apply directly as well as permissions inherited through group association.

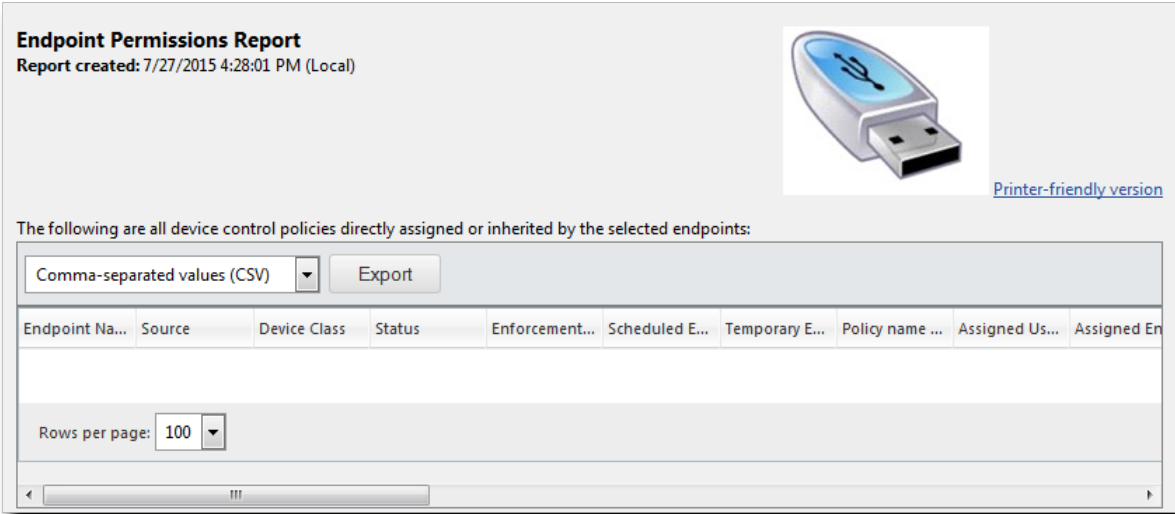


Figure 112: Endpoint Permissions Report

The following table describes each report field and column:

Table 65: Endpoint Permissions Report Field and Column Definitions

Option	Description
Endpoint name	Indicates the name of the endpoint.
Source	Indicates whether the permission applies directly or is inherited.
Device Class	Indicates the device class to which the policy applies.
Status	Indicates whether the policy is enabled or disabled.



Option	Description
Enforcement Times	Indicates the selected setting in the Policy enforcement option of the Device Policy Wizard .
Scheduled Enforcement	Indicates the scheduled time selected in the Policy enforcement option of the Device Policy Wizard . Note: This column will display a value only if the policy is set to run on a schedule.
Temporary Enforcement	Indicates the schedules time for a temporary policy selected in the Policy enforcement option of the Device Policy Wizard . Note: This column will display a value only if the policy is set to run temporarily.
Policy Name	Indicates the name of the policy.
Assigned Users	Indicates the users assigned to the policy.
Assigned Endpoints	Indicates the endpoints assigned to the policy.
Collections	Indicates the device collection associated with the policy.
Priority	Indicates the priority level of the policy as specified in the Device Policy Wizard .
Endpoint Groups	Indicates the endpoint groups assigned to the policy.
Copy Limit	Indicates the copy limit specified in the Device Policy Wizard . Note: If a copy limit has not been specified for the policy, this column will read as None .
Permissions	Indicates the access permissions defined in the Device Policy Wizard .
Permission Connections	Indicates the permission connection type selected in the Device Policy Wizard .
Permission Drive Types	Indicates the permission drive types selected in the Device Policy Wizard .
Permission Encryption	Indicates the encryption settings defined in the Device Policy Wizard .
File Filter	Indicates the file filtering settings defined in the Device Policy Wizard .
Read Shadowing	Indicates the shadow on read settings defined in the Device Policy Wizard .

Option	Description
Write Shadowing	Indicates the shadow on write settings defined in the Device Policy Wizard .
Changed By	Indicates the user who last modified the policy settings.
Last Changed	Indicates the server time when the policy was last modified.

User Permissions Report

The **User Permissions Report** lists the Ivanti Device Control permission settings that apply to a selected user or user group. This report only lists those permissions that directly apply.

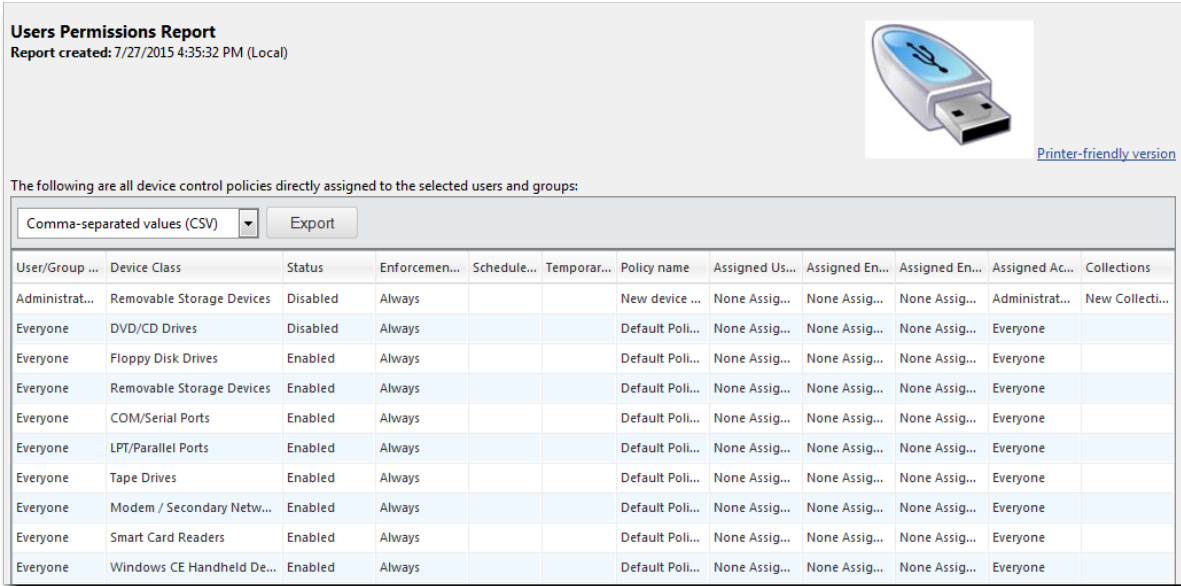


Figure 113: User Permissions Report

The following table describes each report field and column:

Table 66: Endpoint Permissions Report Field and Column Definitions

Option	Description
User/Group Name	Indicates the name of the user or user group.
Device Class	Indicates the device class to which the policy applies.
Status	Indicates whether the policy is enabled or disabled.
Enforcement Times	Indicates the setting selected in the Policy enforcement option of the Device Policy Wizard .

Option	Description
Scheduled Enforcement	Indicates the scheduled time selected in the Policy enforcement option of the Device Policy Wizard .
	Note: This column will display a value only if the policy is set to run on a schedule.
Temporary Enforcement	Indicates the scheduled time for a temporary policy selected in the Policy enforcement option of the Device Policy Wizard .
	Note: This column will display a value only if the policy is set to run temporarily.
Policy Name	Indicates the name of the policy.
Assigned Users	Indicates the users assigned to the policy.
Assigned Endpoints	Indicates the endpoints assigned to the policy.
Collections	Indicates the device collection associated with the policy.
Priority	Indicates the priority level of the policy as specified in the Device Policy Wizard .
Endpoint Groups	Indicates the endpoint groups assigned to the policy.
Copy Limit	Indicates the copy limit specified in the Device Policy Wizard .
	Note: If a copy limit has not been specified for the policy, this column will read as None .
Permissions	Indicates the access permissions defined in the Device Policy Wizard .
Permission Connections	Indicates the permission connection type selected in Device Policy Wizard .
Permission Drive Types	Indicates the permission drive types selected in the Device Policy Wizard .
Permission Encryption	Indicates the encryption settings defined in the Device Policy Wizard .
File Filter	Indicates the file filtering settings defined in the Device Policy Wizard .
Read Shadowing	Indicates the shadow on read settings defined in the Device Policy Wizard .
Write Shadowing	Indicates the shadow on write settings defined in the Device Policy Wizard .

Option	Description
Changed By	Indicates the user who last modified the policy settings.
Last Changed	Indicates the server time when the policy was last modified.



Chapter 10

Managing Individual Users

In this chapter:

- The Directory Sync Schedule Page
- Working with Active Directory Synchronizations
- The Users Page
- Working with Network Users

Some Ivanti Endpoint Security (Ivanti Endpoint Security) modules have policy types that need assignment to specific users (or user groups) as well as to endpoints. These are called *user-based policies*, and users with such policies associated with them are called *individual users*.

Ivanti Device Control has the following user-based policies:

- Device class policy
- Device collection policy
- Media collection policy
- Port control policy

Before these policies can be assigned to individual users, the users must be added to Ivanti Endpoint Security by synchronizing the server with your network's Active Directory. For more information about synchronizing with Active Directory, see [The Directory Sync Schedule Page](#) on page 222.

After synchronization, you can apply Application Control user-based policies to individual users or to organizational units (collections of individual users). For more information, see [The Users Page](#) on page 232.

The Directory Sync Schedule Page

Ivanti Endpoint Security can access your network active directory to associate domain users and groups with product functions. However, to access this functionality, you must first synchronize your Ivanti Endpoint Security Server with your network active directory (AD). Accomplish this task from the **Directory Sync Schedule** page.

Tools > Directory Sync Schedule

Create... Edit... Delete Sync Now Enable Disable Export Options

<input type="checkbox"/>	Name	Sync Server	Sync Source	Frequency	Last Status	Last Status Date	Scheduled Date
<input checked="" type="checkbox"/>	IE-DC-01V - my_company sync	IE-DC-01V	my_company	Weekly: every 1 wee...	Finished	8/17/2015 6:04:21 PM (Server)	8/18/2015 6:00:00 PM (Server)
<div>NameValue</div>							
Sync Duration:		00:04:21					
Last Modified Date:		8/17/2015 8:31:57 PM (Server)					
Last Modified By:		my_company\John.Baker					
Created By:		my_company\Administrator					
Status Details:		Crawl complete					

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

Figure 114: Directory Sync Schedule Page

To open the **Directory Sync Schedule** page:

- 1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**

Synchronizing your server with your Active Directory (AD) compiles a list of network domains, users, and user groups that you can use in the Web console. You can then use these AD objects with product features without accessing the active directory itself.

Note:

- To enable active directory synchronization, open port TCP port 389 on your Ivanti Endpoint Security server and your domain controller, and then complete an active directory synchronization.
- Directory Syncs do not modify Active Directory itself. Your server simply requests information from AD.

About Active Directory Synchronization

You can synchronize active directories in your network with the Ivanti Endpoint Security Server. Data found during synchronization can be used for Ivanti Endpoint Security purposes.

Tools > Directory Sync Schedule

Create...	Edit...	Delete	Sync Now	Enable	Disable	Export	Options
<input type="checkbox"/>	Name	Sync Server	Sync Source	Frequency	Last Status	Last Status Date	Scheduled Date
<input checked="" type="checkbox"/>	IE-DC-01V - my_company sync	IE-DC-01V	my_company	Weekly: every 1 wee...	Finished	8/17/2015 6:04:21 PM (Server)	8/18/2015 6:00:00 PM (Server)
Name		Value					
Sync Duration:		00:04:21					
Last Modified Date:		8/17/2015 8:31:57 PM (Server)					
Last Modified By:		my_company\John.Baker					
Created By:		my_company\Administrator					
Status Details:		Crawl complete					

Rows per page: 1001 of 1 selectedPage 1 of 11

Figure 115: Directory Sync Schedule Page

To open the **Directory Sync Schedule** page:

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**

Synchronizing your server with your Active Directory (AD) compiles a list of network domains, users, and user groups that you can use in the Web console. You can then use these AD objects with product features without accessing the active directory itself.

