Ivanti Device and Application Control 5.3

Device Control User Guide

ivanti | **Endpoint Security**
powered by HEAT

Notices

Table of Contents

ivanti

ivanti

Preface

About This Document

This Device Control User Guide is a resource written for all users of Ivanti Device and Application Control 5.2. This document defines the concepts and procedures for installing, configuring, implementing, and using Ivanti Device and Application Control 5.2.

Tip: Ivanti documentation is updated on a regular basis. To acquire the latest version of this or any other published document, please refer to the Ivanti Product Documentation (https://help.ivanti.com).

Typographical Conventions

The following conventions are used throughout this documentation to help you identify various information types.

Table 1: Typographical Conventions

Convention	Usage
bold	Buttons, menu items, window and screen objects.
bold italics	Wizard names, window names, and page names.
italics	New terms, options, and variables.
`MONOSPACE UPPERCASE`	Keyboard keys.
`BOLD UPPERCASE`	SQL Commands.
`monospace`	File names, path names, programs, executables, command syntax, and property names.

ivanti

Chapter

1

Device Control Overview

In this chapter:

- Product Overview
- Device Control Server, Database and Client Process
- System Requirements

Ivanti offers a complete portfolio of solutions for controlling the use of software applications and devices in your computing environment.

Ivanti Device and Application Control solutions include:

- Device Control, which prevents unauthorized transfer of applications and data by controlling access to input and output devices, such as memory sticks, modems, and PDAs.
- Device Control client for Embedded Devices, which moves beyond the traditional desktop and laptop endpoints to a variety of platforms that include ATMs, industrial robotics, thin clients, set-top boxes, network area storage devices and the myriad of other systems.
- Application Control, which delivers granular control of application execution in an enterprise environment.
- Application Control Server Edition, which delivers application control to protect enterprise servers, such as web servers, e-mail servers, and database servers.

ivanti

Product Overview

The Device Control software application is based on a multi-tier software architecture that processes and stores data for Application Control and Device Control. Users can interact with the application through the client interface. A separate Management Console provides a user interface for network administrators.

The primary components of the Device Control solution are:

- The Device Control database which serves as the central repository of authorization information for devices and applications.
- One or more Application Servers that communicate between the database, the protected clients, and the Management Console.
- The Device Control client, which is installed on each computer, either end-point or server, that you want to protect.
- The Management Console, which provides the administrative user interface for the Application Server.

The following figure illustrates the relationships between the Device Control components.
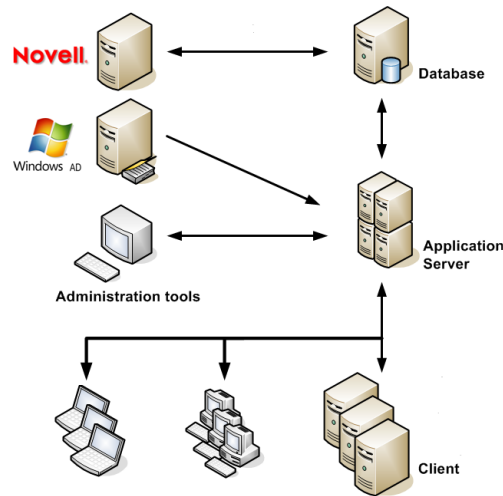
Figure 1: Device Control Component Relationships

Device Control Server, Database and Client Process

The Application Server communicates between the database and the protected client computers.

The following describes the communication process flow between the Device Control servers, database, and clients when using Device Control.
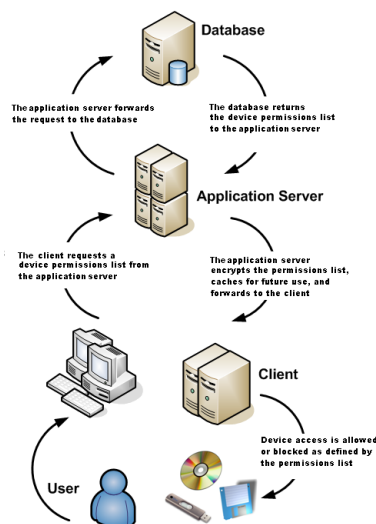
Figure 2: Device Control Process Flow

Using Certification Authority

The Microsoft Certification Authority (CA) issues and manages digital certificates for a network environment.

A digital certificate is a digital document that provides identification credentials for a user, computer, or entity. Digital certificates provide support for public key cryptography because digital certificates contain the public key for the user, computer, or entity identified in the certificate.

As part of a public key infrastructure, the CA validates the public key provided by the requestor of the digital certificate. Ivanti Device and Application Control use the CA with the TLS communication protocol to ensure the integrity of the data encryption process.

Using the Transport Layer Security

The Transport Layer Security (TLS) protocol and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks.

TLS is used in conjunction with Microsoft Certification Authority®, to generate digital certificates. For organizations that use sensitive, confidential information or are subject to stringent security regulation,

ivanti

deploying TLS on the server and client is the best assurance against compromising communication integrity, specifically:

- Peer identity can be authenticated using public key cryptography, allowing the safe exchange of encrypted information.
- Message contents cannot be modified en route between TLS negotiated hosts.

Using TLS with Ivanti Device and Application Control affects:

- Ivanti Device and Application Control client-Application Server communication
- Ivanti Device and Application Control inter-Application Server communication

Device Control Client-Application Server Communication

Ivanti Device and Application Control is based on standard TCP/IP protocols for all communication between clients and servers.

The Device Control client communicates with the Application Server as follows:

- The client connects with the Application Server to:

  - Retrieve device permission updates.
  - Upload client log files.
  - Upload client shadow files.
- The Application Server connects with the client to:

  - Scan the client.
  - Fetch client log files.
  - Fetch client shadow files.
  - Send device permission updates.

Communications are signed by the server with a private key and the client uses the corresponding public key to authenticate server communications. After the client authenticates the server communication using the TLS protocol, the client can transmit data. The following figures illustrates the TLS protocol communication process.
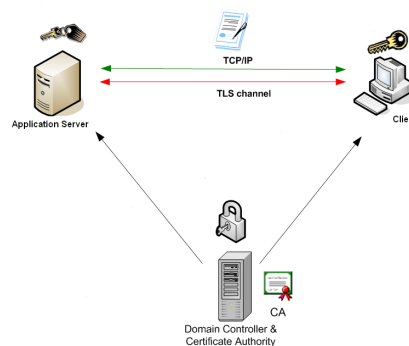
Figure 3: TLS Protocol for Device Control Client-Application Server Communication

Device Control Inter-Application Server Communication

A Ivanti Device and Application Control implementation employing multiple Application Servers uses distributed data file directories (DFDs), combined with TLS authentication to assure the integrity of confidential, sensitive data.

Using the TLS communication protocol assures data encryption authentication when the Application Servers exchange confidential information. Since Application Servers can have multiple DNS names and multiple digital certificates, TLS ensures that the certificate for the Application Server matches the DNS name used by the client and other Application Servers when they communicate. The following figures illustrates the TLS protocol communication process.
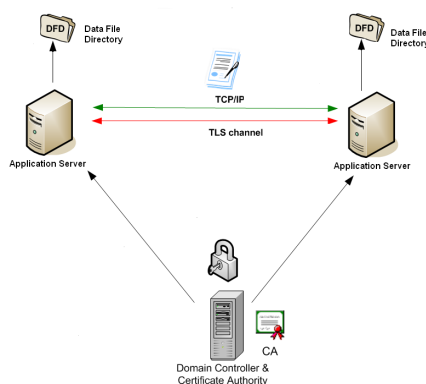
Figure 4: TLS Protocol for Ivanti Device and Application Control Inter-Application Server Communication

System Requirements

The following sections describe the minimum system requirements necessary for successful installation of Ivanti Device and Application Control and the languages supported by the client.

The listed specifications are a minimum; larger network environments, may require additional hardware and software resources. The system requirements for Ivanti Device and Application Control are listed in the following topics.

Important: For installation or upgrade to Ivanti Device and Application Control version 5.2:

- You must have a valid license file that is issued specifically for version 4.5 or later. Confirm that you have the required license file available before you begin installation.
- License files issued before Ivanti Device and Application Control version 4.5 will not work with the Application Server and may cause your Application Servers to stop working.
- The Ivanti Device and Application Control 4.5 license must be installed before you install or upgrade the Ivanti Device and Application Control database, and then the Application Server.
- Request a new license file using the **Downloads** tab on the Self-Service Portal.

ivanti

Minimum Hardware Requirements

The minimum Ivanti Device and Application Control hardware requirements depend upon your service network environment, including the type of database supported, the number of Application Servers you need to support a distributed network, and the number of subscribed clients.

The hardware requirements for Ivanti Device and Application Control vary depending upon the number of servers and clients you manage. The following minimum hardware requirements will support up to:

- 200 connected Ivanti Device and Application Control clients for Device Control
- 50 connected Ivanti Device and Application Control clients for Application Control

Table 2: Minimum Hardware Requirements

Ivanti Device and Application Control Component	Requirement
Database	• 1 GB (4 GB recommended) memory • Pentium® Dual-Core CPU processor or AMD equivalent • 3 GB minimum hard disk drive • 100 MBits/s NIC
Application Server	• 512 MB (1 GB recommended) memory • Pentium® Dual-Core CPU or AMD equivalent • 3 GB minimum hard disk drive • 100 MBits/s NIC
Management Console	• 512 MB (1 GB recommended) memory • 15 MB hard disk drive for installation, and 150 MB additional for application files • 1024 by 768 pixels for display
Client	• 256 MB (1 GB recommended) memory • 10 MB hard disk drive for installation, and several additional GB for full shadowing feature of Device Control • 100 MBits/s NIC

Supported Operating Systems

Ivanti Device and Application Control supports multiple Microsoft Windows operations systems for the Application Server, Management Console, database, and client.

The operating system requirements for Ivanti Device and Application Control components are outlined as follows.

Table 3: Operating System Requirements

Ivanti Device and Application Control Component	Requirement
Database	One of the following: • Microsoft Windows Server 2008 R2 with SP1 (64 bit only) • Microsoft Windows Server 2012 (64-bit only) • Microsoft Windows Server 2012 R2 (64-bit only) • Microsoft Windows Server 2016, Standard, Datacenter and Essentials Edition (64-bit only) • Microsoft Windows Server 2019, Standard, Datacenter and Essentials Edition (64-bit only)
Application Server	One of the following: • Windows Server 2008 R2 with SP1 (64 bit only) • Windows Server 2012 (64-bit only) • Windows Server 2012 R2 (64-bit only) • Windows Server 2016, Standard, Datacenter and Essentials Edition (64-bit only) • Windows Server 2019, Standard, Datacenter and Essentials Edition (64-bit only)
Management Console	One of the following: • Windows 7 SP1 (32-bit and 64-bit) • Windows Server 2008 R2 with SP1 (64 bit only) • Windows Server 2012 (64 bit only) • Windows Server 2012 R2 (64 bit only) • Windows Server 2016, Standard, Datacenter and Essentials Edition (64-bit only) • Windows Server 2019, Standard, Datacenter and Essentials Edition (64-bit only) • Windows 8 and 8.1 (32-bit and 64-bit) • Windows 10 (32-bit and 64-bit)

ivanti

Ivanti Device and Application Control Component	Requirement
Client	One of the following: • Windows Server 2008 R2 (64 bit only) • Windows Server 2012 (64 bit only) • Windows Server 2012 R2 (64 bit only) • Windows Server 2016, Standard, Datacenter and Essentials Edition (64-bit only) • Windows Server 2019, Standard, Datacenter and Essentials Edition (64-bit only) • Windows 7 SP 1 (32-bit and 64-bit) with *KB3033929* • Windows Embedded Standard 7 SP1 (32-bit and 64-bit) with *KB3033929* • Windows 7 Thin PC • Windows 8 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows Embedded 8.1 Industry Pro and Industry Enterprise (64-bit) **NOTE**: *Both these editions are identified as Windows Embedded 8.1 Industry by Microsoft.* • Windows 10 Education, Enterprise, and Professional editions (32-bit and 64-bit) • Citrix XenApp 7.12 • Citrix XenApp 7.14.1 • Citrix XenApp 7.15 • Citrix XenApp 7.17 • Citrix XenApp 7.18 • Citrix XenDesktop 7.12 • Citrix XenDesktop 7.14.1 • Citrix XenDesktop 7.15 • Citrix XenDesktop 7.17 • Citrix XenDesktop 7.18

Important: Windows 7 SP1 (32-bit and 64-bit) and Windows Embedded Standard 7 SP1 (32-bit and 64-bit) both required *KB3033929 (Security Update for Windows 7)* to be installed prior to Ivanti Device and Application Control being installed.

Supported Databases

Ivanti Device and Application Control supports multiple releases of Microsoft® SQL Server®. You should choose the database instance required by your network operating environment and the number of Application Servers and subscribed clients the application must support.

The database requirements for Ivanti Device and Application Control components are outlined as follows.

Table 4: Database Requirements

Ivanti Device and Application Control Component	Requirement
Database	One of the following: • Microsoft SQL Server 2012, Standard, Enterprise, Express Edition (32-bit and 64-bit) • Microsoft SQL Server 2014, Standard, Enterprise, Express Edition (32-bit and 64-bit) • Microsoft SQL Server 2016, Standard, Enterprise, Express Edition (64-bit only) • Microsoft SQL Server 2017, Standard, Enterprise, Express Edition (64-bit only) • Microsoft SQL Server 2019, Standard, Enterprise, Express Edition (64-bit only)

Other Software Requirements

Ivanti Device and Application Control requires the following additional software.

Additional software requirements for Ivanti Device and Application Control components are outlined as follows.

Table 5: Other Software Requirements

Ivanti Device and Application Control Component	Requirement
Database	No additional software requirements.

ivanti

Ivanti Device and Application Control Component	Requirement
Application Server	If you will be encrypting Windows user accounts for centralized Device Control encryption, you will need to install an enterprise level Certificate Authority. See Microsoft Certificate Authority (http://technet.microsoft.com/en-us/library/cc756120.aspx) for additional information about certificates.
	Attention: Certificate authority installation applies to Device Control only for centralized encryption capability. Certificate authority installation applies to both Device Control and Application Control for secure server communications.
	A Certificate Authority is required to use secure communications between clients and servers, and intra-server communications.
Management Console	Microsoft Visual C++ 2017 Redistributable Package
Client	No additional software requirements.

Recommended Configuration

To maximize Ivanti Device and Application Control for operation in a Microsoft Windows environment, you should configure your network environment database and client components using the following suggested configurations.

The recommended configurations for Ivanti Device and Application Control components are outlined as follows. These settings represent the usual default settings, but should be confirmed before beginning Ivanti Device and Application Control installation.