Note:

- To enable active directory synchronization, open port TCP port 389 on your Ivanti Endpoint Security server and your domain controller, and then complete an active directory synchronization.
- Directory Syncs do not modify Active Directory itself. Your server simply requests information from AD.

Viewing the Directory Sync Schedule Page

Navigate to the **Directory Sync Schedule** page to view directory syncs and their details.

View the **Directory Sync Schedule** page by using the navigation menu.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. [Optional] Define the desired filter criteria.
3. [Optional] Perform a task listed in [Working with Active Directory Synchronizations](#) on page 225.

The Directory Sync Schedule Page Toolbar

The page toolbar features buttons you can use to create or edit directory syncs.

The following table describes each toolbar button.

Table 67: Directory Sync Page Toolbar

Button	Description
Create...	Opens the Schedule Directory Sync dialog to create a new AD sync. For additional information, refer to Creating Directory Syncs on page 226.
Edit	Opens the Edit Directory Sync dialog to edit an existing AD sync. For additional information, refer to Editing Directory Syncs on page 228.
Delete	Deletes the selected directory sync(s). For additional information, refer to Deleting Directory Syncs on page 230.
Sync Now	Launches an immediate directory sync. For additional information, refer to Syncing Directories Immediately on page 231.
Enable	Enables the selected disabled directory sync(s). For additional information, refer to Enabling Disabled Directory Syncs on page 231.
Disable	Disables the selected enabled directory sync(s). For additional information, refer to Disabling Directory Syncs on page 231.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options	Opens the Options menu. For additional information refer to The Options Menu on page 63.

The Directory Sync Schedule Page List

After creating directory syncs, you can view information about their configurations and results.

The following table describes each list column.

Table 68: Directory Sync Schedule Page List

Column	Description
Name	The name of the Directory Sync.



Column	Description
Sync Server	The name of the server that hosts the AD with which you server is synchronizing.
Sync Source	The name of the AD domain or AD containers defined for synchronization with you server.
Frequency	The interval between Directory Syncs.
Icon	The icon that indicates the current status of the Directory Sync.
Last Status	The last status of the Directory Sync.
Last Status Date	The date a time the last time the Directory Sync was scheduled or performed an action.
Scheduled Date	The date and time the Directory Sync is next schedule to synchronize.

Each Directory Sync in the page list can be expanded to show more information. Click the **rotating chevron** (>) for a Sync to display this information. The following table describes the information displayed for an expanded Directory Sync.

Table 69: Expanded Directory Sync

Name	Value
Sync Duration	The duration of the last run sync.
Last Modified Date	The date and time the Directory Sync was last edited.
Last Modified By	The user that last modified the Directory Sync (DOMAIN\Username).
Created By	The user that created the Domain Sync (DOMAIN\Username).
Status Details	Any additional information about the Directory Sync.

Working with Active Directory Synchronizations

You can perform several tasks associated with Active Directory synchronizations.

You can perform the following tasks:

- [Creating Directory Syncs](#) on page 226
- [Editing Directory Syncs](#) on page 228
- [Deleting Directory Syncs](#) on page 230
- [Syncing Directories Immediately](#) on page 231
- [Disabling Directory Syncs](#) on page 231
- [Enabling Disabled Directory Syncs](#) on page 231
- [Exporting Directory Sync Information](#) on page 232

Creating Directory Syncs

Use directory syncs to synchronize your active directory (AD) with Ivanti Endpoint Security.

Create directory syncs from the **Directory Sync Schedule** page.

Attention: To successfully complete a directory sync, port 389 must be open on:

- The Ivanti Endpoint Security Server
- The network domain controller

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Click **Create**.

Step Result: The **Schedule Directory Sync** dialog opens.

3. Type the domain controller name in the **Directory server/computer** field.
4. Type the domain name in the **Domain name** field.

Note: If you select the **Specify one or more directory containers as sync sources** options, defining this field is unnecessary.

5. In the **Domain\user name** field, type a user name that authenticates with the domain controller in the following format: DOMAIN\username
6. Type the password associated with the user in the **Password** field.
7. In the **Confirm password**, retype the password.
8. Select the appropriate **Sync scope** option.

These options define whether the directory sync synchronizes with entire directory or individual containers within the directory.

Tip: Select the **Specify one or more directory containers as sync sources** options for one of the following reasons:

- The AD is large, causing long synchronization times.
- Portions of the directory are geographically dispersed and thus require a sync at different starting and ending times.
- Portions of the directory may be updated more frequently than others and thus require a sync at different intervals.
- The credentials defined in the **Domain\user name** field cannot access the entire domain.

Option	Step
To sync the entire domain:	<ol style="list-style-type: none">1. Select the Sync the entire domain (recommended) option.2. Click Next.



Option	Step
To specify one or more directory containers as sync sources:	<ol style="list-style-type: none"> 1. Select the Specify one or more directory containers as sync sources option. 2. Click Next. 3. In the field, type the fully-qualified domain name of the directory containers you want to sync (for example, OU=Sub-Organization Unit,OU=Organization Unit,DC=Domain Controller). 4. Click Add Directory Path. 5. Specify additional directory containers by repeating the previous two steps. 6. Review the Directory Path list. Click the applicable Delete icon to remove directory paths you do not want to add. 7. Click Next.

Step Result: The **Schedule Sync** page opens.

9. Schedule the sync.

Option	Step
To schedule a daily sync:	<ol style="list-style-type: none"> 1. Select the Daily option. 2. Type the desired Start date in a mm/dd/yyyy format. 3. Type the desired Start time in a hh:mm format. You may use 12-hour or 24-hour formatting. 4. In the Run every x days field, type how often you want your sync to run. 5. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a mm/dd/yyyy format.
To schedule a weekly sync:	<ol style="list-style-type: none"> 1. Select the Weekly option. 2. Type the desired Start date in a mm/dd/yyyy format. 3. Type the desired Start time in a hh:mm format. You may use 12-hour or 24-hour formatting. 4. In the Run every x weeks on field, type the desired increment. 5. Select the check boxes associated with the days you want the sync to run. 6. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a mm/dd/yyyy format.

Option	Step
To schedule a monthly sync:	<ol style="list-style-type: none">1. Select the Monthly option.2. Type the desired Start date in a <code>mm/dd/yyyy</code> format.3. Type the desired Start time in a <code>hh:mm</code> format. You may use 12-hour or 24-hour formatting.4. Select an option:<ol style="list-style-type: none">a. To schedule the sync for a specific date, select the Run on the x day every x months option. Then define the day and months fields.b. To schedule the sync for a relative day, select the Run on the x x every x month. Then define the drop-down lists and the months field.5. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a <code>mm/dd/yyyy</code> format.

Note: Rather than typing a specific date or time when scheduling the sync, you may select them from a menu. Click the **Calendar** and **Clock** icons to open these menus.

10. Click **Finish**.

Result: The **Schedule Directory Sync** dialog closes and the sync is scheduled. An item for the sync displays in the **Schedule Directory Sync** page list.

Tip: After you create the sync, select it from the **Schedule Directory Sync** page and click **Sync Now** to run it immediately.

Editing Directory Syncs

After creating a directory sync, you can edit its synchronization schedule and its synchronization target. Edit directory syncs from the **Directory Sync Schedule** page.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Select the check box associated with the directory sync you want to edit.
3. Click **Edit**.

Step Result: The **Schedule Directory Sync** dialog opens.

4. [Optional] Edit the **Directory server/computer** field.
5. [Optional] Edit the **Domain name** field.
6. [Optional] Edit the **Domain\user name** field.
 - a) Edit the **Password** field to the password associated with the new user name.
 - b) Retype the password in the **Confirm password** field.



7. [Optional] Edit the **Sync scope** option.

Follow the applicable substeps to edit the sync scope.

Option	Step
To sync the entire domain:	<ol style="list-style-type: none"> 1. Select the Sync the entire domain (recommended) option. 2. Click Next.
To specify one or more directory containers as sync sources:	<ol style="list-style-type: none"> 1. Select the Specify one or more directory containers as sync sources option. 2. Click Next. 3. In the field, type the fully-qualified domain name of the directory containers you want to sync (for example, OU=Sub-Organization Unit, OU=Organization Unit, DC=Domain Controller). 4. Click Add Directory Path. 5. Specify additional directory containers by repeating the previous two steps. 6. Review the Directory Path list. Click the applicable Delete icon to remove directory paths you do not want to add. 7. Click Next.

8. Schedule the sync.

Option	Step
To schedule a daily sync:	<ol style="list-style-type: none"> 1. Select the Daily option. 2. Type the desired Start date in a <code>mm/dd/yyyy</code> format. 3. Type the desired Start time in a <code>hh:mm</code> format. You may use 12-hour or 24-hour formatting. 4. In the Run every x days field, type how often you want your sync to run. 5. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a <code>mm/dd/yyyy</code> format.

Option	Step
To schedule a weekly sync:	<ol style="list-style-type: none"> 1. Select the Weekly option. 2. Type the desired Start date in a mm/dd/yyyy format. 3. Type the desired Start time in a hh:mm format. You may use 12-hour or 24-hour formatting. 4. In the Run every x weeks on field, type the desired increment. 5. Select the check boxes associated with the days you want the sync to run. 6. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a mm/dd/yyyy format.
To schedule a monthly sync:	<ol style="list-style-type: none"> 1. Select the Monthly option. 2. Type the desired Start date in a mm/dd/yyyy format. 3. Type the desired Start time in a hh:mm format. You may use 12-hour or 24-hour formatting. 4. Select an option: <ol style="list-style-type: none"> a. To schedule the sync for a specific date, select the Run on the x day every x months option. Then define the day and months fields. b. To schedule the sync for a relative day, select the Run on the x x every x month. Then define the drop-down lists and the months field. 5. Schedule an End by date. To schedule an End by date, select the check box and type an end date in a mm/dd/yyyy format.

Note: Rather than typing a specific date or time when scheduling the sync, you may select them from a menu. Click the **Calendar** and **Clock** icons to open these menus.

9. Click **Finish**.

Result: The **Schedule Directory Sync** dialog closes and the changes are saved. The associated list item for the sync changes according to your edits, and the sync runs against the applicable AD at the new schedule time.

Deleting Directory Syncs

Delete Directory Syncs when they are no longer needed.

Delete syncs from the **Directory Sync Schedule** page.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Ensure the page is filtered to display disabled syncs.

3. Select the Directory Syncs you want to delete.
4. Click **Delete**.

Result: The Directory Syncs are deleted.

Syncing Directories Immediately

After creating a directory sync, you can trigger it to synchronize with its targeted Active Directory at any time, regardless of its schedule.

Run immediate directory syncs from the **Directory Sync Schedule** page.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Select the Directory Syncs you want to run immediately.

Note: You can only run immediate directory syncs for enabled syncs. For additional information refer to [Enabling Disabled Directory Syncs](#) on page 231.

3. Click **Sync Now**.

Result: The selected syncs run immediately.

Disabling Directory Syncs

Rather than deleting a directory sync, you can temporarily disable it when unnecessary. Disabling unnecessary directory syncs can improve network bandwidth at the applicable syncs scheduled time.

Disable directory syncs from the **Directory Sync Schedule** page.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Select the Directory Sync you want to disable.

Tip: In some instances, you may need to filter the page to display to show enabled syncs.

3. Click **Disable**.

Result: The selected Directory Sync are disabled and will not run at its scheduled date and times. Synchronization will not occur until the sync is re-enabled.

Enabling Disabled Directory Syncs

After disabling a directory sync, you may re-enable it at any time.

Re-enable directory syncs from the **Directory Sync Schedule** page.

1. From the **Navigation Menu**, select **Tools > Directory Sync Schedule**.
2. Ensure the page is filtered to display disabled Directory Syncs.
3. Select the Directory Syncs you want to re-enable.

4. Click **Enable**.

Result: The selected directory syncs are re-enabled. Synchronization occurs at the next scheduled time.

Exporting Directory Sync Information

To export the directory sync information listed on ***Schedule Sync Schedule*** page to a comma separated value (.csv) file, click the **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information refer to [Exporting Data](#) on page 71.

The Users Page

This page lists users discovered during active directory synchronization jobs (directory syncs). Use this page to view or create individual users, which you can manage using Ivanti Endpoint Security features. This page features a directory tree, which lists users and user groups discovered during directory syncs. You can select items in this tree. After selecting an item, information about that item displays on the page.

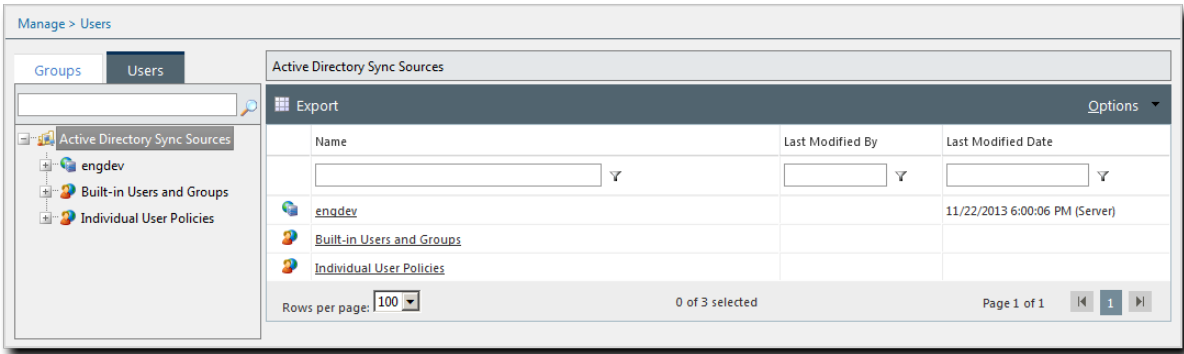


Figure 116: Users Page

The **Users** page contains a breadcrumb that indicates your position in the user browser directory tree. Click links in the breadcrumb to move closer to the directory tree root level.

The User Browser Directory Tree

Use the **User Browser**, a **Users** page pane, to select users found during directory syncs. The number of users in the tree depends on the number of users detected during syncs.

Click an **Expand** icon (+) to view active directory sync sources, built-in users and groups, or individual user policies. By expanding the tree, information for selected items becomes more detailed.

To display detailed user information, select a user or group name. After selecting a user or group name from **Built-in Users and Groups** or **Individual User Policies**, use the **View** list to access different

views. After selecting a **Built-in Users and Groups** or **Individual User Policies** item, you can select from the following view:

- **Information**
- **Application Control Policies**
- **Device Control Policies**

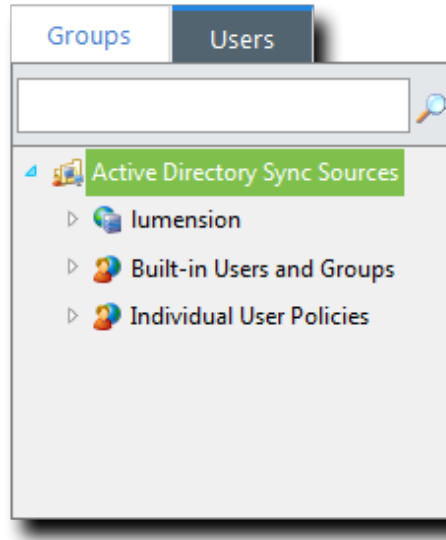


Figure 117: User Browser Directory Tree

Tip: Click the **Groups** tab to open the **Groups** page.

The Users Page Toolbar

This toolbar contains buttons related to assignment of policies to individual users. The buttons that display change based on the item selected from the **User Browser** directory tree.

The following topics describe the toolbar buttons that display based on the **User Browser** directory tree item selected:

- [The Users Page Toolbar \(Active Directory Sync Sources\)](#) on page 234
- [The Users Page Toolbar \(Built-in Users and Groups\)](#) on page 234
- [The Users Page Toolbar \(Built-in Users and Groups Items\)](#) on page 235
- [The Users Page Toolbar \(Individual User Policies\)](#) on page 236
- [The Users Page Toolbar \(Individual User Policies Items\)](#) on page 237

The Users Page Toolbar (Active Directory Sync Sources)

This toolbar contains buttons related to data exportation.

The following table describes the buttons available when **Active Directory Sync Sources** is selected from the **User Browser** directory tree.

Table 70: Users Page Toolbar Buttons (Active Directory Sync Sources)

Button	Description
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

Note: The *Users* page toolbar only appears when the **Application Control Policies** or the **Device Control Policies** view is selected.

The Users Page Toolbar (Built-in Users and Groups)

This toolbar contains buttons related to data exportation.

The following table describes the buttons available when **Active Directory Sync Sources** is selected from the **User Browser** directory tree.

Table 71: Users Page Toolbar Buttons (Active Directory Sync Sources)

Button	Description
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

Note: The *Users* page toolbar only appears when the **Application Control Policies** or the **Device Control Policies** view is selected.



The Users Page Toolbar (Built-in Users and Groups Items)

This toolbar contains buttons related to data exportation.

The following table describes the buttons available when an item is selected from the **Built-in Users and Groups** subitems in the **User Browser** directory tree and the **Application Control Policies** view is selected (Application Control only).

Table 72: Users Page Toolbar Buttons (Built-in Users and Groups Items)

Button	Description
Unassign	Unassigns the selected policy (or policies) from the selected user(s). For additional information, refer to Unassigning Policies from Users on page 246.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71. Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

The following table describes the buttons available when an item is selected from the **Built-in Users and Groups** subitems in the **User Browser** directory tree and the **Device Control Policies** view is selected (Device Control only).

Table 73: Users Page Toolbar Buttons (Built-in Users and Groups Items)

Button	Description
Create...	Opens the Create menu.
Device Class Policy (Create... Menu Item)	Opens the Device Class Policy Wizard . Use this wizard to create a device class policy. When you complete the wizard, the policy is assigned to selected user or group.
Device Collection Policy (Create... Menu Item)	Opens the Device Collection Policy Wizard . Use this wizard to create a device collection policy. When you complete the wizard, the policy is assigned to selected user or group.
Media Collection Policy (Create... Menu Item)	Opens the Media Collection Policy Wizard . Use this wizard to create a media collection class policy. When you complete the wizard, the policy is assigned to selected user or group.

Button	Description
Port Collection Policy (Create... Menu Item)	Opens the Port Collection Wizard . Use this wizard to create a port collection policy. When you complete the wizard, the policy is assigned to selected user or group
Assign...	Opens the Assign Policy dialog. Use this dialog to assign an existing policy to the user or group.
Unassign	Unassigns any policies assigned to the selected user or group.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71. Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

Note: The **Users** page toolbar only appears when the **Application Control Policies** or the **Device Control Policies** view is selected.

The Users Page Toolbar (Individual User Policies)

This toolbar contains buttons related to individual user management and data exportation.

The following table describes the toolbar buttons that are available when **Individual User Policies** is selected from the **User Browser** directory tree.

Table 74: Users Page Toolbar Buttons (Individual User Policies)

Button	Description
Add	Adds a user to Individual User Policies . For additional information on adding users to Individual User Policies , refer to Adding an Individual User to a Policy on page 244.
Remove	Removes a user from Individual User Policies . For additional information on removing users from Individual User Policies , refer to Removing an Individual User from the User Browser on page 245.

Button	Description
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

Note: The **Users** page toolbar only appears when the **Application Control Policies** or the **Device Control Policies** view is selected.

The Users Page Toolbar (Individual User Policies Items)

This toolbar contains buttons related to data exportation.

The following table describes the buttons available when an item is selected from the **Individual User Policies** subitems in the **User Browser** directory tree.

Table 75: Users Page Toolbar Buttons (Individual User Policies Items)

Button	Description
Unassign	Unassigns the selected policy (or policies) from the selected user(s). For additional information, refer to Unassigning Policies from Users on page 246.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 71.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the Options menu.

Note: The **Users** page toolbar only appears when the **Application Control Policies** or the **Device Control Policies** view is selected.

The Users Page List

On the main portion of the **Users** page, information about the item selected from the **User Browser** directory tree is displayed. This main portion is called the **Users** page list.

Information displayed in the list changes depending on the item selected from the **User Browser**.

The following topics describe the information that displays when you select a **User Browser** directory tree item:

- [The Users Page List \(Active Directory Sync Sources\)](#) on page 238
- [The Users Page List \(Built-in Users and Groups\)](#) on page 238
- [The Users Page List \(Built-in Users and Groups Items\)](#) on page 239
- [The Users Page List \(Individual User Policies\)](#) on page 241
- [The Users Page List \(Individual User Policies Items\)](#) on page 242

The Users Page List (Active Directory Sync Sources)

When **Active Directory Sync Sources** is selected from the **Users** page **User Browser** directory tree, information about built-in users and groups and individual user policies is displayed.

The following table describes each column that displays when **Active Directory Sync Sources** is selected.

Table 76: Users Page List (Active Directory Sync Sources)

Column	Description
Name	The name of an active directory sync source. Clicking a Name link selects the applicable group within the User Browser directory tree.
Last Modified By	The Ivanti Endpoint Security user that last modified an item within the applicable sync source.
Last Modified Date	The date that the sync source was last modified.

The Users Page List (Built-in Users and Groups)

When **Built-in Users and Groups** is selected from the **Users Browser** directory tree, information about standard built-in users and groups found in active directories are displayed.

The following table describes each column that displays when **Built-in Users and Groups** is selected.

Table 77: Users Page List (Built-in Users and Groups)

Column	Description
Name	The name of a user or group built in to active directory.
Last Modified By	The last user that last modified an item within the applicable sync source.
Last Modified Date	The date that the sync source was last modified.



The Users Page List (Built-in Users and Groups Items)

When an item under **Built-in Users and Groups** is selected from the **User Browser** directory tree, information about that built-in user or group is displayed.

There are several views for each **Built-in Users and Groups** item. After you select a **Built-in Users and Groups** item, you can change the data displayed by selecting a different item from the **View** list. You can select from the following views:

- **Information**
- **Application Control Policies** (Application Control only)
- **Device Control Policies** (Device Control only)

The following table describes each field that displays when a **Built-in Users and Groups** item is selected from the **User Browser** and **Information** is selected from the **View** list.

Table 78: Users Page List (Information View)

Field	Description
Name	The name of the built-in user or group.
Distinguished Name	The organizational unit and common name for the select item.
Last Modified Date	The date the user or group was last modified.
Last Modified By	The user that last modified the user or group.
Sync Name	The name of the sync job that detected the user or group.
Frequency	The frequency of the sync job that detected the user or group.
Last Status	The last status of the sync job that detected the user or group.
Last Status Date	The date that the last status was updated.
Started On	The date the sync job that detected the user or group first ran.
Ended On	The date the sync job that detected the user or group is scheduled to run for the last time.

The following table describes each column that displays when a **Built-in Users and Groups** item is selected from the **User Browser** directory tree and **Application Control Policies** is selected from the **View** list.

Table 79: Users Page List (Application Control Policies View)

Column	Description
Action	Contains a Remove icon you can use to unassign the policy from the selected user.

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (Denied Applications , Supplemental Easy Lockdown/Auditor, Trusted Path, and Local Authorization).
Blocking	Indicates the policy blocking value (N/A, Off, Non-authorized).
Logging	Indicates the policy logging value (Off, On, Authorized, Non-authorized, Non-authorized Authorized)
Source	Indicates the policy source (Assigned or Unassigned).
Assigned Date	Indicates the date and time the policy was assigned to the selected network user.