Table 6: Recommended Configuration

Ivanti Device and Application Control Component	Requirement
Database	• Change the Windows **Event Viewer** settings to 1024 KB and choose to overwrite events as necessary. • Change Windows **Performance** settings to prioritize for background applications.
Application Server	None recommended.
Management Console	None recommended.

Ivanti Device and Application Control Component	Requirement
Client	• If you are using Active Directory, configure a corresponding Domain Name System (DNS) server as Active Directory (AD) integrated and create a reverse lookup zone, to provide for name resolution within the Management Console. • Configure NIC to receive IP from DHCP service. • Change the Windows **Event Viewer** settings to 1024 KB and choose to overwrite events as necessary.

Client Supported Languages

The Ivanti Device and Application Control client supports multiple languages in text format.

The Ivanti Device and Application Control client is supported in the following languages:

- English
- French
- Italian
- German
- Spanish
- Japanese
- Simplified Chinese
- Traditional Chinese
- Russian
- Dutch
- Portuguese
- Swedish

ivanti

Chapter

2

Using the Management Console

In this chapter:

- Getting Started with Device Control
- The Device Permissions Setup Process
- Accessing the Management Console
- Common Functions within the Management Console
- License Expiration

The Management Console provides direct access to system management, configuration, file authorization, reporting, and logging functions.

The Management Console allows the user to communicate with an Application Server to send and retrieve device permissions data from the database. The data is then sent from the server to a Ivanti Device and Application Control client, thereby establishing device control on the client.

Getting Started with Device Control

You start with Device Control by installing the application, which includes all server and database components, the Management Console, and the Device Control clients. Then you use the Management Console to define user and device permissions for encryption of removable storage devices.

You must begin the installation process with a clean computer that fulfills the minimum software and hardware requirements. You must resolve all hardware and software conflicts prior to installing Ivanti

ivanti

Device and Application Control solutions and install the latest operating system and database service packs. Refer to the following processes to identify tasks when using Device Control.
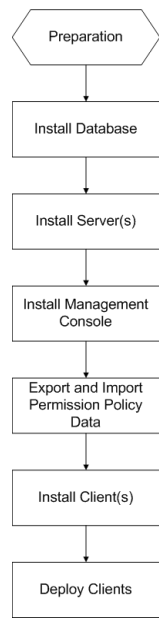
Figure 5: Device Control Installation

The Device Permissions Setup Process

After successfully installing Application Control, an administrator uses the Management Console to configure and define user access permissions and device permission rules required in a Ivanti Device and Application Control environment that specify which devices each user can access, as described by the following process flow.

The *Enterprise Administrator* defines administrative roles for network *Administrator*s that have restricted access to the Management Console.

After defining *Administrator* roles, the *Enterprise Administrator* assigns the roles to *Administrator*s using the **User Access** tool.

*Administrator*s add computers to a domain group or computer workgroup in the **Machine-specific settings** structure of the *Device Explorer*.

Define user access permission rules for a devices, device classes, device groups, device models, and computers, by assigning one or more users or user groups to the devices. Initially, the default permissions for all devices that connect to a computer running the Ivanti Device and Application Control client is **None**, which means that all user access is denied.
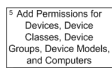
5 Add Permissions for Devices, Device Classes, Device Groups, Device Models, and Computers	Assign permission rules for users to access devices, device classes, device groups, device models, and computers.
6 Assign Computer-Specific Access to Devices for Users and/ or User Groups	Assign computer-specific permission rules for users to access devices and device classes.

Permissions determine access to devices for authorized users or groups on any computer protected by Ivanti Device and Application Control. You can change rules to grant, extend, or deny permissions. You can allow access to CD/DVD-ROMs for specific users or groups that otherwise do not have access as defined by permissions policies, because users cannot use unauthorized CD/DVDs.

Accessing the Management Console

Access to the Management Console is controlled using the login and logout functions provided by the Management Console. Only authorized administrators may access the Application Server.

The Management Console is a Windows application that conforms to standard conventions. From the Management Console, you navigate through the system with menu bars, scroll bars, icons, lists, and checkboxes.

Logging In to the Management Console

You access the application by logging in to the Management Console.

1. Select **Start** > **Programs** > **Ivanti** > **Endpoint Security** > **Ivanti Device and Application Control Management Console** > **Ivanti Device and Application Control Management Console**.

   Step Result: Each time you access the Management Console, the ***Connect to* Ivanti Device and Application Control Application Server** dialog appears.

2. From the **Application Server** drop-down list, select the Application Server you want to connect to.

   You can type the server name as an IP address with port if required in square brackets, NetBios name, or fully qualified domain name in the **Application Server** field.

3. Select one of the following options:

Option	Description
Use current user	By default the system connects to the Application Server using your credentials.

ivanti

Option	Description
Log in as	Type the user name in the **Username** field and type the password in the **Password** field.
	Tip: Precede the user name by a computer workstation name and backslash for a local user, or by a domain name and backslash for domain users.

4. Click **OK**.

    Step Result: The *Connect to* **Ivanti Device and Application Control Application Server** dialog closes.

Result: The *Ivanti Device and Application Control Management Console* window opens.

Logging Out of the Management Console

When you log out from the Management Console you can choose to terminate the adminstrative session or disconnect from the Application Server.

1. To disconnect from the Application Server, select **File** from the navigation bar.

2. Select one of the following options:

Option	Description
Disconnect	The Management Console remains open.
Exit	The Management Console closes.

Result: The **Disconnect** or **Exit** action terminates your current administrative session.

Common Functions within the Management Console

Ivanti Device and Application Control uses standard browsing conventions and navigational functions.

Features specific to the Management Console include menu selections for *Modules*, *Tools*, and Reports. From the console, you can access the Ivanti Device and Application Control *Control Panel* features that you have administrative user access for. You can use the navigation bar to access administrative options and Ivanti Device and Application Control control features.

Common Conventions

This application supports user interface conventions common to most Web applications.

Table 7: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Type data into these fields, which allow the system to retrieve matching criteria or to enter new information.
Drop-Down Menus	Displays a list to select preconfigured values.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to enable a feature, disable a feature, or initiate function for a list item. Some lists also include a **Select All** check box that lets you select all the available listed items on that page (and any remaining pages).
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by ascending (default) or descending order within a respective column by clicking on a (enabled) column header.
Mouseovers	Additional information may be displayed by hovering your mouse pointer over an item.
Auto Refresh	Where present and when selected, the auto refresh function automatically refreshes the page every 15 seconds.
Scrollbars	Drag to see additional data that does not fit the window.
Tabs	Click on the tab name to switch to different information related to the specific page or dialog.
Bread Crumb	Names the page you are currently viewing, that page's parent page (if applicable), and the navigation menu item that opened the displayed page. If viewing a page that is child of another page, you can view the parent page by clicking the bread crumb, which also serves as a link, allowing you to retrace your steps.
Tip: Most system pages support right-click.	

ivanti

Viewing the Management Console

The Management Console graphically displays the administrative user features for the application.

The *Management Console* window is divided into four panels:

- The **Control Panel** provides access to Ivanti Device and Application Control modules, tools, reports, and help functions.
- The main panel displays a window for the module currently selected from the **Control Panel**. Modules remain open and arranged as stacked tabs until closed.
- The **Connection** panel shows information about the current user. You can use the scrollbar to navigate through the text.
- The **Output** panel displays system processing information and error messages.

You can also view the following bars in the *Management Console* window:

- The navigation bar provides access to different Ivanti Device and Application Control functions and commands. Some of these commands and functions depend on the module you are currently using.
- The status bar displays information about the condition of the console.
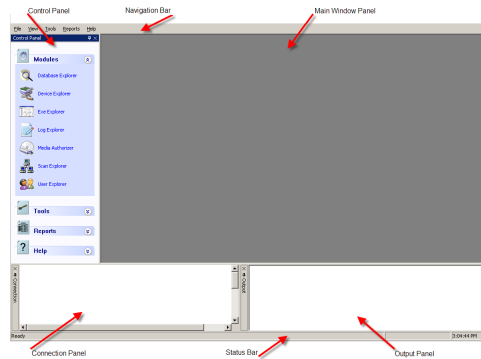
Figure 6: Management Console

Using the Management Console Control Panel

The **Control Panel**, adjacent to the **Management Console** main window, provides access the **Modules**, **Tools**, **Reports**, and **Help** administrative user features.

You can perform the following tasks using the **Control Panel**:

- Use the application control **Modules** to administer routine Ivanti Device and Application Control control tasks.
- Generate **Reports** for users, file groups, Ivanti Device and Application Control clients, and administrator actions.
- Perform system administrative tasks using **Tools**.
- Get **Help**.

Resizing and Repositioning Panels

You can resize and reposition the Management Console panels.

You can customize the appearance of the main window as follows:

- Drag a panel, by selecting the title bar, to any position on the main page.
- Float a panel in any position in the window, to share the main window with open **Modules**.
- Dock a panel to minimize the appearance in the main window. The docked panel appears as a tab at the edge of the main window.
- Scroll across an active panel.
- Close an active panel by clicking the **Close** icon.
- Double click a panel title bar to return to the original position on the main screen.
- Right-click a floating panel title bar to display a drop down menu to restore, move, size, minimize, maximize, or close the panel.

Use the icons listed in the following table to resize or reposition a panel:

Table 8: Resizing and Repositioning Panels

Icon	Function
🖈	Float a panel
🖈	Dock a panel
◂ ▸	Scroll left or right
⊠	Close an active panel

Organizing Columns for Display

You can customize the graphical display for columns in the *Log Explorer* module.

You can reorganize columns by headings only for the *Log Explorer* module.

1. Select the *Log Explorer* module from the Ivanti Device and Application Control *Control Panel*.

   Step Result: The *Explorer* window opens for the module you select.

2. Right-click the table header row of the *Explorer* main window.

   Step Result: A right-mouse menu opens showing all available columns for display. The menu options shown vary according to the Ivanti Device and Application Control control module you select and your license type.

3. Select a column name from the list. A check beside the column name enables the column for display in the *Explorer* window.

ivanti

4. To organize columns, select **Choose Columns...**.

   Step Result: The *Choose Columns* dialog opens.
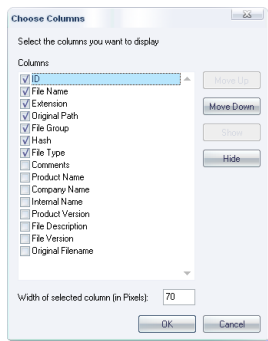
Figure 7: Choose Columns Dialog

5. Choose any of the following options from the *Choose Columns* dialog:

Item	Description
Column	Select or clear the check box for a column. You can modify the column width in the **Width of selected column** field.
Move Up	Shifts the column name description up one place in the dialog list.
Move Down	Shifts the column name description down one place in the dialog list.
Hide	Masks the column display.
Show	Displays the column.

6. Click **OK**.

Result: The *Choose Columns* dialog closes. The *Explorer* window shows the selected columns and associated attributes.

Using the File Menu

The **File** menu displays options for managing the Application Server from the main window. You can also print and save the contents displayed in the main window of the Management Console.

The following table describes the **File** menu items and functions:

Table 9: File Menu

Menu Item	Description
Connect	Establishes communication between the Management Console and a Application Server connected to another computer or user.
Disconnect	Detaches the Management Console from the current Application Server.
Save as	Saves the contents of the main window in `.html` format for exporting data to any `.html` compliant application.
Print	Prints the active report window.
Exit	Exits the current Management Console administrative session.

Using the View Menu

The **View** menu displays options for controlling the appearance of the main panel within the *Management Console*.

The following table describes the **View** menu items and functions:

Table 10: The View Menu

Menu Item	Description
Modules	Shows a submenu for selecting a module.
Control Panel	Shows or hides the menu for selecting **Modules**, **Tools**, **Reports**, and **Help**.
Output	Shows or hides the *Output* window, which displays a log of system activity.
Connection	Shows or hides the *Connection* window, which displays real-time system operating information.
Status bar	Shows or hides the status bar.

ivanti

Using the Tools Menu

The following table describes the **Tools** menu items and functions:

Table 11: Tools Menu

Menu Item	Description
Synchronize Domain Members	Updates the database using a current list of users and groups for a domain or machine.
Database Maintenance	Deletes log and computer database scan files created before a specified date.
User Access	Defines *Enterprise Administrators* and *Administrators* by allowing you to assign access rights for setting permissions and viewing audit information for administrator actions.
Password Recovery Wizard	Allows administrator access to recover a password to unlock an encrypted storage device.
Default Options	Changes the default option settings for users and computers.
Send Updates to All Computers	Transmits the latest setting and permission changes to all managed devices. Changes can be sent manually or automatically when computers restart or at the next login event.
Send Updates to	Transmits the latest setting and permission changes to specific computers on the network.
Export Settings	Places file authorization settings in an external file that can be sent to clients working offline to update file authorization lists.
Endpoint Maintenance	Creates and saves maintenance tickets for computers and computer groups that allows modification of protected files and registries for clients.
Temporary Permission Offline	Generates a code that can be communicated to users by phone to grant them device permissions on a temporary basis when working without a network connection.

Using the Reports Menu

The **Reports** menu displays options to save or print information about Device Control system operations.

The following table describes the **Reports** menu items and functions:

Table 12: Report Menu

Menu item	Description
User Permissions	Shows device permissions associated with one or more users.

Menu item	Description
Device Permissions	Shows users permissions for each device.
Computer Permissions	Shows permissions assigned to each user for the use of the different devices associated with a particular computer.
Media by Users	Shows DVD and CD types and encrypted media a selected user is allowed to access.
	Note: DVDs and CDs authorized for a user resulting from group membership are not listed.
Users by Medium	Shows users or groups allowed to use each authorized CD/DVD and specific encrypted media.
Shadowing by Device	Shows the users who transfer data from specific devices.
Shadowing by User	Shows the total amount of data transferred from different devices for all users.
Machine Options	Shows all the computer options defined in the system.
Client Status	Shows the hardening options, client version, and log and policy file status.
Server Settings	Shows how your Application Server is configured.

The Explorer Menu

The **Explorer** menu displays options that vary based upon the module selected in the **Control Panel**. The following tables describe the **Explorer** menu items and functions.

Attention: There is no **Explorer** menu for the **Media Authorizer** module.