Additionally, when the **Application Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 80: Users Page List Expanded Items (Application Control Policies View)

Field	Description
Created by	The Ivanti Endpoint Security user who created the policy applied to the selected network user.
Created date	The date and time the policy was created.
Last updated by	The Ivanti Endpoint Security user who last modified the applicable policy.
Last updated date	The date and time the policy was last modified.
Trusted Paths	The trusted path(s) applied to the selected network user.
	Note: This field only appears for Trusted Path policies.

The following table describes each column that displays when a **Built-in Users and Groups** item is selected from the **User Browser** directory tree and **Device Control Policies** is selected from the **View** list.

Table 81: Users Page List (Device Control Policies View)

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.

Column	Description
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (Device Class Policy, Device Collection Policy, Media Collection Policy, and Port Control Policy).
Device Collection	Indicates the device collection the policy applies to.
Source	Indicates the policy source (Assigned or Unassigned).
Device Class	Indicates the device class the policy applies to.
Last Update	Indicates the date and time the policy was last updated.

Additionally, when the **Device Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 82: Users Page List Expanded Items (Device Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.
Description	The description of the individual policy.

The Users Page List (Individual User Policies)

When **Individual User Policies** is selected from the **User Browser** directory tree, a list of manually added network users that have policies directly applied to them is displayed.

The following table describes each column that displays when **Individual User Policies** is selected.

Table 83: Users Page List (Individual User Policies)

Column	Description
Name	The name of the user. Click the name to move to that user in the User Browser directory tree.
Email	The email address of the user.
Last Modified By	The user that last modified the user within the User Browser directory tree.
Last Modified Date	The date that the user was last modified.

The Users Page List (Individual User Policies Items)

When you select an item beneath **Individual User Policies** in the **Users Browser** directory tree, information about that user and its associated policies are displayed.

There are several views for each **Individual User Policies** item. After you select a **Individual User Policies** item, you can change the data displayed by selecting a different item from the **View** list. You can select from the following views:

- **Information**
- **Application Control Policies** (Application Control only)
- **Device Control Policies** (Device Control only)

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Information** is selected from the **View** list.

Table 84: Users Page List (Information View)

Field	Description
Name	The name of the individually added user or group.
Distinguished Name	The organizational unit and common name for the select item.
Last Modified Date	The date the user or group was last modified.
Last Modified By	The user that last modified the user or group.
Sync Name	The name of the sync job that detected the user or group.
Frequency	The frequency of the sync job that detected the user or group.
Last Status	The last status of the sync job that detected the user or group.
Last Status Date	The date that the last status was updated.
Started On	The date the sync job that detected the user or group first ran.
Ended On	The date the sync job that detected the user or group is scheduled to run for the last time.

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Application Controll Policies** is selected from the **View** list.

Table 85: Users Page List (Application Control Policies View)

Column	Description
Action	Contains a Remove icon you can user to unassign the policy from the selected user.



Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (Denied Applications , Supplemental Easy Lockdown/Auditor, Trusted Path, and Local Authorization).
Blocking	Indicates the policy blocking value (N/A, Off, Non-authorized).
Logging	Indicates the policy logging value (Off, On, Authorized, Non-authorized, Non-authorized Authorized)
Source	Indicates the policy source (Assigned or Unassigned).
Assigned Date	Indicates the date and time the policy was assigned to the selected network user.

Additionally, when the **Application Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 86: Users Page List Expanded Items (Application Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Device Control Policies** is selected from the **View** list.

Table 87: Users Page List (Device Control Policies View)

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (Device Class Policy, Device Collection Policy, Media Collection Policy, Port Control Policy)
Device Class	Indicates the device class the policy applies to.
Device Collection	Indicates the device collection the policy applies to.

Column	Description
Source	Indicates the policy source (Assigned or Unassigned).
Last Update	Indicates the date and time the policy was last updated.

Additionally, when the **Device Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 88: Users Page List Expanded Items (Device Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.
Description	The description of the individual policy.

Working with Network Users

After directory syncs complete, you can incorporate user data into management of denied application, supplemental easy lockdown/auditory, trusted path, and local authorization policies. Tasks associated with users found during directory syncs are completed from the **Users** page.

You can perform the following tasks related to network users:

- [Adding an Individual User to a Policy](#) on page 244
- [Removing an Individual User from the User Browser](#) on page 245
- [Unassigning Policies from Users](#) on page 246
- [Exporting User Data](#) on page 246

Adding an Individual User to a Policy

You can add one or more individual users to a policy using the **Add Individual Users** dialog.

This dialog is accessed by clicking the **Add Individual User** button on a **User** pane. This feature is available on wizards that support user assignment.

1. Search for users using either of the following methods:

Option	Steps
Search for all users	Leave the Username field blank and click Search . This returns all existing users in the current domain.



Option	Steps
Search for one or more selected users	1. Type a user name in the Username field.
	Note: Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches
	2. Click Search .

Step Result: One or more users appear in the results list.

Note: If you cannot find the user(s) you want, try searching other available domains. Select a searchable domain controller from the **Domain** drop-down list.

2. Select one or more users.

3. Click **Add Users**.

Step Result: The users are added to the selection list.

4. Click **OK**.

Step Result: The **Add Individual Users** dialog closes and you return to the **Users** pane of the policy wizard, with the new user(s) added to the **Users** list.

Removing an Individual User from the User Browser

When you no longer want to apply a policy to an individual user, remove that user from **Individual User Policies** in the **User Browser** directory tree.

Remove individual users from the **User Browser** from the **Users** page.

1. Select **Manage > Users**.

Step Result: The **Users** page opens.

2. Expand the directory tree to **Individual User Policies**.

3. From the page list, select the individual user(s) you want to remove.

4. Click **Remove**.

Step Result: A dialog opens, asking if you want to remove the selected user(s).

5. Click **OK**.

Result: The user is removed from **Individual User Policies**.

Unassigning Policies from Users

You can unassign user-based Application Control policies from individual users. You can unassign policies from **Built-in Users and Groups** items and **Individual User Policies** items.

Unassign policies from individual users from the **Users** page.

1. Select **Manage > Users**.
2. Expand the **User Browser** directory tree to the user you want to remove a policy from.
Users can be found in the following User Browser directory tree items:
 - **Built-in Users and Groups**
 - **Individual User Policies**
3. Ensure the **Application Control Policies** view is selected.
4. From the list, select the policy (or policies) you want to unassign.
5. Click **Unassign**.

Exporting User Data

From the **Users** page, you can export all information about the item selected from the User Browser directory tree to a comma separated value (.csv) file. The exported information, which changes based on the **View** selected, can be used for reporting and analytical purposes.

For additional information, refer to [Exporting Data](#) on page 71.

Chapter

11

Using the Device Control Client

In this chapter:

- Device Control Client Menu
- About Encrypting Devices
- Using the Encrypt Medium Utility
- Transferring Encryption Keys

The Device Control client provides user access to encryption options for CD/DVDs and removable storage devices. A user can encrypt and manage devices with the client, provided that the network administrator establishes the necessary device permission and user access policies with the Management Console.

Device Control Client Menu

When you right-click the Device Control icon from the system tray, the client options menu displays.

Option	Description
Status	Displays a summary of all permissions, copy limits, shadowing settings, and file type filters that apply to devices and device classes for the Device Control client user that is logged on.
Request temporary access offline	Allows you to change a password on a temporary basis, in cooperation with a Device Control administrator, when you are not connected to the corporate network.
Create an Encrypted CD/DVD	Allows you to encrypt CD/DVD media.

About Encrypting Devices

You can use the Ivanti Device and Application Control client to encrypt devices from your computer, without the assistance of a network administrator.

You can use the client to perform the following tasks:

- Open portable media.
- Decrypt encrypted removable storage devices.
- Encrypt removable storage devices for Windows and passphrase users.
- Export an encryption key from a removable storage device to a file.

Encrypting CD/DVDs for Multiple Users

Using the Ivanti Device and Application Control client, you can encrypt CD/DVDs for multiple users from a client computer.

Prerequisites:

Insert a CD or DVD for encryption.

Note: You may receive an encryption request notice regarding read/encrypt/write privileges, if the administrator enables the Encryption notification default option. For more information, see [The Ivanti Device Control Options Page](#) on page 189.

You can specify additional users by passphrase or by Windows® Active Directory. Advanced encryption options allow you to save or erase all existing data on the device. You may also select encryption options that determine whether the device can be used outside of the corporate network.

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

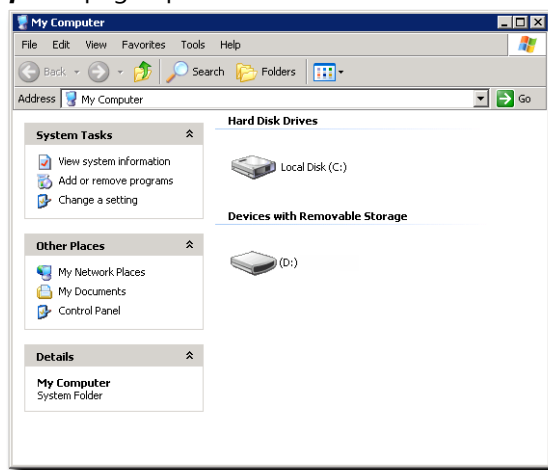


Figure 118: My Computer Page

2. Right-click the CD/DVD label name to encrypt.

Step Result: The CD/DVD encryption shortcut menu opens.

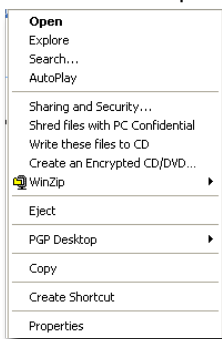


Figure 119: CD/DVD Encryption Menu

3. Click **Create an Encrypted CD/DVD**.

Step Result: The **Secure Volume Browser** dialog opens.

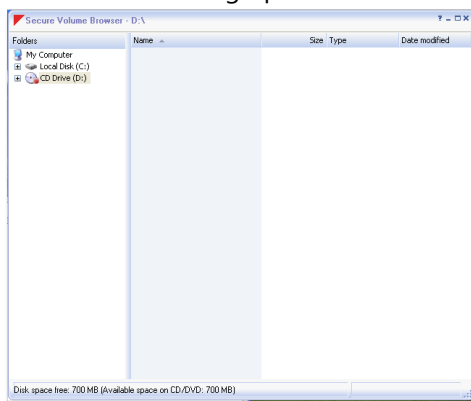


Figure 120: Secure Volume Browser Dialog

4. Add the files to the CD/DVD that you want to encrypt.

5. Right-click the CD/DVD label name for encryption.

Step Result: The CD/DVD encryption shortcut menu opens.

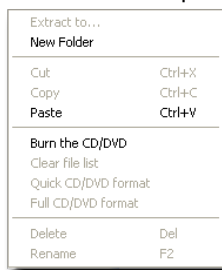


Figure 121: CD/DVD Menu

6. Click **Burn the CD/DVD**.

Step Result: After retrieving information for the logged in user, the **Add Passphrase** dialog opens.

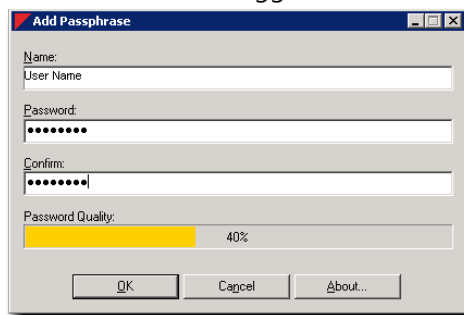


Figure 122: Add Passphrase Dialog

Important: In the **Name** field, *Primary User* is preselected and shaded because you must enter a the primary user password before proceeding.

7. Type a password in the **Password** field, and retype the password in the **Confirm** field.

8. Click **OK**.

Step Result: The **Encrypt Medium** dialog opens, showing the name of the logged in user and the Primary User passphrase user.

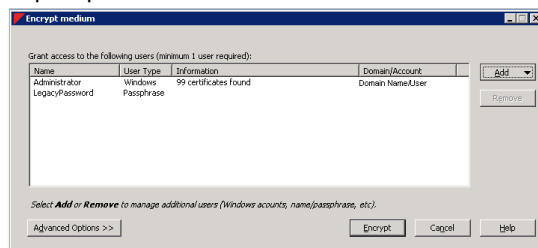


Figure 123: Encrypt Medium Dialog

9. Click **Add**.

Important: At least one user who is allowed access to the encrypted device must be listed. For CD/DVD encryption, one passphrase user is required to be listed.

Step Result: Options for adding users display.

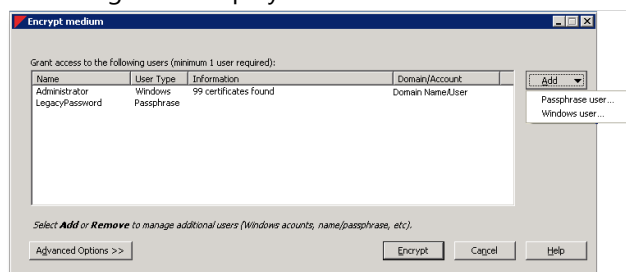


Figure 124: Encrypt Medium Dialog - Add User

10. Select one of the following options:

These options depend upon your environment and configuration.

Option	Description
Passphrase user	Adds a user name with password access.

Option	Description
Windows user	Adds users or groups of users listed in your company directory.

Step Result: Depending on the option you select, one of the following dialogs opens. If you select **Passphrase user**, the **Add Passphrase** dialog opens.

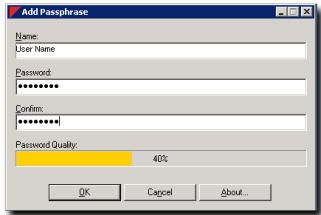


Figure 125: Add Passphrase Dialog

If you selected **Windows user**, the **Select Users or Groups** dialog opens.

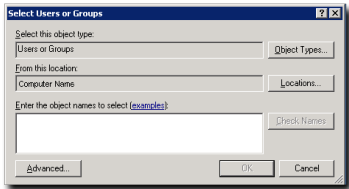


Figure 126: Select Users or Groups Dialog

11.Perform one of the following steps.

12.To add a **Passphrase user**:

- a) Type a user name in the **Name** field.
- b) Type a **Password** in the corresponding field, and then retype the password to **Confirm** in the corresponding field.
- c) Click **OK**.

Step Result: The user name is added to the list shown in the **Encrypt Medium** dialog.

13.To add a **Windows user** in the **Enter the object names to select field**, enter the names of the users to add to the list, using one of the following formats:

Object Name	Example
Display Name	FirstName LastName
UserName	User1
ObjectName@DomainName	User1@Domain1

Object Name	Example
DomainName\ObjectName	Domain\User1

a) To verify the object name, click **Check Names**.

Step Result: The object name is verified and underlined when correctly entered.

14. When you finish adding users, click **Next**.

Step Result: The **Burning Encrypted Media** dialog opens.

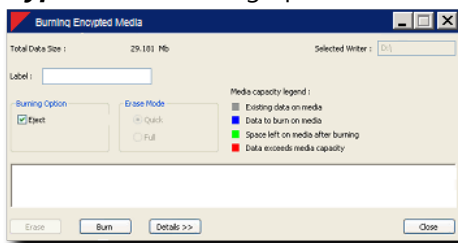


Figure 127: Burning Encrypted Media Dialog

Note: You may enter a volume label and/or choose to eject the CD/DVD when finished burning.

15. Click **Burn**.

Important: Anything shown in red will not be encrypted.

16. When encryption is complete, click **Close**.

Result: The CD/DVD is encrypted for the specified users. The encrypted CD/DVD automatically unlocks when inserted on a client computer. When inserting the encrypted CD/DVD on a non-client computer, the user is prompted to enter a password.

Note: If a valid digital certificate cannot be retrieved for the Windows user you are adding, you receive the following message in the **Encrypt Medium** dialog: No certificates found; user will not be added.

Managing Device Passwords

You can change and recover user passwords for an encrypted device from the **Manage Device** dialog of the client.

To manage device passwords for encrypted devices from your computer using the Windows Explorer:

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

2. Right-click the name of the device listed under **Devices with Removable Storage** and select **Managing Devices**.

Step Result: The **Manage Device** dialog opens.

3. Select a user from the list.
4. Click **Change**.

Step Result: The **Change Password** dialog opens.

5. Type your current password in the **Old Password** field.
6. Type a new password in the **Password** field.
7. Retype the new password in the **Confirm** field.
8. Click **OK**.

Step Result: The **Change Password** dialog closes and you return to the **Manage Device** window.

9. Click **OK**.

Result: You receive a confirmation message that the password change applies to your device.

Manage Device

You can change user passwords for encrypted devices from the **Manage Device** window.

1. Click **Unlock**.
2. In the **Unlock Medium** dialog, enter the password you used to encrypt the device.

Note: If the **Support older product versions** check box is displayed, and there are multiple **Passphrase** users on the device, you may select this option to use the new password to access the device on computers using older versions of Device Control.

3. Select a **User** from the list shown.
4. Click **Change**.

Step Result: The **Change Password** dialog opens.

5. To change your password:
 - a) Type your **Old Password** in the field provided.
 - b) Type a new password in the **Password** field.
 - c) Retype the new password in the **Confirm** field.

6. If you select **Advanced Options**, the shaded options show how the device was encrypted, as described in the following table.

Option	Description
Encrypted for portable use (128 GB limit)	Allows use of an encrypted device on any computer running Microsoft® Windows®.
Encrypted for internal use (2 TB limit)	Allows use of devices only inside your network on computers that are managed by Device Control.

7. Click **OK**.

Result: A confirmation message is sent indicating that the password change has been applied.

Unlocking Media

You can unlock an encrypted removable storage device attached to a computer running the client using Windows Explorer.

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

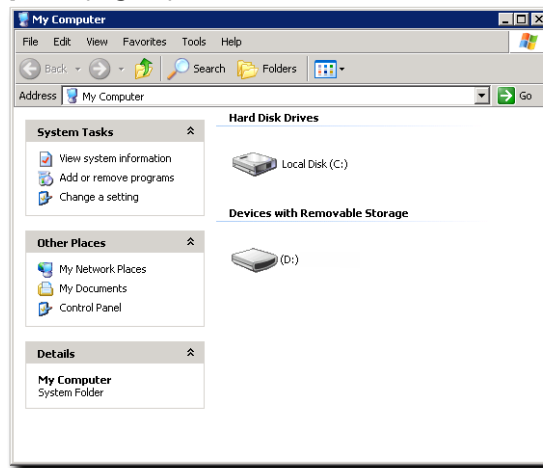


Figure 128: My Computer Page

2. Right-click the name of the device listed under **Devices with Removable Storage**.
3. Select **Unlock Medium**.

Step Result: **RTNotify** sends a message to the user confirming that the device is unlocked.

4. Click **OK**.

Result: The removable storage device is unlocked.

Opening Portable Media

You can open encrypted removable storage devices as portable media using Windows Explorer.

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

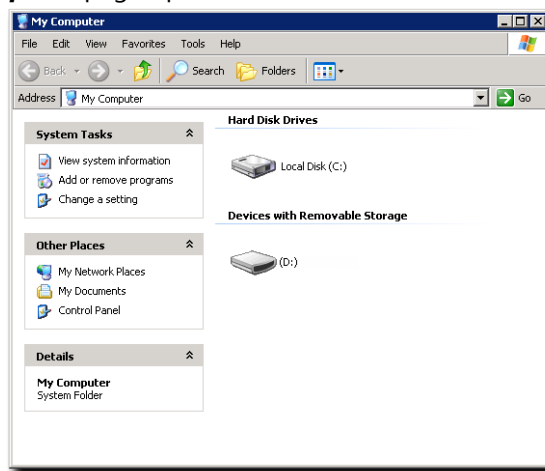


Figure 129: My Computer Page

2. Select the name of the device listed under **Devices with Removable Storage**.
3. Right-click **Open as Portable Media Device**.

Result: The removable storage device is shown as open on the **My Computer** page.

Decrypting Media

Using the Ivanti Device and Application Control client, you can decrypt removable storage devices encrypted by Device Control.

Caution: Decrypting a medium is the same as formatting a medium and all data on the medium will be erased.

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

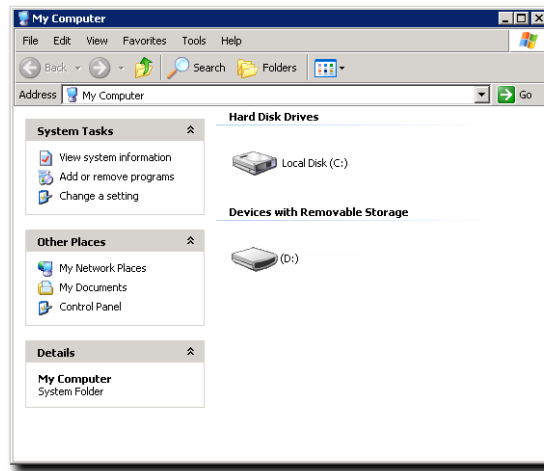


Figure 130: My Computer Page

2. Right-click the name of the device listed under **Devices with Removable Storage**.
3. Select **Decrypt Medium**.

Step Result: The **Ivanti Device and Application Control Decrypt Medium** dialog opens.

Attention: You may be prompted to enter a passphrase for a *Passphrase User* depending upon the users added when the medium was encrypted.

4. Click **OK**.

Result: The removable storage device is decrypted.

Using the Encrypt Medium Utility

The **Encrypt Medium** utility provides a wizard that allows you to select encryption options to easily encrypt a removable storage device that can be used with or without a network connection.

Using the **Encrypt Medium** utility you can perform the following tasks:

- Select an encryption access method that determines whether the removable storage device can be used inside (non-portable encryptions) or outside (portable encryption) of your corporate network.
- Assign user access for Windows® Active Directory users or password users.
- Save or erase existing data stored on the device.
- Securely erase unused space on the device.

The wizard pages that a user can access, based the **Encrypt Medium** utility configuration options, are described by the following process flow. See [The Ivanti Device Control Options Page](#) on page 189 for additional information about using the default options that govern encryption.

1
Select Access
Method

The **Select Access Method** page is available for non-portable and the combined portable-non-portable encryption access options that are configured by the network administrator as follows.

- The **Microsoft CA Key Provider** default option value is set to **Enabled**.
- The encryption permissions are set to **Encrypt** and **Export to Media**.

2
User Access to
Device

The **User Access** page is not available when the non-portable encryption access options are configured by the network administrator as follows.

- The **Microsoft CA Key Provider** default option value is set to **Enabled**.
- The encryption permissions are set to **Encrypt** only.

3
Add Additional
User

The **Add User** page is only available when a user can access the **User Access to Device** page.

4
User List

The **User List** page is only available when a user accesses the **Add User** page.

5
Data Integrity

The **Data Integrity** page is available as follows.

- Data must be stored on the removable storage device.
- The **Encryption Retain Data** default option set to **Selected** or **Unselected**.
- The user must have **Read** permission.

6
Secure
Unused Space

The **Secure Unused Space** page is available as follows.

- The **Clear unused space when encrypting** default option set to **Disabled**.

7
Start
Encryption

The **Start Encryption** page is always available to users in any encryption scenario.

Portable Device Encryption Permission

Portable device encryption options can be assigned on a user or user group basis. Device permissions combined with specific device encryption default settings govern the behaviour of the **Encrypt Medium** utility that runs on the client.

Prerequisites:

Set the **Password Complexity** and **Password Minimum Length** options. For detailed information about setting the **Password Complexity** and **Password Minimum Length** options for user password requirements, see [The Ivanti Device Control Options Page](#) on page 189.

An administrator must set the device encryption default options and permissions to enable the **Encrypt Medium** utility option for portable device access. Using portable encryption options, encrypted devices can be accessed on any Microsoft Windows computer.

1. In the Device Control application, select **Tools > Options**.

Step Result: The **Options** page displays.