Table 13: Device Explorer Module Menu

Menu Item	Description
Manage Devices	Adds and removes devices that can be administered using permissions.
Insert Computer	Adds a computer to the computer-specific settings section of the **Device Explorer** module or a computer group.
Add/Modify Permissions	Defines and changes general permissions.
Add/Modify Online Permission	Defines and changes device permissions to be applied when a computer is connected to the network.

ivanti

Menu Item	Description
Add/Modify Offline Permissions	Defines and changes device permissions to be applied when a computer is not connected to the network.
Add/Modify Scheduled Permissions	Defines and changes scheduled permissions.
Add/Modify Shadow Settings	Creates and modifies the rules used to generate copies of files that users have transferred from authorized devices.
Add/Modify Copy Limits	Defines and changes file copying quota limits.
Add Temporary Permissions	Defines provisional permissions.
Remove	Deletes a selected permission, device group, computer, or computer group.
Add Event Notification	Defines a message to inform the user of an incident.
Insert Device Group	Adds a device classification group.
Rename Device Group	Changes the name of device classification group.
Insert Computer Group	Adds a computer classification group.
Rename Computer Group	Changes the name of a computer classification group.

Table 14: Log Explorer Module Menu

Menu Item	Description
Fetch log	Obtains the latest log data from a client.

Using the Window Menu

The **Window** menu provides options to control the navigation and display of open windows within the *Management Console*.

The following table describes the *Window* menu options.

Table 15: Window Menu

Menu Item	Description
Cascade	Displays open windows in an overlapping arrangement.
Tile	Displays open windows in a side-by-side arrangement.

Using the Help Menu

The **Help** menu displays option for using help features.

The following table describes the **Help** menu items and functions.

Table 16: Help Menu

Menu Item	Description
Contents	Displays the **Contents** tab of the **Help** file.
Search	Finds a specific topic in the **Help** file.
Index	Displays the **Help** index page.
About	Displays information about your installed version of Ivanti Device and Application Control.
Ivanti on the Web	Redirects to the Ivanti home page for up-to-date information, resources, and support.
Ivanti Knowledgebase	Provides direct access to the Ivanti knowledge base, a source of tips, questions and answers, and how-to articles.

Device Control Modules

The Device Control **Modules** provide access to the functions necessary for configuring and managing and are grouped into three modules, represented by the icons in the **Modules** section of the **Control Panel**.

The following table describes the functions of the **Modules** icons.

Table 17: Device Control Modules

Module	Icon	Description
Device Explorer		Grants access to input/output (I/O) devices for specific users or groups. Establishes copy limits and activates file shadowing. Allows users to encrypt removable devices *on-the-fly* for decentralized encryption.
Log Explorer		Shows records of files transferred from any computer to authorized I/O devices and the contents of the files (shadowing). Shows user attempts to access or connect unauthorized devices. Provides templates to create customized reports.
Media Authorizer		Provides for central encryption of removable devices. Allows for users to access specific CD/DVD. Allows for users to use specific encrypted media.

ivanti

License Expiration

A license expiration **_Warning_** message displays, if you are a subscription user, when you log in to the **_Management Console_**.

The following table describes the types of license expiration warnings.

Expiration Period	Warning Message	Frequency
Expired	`The license has expired.`	Once
Less than one day	`The license will expire in x hours.` `The license will expire in x minutes.`	Once per hour
Less than 60 days	`The license will expire in x days.`	Once per day
More than 60 days	No message.	Not applicable

Note: When you must renew or add a license, contact your Ivanti representative.

Chapter

3

Using Modules

Device Control modules are based upon the type of user access or device permission rules that you want to establish. Using the Management Consoleyou can access to the Device Control modules.

Device Control consists of a series of task-oriented modules. Depending on the task, you may use one of the following modules in the Management Console **Control Panel**:

• **Device Explorer** to manage all peripheral device classes and add permission rules for users and user groups.
• **Media Authorizer** to encrypt removable storage media and authorize user access to CD/DVD media.
• **Log Explorer** to explore and analyze user and administrator activity logs.

Working with Device Explorer

Default permission rules are created and configured when you install Device Control. These rules include file shadowing and read/write permissions for some devices. An administrator uses the **Device Explorer** module to define new device permission rules for users, groups, computers, or devices.

With the **Device Explorer** module of Device Control, Ivanti Device and Application Control administrators can:

• Create and modify permission rules for user access to encrypted removable storage media.
• Identify users who must encrypt removable storage media before use.
• Manage removable storage media by adding and removing devices from the Ivanti Device and Application Control database.
• Define bus types according to device class for assigning user access permission rules.

ivanti

The following types of user access permission rules can be assigned using the **Device Explorer**:

- Read data.
- Read/write data.
- No access to data.
- Access only encrypted removable storage media.
- Create online device access.
- Create offline device access.
- Schedule device access.
- Create temporary device access.
- Establish data copying limits.
- Encrypt and decrypt removable storage media.
- Export and import encryption keys for device access outside of the Ivanti Device and Application Control system.

Device Explorer Window

An administrator uses the **Device Explorer** hierarchy to create and manage device and computer user groups, as well as, assign permission rules for online, offline, temporary and scheduled device use. The **Device Explorer** module is also used to create and manage file shadowing rules.

The main window of the **Device Explorer** module displays a hierarchical structure of device classes, which is divided into two primary levels:

- **Default settings** which contain the user access permission rules that apply to every computer.
- **Machine-specific settings** which contain unique user access permission rules that apply to a specific computer or group of computers.
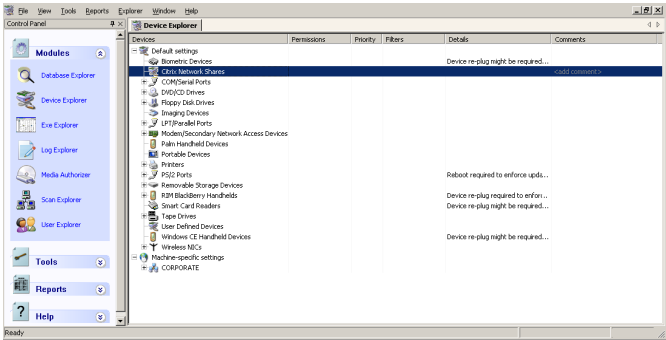
Figure 8: Device Explorer Main Window

The **Device Explorer** window is further divided into the following columns:

Table 18: Device Explorer Window Column Descriptions

Column	Description
Devices	Lists device classes and users or user groups with permission to access devices.

Column	Description
Permissions	Shows a description of the type of permission provided to users and user groups listed in the **Devices** column.
Priority	Shows a priority of **High** or **Low** assigned to rules listed in the **Permissions** column.
Filters	Shows a description of the file type filtering rules assigned to rules listed in the **Permissions** column.
Details	Shows a description of permissions rules details.
Comments	Ivanti Device and Application Control administrators can select permission rules and enter comments by clicking the **Comments** column heading.

Managing Devices

When Device Control is initially installed, all removable storage devices that belong to standard Microsoft Windows® device classes are identified and added to the database. You can set up and manage user access permission rules for the different models and specific device types using the *Device Explorer*.

Using the *Device Explorer* you can add devices and device types for computers and add computers that are not included in the *Active Directory* structure. You can define general user access permission policies based on the predefined device classes.

Restriction: You can add specific device models to all base device classes, except the **PS/2 ports** classes.

Device Types Supported

Device Control supports a wide range of device types that represent key sources of confidential data security breaches. You can define user access permission at the device class level to restrict access to specific device types. Device Control can detect *plug-and-play* devices.

The device types you can manage using Device Control are described in the following table.

Table 19: Supported Device Types

Device Type	Description
Biometric Devices	Includes *Password Managers* and *FingerPrint* readers.
Citrix Network Shares	Includes any mapped drive, whether a mapped network drive or a locally mapped device, when accessed through either a Citrix–delivered application or the Citrix desktop.
COM/Serial Ports	Includes serial ports and devices that use COM device drivers, such as modems, null modems and terminal adaptors. Some *PDA* cradles use a virtual serial port, even when connected through the *USB* port.

ivanti

Device Type	Description
DVD/CD Drives	Includes CD-ROM and DVD access for full device lock and unlock.
Floppy Disk Drives	Includes disk drive access for complete lock and unlock mode or read-only mode of conventional diskettes and high capacity drives.
Imaging Devices	Includes USB or SCSI devices, scanners, and webcam.
Keyboards/Mice	Includes keyboards/mice that use USB, PS/2, and Bluetooth.
LPT/Parallel Ports	Includes conventional parallel printer ports and variants such as ECB and Dongles.
Modems/Secondary Network Access Devices	Includes internal and external devices. Secondary network devices do not connect through normal channels.
Palm Handheld Devices	Includes conventional types of this device.
Portable Devices	Includes smart storage devices such as MP3 players, digital still cameras, mobile phones, mobile storage devices, and Windows Mobile 6.x OS PDAs.
Printers	Includes print devices attached directly to a print server or directly to a network through a network adapter card.
PS/2 Ports	Includes the conventional type of port used to connect keyboards.
Removable Storage Devices	Includes chip- and disk-based devices that are not floppy or CD-ROM devices, such as Jaz and PCMCIA hard drives and USB memory devices such as memory stick, Disk on Key, AIP, and most USB-connected MP3 players and digital cameras.
	Note: Non-system hard drives are treated as removable storage devices.
RIM Blackberry Handhelds	Includes handheld computers and mobile phones from Research in Motion (RIM) BlackBerry connected to a computer through a USB port.
Smart Card Readers	Includes eToken and fingerprint readers for smart cards.
Tape Drives	Includes conventional internal and external tape drives of any capacity.
User Defined Devices	Includes devices that do not fit standard categories, such as some PDAs, non-Compaq iPAQ, USB, non-Palm handheld USB, Qtec, HTC and webcams.

Device Type	Description
Virtualized USB Devices	Includes generic redirects to USB devices in virtualized environments (Citrix and VMWare).
Windows CE Handheld Devices	Includes the HP iPAQ® or XDA, Windows Mobile 5 CE® devices and Windows CE® computers connected through a USB port.
Wireless Network Interface Cards (NICs)	Includes the device option to configure client permission rules use a wireless LAN adaptor.

Device Permission Default Settings

When Device Control is initially installed, default user access permission rules apply to all supported predefined device classes.

The following table describes default permission settings for the predefined devices classes.

Table 20: Device Default Settings

Device Class	Permission	Shadow	Copy Limit
COM/Serial Ports	No access	Disable	Not available
CD/DVD Drives	No access	Disable	Not available
Floppy Disk Drives	No access	Disable	Not available
Keyboards/Mice	Read/Write (Low Priority)	Not available	Not available
LPT/Parallel Ports	No access	Disable	Not available
Portable Devices	No access	Disable	No limit
PS/2 Ports	Read/Write (Low Priority)	Not available	Not available
Removable Storage Devices	No access	Disable	No limit
Wireless Network Interface Cards (NICs)	Read/Write (Low Priority)	Not available	Not available

ivanti

Device Permission Restrictions

Based upon Microsoft® driver design or the device manufacturer design, some restrictions apply to devices when assigning user access permission.

The following table shows the allowable user access permissions and restrictions for each predefined device class.

Table 21: Device Permission Restrictions

Device Class	Permission Allowed	Restriction
Biometric Devices	Read-Write/None; Select bus type	Only for `LocalSystem` or `Everyone`.
Citrix Network Shares	Read-Write/None	Any user or user group.
COM/Serial Ports	Read-Write/None; Select bus type	Any user or user group.
CD/DVD Drives	Read only/Read-Write/None; Select bus type	Any user or user group.
Floppy Disk Drives	Read only/Read-Write/None; Select bus type	Any user or user group.
Keyboards/Mice	Read only/Read-Write/None; Select bus type	Only for `Everyone`.
Imaging Devices	Read-Write/None; Select bus type	Any user or user group.
LPT/Parallel Ports	Read only/Read-Write/None; Select bus type	Any user or user group.
Modems/Secondary Network Access Devices	Read-Write/None; Select bus type	For regular modems, any user or group.
	Read-Write/None; Select bus type	For ISDN modems or network adapters, only for the `Everyone` group.
Palm Handheld Devices	Read-Write/None; Select bus type	Any user or user group.
Portable Devices	Read-only/Read-Write/None	Any user or user group.
Printers	Read-Write/None; Select bus type	Any user or user group.
PS/2 Ports	Read-Write/None; Select bus type	Only for `LocalSystem` or `Everyone`.
Removable Storage Devices	Read-Write/None; Select bus type	Any user or user group.
	Encrypt, Decrypt, Export, Import; Select bus and drive type	Any user or user group.

Device Class	Permission Allowed	Restriction
RIM Blackberry Handhelds	Read-Write/None	Any user or user group.
Smart Card Readers	Read-Write/None; Select bus type	Only for `LocalSystem` or `Everyone`.
Tape Drives	Read-Write/None; Select bus type	Any user or user group.
User Defined Devices	Read-Write/None	Any user or user group.
Virtualized USB Devices	Read-Write/None	Any user or user group.
Windows CE Handheld Devices	Read-Write/None	Any user or user group.
Wireless Network Interface Cards (NICs)	Read-Write/None	Only for `Everyone`.

Add Computers

You can add computers to a domain group or computer workgroup in the **Machine-specific settings** structure of the *Device Explorer*.

When Device Control is used for computers in a workgroup, rather than a domain, then there is no domain controller list of users. You must add the computers individually to a workgroup.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.
2. Right-click the **Machine-specific settings** level in the hierarchical device structure.
3. From the right-mouse menu, select **Insert Computer**.
4. From the *Select Computer* dialog, click **Search**.
5. Select one or more computers from the list shown.
   a) To add a computer that is not listed, click **Add**.
   b) Type the name of the computer to be added in the corresponding field.
6. Click **OK**.

Result: The computers you selected are added to the domain group.

> **Tip:** You can drag-and-drop computers from one group to another, or you can right-click a computer and use **Cut** and **Paste** from the right-mouse menu.

Create Computer Groups

You can create computer groups to organize computers into logical units that share unique device permissions for the group.

Computer groups are virtual groups that do not have relationships with each other in the *Active Directory*.

ivanti

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. Right-click the domain group under the **Machine-specific settings** level in the hierarchical device structure.

3. From the right-mouse menu, select **Insert Computer Group**.

    Step Result: The right-mouse menu opens.

Insert Computer...	Ctrl+A
Insert Computer Group...	Ctrl+O
Paste	Ctrl+V

Figure 9: Computer Group Menu

4. Type a name for the computer group in the in the **New Folder** directory.

5. Press ENTER.

Result: The new computer sub-group is shown in the *Machine-specific settings* hierarchical structure.

> **Tip:** You can drag-and-drop computers from one group to another, or you can right-click a computer and use **Cut** and **Paste** from the right-mouse menu.

View Hidden Computers

You can view computer group(s) to show any hidden computers when you want to change permissions, move the computer(s) to other groups, or remove the computer(s) from existing groups.

Computers may be hidden from view in the *Device Explorer* window when the computers have not been assigned user access permission rules. The computer names are hidden to minimize the number of computers shown.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. From the **Machine-specific setting** division of the hierarchical device structure, right-click a computer group to view the hidden computers.