2. Select the **Device Control** tab.

3. Select **Disabled** from the **Microsoft CA Key Provider** dropdown list.

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

Step Result: The **Device Control Policies** page opens.

5. Click **Create**.

Step Result: The policy type drop-down menu appears.

6. Select **Create class policy**.

Step Result: The **Device Class Policy** wizard appears.

Figure 131: Device Class Policy Wizard

7. Type the **Policy name**.

8. Select the **Override priority**.

You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.

9. Select **Removable Storage Devices** from the **Device class** dropdown list.

10. Select the **Permission settings** check box.

11.[Optional] Select the **Shadow settings** check box.

Shadow settings can only be enabled for the COM/Serial Ports, CD/DVD Drives, Floppy Disk Drives, LPT/Parallel Ports, and Removable Storage Devices classes.

12.[Optional] Select the **Daily copy limit** check box. Specify a copy limit value in the text box.

Note: Only one copy limit setting per device class will be enforced. For example, copy limits configured for removable storage devices apply to hard drives and non-hard drives. To avoid ambiguity, it is recommended that you do not combine copy limit policies and permissions policies.

13. Select the desired policy enforcement option.

Option	Description
Always	The policy will apply at all times.
Online only	The policy will apply only when the endpoint/user/group is connected to the server.
Offline only	The policy will apply only when the endpoint/user/group is disconnected from the server.
Scheduled	The policy will apply only during a set schedule.
Temporary	The policy will give one-time access for a specified period.

Depending on the option you choose, additional settings are available in the right-side box.

14. Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default, indicating that the policy is applicable immediately. If you want to delay when the policy will begin working, select **Disable**.

15. Click **Next**.

Step Result: The **Permission Settings** page opens.

Figure 132: Permission Settings

16. Select the **Allow access with following** radio button.

17. Select *Encrypt*.**18. [Optional] Select any other permission that you want to apply.**

For more information on setting permissions, refer to [Permission Settings for a Policy](#) on page 122.

19. Choose which *Connections* will apply.**20. Select the applicable *Drives*.****21. Select *Unencrypted/Unknown encryption type* from *Encryption* group box.****22. Click *Next*.**

Step Result: The *File Filter Settings* page opens.

Note: This page will only appear if you select **File Filters** in the *Permission Settings* page.

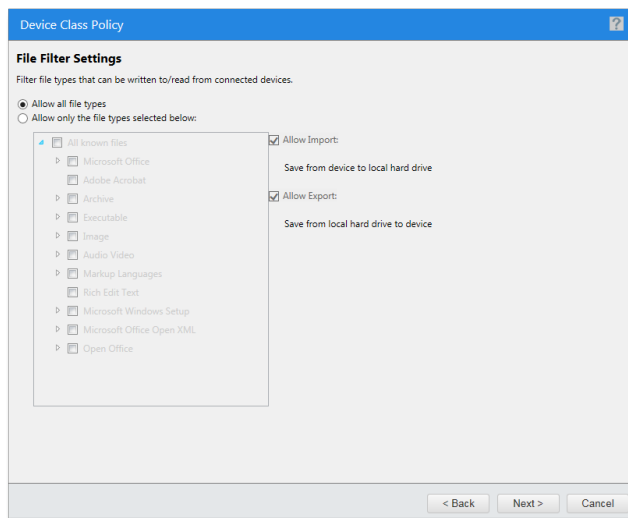


Figure 133: File Filter Settings

23. Specify the file type filtering options.

For more information on file type filters, see [File Type Filtering](#) on page 125.

24. Click **Next**.

Step Result: The **Shadow Settings** page opens.

Note: This page will only appear if you select **Shadow settings** in the **Policy details** page.

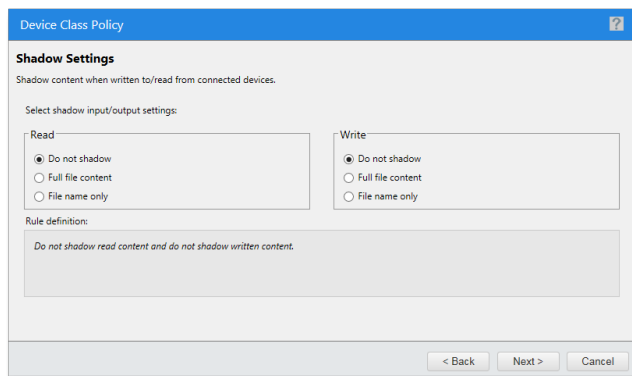


Figure 134: Shadow Settings

25. Specify the shadow settings.

For more information on shadowing devices, see [File Shadowing](#) on page 129.

26.Click **Next**.

Step Result: The ***Assign policy to users, groups and/or endpoints*** page opens.

Note: This page is skipped when the wizard is launched from the ***Groups, Endpoints, or Users*** page of the **Manage** menu.

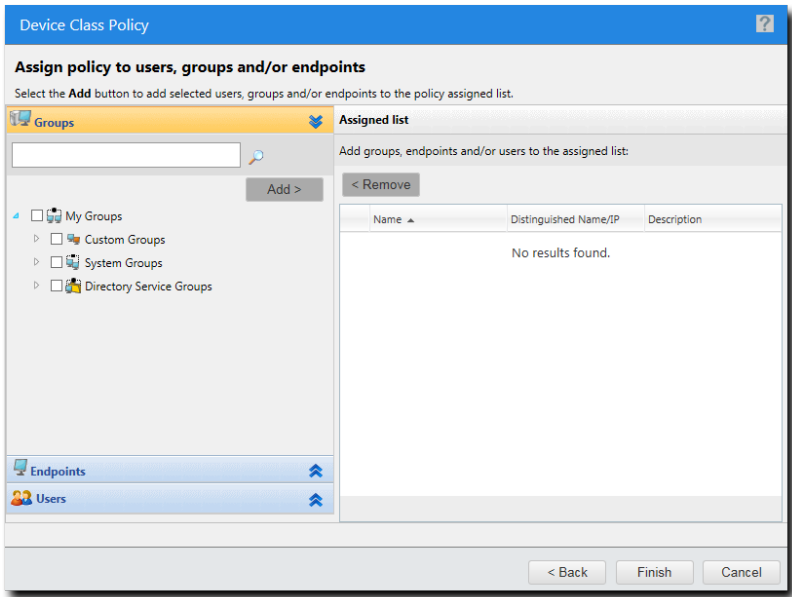


Figure 135: Assign Policy to users, groups and/or endpoints

27.Select the group, endpoint, or user to which the policy will apply.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Add.
To add individual endpoints	<ol style="list-style-type: none">1. Select an endpoint or endpoints from the Endpoints list.2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none">1. Select users or usergroups from the Users list.2. Click Add.
To remove groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Remove.



Option	Description
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

28. Click **Finish**.

Step Result: The **Device Class Policy** wizard closes.

Result: The **Secure Volume Browser** (SVolBro) is installed on the device during encryption. SVolBro runs on any supported Microsoft Windows computer and prompts the user for a password that allows device access, regardless of whether the machine runs the Device Control client or not. The password protects the encryption key, which is exported to the device during encryption.

When a user attempts to access an unencrypted removable storage device, the **Encrypt Medium** utility launches and guides the user through the device encryption process. The user will create a password for access to the encrypted device.

The following table shows the **Encrypt Medium** pages that the user can see based on the encryption options configuration.

Nonportable Device Encryption Permission

Non-portable device encryption options can be assigned on a user or user group basis. Device permissions combined with specific device encryption default settings govern the behaviour of the **Encrypt Medium** utility that runs on the client.

Prerequisites:

You must have a properly configured and working Microsoft® Certificate Authority which can issue certificates to users for the purpose of encryption.

An administrator must set the device encryption default options and permissions to enable the **Encrypt Medium** utility option for non-portable device access. Non-portable device access encryption forces users to encrypt devices for use only on computers running the Device Control client that are connected to the corporate network.

1. In the Device Control application, select **Tools > Options**.

Step Result: The **Options** page displays.

2. Select the **Device Control** tab.

3. Select **Enabled** from the **Microsoft CA Key Provider** dropdown list.

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

Step Result: The **Device Control Policies** page opens.

5. Click **Create**.

Step Result: The policy type drop-down menu appears.

6. Select **Create class policy**.

Step Result: The **Device Class Policy** wizard appears.

Figure 136: Device Class Policy Wizard

7. Type the **Policy name**.

8. Select the **Override priority**.

You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.

9. Select **Removable Storage Devices** from the **Device class** dropdown list.

10. Select the **Permission settings** check box.

11.[Optional] Select the **Shadow settings** check box.

Shadow settings can only be enabled for the COM/Serial Ports, CD/DVD Drives, Floppy Disk Drives, LPT/Parallel Ports, and Removable Storage Devices classes.

12.[Optional] Select the **Daily copy limit** check box. Specify a copy limit value in the text box.

Note: Only one copy limit setting per device class will be enforced. For example, copy limits configured for removable storage devices apply to hard drives and non-hard drives. To avoid ambiguity, it is recommended that you do not combine copy limit policies and permissions policies.

13.Select the desired policy enforcement option. You can choose from the following options:

Option	Description
Always	The policy will apply at all times.
Online only	The policy will apply only when the endpoint/user/group is connected to the server.
Offline only	The policy will apply only when the endpoint/user/group is disconnected from the server.
Scheduled	The policy will apply only during a set schedule.
Temporary	The policy will give one-time access for a specified period.

Depending on the option you choose, additional settings are available in the right-side box.

14.Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default. If you want to delay when the policy will begin working, select **Disable**.

15. Click Next.

Step Result: The **Permission Settings** page opens.

Figure 137: Permission Settings

16. Select the **Allow access with following radio button.****17. Select **Encrypt**.****18. [Optional] Select any other permission that you want to apply.**

For more information on setting permissions, refer to [Permission Settings for a Policy](#) on page 122.

19. Choose which **Connections will apply.****20. Select the applicable **Drives**.****21. Select **Unencrypted/Unknown encryption type** from **Encryption** group box.**

22. Click **Next**.

Step Result: The **File Filter Settings** page opens.

Note: This page will only appear if you select **File Filters** in the **Permission Settings** page.

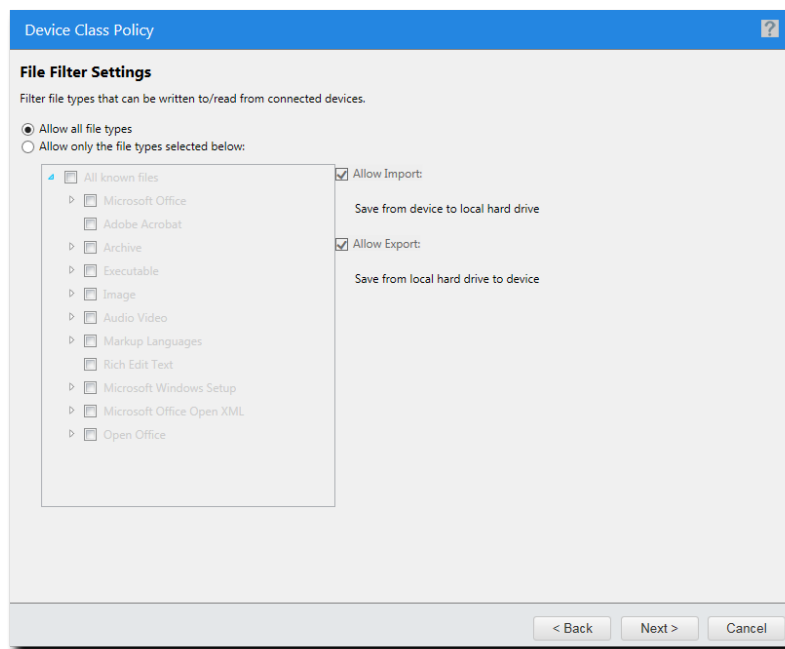


Figure 138: File Filter Settings

23. Specify the file type filtering options.

For more information on file type filters, see [File Type Filtering](#) on page 125.

24. Click **Next**.

Step Result: The **Shadow Settings** page opens.

Note: This page will only appear if you select **Shadow settings** in the **Policy details** page.

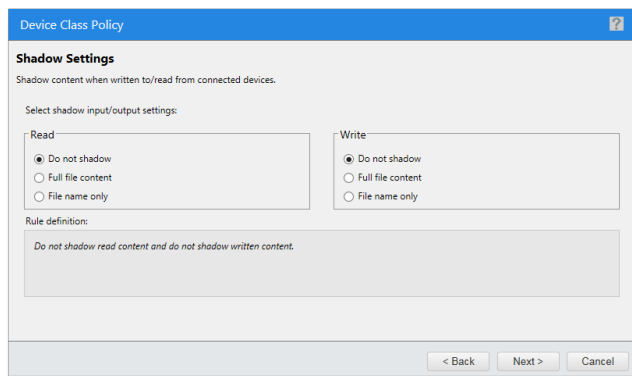


Figure 139: Shadow Settings

25. Specify the shadow settings.

For more information on shadowing devices, see [File Shadowing](#) on page 129.

26. Click **Next**.

Step Result: The **Assign policy to users, groups and/or endpoints** page opens.

Note: This page is skipped when the wizard is launched from the **Groups**, **Endpoints**, or **Users** page of the **Manage** menu.

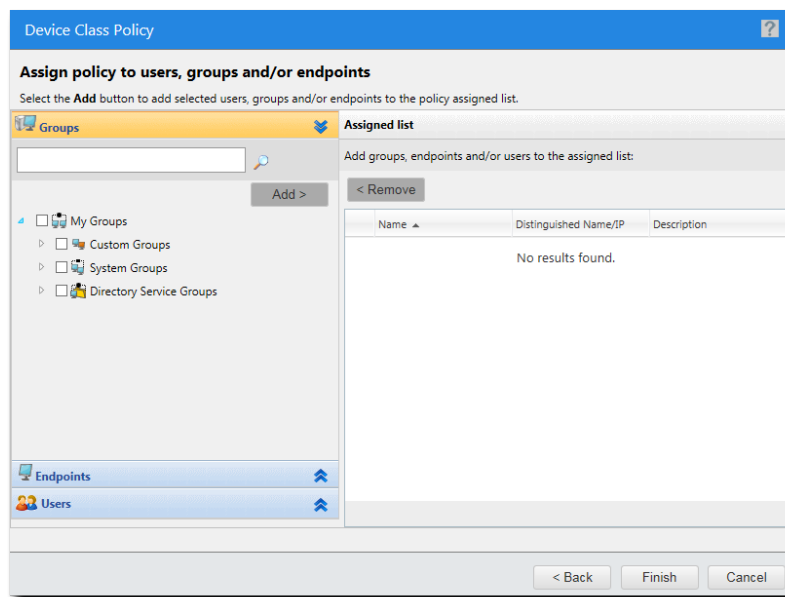


Figure 140: Assign Policy to Users, Groups and/or Endpoints

27. Select the group, endpoint, or user to which the policy applies.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Add.
To add individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Add.
To remove groups of endpoints	<ol style="list-style-type: none"> 1. Select a group or groups from the Groups list. 2. Click Remove.

Option	Description
To remove individual endpoints	<ol style="list-style-type: none"> 1. Select an endpoint or endpoints from the Endpoints list. 2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none"> 1. Select users or usergroups from the Users list. 2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in the **Assigned List**.

28. Click **Finish**.

Step Result: The **Device Class Policy** wizard closes.

Result: A user is forced to encrypt unencrypted devices before access to the device is allowed. No password is required for device access. After encrypting the device, the user can only access the device on computers running the client.

When a user attempts to access an unencrypted removable storage device, the **Encrypt Medium** utility launches and guides the user through the device encryption process.

Important: Verify that users have **Read** and/or **Write** permissions for devices encrypted using **Self Contained Encryption**.

Portable and Nonportable Device Encryption Permission

Portable and non-portable device encryption options can be assigned on a user or user group basis. Device permissions combined with specific device encryption default settings govern the behaviour of the **Encrypt Medium** utility that runs on the client.

Prerequisites:

- You must have a properly configured and working Microsoft® Certificate Authority which can issue certificates to users for the purpose of encryption.
- You may set the **Password Complexity** and **Password Minimum Length** options for user password requirements, using the **Tools > Default Options > Computer** tab. For detailed information about using options, see [The Ivanti Device Control Options Page](#) on page 189.

An administrator must set the device encryption default options and permissions to enable the **Encrypt Medium** utility option for portable and non-portable device access.

1. In the Device Control application, select **Tools > Default Options**.

Step Result: The **Options** page opens.

2. Select the **Device Control** tab.
3. Select **Enabled** from the **Microsoft CA key provider** dropdown list.

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

Step Result: The **Device Control Policies** page opens.

5. Initiate creation of a device class policy.

a) Click **Create**.

Step Result: The policy type drop-down menu appears.

b) Select **Create class policy**.

Step Result: The **Device Class Policy** wizard appears.

Figure 141: Device Class Policy Wizard

6. Type the **Policy name**.

7. Select the **Override priority**.

You can choose between **Normal (Default)** and **High (Overrides Normal Priority)**.

8. Select **Removable Storage Devices** from the **Device class** dropdown list.

9. Select the **Permission settings** check box.

10.[Optional] Select the **Shadow settings** check box.

Shadow settings can only be enabled for the COM/Serial Ports, CD/DVD Drives, Floppy Disk Drives, LPT/Parallel Ports, and Removable Storage Devices classes.

11.[Optional] Select the **Daily copy limit** check box. Specify a copy limit value in the text box.

Note: Only one copy limit setting per device class will be enforced. For example, copy limits configured for removable storage devices apply to hard drives and non-hard drives. To avoid ambiguity, it is recommended that you do not combine copy limit policies and permissions policies.

12.Select the desired policy enforcement option.

Option	Description
Always	The policy will apply at all times.
Online only	The policy will apply only when the endpoint/user/group is connected to the server.
Offline only	The policy will apply only when the endpoint/user/group is disconnected from the server.
Scheduled	The policy will apply only during a set schedule.
Temporary	The policy will give one-time access for a specified period.

Depending on the option you choose, additional settings are available in the right-side box.

13.Select whether you want the policy to be applicable immediately.

The **Enable** radio button is selected by default. If you want to delay when the policy will begin working, select **Disable**.

14.Click **Next**.

Step Result: The **Permission Settings** page opens.

Figure 142: Permission Settings

15.Select the **Allow access with following** radio button.**16.**Select **Encrypt**.**17.**[Optional] Select any other permission that you want to apply.

For more information on setting permissions, refer to [Permission Settings for a Policy](#) on page 122.

18.Choose which **Connections** will apply.**19.**Select the applicable **Drives**.**20.**Select **Unencrypted/Unknown encryption type** from **Encryption** group box.

21. Click **Next**.

Step Result: The **File Filter Settings** page opens.

Note: This page will only appear if you select **File Filters** in the **Permission Settings** page.

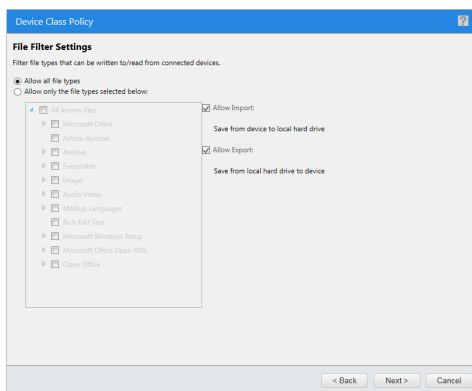


Figure 143: File Filter Settings

22. Specify the file filtering options.

For more information on file filters, see [File Type Filtering](#) on page 125.

23. Click **Next**.

Step Result: The **Shadow Settings** page opens.

Note: This page will only appear if you select **Shadow settings** in the **Policy details** page.

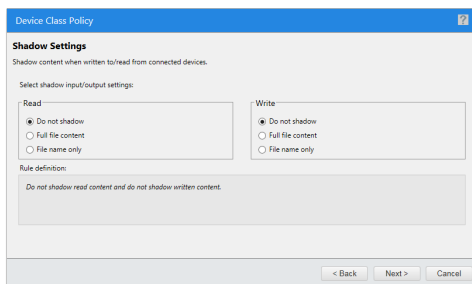


Figure 144: Shadow Settings

]

24. Specify the shadow settings.

For more information on shadowing devices, see [File Shadowing](#) on page 129.

25.Click **Next**.

Step Result: The ***Assign policy to users, groups and/or endpoints*** page opens.

Note: This page is skipped when the wizard is launched from the ***Groups, Endpoints,*** or ***Users*** page of the **Manage** menu.

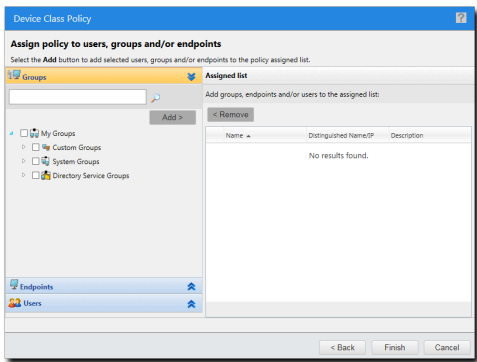


Figure 145: Assign Policy to Users, Groups and/or Endpoints

26.Select the group, endpoint, or user the policy will apply to.

Option	Description
To add groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Add.
To add individual endpoints	<ol style="list-style-type: none">1. Select an endpoint or endpoints from the Endpoints list.2. Click Add.
To add individual users or user groups	<ol style="list-style-type: none">1. Select users or usergroups from the Users list.2. Click Add.
To remove groups of endpoints	<ol style="list-style-type: none">1. Select a group or groups from the Groups list.2. Click Remove.
To remove individual endpoints	<ol style="list-style-type: none">1. Select an endpoint or endpoints from the Endpoints list.2. Click Remove.
To remove individual users or user groups	<ol style="list-style-type: none">1. Select users or usergroups from the Users list.2. Click Remove.

Step Result: The selected groups, users, or endpoints are displayed in then **Assigned List**.



27. Click **Finish**.

Step Result: The **Device Class Policy** wizard closes.

Result: When a user attempts to access an unencrypted removable storage device, the option **Encrypt Medium** utility launches and guides the user through the device encryption process.

- If a user selects the **Non-portable** encryption option, then the user is forced to encrypt unencrypted devices before access to the device is allowed. After encrypting the device, the user can only access the device any computer running the Device Control client; no password is required for device access.
- If a user selects the **Portable** encryption option, then the **Secure Volume Browser** (SVolBro) is installed on the device during encryption. SVolBro runs on any supported Microsoft Windows computer and prompts the user for a password that allows device access, regardless whether the computer runs the Device Control client. The password protects the encryption key, which is exported to the device during encryption.

My Computer Page

You launch the **Encrypt Medium** utility from the Windows **My Computer** page.

Prerequisites:

Attach a *removable storage device* for encryption.

You only use this page and task steps when you have a device continuously attached to the computer running the Device Control client. For example, you attach device that you decrypt and decide to re-encrypt without removing the device from the computer.

Attention: If you detach and reattach the device to the computer running the Device Control client, the **Encrypt Medium** will automatically launch, and you will not see this page.

1. Depending on your operating system, select **Start > My Computer** or **Start > Computer**.

Step Result: The **My Computer** page opens.

2. Right-click the name of the device listed under **Devices with Removable Storage**.
3. Select **Encrypt Medium**.
4. Click **Next**.

Step Result: Depending upon the encryption method options authorized by your administrator:

- The **Select Access Method** page opens for access to portable and non-portable encryption.
- The **User Access to Device** page opens for access to enforced portable encryption.
- The **Start Encryption** page opens for access to enforced non-portable encryption.

Important: If you are encrypting a device that is 128 GB or larger, access to portable encryption will not be available.