3. Select **Show All Members** from the right-mouse menu.

Result: A list of all computers included in the computer group selected is shown.

Manage Computers

You can rename computer groups, device groups, and devices in a device class belonging to the default settings tree in the *Device Explorer* module.

To customize the appearance of *Device Explorer* hierarchy to reflect your operating environment, you can rename and remove computer groups as follows.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. From the **Machine-specific setting** division of the hierarchical device structure, right-click a computer group.

3. Select on the following options from the right-mouse menu:

Option	Description
Rename Computer Group	Renames the selected computer group.
Remove Computer Group	Removes the selected computer group for the hierarchical structure.

Result: The computer group is renamed or removed immediately from the hierarchical device structure in the **_Device Explorer_** window.

Create Device Groups
You can organize devices into logical groupings that can share unique user access permissions.

You can:

- Create a new device class group at the upper level.
- Add devices to the same device class group.
- Move devices between groups.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. Expand the hierarchical device structure from **Default settings** level.

3. Right-click any device class at the highest level.
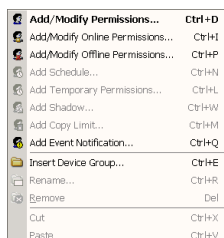
Figure 10: Device Group Menu

4. Select **Insert Device Group** from the right-mouse menu.

    Step Result: A new device sub-class group structure is displayed.

5. Type a name for the new device group sub-class.

6. Press ENTER.

Result: You can add any device of the same device class to the new device group.

> **Tip:** You can drag-and-drop devices from one device group to another wiithin the same device class, or you can right-click a device and use **Cut** and **Paste** from the right-mouse menu to move devices between groups.

ivanti

Manage Devices

Within a device class, you can create groups that contain models or unique device IDs. Managing devices in groups reduces the administrative burden for assigning and tracking device permissions.

You can assign device permissions at the following levels:

- Class
- Group
- Model
- Unique Device ID

Restriction: You can not add specific device model types to the **PS/2 Ports** class.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the hierarchical device structure shown in the *Device Explorer* window, right-click **Default settings**.

3. Select **Manage Devices** from the right-mouse menu.

   Step Result: The *Manage Devices* dialog opens.
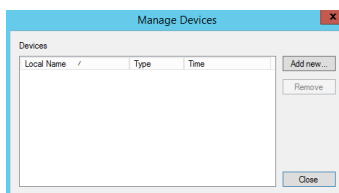
Figure 11: Manage Devices Dialog

4. Click **Add new**.

   Step Result: The *Devices* dialog opens.
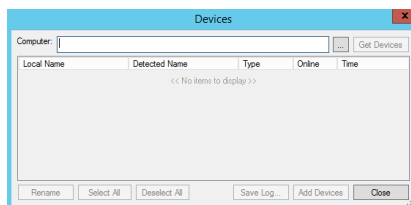
Figure 12: Devices Dialog

5. Click the ellipses to show a list of computer names registered in the Active Directory, synchronized to the database, and/or logged in to the network.

6. Select a computer from the *Select Computer* dialog and click **OK**.

7. Click **Get Devices**.

> **Step Result:** The *Devices* dialog refreshes to show a list of devices detected for the computer you selected. Information available:

Column	Description
Local Name	Customizable name associated with the device in the Management Console.
Detected Name	Device name as detected by the agent.
Type	Functional capability of the device. For example, `Removable Storage Device` or `Printer`.
Online	Indicates the connection status of the device to the endpoint (`Yes` or `No`). `Unknown` displays when a device on a pre-4.6 endpoint is queried by the Management Console.
Time	Time and date the device was last detected.
Unique ID	Unique identifier for the device.

8. Select device(s) using the check box adjacent to the device name.

9. Click **Add Devices**.

> **Step Result:** The *Devices* dialog refreshes showing the devices you added as greyed selections.

> > **Tip:** You can save a log entry for all the devices connected to the selected computer by clicking **Save Log**.

10. Click **Close**.

Result: The new device(s) are shown in the *Device Explorer* window.

Adding a Network Printer to Device Explorer
As network printers do not have unique ID, you must add them to the Printers device class in Device Explorer through a `WRITE-DENIED` event in the Log Explorer.

Prerequisites:

You must have attempted to print to the network printer to create a `WRITE_DENIED` action.

1. From the Management Console, select **View** > **Modules** > **Log Explorer**.

> **Step Result:** *Log Explorer* window opens.

2. Click **Fetch Log**.

> **Step Result:** The *Select Computer* dialog opens and prompts you to specify the client computer to fetch the logs from.

ivanti

3. Click **Search or Browse** and select the appropriate computer from the list.

4. Click **OK**.

> **Step Result:** The computer logs are uploaded to the Application Server and stored in the database. Updated log files are shown in the *Log Explorer* window.

5. Find the `WRITE-DENIED` event generated by the network printer in the *Log Explorer* window

6. Right-click on the event and select **Add Device(s)**.

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

7. Select the check box beside the network printer name and click **Add Devices**.

> **Step Result:** The network printer is added to the Printers device class.

8. Click **Close**.

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

Result: The network printer will appear under the Printers node in the Device Explorer. You can now assign permissions to it.

Microsoft Virtual Desktop Infrastructure Limitations

Learn about the limitations of managing USB Virtual Devices in Microsoft VDI.

- Only SB devices are supported and are not connected as actual devices (no encryption, filtering supported):

  - Windows Portable devices don't expose a file system: they have no drive letter and aren't exposed via `\\tsclient\X`
  - DVD burning isn't done via file system so it isn't supported by `\\tsclient\X` exposed drives.
  - Shadowing isn't supported on `\\tsclient\X` exposed drives.
  - Printing isn't done via `\\tsclient\X` exposed drives.

- The thin client requires adding the ESDI DLL to the system32 folder and the regkey set to point to it.
- No encryption of devices is supported as they are not connected as USB.
- Device log events can be used to create special device permissions. The device is not connected so requesting a devices list from the machine will not work.
- File shadowing is not supported as devices are not in a mode where files are intercepted as being copied.

Managing Permissions

To define user access permission rules for a device or device class, you must assign one or more users or user groups to the device.

You use the *Permissions* dialog in the *Device Explorer* module to manage permission rules for user access to peripheral devices. Initially, the default permissions for all devices that connect to a computer running the Ivanti Device and Application Control client is **None**, which means that all user access is denied.

Permissions Dialog

An administrator uses the ***Permissions*** dialog to create and manage permission rules for devices and associate these rules with user and user group access rights.

The ***Permissions*** dialog is the primary tool that an administrator uses to:

- Assign and manage user access permission rules for devices connected to client computers.
- Force encryption of removable storage media that users are permitted to access.

The ***Permissions*** dialog is composed of five panels:

- ***User/Group***
- ***Permissions***
- ***Encryption***
- ***Bus***
- ***Drive***
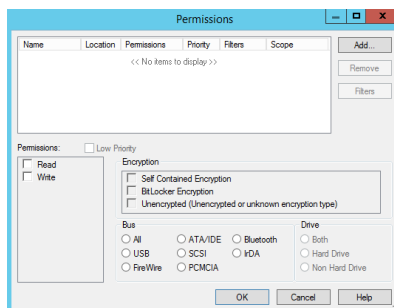
Figure 13: Permission Dialog

The following tables described the ***Permissions*** dialog panels.

Table 22: User/Group Panel

Column	Description
Name	Shows the name of the user or user group.
Location	Shows the user domain or work group name.
Permissions	Lists the rules defined by the ***Permissions*** panel.
Priority	Shows the permission priority specified as **High** or **Low**.
Filters	Shows the file types that the user or user group can access.

ivanti

Column	Description
Scope	Shows the permission defined in the **Encryption**, **Bus**, and **Drive** panels.

Table 23: Permissions Panel

Option	Description
Read	A user or user group has read access.
Write	A user or user group has write access.
Encrypt	A user or user group can encrypt devices.
Decrypt	A user or user group can decrypt an encrypted device.
Export to file	The passphrases or public keys from user certificates are used to create a symmetric key for device encryption. When the **Self Contained Encryption** option is selected, the encryption key can be stored in a separate file and password protected. This is the most secure method, because the encryption key and the encrypted data can be transported separately.
Export to media	The passphrases or public keys from user certificates are used to create the symmetric key used to encrypt a device. When the **Self Contained Encryption** option is selected, the encryption key can be stored on the same device used for encryption and password protected. The only protection of the data is the password itself.
Import	When the **Self Contained Encryption** option is selected, a user can access encrypted media by specifying a separate key file, which is not stored on the encrypted media, and providing the associated password.

Restriction: Permission to **Encrypt**, **Decrypt**, **Export to file**, **Export to media**, and **Import** is available only for the **Removable Storage Devices** class.

Table 24: Encryption Panel

Option	Description
Self Contained Encryption	The assigned **Permissions** apply to the device when encrypted with Device Control self-contained encryption technology.
BitLocker Encryption	The assigned **Permissions** apply to the device when encrypted with BitLocker Drive Encryption.

Option	Description
Unencrypted (Unencrypted or unknown encryption type)	The assigned **Permissions** apply to the device when unencrypted or encrypted with an unsupported technology.

Table 25: Bus Panel

Option	Description
All	**Permissions** apply when a device is connected through any bus connection.
USB	**Permissions** apply when a device is connected through a USB 1.1 and 2.0 or higher standard interface.
Firewire	**Permissions** apply when a device is connected through a Firewire IEEE 1394 standard interface.
ATA/IDE	**Permissions** apply when a device is connected through the ATA/IDE, SDATA-1, SATA-2 and eSATA variants interfaces.
SCSI	**Permissions** apply when a device is connected through the SCSI narrow, wide and ultra variants interfaces.
PCMCIA	**Permissions** apply when a device is connected through the PCMCIA CARDBUS interface, including the Expresscard/34 and /54 variants.
Bluetooth	**Permissions** apply when a device is connected through the Bluetooth standard interface.
	Note: A Bluetooth device must be restarted for a permission change to take effect.
IrDA	Permissions apply when a device is connected through the IrDA (infrared) standard interface.

Restriction: Only standard interface types supported by the device class you select are available for defining permissions.

Table 26: Drive Panel

Options	Description
Both	Permission rules apply to the hard drive and non-hard drive for the device class selected.
Hard Drive	Permission rules apply only to the hard drive for the device class selected.

ivanti

Options	Description
Non-Hard Drive	Permission rules apply to the non-hard drive for the device class (including Removable Storage Devices) selected.

Default Settings Permissions Priority

For device permissions assigned to a user or user group, priority settings govern whether a **Machine-specific Settings** permission rule can override a **Default Settings** permission rule.

You can change the priority for **Default Settings** and **Machine-specific Settings** permission rules from **High** to **Low**. All permissions are automatically assigned **High** priority by default. Permissions can be assigned as:

- Read
- Read/Write
- None

- When a **Default Settings** permission rule is set as **None** and the permission priority is set as **High** priority, a **Machine-specific Settings** permission rule cannot override the **Default Settings** permission rule.
- When a **Default Settings** permission rule is set as **None** and the permission priority is set a **Low** priority, a **Machine-specific Settings** permission rule set as **High** priority can override the **Default Settings** permission rule.
- When a **Machine-specific Settings** permission rule is set as **None** and the permission priority is set as **High** priority, a **Machine-specific Settings** permission rule can override the **Default Settings** permission rule.

The following table illustrates how permission are applied for combinations **Default Settings** and **Machine-specific Settings**, depending upon priority settings.

Note: Configuring permissions in Default Settings is optional. If no permission is defined at any level, the default behavior enforced is to block access to the device.

Table 27: Default Settings Permissions Priority

Default Setting	Default Settings Permission Priority	Computer Specific (or Device) Permission	Computer Specific (or Device) Permission Priority	Resulting Permission
Read	High	Read/Write	High	Read/Write
			Low	Read/Write
		None	High	None
			Low	Read
		Read	High	Read

Default Setting	Default Settings Permission Priority	Computer Specific (or Device) Permission	Computer Specific (or Device) Permission Priority	Resulting Permission
			Low	Read
	Low	Read/Write	High	Read/Write
			Low	Read/Write
		None	High	None
			Low	None
		Read	High	Read
			Low	Read
Read/Write	High	Read/Write	High	Read/Write
			Low	Read/Write
		None	High	None
			Low	Read/Write
		Read	High	Read/Write
			Low	Read/Write
	Low	Read/Write	High	Read/Write
			Low	Read/Write
		None	High	None
			Low	None
		Read	High	Read/Write
			Low	Read/Write
None	High	Read/Write	High	None
			Low	None
		None	High	None
			Low	None
		Read	High	None
			Low	None

ivanti

Default Setting	Default Settings Permission Priority	Computer Specific (or Device) Permission	Computer Specific (or Device) Permission Priority	Resulting Permission
	Low	Read/Write	High	Read/Write
			Low	None
		None	High	None
			Low	None
		Read	High	Read
			Low	None

The following diagram can be used to determine the resultant policy permission when two policies that contain different permissions merge:
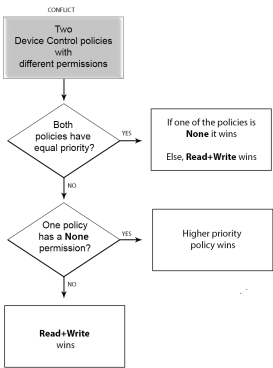
Figure 14: Policy Permission Resultant Policy Determination Diagram

File Filters

You can assign file filters to user access permissions rules that limit access to specific file types.

The following rules apply to file filters.

- You can define separate file filtering rules for **Read**, **Write**, and **Read/Write** permissions.
- File filters are only available for use with the **Removable Storage Devices**, **Floppy Disk Drives**, **Portable Devices** and **DVD/CD Drives** device classes.

> **Note:** If you activate the File Filtering feature for the DVD/CD class, the user will not be able to burn such media. In the *File Type Filtering* dialog under the *Permissions* section, you will not be able to select the **Export** option when file filtering is activated for this class. The user will be able to burn a DVD/CD once the file filtering is deleted.

- You can only assign file filtering rules individually to users and user groups.
- Permissions rules without file filtering always take precedence over rules with file filtering.
- When using *File Type Filtering* you cannot burn CD/DVD media.
- *File Type Filtering* rules cannot be combined with the **Bus** option in the same permissions rule.
- The archive types supported by File Filters are: Zip Compressed Archive, Protected Zip Compressed Archive, WinRAR Compressed Archive, Protected WinRAR Compressed Archive, WinACE Compressed Archive, Microsoft Cabinet Compressed Archive, Microsoft LZ Compressed Archive, PRIM'X ZED Compressed Archive, 7-zip Compressed Archive, Protected 7-zip Compressed Archive, GZip Compressed Archive, ISO Compressed Archive, VHD Compressed Archive.

BitLocker Encrypted Devices

You can use BitLocker encrypted devices in a Device Control environment.

Windows BitLocker Drive Encryption is a security feature that provides data protection by encrypting all data stored on a Windows operating system volume. Using the Management Console with BitLocker encrypted devices, you can:

- Assign user and user group access permission rules to devices. Permission rules can only be assigned to the Removable Storage Devices class.
- Add shadowing rules.
- Review log entries for user attempts to access devices by using the Log Explorer.
- Review log entries for administrative actions for BitLocker permissions actions.
- Generated reports for BitLocker permissions rules using the Device Permissions report.

Assigning Permission to a BitLocker Encrypted Device

You can authorize the use of a device encrypted with BitLocker Drive Encryption from the *Permissions* dialog.

BitLocker is a data protection feature that provides security by encrypting all data stored on a Windows operating system volume.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the *Default settings* or *Machine-specific settings* division of the Device Explorer hierarchical structure, right-click a **Removeable Storage Devices** node.

ivanti

3. Select **Add/Modify Permissions** from the right-mouse menu.

   Step Result: The *Permissions* dialog opens.

4. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse**

6. Select a user or user group, then click **OK**.

7. In the **Permissions** dialog, select the user or user group to assign user access permission rules.

8. In the *Encryption* section, select **BitLocker Encryption**.
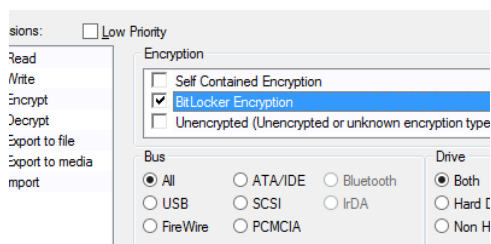
Figure 15: Encryption section

9. In the *Permissions* section, select **Read** and/or **Write**.

10. Click **OK**.

Result: The BitLocker encrypted device is authorized for use for the selected users or user groups. The Removeable Storage Device status on the endpoint will display as BitLocker Encrypted.

Figure 16: Endpoint Status Dialog

Working with Custom File Types

When the type of file you want to detect is not already supported directly by Device Control, you can extend the file type recognition capability by configuring a custom filter.

Manage Custom File Types Dialog

Use the **Manage Custom File Types** dialog dialog to add, edit and remove custom file type definitions.

On this dialog you can:

- View the available custom file types.
- Add a new custom file type. See Adding a Custom File Type Filter on page 63
- Edit an existing custom file type. See Editing a Custom File Type Filter on page 67
- Remove a custom file type. See Removing a Custom File Type Filter on page 67
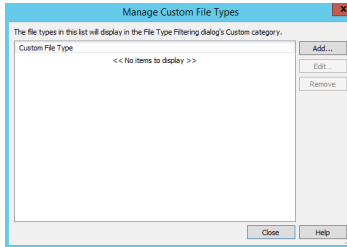
Figure 17: Manage Custom File Types dialog

ivanti

New Custom File Type Dialog

Use the **New Custom File Type** dialog to define the steps required to detect the file type you want to limit access to. It is launched by clicking **Add** on the **Manage Custom File Types** dialog.

On this dialog you can:

- Enter a name that will be displayed in the file type filtering dialog.
- View the steps already defined for detecting this custom file type.
- Add Steps to the filter:

Search for Bytes	Search for a byte string within a file, which is unique to the file type you want to detect.
Read a Variable	Create a variable that reads an integer value at a specific position in the file.
Change Current Position	Change the current position of the reference point.
Check End of File	Check if the current position is the end of the file.

- Edit an existing Step by selecting it and clicking **Edit**. See Editing a Custom File Type Filter on page 67.
- Remove an existing Step by selecting it and clicking **Remove**. See Removing a Custom File Type Filter on page 67.
- Move a Step's position in the sequence by selecting it and clicking **Move Up** and **Move Down**.

Figure 18: New Custom File Type dialog

Edit Custom File Type Dialog
Use the **Edit Custom File Types** dialog to add or change steps required to detect the file type you want to limit access to. It is launched by selecting an existing definition in the **Manage Custom File Types** dialog and clicking **Edit**.

On this dialog you can:

- Edit the name displayed in the file type filtering dialog.
- View a list of the Steps defined for detecting the file type, ordered sequentially.
- Add Steps to the filter:

Search for Bytes	Search for a byte string within a file, which is unique to the file type you want to detect.
Read a Variable	Create a variable that reads an integer value at a specific position in the file.
Change Current Position	Change the current position of the reference point.
Check End of File	Check if the current position is the end of the file.

- Edit an existing Step by selecting it and clicking **Edit**. See Editing a Custom File Type Filter on page 67.
- Remove an existing Step by selecting it and clicking **Remove**. See Removing a Custom File Type Filter on page 67.
- Move a Step's position in the sequence by selecting it and clicking **Move Up** and **Move Down**.

ivanti

Search for Bytes Dialog

Use the **Search for Bytes** dialog to provide a string of bytes unique to the file type you want to detect and limit access to. It is launched in the **New Custom File Type** or **Edit Custom File Type** dialogs by selecting **Add** > **Search for Bytes**.

On this dialog you can:

- Enter a string of bytes in hexidecimal notation unique to the file type you want to detect. Spaces, and line breaks are allowed. For example, `02 BF 03`.
- Set a Reference Point from where the system is to start its search for the byte string:

The beginning of the file	Search starts from the beginning of the file (Byte 0).
The current file position	Search starts at the current position of the Reference Point.
The end of the file	Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset.

Note: If the bytes are found, the current position is changed to the byte after the end of the matching byte string.

- Set an offset value to have the system search for the string from a particular location in the file:

Use this offset	Enter a value that represents the number of bytes from the Reference Point the system should search for the unique byte string. Negative values go left from the Reference Point.
Use the offset in this variable	Select the value contained in a pre-defined variable to set the number of bytes from the Reference Point, the system should look for the uniqe byte string.

- Set a byte range within which the system is to confine its search for the byte string:

Bytes must start within this distance of the offset	Enter a value that represents the length of the byte range from the offset, where the system is to search for the beginning of the byte string.
Use the distance in this variable	Select the value contained in a pre-defined variable to set the length of the byte range from the current position, where the system is to search for the beginning of the byte string.

Figure 19: Search for Bytes dialog

Read a Variable Dialog

Use the **Read a Variable** dialog to define a variable that reads an integer. It is launched in the **New Custom File Type** or **Edit Custom File Type** dialogs by selecting **Add** > **Read a Variable**.

On this dialog you can:

- Set the name of the variable.
- Set the integer size in bytes. 1, 2, 4, and 8 are the available options.
- Set an endian format option for the integer value:

Note: Endian format does not apply to 1 byte integers.	
Little endian	Low-order byte is stored at the lowest address, and the high-order byte at the highest address.
Big endian	High-order byte is stored at the lowest address, and the low-order byte at the highest address.

- Set a Reference Point from where the system is to start its search for the integer:

The beginning of the file	Search starts from the beginning of the file (Byte 0).
The current file position	Search starts at the current position of the Reference Point.
The end of the file	Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset.

Note: If the integer is found, the current position is changed to the first byte after the integer.

- set an offset value to have the system search for the integer from a particular location in the file:

Use this offset	Enter a value that represents the number of bytes from the Reference Point that the system should read the integer value to the variable from. Negative values go left from the Reference Point.
Use the offset in this variable	Select the value contained in a pre-defined variable to set the length of the byte range from the current position, where the system is to search for the integer value to be saved in the variable.

Figure 20: Read a Variable dialog

ivanti

Change Current Position Dialog
Use the ***Change Current Position*** dialog to move the current position used in later steps. It is launched in the ***New Custom File Type*** or ***Edit Custom File Type*** dialogs by selecting **Add** > **Change Current Position**.

On this dialog you can:

• Change the position of the Reference Point:

The beginning of the file	Search starts from the beginning of the file (Byte 0).
The current file position	Search starts at the current position of the Reference Point.
The end of the file	Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset.

• Move a number of bytes from the Reference Point:

Use this offset	Enter a value that represents the number of bytes from the Reference Point, where the pointer should be moved to. Negative values go left from the Reference Point.
Use the offset in this variable	Select a variable containing an integer value that represents the number of bytes from the Reference Point, where the pointer should be moved to.

Figure 21: Change Current Position dialog

Check End of File Dialog
Use the ***Check End of File*** dialog to add a step that succeeds if the current position is the end of the file. It is launched in the ***New Custom File Type*** or ***Edit Custom File Type*** dialogs by selecting **Add** > **Check End of File**.

No setting are required for this step.

Figure 22: Check End of File dialog

Adding a Custom File Type Filter
You can add a custom file type to the File Filters collection by creating a custom file type filter and configuring steps to identify the file type.

Prerequisites:

- Research the file format. Many file formats are documented publicly on the Internet. Understanding and using the characteristics that are specific to the file type you want to build a filter for will result in more accurate file identification.
- Gather multiple samples of the file type you want to filter. Ensure the samples are from different sources, represent various versions, and created on assorted operating systems.
- You must have hex editor software that enables you to view the bytes in any file in hexadecimal format.
- Identify a few bytes common to all the sample files. If you use a filter that has too many bytes specified, some files of that type will not be recognized as such. If you use too few bytes, then some files that are not of that type will erroneously be recognized as files of that type.

1. In the **Control Panel** pane under the **Modules** section, select **Device Explorer**.

2. In the navigation bar, select **Explorer** > **Manage Custom File Types**.

   Step Result: The **Manage Custom File Types** dialog opens.

3. Click **Add**.

   Step Result: The **New Custom File Type** dialog opens.

4. Enter a name in the **Name** field.

   The name will be displayed in the **File Type Filtering** dialog.

You must create at least one step to detect the file type. The steps you configure will run in the order they are placed in the **Steps to detect the file type** section. If all steps succeed then the file is determined to be of the type you want to filter. If one step fails the file type is determined not to be of that type.

ivanti

For example, a common step sequence is:

- Search for particular bytes at the beginning of the file.
- Move to an offset from the beginning of the file and read in a variable. Then move the current position by the offset in that variable, and then check for end of file.
- Move to an offset from the beginning of the file and read in a variable. Move the current position by the offset in that variable, and then search for specific bytes.
- Search for bytes at the beginning of the file. Read in a variable. Move to a given offset. Read in another variable. Move to a postion of beginning of file plus the value in Variable 1, then check for specfic bytes. Move to the end of file position minus the value in Variable 2, then check for specific bytes.

5. Add steps to detect the type of file you want to filter:

Option	Description
Search for Bytes	Provide a byte string unique to the file type you want to detect: 1. Select **Add** > **Search for Bytes**. The Search for Bytes dialog opens. 2. In the **Bytes to search for, in hexidecimal notation** field, enter the string of bytes you have identified as unique to the file type you want to detect. 3. From the **Reference Point** drop-down, select the point from where the system is to start its search for the byte string: • **The beginning of the file**: Search starts from the beginning of the file (Byte 0). • **The current file position**: Search starts at the current position of the Reference Point. • **The end of the file**: Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset. **Note:** If the bytes are found, the current position is changed to the byte after the end of the matching byte string. 4. Select an option and set an offset value to have the system start its search for the byte string from a particular location in the file: • **Use this offset**: Enter a value that represents the number of bytes from the Reference Point the system should look for the unique byte string. Negative values go left from the Reference Point. • **Use the offset in this variable**: Select the value contained in a pre-defined variable to set the number of bytes from the Reference Point, the system should look for the uniqe byte string. 5. Select an option and set a byte range within which the system is to confine its search for the byte string. • **Bytes must start within this distance of the offset**: Enter

Option	Description

Read a Variable	Create a variable that reads an integer:
	
	1. Select **Add** > **Read a Variable**. The Read a Variable dialog opens.
	2. In the **Variable name** field, enter a name.
	3. From the **Integer size in bytes** drop-down, select the number of bytes the integer has. 1, 2, 4, and 8 are the available options.
	4. In the **Byte Order** section, select an endian format option for the integer value:
	
	Note: An endianness format does not apply to 1 byte integers.
	
	   • **Little endian**: Low-order byte is stored at the lowest address, and the high-order byte at the highest address.
	   • **Big endian**: High-order byte is stored at the lowest address, and the low-order byte at the highest address.
	5. From the **Reference Point** drop-down, select the point from where the system is to start searching for the integer:
	
	   • **The beginning of the file**: Search starts from the beginning of the file (Byte 0).
	   • **The current file position**: Search starts at the current position of the Reference Point.
	   • **The end of the file**: Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset.
	
	Note: If the integer is found, the current position is changed to the first byte after the integer.
	
	6. Select an option and set an offset value to have the system search for the integer from a particular location in the file:
	
	   • **Use this offset**: Enter a value that represents the number of bytes from the Reference Point that the system should read the integer value to the variable from. Negative values go left from the Reference Point.
	   • **Use the offset in this variable**: Select the value contained in a pre-defined variable to set the length of the byte range from the current position, where the system is to search for the integer value to be saved in the variable.
	7. Click **Save**.

ivanti

Option	Description

Change Current Position	Move the current position used in previous steps:
	
	1. Select **Add** > **Change Current Position**. The Change Current Position dialog opens.
	2. From the **Reference Point** drop-down, select the point to where the pointer is to be moved:
	
	   • **The beginning of the file**: Search starts from the beginning of the file (Byte 0).
	   • **The current file position**: Search starts at the current position of the Reference Point.
	   • **The end of the file**: Search starts after the last byte in the file. If this Reference Point is selected, you must use a negative offset.
	
	Note: If the current position can be moved in the manner indicated in this step, it is changed and the step succeeds. If not, for example if the pointer is at the beginning of the file and the position changes to 5 bytes to the left, the step fails and the file is determined not to be of the custom file type.
	
	3. Select an option and set an offset value:
	
	   • **Use this offset**: Enter a value that represents the number of bytes from the Reference Point, where the pointer should be moved to. Negative values go left from the Reference Point.
	   • **Use the offset in this variable**: Select a variable containing an integer value that represents the number of bytes from the Reference Point, where the pointer should be moved to.
	4. Click **Save**.

End of File	Check if the current position is the end of the file: 1. Select **Add** > **Check End of File**.The Check End of File dialog opens. No settings are required. 2. Click **Save**. This step succeeds if the current pointer position is the end of the file. This step does not change the current position. If the current position is not the end of the file when this step is performed, the file is determined not to be of the custom file type and no further steps are performed.

6. After you have finished adding the custom file type steps, click **Save** in the *New Custom File Type* dialog.

Result: The new custom file type is added and appears:

- Within the *Custom File Types* list of the *Manage Custom File Types* dialog.
- Under the **Custom** node in the *File Type Filtering* dialog when configuring permissions.