Select Access Method Page

The **Select Access Method** page provides options for encrypting devices based on device volume size.

The **Select Access Method** page is only available for the non-portable (internal use only) and the combined portable and non-portable encryption access options that are configured by the network administrator.

1. Specify a user access method by selecting one of the following options shown on the **Select Access Method** page.

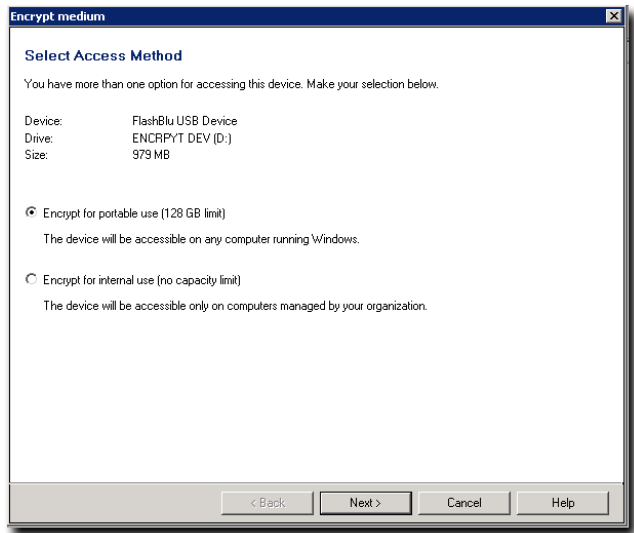


Figure 146: Select Access Method Page

Option	Description
Encrypt for portable use (128 GB limit)	Allows use of an encrypted device on any computer running Microsoft® Windows®. This encryption access method is called <i>Portable</i> .
Encrypted for internal use (2 TB limit)	Allows use of devices only inside your network on computers that run are managed by Device Control. This encryption access method is called <i>Non-portable</i> .

2. Click **Next**.

Step Result: The **User Access to Device** page opens, if you are using the portable encryption access method. If you are using the non-portable access method, the **Data Integrity** page opens if the device contains data, you have Read permission, and the default option to retain data during encryption is enabled.



User Access to Device Page

The **User Access to Device** page allows you to specify a user name and password to provide easy access to the encrypted device.

1. Type a user name in the **User name** field.

Figure 147: User Access to Device Page

Important: The first password user is always named `Primary User`, which is compatible with previous versions of Device Control.

2. Type a **Password** in the corresponding field, and then retype the password to **Confirm** in the corresponding field.
3. If you wish to add other users for access to the encrypted device, click **Add User**.

Attention: When your device is larger than 128 GB or you are using non-portable encryption, you can only add one user and you must use the preset `Primary User` user name.

Step Result: The **Add User** page opens.

4. Click **Next**, if you are not adding other users for access to the encrypted device.

Step Result: The **Data Integrity** page opens.

Add User Page

The **Add Additional User** page allows you to add users by user types that can access the encrypted device.

Options for adding users are shown on the **Add Additional User** page.

Important: At least one user who is allowed access to the encrypted device must be listed.

1. To add a Windows Active Directory user:
 - a) Select **Add Windows user**.
 - b) Click **OK**.

Step Result: The **Select Users or Groups** dialog opens.
 - c) To add a **Windows user** in the **Enter the object names to select field**, enter the names of the users to add to the list, using one of the following formats:

Table 89: User Name Format Examples

Object Name	Example
Display Name	FirstName LastName
UserName	User1
ObjectName@DomainName	User1@Domain1
DomainName\ObjectName	Domain\User1

- d) To verify the user name, click **Check Names**.

Step Result: The user name is verified and underlined when correctly entered.
 - e) Click **OK**.
2. To add a unique user name and password:
 - a) Type a user name in the **Name** field.

Important: The first password user is always named `Primary User`, which is compatible with previous versions of Device Control.
 - b) Type a **Password** in the corresponding field, and then retype the password to **Confirm** in the corresponding field.



c) Click **OK**.

Result: The user name(s) are added to the list shown in the **User List** page. You may continue to add users to the device using the previously described steps. You may also remove users from the list by clicking on the **Recycling Bin** icon to the left of a user name.

After Completing This Task:

After reviewing the user names added to the **User List** page, click **Next** and the **Data Integrity** page opens.

Attention: When the device does not contain any data, or your administrator has preselected one of the **Data Integrity** options, either the **Secure Unused Space** page or the **Start Encryption** page opens next.

User List Page

The **User List** page provides the opportunity to review the user access list and add other users as necessary.

The user name(s) added to the user access list is shown on the **User List** page.

1. Review the user access list on the **User List** page.
2. [Optional] Click **Add User** to add more users.
3. [Optional] Click the **Recycle Bin** icon to remove users.
4. When you are finished, click **Next**.

Step Result: The **Data Integrity** page opens.

Attention: If you have no data stored on the device you are encrypting and the policy to erase unused storage space is enforced by your administrator, the **Start Encryption** page opens next.

Data Integrity Page

The **Data Integrity** page provides options to save or delete files during the encryption process that are currently stored on the device.

If the policy to automatically retain data stored on the device is enforce by your administrator, this page is not available.

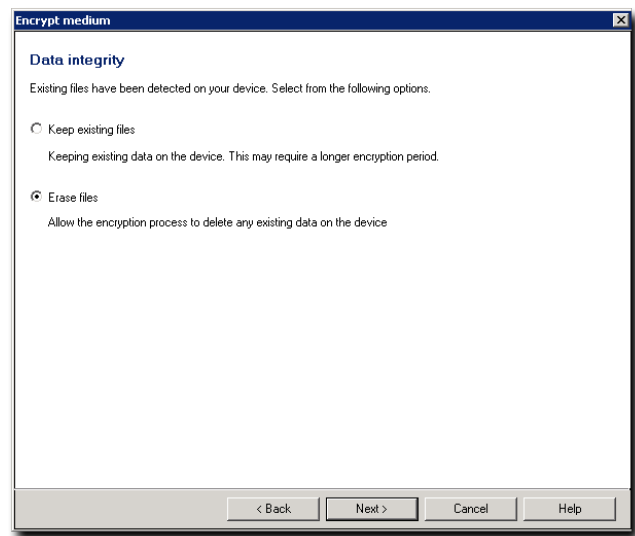


Figure 148: Data Integrity Page

1. Select one of the following options:

Option	Description
Keep existing files	Saves and encrypts all files stored on the device, during the encryption process. This option extends the time required to encrypt the device.
Erase files	Deletes all files stored on the device, during the encryption process. This option extends the time required to encrypt the device.

Restriction: If the option to **Keep existing files** or **Erase Files** is shaded, then that option is preselected by the administrator and cannot be changed.

2. Click **Next**.

Step Result: The **Secure Unused Space** page opens.

Attention: If you have no data stored on the device you are encrypting and the policy to erase unused storage space is enforced by your administrator, the **Start Encryption** page opens next.

Secure Unused Space Page

The **Secure Unused Space** page provides the option to permanently erase files and securely remove data from unused sectors on the device to prevent unauthorized data recovery.

1. Select **Erase fragments in unused space on device (requires a longer encryption period)** to erase data from the unused sectors on the device.

This is the most secure method for data encryption by preventing unauthorized attempts to recover confidential or sensitive information that may have been deleted by a user but still resides on the device.

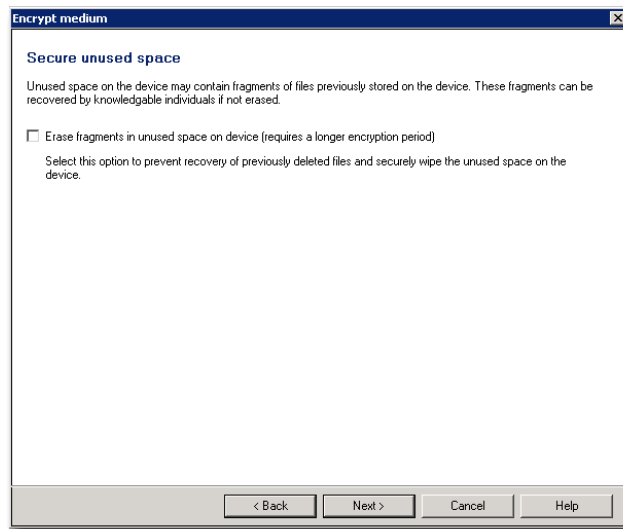


Figure 149: Secure Unused Space Page

Important: This step is entirely optional. You may proceed without choosing to erase data from the unused space on the device.

2. Click **Next**.

Step Result: The **Start Encryption** page opens.

Start Encryption Page

The **Start Encryption** page shows a summary of the users and encryption method options selected for encrypting the specified device.

1. Review the device encryption summary.

The **Start Encryption** page lists the names and types of users allowed to access the device.

2. When you are satisfied with the list of users allowed to access the device, click **Encrypt**.

Step Result: The **RTNotify** warning dialog opens.

3. Click **OK**.

Step Result: The **Encrypt Medium** dialog opens, showing a progress bar for the encryption process.

4. Click **Close**.

Result: The device is encrypted for the users specified.

Attention: If a valid digital certificate cannot be retrieved for the Windows user you are adding, you receive the following message in the **Encrypt Medium** dialog: No certificates found; user will not be added.

Transferring Encryption Keys

Users can transfer encryption keys between removable storage devices and computers by exporting and importing the encryption keys.

Ivanti Device Control administrators can export and import encryption keys for the user using the **Media Authorizer** module. Encryption keys can be exported to a file or device, and imported from a device. Export to a file is the most secure method for transferring encryption keys. Transferring an encryption key directly to a device is less secure because security is primarily dependent upon the password complexity.

Export an Encryption Key

A user can transfer an encryption key from a computer to a device by exporting the encryption key to a file or device.

Prerequisites:

- An administrator must assign users access to the media.
 - An administrator must assign device permissions to allow the user to export an encryption key to a file or device.
 - A user must attach the device to the computer.
-

Exporting the encryption key directly to the encrypted device is significantly less secure because the level of difficulty required to access the data is directly linked to the device password complexity.

1. Open Windows Explorer®.
2. Right-click the device.
3. Select **Export medium key**.

Step Result: The **Export Medium Key** dialog opens.

4. In the **Export key to** panel, select one of the following options:

Option	Description
Medium	Exports the encryption key to the attached device.
Folder	Exports the encryption key to a file folder that the user specifies.

a) When you select the folder option, click the ellipses to locate a folder.

5. In the **Password** field, type a password.

Restriction: When the administrator defines the encrypted media password option to require password complexity, the password meet the following criteria:

- Contain at least six characters.
- Contain upper and lower case letters.
- Contain numbers.
- Contain at least one non-alphabetical character.

6. In the **Confirm** field, retype the password.
7. Click **OK**.

Result: The encryption key is sent directly to the device or to the folder you specified. Using the password, a user can import the encryption key from the device or file to access encrypted media.

Import Encryption Key

A user can unlock an encrypted device by importing the encryption key from the device or a file containing the encryption key.

Prerequisites:

- An administrator must assign users access to the media.
- An administrator must assign device permissions to allow the user to export an encryption key to a file or device.
- A user must attach the encrypted device to the computer.
- A user must have the password for the encryption key.
- A user must export the device encryption key to the encrypted device or a computer file containing the encryption key.

A network administrator can delegate to trusted users the right to access Device Control encrypted media by importing an encryption key from a separately transmitted file.

1. Open Windows Explorer®.
2. Right-click the device name.
3. Select **Unlock medium**.

Step Result: The ***Import Medium Key*** dialog opens.

4. In the ***Import key from*** panel, select one of the following options:

Option	Description
Medium	Imports the encryption key from the attached device.
Folder	Imports the encryption key from the file folder that the user specifies.

- a) When you select the folder option, click the ellipses to locate the folder containing the encryption key.
5. In the **Password** field, type the password.
 6. Click **OK**.

Result: The encrypted device is unlocked and accessible to the user through Windows Explorer®.