After Completing This Task:
Now you can:

- Use the newly created custom file type by navigating to the file filtering dialog, expanding the **Custom** section, and selecting the custom file type they created, then selecting **Import / Export** within the permission.
- Edit the custom file type filter by selecting it in the Manage Custom File Types dialog and clicking **Edit**.
- Remove the custom file type filter by selecting it in the Manage Custom File Types dialog and clicking **Remove**.

Editing a Custom File Type Filter
You can edit the configuration of an existing custom file type filter to improve its efficiency and assure the consistent limiting of access to specific file types.

1. In the *Control Panel* pane under the *Modules* section, select **Device Explorer**.

2. In the navigation bar, select **Explorer** > **Manage Custom File Types**.

   Step Result: The *Manage Custom File Types* dialog opens.

3. In the Custom File Type list, select the filter you want to edit.

4. Click **Edit**.

   Step Result: The **Edit Custom File Type** dialog is displayed.

5. In the **Steps** list, select a step tha requires updating and click **Edit**.
   You can remove a step that is no longer required by selecting it and clicking **Remove**.

6. After you have finished editing the custom file type steps, click **Save**.

Result: The custom file type filter is updated with your edits.

Removing a Custom File Type Filter
You can remove selected custom file type filters from the available list.

1. In the *Control Panel* pane under the *Modules* section, select **Device Explorer**.

2. In the navigation bar, select **Explorer** > **Manage Custom File Types** >.

   Step Result: The *Manage Custom File Types* dialog opens.

3. In the Custom File Type list, select the filter you want to remove.

ivanti

4. Click **Remove**.

> **Step Result:** The selected filter is removed from the list.

Result: The custom file type filter is removed from the system.

Assign Permissions by Devices

You can assign permission rules for users to access devices and device classes with any computer the user selects.

Permission rules can be assigned in the *Device Explorer* to the:

- Root node of the **Default settings** hierarchy.
- Device class node of the **Default settings** hierarchy.
- Device group within a device class node shown in the **Default settings** hierarchy.
- Device by make and/or model.
- Device by unique serial number.

> **Note:** Root node permissions are assigned to the root of the *Device Explorer* hierarchy and apply to all devices for specific users or user groups.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. Right-click a node from the **Default settings** division of the *Device Explorer* hierarchical structure.

3. Select **Add/Modify Permissions** from the right-mouse menu.

> **Step Result:** The *Permissions* dialog opens.

4. Click **Add**.

> **Step Result:** The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse**.

6. Select a user or user group.

7. Click **OK**.

8. In the *Permissions* dialog, select the user or user group to assign user access permission rules.

9. Select the permission options.

> **Important:** Only the permissions options available for the device or device class selected are shown.

10. To limit user access to certain file types, click **Filter**.

> **Restriction:** File filtering is available only for the **Removable Storage Devices**, **Floppy Disk Drives**, **Portable Devices** and **CD/DVD Drives** device classes.

Step Result: The *File Type Filtering* dialog opens.
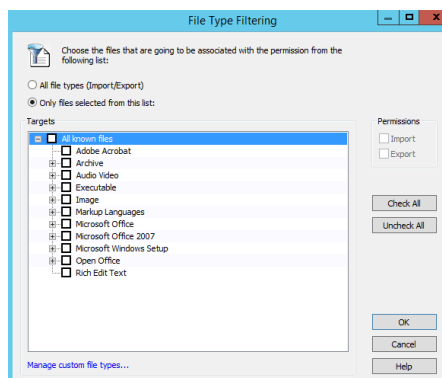
Figure 23: File Type Filtering Dialog

11. Select one of the following options:

Option	Description
All file types (Import/ Export)	Permission rules apply to all file types that are imported and exported by the user or user group for the specified device or device class.
Only files selected from this list:	Permission rules apply to only to selected file types that are imported and/or exported by the user or user group for the specified device or device class.

A complete list of the file filter types supported by Device Control is shown in the *Targets* panel. Select file types using the check boxes adjacent to the file type name. You can also select **Manage custom file types...** to add, edit or remove custom file types.

12. In the *Permissions* panel, select one or both of the following options:

Option	Description
Export	Allows a user to copy files from the Ivanti Device and Application Control client computer to an external device.
Import	Allows a user to copy files from an external device to the Ivanti Device and Application Control client computer.

> **Important:** You must select **Import** or **Export** at a minimum, to enforce file filtering rules.

ivanti

13. Click **OK**.

14. In the *Permissions* dialog, click **OK**.

Result: The **Permissions**, **Priority**, and **Filters** you assign to the device or device class are shown in the *Device Explorer* hierarchical structure.

After Completing This Task:

You should send new or updated permissions immediately to Ivanti Device and Application Control client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients immediately, they automatically receive updates when they restart or at next user log in.

Assign Permission by Computers

You can assign computer-specific permission rules for users to access devices and device classes.

Permission rules can be assigned in the *Device Explorer* to the:

- Group settings node for a computer group shown in the **Machine-specific settings** hierarchy.
- Computer that is a member of an existing domain or workgroup shown in the **Machine-specific settings** hierarchy.

1. In the Management Console select **View** > **Modules** > **Device Explorer** .

2. Select a computer or computer group from the **Machine-specific settings** division of the *Device Explorer* hierarchical structure.

   Step Result: A list of device classes and devices is shown in the *Device Explorer* hierarchical structure.

3. Select **Add/Modify Permissions** from the right-mouse menu.

   Step Result: The *Permissions* dialog opens.

4. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse**.

6. Select a user or user group.

7. In the *Permissions* dialog, select the user or user group to assign user access permission rules.

8. Select the permission options.

   Important: Only the permissions options available for the device or device class selected are shown.

9. Click **OK**.

Result: The **Permissions**, **Priority**, and **Filters** you assign to the device or device class are shown in the *Device Explorer* hierarchical structure.

Manage Online Permission

You can define online user access permission rules that govern wireless device use when the client is connected to the Application Server.

An *online* state exists when a device is attached to client computer that is under the control of a network server, or is connected to the Application Server.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** division of the *Device Explorer* hierarchical structure, right-click a device or device class.

3. Select **Online Permissions** from the right-mouse menu.

4. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse** to select a user or user group.

6. Select the user or user group and click **Next**.

7. Select from the listed user access options.

   Restriction: Only user access options for the device class selected are shown.

8. Click **OK**.

Result: The network-connected user group permission rules are shown in the **Details** column of the *Device Explorer* hierarchical structure.

Manage Offline Permissions

You can define offline user access permission rules that govern wireless device use when the client is disconnected from the Application Server.

An offline state exists when a device is attached to a client computer that is not under the control of your network server, or is not connected to the Application Server. Occasionally, a user may need to modify a device permissions when the user is not connected to the network and needs to access a file stored on a removable storage device.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** division of the *Device Explorer* hierarchical structure, right-click a device or device class.

3. Select **Offline Permissions** from the right-mouse menu.

4. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse** to select a user or user group.

6. Select the user or user group and click **Next**.

ivanti

7. Select from the listed user access options.

> **Restriction:** Only user access options for the device class selected are shown.

8. Click **OK**.

Result: The non-network connected user group permission rules are shown in the **Details** column of the *Device Explorer* hierarchical structure.

Assign Scheduled Permissions to Users
You can schedule user access permissions rules to limit the use of devices to hourly and daily periods of the week.

You can assign global or computer-specific scheduled device permissions for users and user groups.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** division of the *Device Explorer* hierarchical structure, right-click a device or device class.

3. Select **Add Schedule** from the right-mouse menu.

> **Step Result:** The *Choose User on Default Settings* dialog opens, per selected device.

4. Click **Add**.

> **Step Result:** The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse** to select a user or user group.

6. Select a user or user group and click **OK**.

> **Step Result:** The *Choose User on Default Settings* (per selected device) dialog opens.

7. Select the user or user group and click **Next**.

8. Select from the listed user access options.

> **Restriction:** Only user access options for the device class selected are shown.

9. Click **Next**.

> **Step Result:** The *Choose Timeframe* dialog opens.

10. Specify hourly time ranges using the **To** and **From** field dropdown lists.

11. Select one or more weekdays from the **Weekdays** panel.

12. Click **Next**.

13. Click **Finish**.

Result: The scheduled permission access rule appears in the **Details** column of the *Device Explorer* window.

Assign Temporary Permissions to Users
You can assign time-limited, once-per-occurrence permission rules on a computer-specific basis for user access to a device.

An administrator can allow access to a device for a limited period without having to subsequently delete the permission. This provides some reduction in administrative burden.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. From the **Machine-specific settings** division of the *Device Explorer* hierarchical structure, select computer or computer group.

3. Right-click a device or device class.

4. Select **Add Temporary Permissions** from the right-mouse menu.

   Step Result: The *Choose User on* (per selected device) dialog opens.

5. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

6. Click **Search** or **Browse** to select a user or user group.

7. Select a user or user group and click **OK**.

   Step Result: The *Choose Permission* dialog opens.

8. Click **Next**.

9. Select the **Read** and/or **Write** permissions that you want to apply.

10. Click **Next**.

    Step Result: The *Choose Period* dialog opens.

11. Select one of the following options:

Options	Action
Immediately	Permission rules apply immediately (within 5 minutes).
From	Permission rules apply for the period you specify.

12. Click **Next**.

13. Click **Finish**.

Result: The temporary permission access rules appear in the **Details** column of the *Device Explorer* window.

ivanti

Permission Priority Precedence
Permission for users to access removable storage media is assigned by rules defined in both the **Device Explorer** and **Media Authorizer** modules.

When rules are defined in both *Device Explorer* and *Media Authorizer* modules, the permission priority precedence is established as follows:

1. When default user permissions are not defined in the **Device Explorer**, user or user group access defined in the **Media Authorizer** takes precedence.
2. When **Read** or **Write** access is not defined for a user or user group in the **Device Explorer** module, this rule takes precedence over any other permission rule definitions.
3. User group permissions defined in the **Media Authorizer** are additive; a user can access removable storage media for all assigned member user groups.
4. A **Media Authorizer** permission can only be overridden by a **Temporary Permission Offline**.

Permission Priority Order
When a user is in multiple groups or has a specific permission set applied, conflicts are resolved using a defined priority order.

Permission priority is set in this order (highest priority first):

1. Temporary Offline Permission
2. Media Authorizer Permission (more information on Media Authorizer in)
3. Normal/Online/Offline Permission

   a. High None
   b. High Positive
   c. Low None
   d. Low Positive
4. Temporary Permission
5. Scheduled Permission

Add Shadowing

An administrator can establish visibility for the file content read from and written to devices connected to clients. This type of visibility is referred to as file shadowing.

File shadowing can be applied to the following device classes:

- **COM/Serial Ports**
- **DVD/CD Drives**

> **Note:** When burning to a CD/DVD/BD, files burned only during a single/first session are shadowed.

- **LPT/Parallel Ports**
- **Floppy Disk Drives**
- **Printers**

> **Note:**
> - You can only assign shadowing to the main printer class under default settings or to a special PC under Machine-specific settings.
> - Only print jobs sent to printers that use the Microsoft Windows Print Spooler service are shadowed.

- **Removable Storage Devices**

You can also apply file shadowing to:

- Device groups
- Computer-specific devices or device model types

1. In the Management Console select **View** > **Modules** > **Device Explorer**.
2. From the **Default settings** division of the **Device Explorer** hierarchy, right-click a device, device class, or device type.
3. Select **Add Shadow** from the right-mouse menu.
4. Click **Add**.

   Step Result: The **Select Group, User, Local Group, Local User** dialog opens.

5. Select the user or user group and click **Next**.

Step Result: The *Choose Bus* dialog opens.
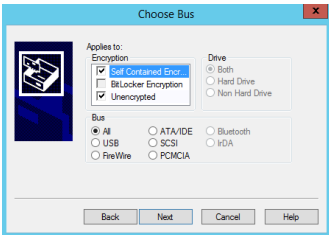
Figure 24: Choose Bus Dialog

6. Select **All** or individual bus types.

Important: The available bus types shown are dependent upon the device class you select. The *Encryption* panel is only active, with all options selected by default, for the **Removable Storage Devices** and **DVD/CD Drives** device classes.

7. Select a **Drive** option.

8. Click **Next**.

Step Result: The *Choose Permissions* dialog opens.
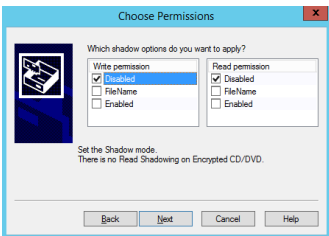
Figure 25: Choose Permission Dialog

9. In the *Read* and/or *Write* panels, choose one of the following options:

Option	Description
Disabled	File content copying is not active.
FileName	File content copying is not active; only the file name for a file copied to or from a device is saved in the Ivanti Device and Application Control database.

Option	Description
Enabled	File content copying is active.

Restriction: Only the *Write* panel is active for the **COM/Serial Ports**, **LPT/Parallel Ports** and **Printers** device classes.

10. Click **Next**.

11. From the *Finish* dialog, click **Finish**.

Result: The shadow rule permission details are shown in the **Permissions** column of the *Device Explorer* hierarchical structure. The shadow permission details are displayed in the *Permissions* column of the *Device Explorer* module. A value of **R** means that shadowing is enabled for files read to and from the device, **W** means that it is on when files are written to and from the device; no letter means that shadowing is enabled for both reading and writing files. You can review shadowed files using the *Log Explorer* module.

Manage Shadowing
You can modify and remove shadow rules for users and user groups.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** node of the *Device Explorer* hierarchical structure, right-click an existing user or user group **Shadow** entry listed under a device, device class, or device type.

3. From the right-mouse menu, select one of the following options:

Option	Description
Modify Shadow	Modifies an existing shadow rule for a user or user group.
Remove Shadow	Deletes shadow rule for the selected user or user group.

Result: The shadow rule permission changes are shown in the **Permissions** column of the *Device Explorer* hierarchical structure.

ivanti

Behaviors Specific to Shadowing Files Burned to CD/DVD/BD

Unique behaviors are exhibited by the system when gathering shadowing data for files burned to CD/DVD/BD.

- File shadowing is not supported when burning in RAW mode and writing will be blocked.
- "Volume Label" column in Log Explorer will not contain a value when a disc is burned using Windows Explorer (Mastering or Live File System).
- No file name information is provided about the files burned during a second disc or subsequent sessions for a multi-session disc when using Windows Mastering or third-party burning software.
- Information contained in the `cd-or-dvd-analysis.log`, for example Write Type and Data Block Format, is incorrect when burning media other than a CD.
- The shadow file generated during a disc format using Live File System will contain all the writes performed during the process. The size of the file is typically 2500KiB, but can be 4GB (DVD-RAM) or 47GB (BD-RE). The file size can match the disc capacity.
- After a successful disc burning using Windows Explorer (Mastering or Live File system), shadowed file information is sent to the server with two additional files: `CD-or-DVD-analysis-log.txt` and `CD-or-DVD-error-log.txt`.

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.

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	1. Open a command prompt. 2. Enter: `copy <filename.prn> /B \\<printer-server> \<printer-share-name>`
	Note: • `<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 `PRN` file format is printer dependent.

Option	Description
Opening a shadowed print file using a utility for viewing print spooler files in formats appropriate for your printer.	As the `PRN` 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 `PRN` file extension.

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

Add Copy Limit

You can create permission rules for users and user groups that limit the amount of data that can be copied to a device on a daily basis. These are copy limit rules.

When a user reaches the copy limit, they cannot copy, move, or replace files on a device.

Restriction: You can only define copy limits for the **Floppy Disk Drive** and **Removable Storage Devices** device classes.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.
2. In the **Default settings** or **Machine-specific settings** division of the *Device Explorer* hierarchical structure, right-click a device class.
3. Select **Copy Limit** from the right-mouse menu.
4. Click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse** to select a user or user group.
6. Select the user or user group and click **Next**.
7. In the *Choose Permission* dialog, enter a value in the **Assign Copy Limit** field.

   The value entered represents data in megabytes (MB). The default setting of zero (0) represents an unlimited copy limit value. The user daily copied data total automatically resets to zero at midnight, locally.

8. Click **Next**.
9. From the *Finish* dialog, click **Finish**.

Result: The copy limit rule permission details are shown in the **Details** and **Permissions** columns of the *Device Explorer* hierarchical structure.

Remove Copy Limit

You can remove copy limit rules established for a device.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

ivanti

2. In the **Default settings** or **Machine-specific settings** node of the *Device Explorer* hierarchical structure, right-click an existing user or user group **Copy Limit** entry listed under a device, device class, or device type.

3. Select **Remove Copy Limit** from the right-mouse menu.

Result: The copy limit rule permission changes are removed from the **Details** and **Permissions** columns of the *Device Explorer* hierarchical structure.

Add Event Notification
You can create an event notification permission rule that shows a customized message to a user who attempts to access an unauthorized device through a client computer.

Event notification rules can be created at the following levels in the *Device Explorer* hierarchical structure:

- **Default settings** root node
- **Default settings** device class node
- Specific device node
- Device group node
- **Machine-specific settings** computer node

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** or **Machine-specific settings** division of the *Device Explorer* hierarchical structure, right-click a device class.

3. Select **Add Event Notification** from the right-mouse menu.

4. Click **Add**.

 Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

5. Click **Search** or **Browse** to select a user or user group.

6. Select the user or user group and click **OK**.

7. Click **Next**.

 Step Result: The *Choose Event Notification settings* dialog opens.
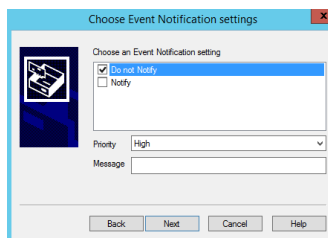
Figure 26: Choose Event Notification Settings Dialog

8. From the **Choose an Event Notification setting** panel, select one of the following options:

Option	Description
Do not Notify	No message is sent when a user attempts to access an unauthorized device.
Notify	A message is sent to the user when attempting to access an unauthorized device.

9. From the **Priority** dropdown list, select one of the following options:
   - **High**
   - **Medium High**
   - **Medium**
   - **Low**
   - **Lowest**

10. In the **Message** field, type a message the user receives when notified of an event.

11. Click **Next**.

12. From the *Finish* dialog, click **Finish**.

Result: The event notification rule permission details are shown in the **Details**, **Priority**, and **Permissions** columns of the *Device Explorer* hierarchical structure.

Manage Event Notification
You can modify and remove event notification rules for users and user groups.

1. In the Management Console select **View** > **Modules** > **Device Explorer**.

2. In the **Default settings** or **Machine-specific settings** node of the *Device Explorer* hierarchical structure, right-click an existing user or user group **Event Notification** entry listed under a device, device class, or device type.

3. From the right-mouse menu, select one of the following options:

Option	Description
Modify Event Notification	Modifies an existing event notification rule for a user or user group.
Remove Notification	Deletes event notification rule for the selected user or user group.

Result: The event notification rule permission changes are shown in the **Permissions**, **Priority**, and **Details** columns of the *Device Explorer* hierarchical structure.

ivanti

Creating a Data Loss Prevention (DLP) Filter
You can define a filter string that can be used against the contents of all MS Office and PDF documents to block or shadow the files.

Prerequisites:

The Windows Search Service must be configured for PDF and MS Office files types you want to search within.

1. Select **Tools** > **Default Options**

2. Select the **Computer** tab.

3. Select **DLP filter** from the option list.

4. Clear **Not configured**.

5. In the **DLP filter** field, enter a filter string that meets AQS requirements.

6. Click **OK**.

Result: A global Data Loss Prevention filter is created.

After Completing This Task:
Now you can assign the filter to users and groups.

Assigning a Data Loss Prevention Filter to a Specific User or Group
You can assign a data loss prevention filer to a specific user or group through a device's Permission dialog.

Prerequisites:

- The Windows Search Service must be configured for the PDF and MS Office files types you want to search within.
- You have created a global Data Loss Prevention filter.

1. In the Modules section, select **Device Explorer**.

2. Right-click a device type and select **Add/Modify Permissions**.

3. Select an existing or define a new permissions.

4. Click **DLP**. The Data Loss Prevention dialog opens.

5. Choose the files to associate with the permission.

6. Click **OK**.

Result: The Data Loss Prevention filter is assigned to the selected user or group. Each time a file containing the filter string is accessed a WRITE-DENIED event is created.

File Type Filtering and Data Loss Prevention Combination Matrix
Learn the behaviors to expect when using different types of File Type Filtering and Data Loss
Prevention permission combinations.

Table 28:

Access Rights	FTF Settings Dialog		DLP Settings Dialog		Behavior		
	FileType1	FileType2	FileType1	FileType2	Operation on FileType1	Operation on FileType2	Operation on other types
R/W	unchecked	unchecked	unchecked	unchecked	yes	yes	yes
R/W	checked	unchecked	unchecked	unchecked	yes	no	no
R/W	unchecked	checked	unchecked	unchecked	no	yes	no
R/W	checked	checked	checked	unchecked	yes	yes	no
R/W	unchecked	unchecked	checked	unchecked	DLP	no	no
R/W	checked	unchecked	checked	unchecked	DLP	no	no
R/W	unchecked	checked	checked	unchecked	DLP	yes	no
R/W	checked	checked	checked	unchecked	DLP	yes	no
R/W	unchecked	unchecked	unchecked	checked	no	DLP	no
R/W	checked	unchecked	unchecked	checked	yes	DLP	no
R/W	unchecked	checked	unchecked	checked	no	DLP	no
R/W	checked	checked	unchecked	checked	yes	DLP	no
R/W	unchecked	unchecked	checked	checked	DLP	DLP	no
R/W	checked	unchecked	checked	checked	DLP	DLP	no
R/W	unchecked	checked	checked	checked	DLP	DLP	no
R/W	checked	checked	checked	checked	DLP	DLP	no

ivanti

Working with Media Authorizer

The Device Control **Media Authorizer** module provides administrators the ability to encrypt non-bootable hard disk or flash removable storage media, and authorize user access to the encrypted media. Removable storage media are defined for Device Control as any device recognized by the Windows *removable storage devices* class through the *plug-and-play* feature.

With the **Media Authorizer** you can:

- Add CD/DVD media to the database.
- Authorize user access to individually specified CD/DVD media in the network environment.
- Perform centralized data encryption for removable storage media.
- Perform centralized data encryption for removable storage media used when computers and users are connected to your network environment.
- Rename CD/DVD disk media that has been added to the database.
- Authorize user access to encrypted removable storage media in the network environment.
- Export encryption keys to provide access to encrypted media used outside your network environment.

The Media Authorizer Window

The **Media Authorizer** window provides primary administrative access for adding CD/DVDs and encrypted removable storage devices to the database, as well as, authorizing specific user access to the devices.

The **Media Authorizer** window consists of the following components:

- **Users by Medium** tab
- **Media by User** tab

User by Medium Tab

You use the *User by Medium* tab to add and remove storage devices from the database, as well as, assign user access to removable storage media.

You encrypt removable storage media when you use the Media Authorizer to add the devices to the database. The *User by Medium* tab consists of two panels:

- *Media*
- *Associated Users*
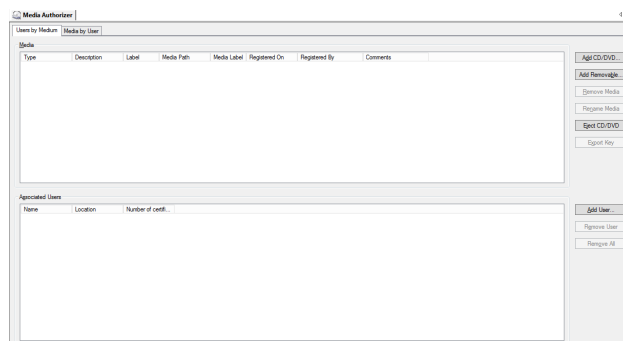
Figure 27: Users by Medium Tab

The following tables describe the columns in the *Media* and *Associated Users* panel.

Table 29: Media Panel Columns

Column	Description
Description	Shows the name for the removable storage medium.
Label	Shows the user-defined medium label.
Media Path	Shows the full path name used for encrypting the medium.
Media Label	Shows the media label shown in the medium Windows properties dialog.

Table 30: Associated Users Panel Columns

Column	Description
Name	Shows the name of the user assigned access to the selected removable storage medium.
Location	Shows the computer location for the assigned user.

ivanti

Assign User Access to Media

You can authorize specific user access to removable storage media and CD/DVDs.

Prerequisites:

You must complete one of the following tasks before you can assign access to media:

- Encrypt removable media.
- Add CD/DVD media to the database.

You can assign specify user access for the encrypted removable storage medium that you select as follows.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

2. Select one of the following options:

Option	Description
Add CD/DVD	Adds the designated CD/DVD to the database.
Add Removable	Adds the designated removable storage medium to the database.

3. In the **Media** panel, select one of the following options from the **Type** column:

    - **CD/DVD**
    - **Removable storage medium**

4. Click **Add User**.

5. From the **Select Group, User, Local Group, Local User** dialog, click **Search** or **Browse**.

6. Select user(s) from the list shown.

   Restriction: You can only assign users, not groups, to encrypted removable storage media.

7. Click **OK**.

Result: The selected user(s) is assigned access to the encrypted removable storage medium that you specified.

Remove User Access to Media

You can remove specific user access to encrypted removable storage media and CD/DVDs.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

2. In the **Media** panel, select one of the following options from the **Type** column:

    - **CD/DVD**
    - **Removable storage medium**

3. In the ***Associated User*** panel, select the user(s).

4. Click **Remove User**.

Result: The user(s) are removed from the ***Associated Users*** list and cannot access the specified encrypted removable storage media.

Export Encryption Key

A Ivanti Device and Application Control administrator can export the media encryption key to the removable storage medium or a designated file, when removable storage devices must be exchanged between users in different organizations.

Prerequisites:

You must manually unlock the key with the associated password, before you can export the media key.

You can export the media encryption key to the removable storage device or a file, which can be transmitted separately to a device user.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

2. Click **Export Key**.

3. Choose one of the following options:

Option	Description
Medium	Exports the encryption key to the removable storage medium.
Folder	Exports the encryption key to a file in a folder you specify.

4. In the **Password** field, type a new password.

5. In the **Confirm** field, retype the new password.

6. Click **OK**.

Result: The encryption key is exported to medium or file that you designated.

Eject CD/DVD

You can eject a CD/DVD from your computer through the Management Console.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

2. Click **Eject CD/DVD**.

Result: The CD/DVD is ejected from the computer immediately.

ivanti

Media by User Tab

You can use the *Media by User* tab to assign individual user access to encrypted removable storage media.

The *Media by User* tab consists of two panels:

- *Users*
- *Media*
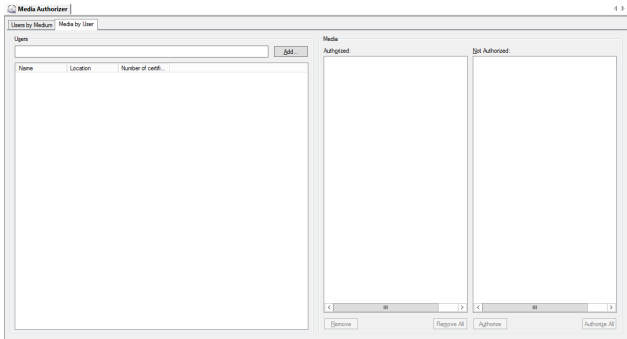
Figure 28: Media by User Tab

The following tables describe the columns in the *Media* and *Users* panels.

Table 31: Users Panel Columns

Column	Description
Name	Shows the name of the user assigned access to the selected removable storage medium.
Location	Shows the computer location for the assigned user.

Table 32: Media Panel Columns

Column	Description
Not Authorized	List of removable storage media that are not authorized for the user selected.
Authorized	List of removable storage media that are authorized for the user selected.

Assign Media to Users

You can assign users to CD/DVDs and encrypted removable storage media that are contained in the Ivanti Device and Application Control database.

You can authorize access for specific users to use CDs/DVDs and encrypted removable storage devices after added the devices to the database, as follows:

- Grant permissions to use specific CD/DVDs for users who do not usually have access to the CD/DVDdrive.
- Allow specific users to access encrypted media.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Media by User** tab.

2. Click **Add**.

   Step Result: The ***Select Group, User, Local Group, Local User*** dialog opens.

3. Click **Search** or **Browse**.

4. Select user(s) from the list shown.

   Restriction: You can only assign users, not groups, to encrypted removable storage media.

5. In the ***Media*** panel, select the media from the **Not Authorized** list.

6. Click **Authorize**.

Result: Access to the specified media is authorized for the user you selected.

Remove Media from Users

You can remove user access to CD/DVD and encrypted storage media contained in the Ivanti Device and Application Control database.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Media by User** tab.

2. In the ***Media*** panel, select one of the following options:

Option	Action
Remove a CD/DVD.	Select the DVD/CD from the **Authorized** list.
Remove an encrypted removable storage medium.	Attach the medium to the Ivanti Device and Application Control administrator computer and select the medium from the **Authorized** list.
Remove lost or damaged encrypted removable storage medium.	Select the medium from the **Authorized** list.

ivanti

3. Click **Remove Media**.

Result: Active user access authorization for the selected encrypted removable storage media is removed from the Ivanti Device and Application Control database.

Rename Removable Media
You can rename removable storage media.

1. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Media by User** tab.

2. In the *Media* panel, select one of the following options from the **Type** column:

- **CD/DVD**
- **Removable storage medium**

3. Click **Rename Media**.

   Step Result: The *Rename Item* dialog opens.

4. Type a new name in the **Please enter the new description for this item** field.

   Tip: Click **Get Device Label** to recover this information directly from the medium.

5. Type a new label (up to 11 alphanumeric characters) in the **Please enter the new label for this item** field.

6. Click **OK**.

Result: The new medium name is listed in the *Media* panel.

Encrypting Removable Media

Device Control uses encryption to control the use of removable storage media. After a user is assigned authorized access to the encrypted removable storage media, the client provides transparent data encryption and decryption.

Encryption provides:

- Tamper-proof media identification by associating the device identifier with the device encryption key.
- Prohibited access to data stored on media when the media is used on a computer that does not run Device Control.

Ivanti Device and Application Control uses the Advanced Encryption Technology (AES) encryption algorithm to cipher the media with 32 byte (256 bit) encryption keys. The encryption process employs the Microsoft Certification Authority® for the Active Directory domain to deliver the encryption keys to users.

Encrypt Removable Media
An administrator must add removable storage media to the database before encryption takes place. During encryption a unique cryptographic identifier is written to the device, which is then encrypted.

Prerequisites:

For encryption to work successfully, the following conditions must be met:

- Use Microsoft Windows Active Directory domains for:

  - Microsoft Windows 2003®R2
  - Microsoft Windows 2008®
  - Microsoft Windows Server 2012®R2

- The administrator must have administrative rights for the computer where encryption takes place.
- A Microsoft Certification Authority® is available and published.
- A Ivanti Device and Application Control client is installed on the same computer as the Management Console where encryption takes place.
- Attach the removable storage media to the client computer and use the **Device Explorer** to add the device to the database.

During encryption, a unique cryptographic identifier is written to the device that encrypts the device.

1. Connect the medium to the computer being used for encryption.

2. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

3. Click **Add Removable**.

   Step Result: The **Add Removable Media** dialog opens.

4. From the **Drive** drop-down list, select the letter corresponding to the drive you are encrypting.

5. In the **Description** field, enter a free text description.

6. In the **Label** field, enter a label (maximum 11 alphanumeric characters) that will be used after the medium is formatted.

ivanti

7. From the **Encryption** drop-down list, select one of the following options:

Encryption Method	Description
Full & Slow (secure for existing data)	• Encrypts the media and preserves any existing data stored on the device. • Encryption is applied to all free sectors of the media. • All data is encrypted. • Requires using the Stand-Alone Decryption tool (SADEC) for access to the media from non-Ivanti Device and Application Control computers. This method is the most secure for encryption and can be very slow.
Quick Format (insecure for existing data)	• Encrypts the media and removes all existing stored data. • All data stored on the device is erased. • Requires using the Stand-Alone Decryption tool (SADEC) for access to the media from non-Ivanti Device and Application Control computers. This quick encryption method is not recommended for media containing sensitive data.
Easy Exchange (insecure for existing data)	• Encrypts the media quickly and removes all existing stored data. • Allows access to the media from non-Ivanti Device and Application Control computers. The encryption is done in a single file or multiple files (depending on removable media capacity) using a FAT structure. **Tip:** When you encrypt media using the client (decentralized encryption) you may opt to retain existing data during encryption.

8. Click **OK**.

Result: The removable storage medium is encrypted and added to the database.

Add CD/DVD Media
An administrator can add CD/DVD media to the database.

Prerequisites:

To successfully add CD/DVD media to the database, the following conditions must be met:

- The administrator have **Read** or **Read/Write** permission assigned as using the ***Device Explorer*** module.
- A client is installed on the same computer as the Management Console where user access is authorized.

1. In the Management Console select **View** > **Modules** > **Media Authorizer**.

2. Click **Add CD/DVD**.

   Step Result: You are prompted to insert a CD/DVD.

3. Insert the CD/DVD.

   Step Result: The ***Media Authorizer*** calculates a unique cryptographic signature and displays the ***Media Name*** dialog.

4. Click **OK**.

Result: The **Media Name** label is used to register the CD/DVD in the database.

Encrypt Removable Media without Certificate Authority
You can encrypt removable storage media without a Microsoft Certification Authority®.

Prerequisites:

For encryption to work successfully, the following conditions must be met:

- Use Microsoft Windows Active Directory domains for:

  - Microsoft Windows 2003®R2
  - Microsoft Windows 2008®
  - Microsoft Windows Server 2012®R2

- The administrator must have administrative rights for the computer where encryption takes place.
- A Ivanti Device and Application Control client is installed on the same computer as the Management Console where encryption takes place.
- Attach the removable storage media to the client computer and use the ***Device Explorer*** to add the device to the database. See Manage Devices for additional information about adding removable storage media to the database.
- Close all applications that are accessible to the removable storage medium.

During encryption, a unique cryptographic identifier is written to the device that encrypts the device.

ivanti

1. In the Management Console select **View** > **Modules** > **Device Explorer** > **Add/Modify Permissions**.

   Step Result: The *Permissions* dialog opens.

2. In the *Permissions* dialog, select the following options:
   - **Encrypt** - A user or user group can encrypt devices.
   - **Export to media** - The passphrases or public keys from user certificates are used to create the symmetric key used to encrypt a device can be exported to the encrypted device when the **Self Contained Encryption** option is selected.

3. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

4. Click **Add Removable**.

   Step Result: The *Add Removable Media* dialog opens.

5. From the **Drive** drop-down list, select the letter corresponding to the drive you are encrypting.

6. In the **Description** field, enter a free text description.

7. In the **Label** field, enter a label (maximum 11 alphanumeric characters) that will be used after the medium is formatted.

8. From the **Encryption** drop-down list, select one of the following options:

Encryption Method	Description
Full & Slow (secure for existing data)	• Encrypts the media and preserves any existing data stored on the device. • Encryption is applied to all free sectors of the media. • All data is encrypted. • Requires using the Stand-Alone Decryption tool (SADEC) for access to the media from non-Ivanti Device and Application Control computers. This method is the most secure for encryption and can be very slow.
Quick Format (insecure for existing data)	• Encrypts the media and removes all existing stored data. • All data stored on the device is erased. • Requires using the Stand-Alone Decryption tool (SADEC) for access to the media from non-Ivanti Device and Application Control computers. This quick encryption method is not recommended for media containing sensitive data.
Easy Exchange (insecure for existing data)	• Encrypts the media quickly and removes all existing stored data. • Allows access to the media from non-Ivanti Device and Application Control computers. The encryption is done in a single file or multiple files (depending on removable media capacity) using a FAT structure.
	Tip: When you encrypt media using the client (decentralized encryption) you may opt to retain existing data during encryption.

9. Click **OK**.

    Step Result: The removable storage medium is encrypted, added to the database, and the encryption key is exported to the removable storage medium.

10. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

11. Click **Remove Media**.

    Step Result: A dialog opens prompting you to confirm deletion of the medium from the database.

12. Click **Yes**.

ivanti

13. In the Management Console select **View** > **Modules** > **Device Explorer** > **Add/Modify Permissions**.

14. In the *Permissions* dialog, select the following options:

- **Read** - A user or user group has read access.
- **Write** - A user or user group has write access.
- **Import** - The user or user group can import an external encryption key when the **Self Contained Encryption** option is selected.

Result: Users assigned permission to use the removable storage medium can access the medium using the password generated during encryption.

Import Externally Encrypted Removable Media
You can import data from an externally encrypted device.

Prerequisites:

To successfully import data from an externally encrypted device, the following conditions must be met:

- A client is installed on the same computer as the Management Console where import takes place.
- Use Active Directory domains for:

  - Microsoft Windows 2003®R2
  - Microsoft Windows 2008®
  - Microsoft Windows Server 2012®R2

- The administrator has administrative rights for the computer used to import the encrypted media.
- The user must be assigned permission to access the **Removable Storage Devices** class.
- The user must have the password and encryption key for the encrypted removable media.

1. Connect the medium to the computer used for encryption.

2. In the Management Console select **View** > **Modules** > **Media Authorizer** > **Users by Medium** tab.

3. Click **Add Removable**.

   Step Result: The *Add Removable Media* dialog opens.

4. From the **Encryption** drop-down list, select **Import (secure for existing data)**.

5. In the **Password** field, type the password for the encrypted removable storage medium.

Result: The medium is added to the database and can be viewed in the *Media* panel.

After Completing This Task:

To provide user access to the removable storage medium, you must assign users to access the media.

Working with Log Explorer

Every endpoint protected by Ivanti Device and Application Control generates activity logs for administrator and user-defined client actions.

Log Explorer activity logs that record device connection attempts and denials. In addition, all tasks performed in the Management Console generate audit logs showing actions carried out by administrators, such as changing user access rights and device permissions. The information in these logs is sent to the database and can be viewed through the **Log Explorer** module of the Management Console.

If you have appropriate administrative privileges, you can use the **Log Explorer** module to view logs of user input/output (I/O) device activities including:

- Unsuccessful attempts to access I/O devices from client computers.
- Records showing when devices are connected from a client computer.
- Client errors.
- Files copied by a user to a device connected to a client computer.
- Files read from a device connected to a client computer.

With the **Log Explorer** module you can also:

- Sort, add criteria, define columns, create templates, and organize information.
- Monitor the activities of administrators using audit log information.
- Save the results of querying log entries.
- Generate on-demand or automatic reports containing details of user input or output (I/O) device actions or administrator actions.
- Generate custom reports using templates.

ivanti

The Log Explorer Window

The *Log Explorer* window is the primary mode for administrator interaction with *Log Explorer* module functions.

The *Log Explorer* window consists of the following components:

- Navigation control bar
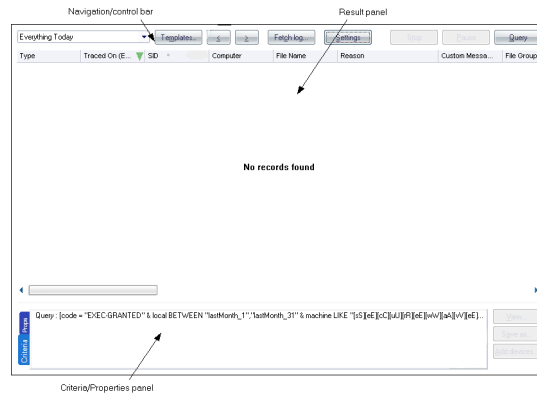- *Results* panel
- *Criteria/Properties* panel

Figure 29: Log Explorer Window

Navigation Control Bar

You can use the navigation control bar to select a template or navigate and control your results.

Figure 30: Navigation/Control Bar

The following table describes the features of the navigation control bar.

Table 33: Log Explorer Navigation Control Bar

Control	Description
Templates	Create a new template or select from your recently used templates list, shown as a drop-down list.
Previous	Allows you to navigate backward to the previous query result list stored internally, when you are performing multiple queries.
Next	Allows you to navigate forward to the query result list stored internally, when you are performing multiple queries.
Query	Retrieves all log entries that match the criteria defined in the current template.

Column Headers

The column headers display the title of the columns.

In addition to displaying column titles, you can use column headers to:

- Sort results to classify the results and display them in a specified order depending on the value for the log entry (or log entries) in one or more columns.
- Show/hide columns to determine what information is displayed for each result in the report.
- Change the size of the displayed columns by dragging the column header dividers to the left or right.
- Change the order in which the columns are displayed by dragging and dropping the column titles in the column headers.
- Group log entries to display a single report row corresponding to multiple log entries grouped according to the values in one column.
- Display computed columns to display calculated values such as a count of the number of log entries in a grouped result, the maximum value, minimum value, sum of values, or average value.
- You can make changes to the columns to display different information from the log entries without re-executing the query.
- You can also use the column context menu to access the advanced query settings for the template.

Note: Any *on-the-fly* changes you make to the column headers are saved in the template that you are currently using.

Show/Hide Columns

You can show or hide selected columns of log entry information.

Prerequisites:

You must select a template that displays query results in the **Log Explorer** window.

ivanti

1. Right-click the column header row to display the field names for the fields displayed in the **Results** panel.

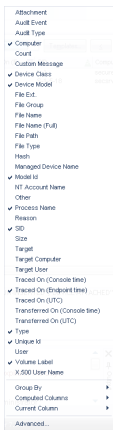   **Step Result:** A right-mouse menu appears showing all the column names.

Figure 31: Columns Right-Mouse Menu

2. Click a field name showing a check mark to hide the column, or a field name without a check mark to show the column.

Result: The names of the columns that you selected are shown or hidden in the **Results** panel.

Group Log Entries

You can group multiple log entries into single report rows according to the values in one or more column log entries.

Prerequisites:

You must select a template that displays query results in the **Log Explorer** window.

1. Right-click the column header row to display the field names for the fields displayed in the ***Results*** panel.

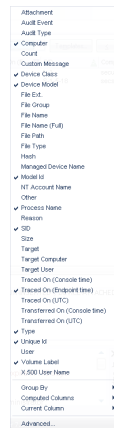   **Step Result:** A right-mouse menu appears showing all the column names.

Figure 32: Columns Right-Mouse Menu

2. Select **Group by** from the menu.

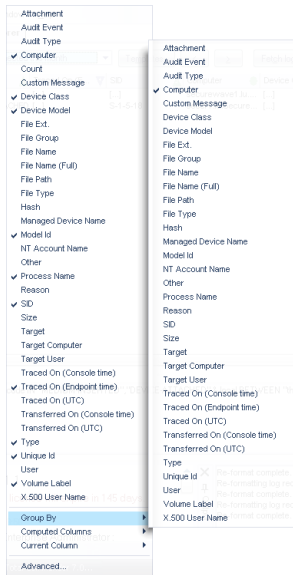**3.** Check the column you want to group your template query results by.

Figure 33: Group By Option

Result: The log report results are grouped by the column you selected. Primary groups are denoted by a green circle shown in the column title when a column is used to group results, as illustrated by the following:
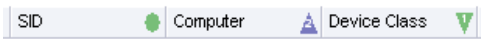
Figure 34: Column Title Primary Group

You can repeat the above procedure to create subgroups. Secondary subgroups are denoted by a blue circle with the number 2 shown in the column title when a column is used to group results, as illustrated by the following:

Figure 35: Column Title Subgroup

Computed Columns
You can include computed columns in your report.

Prerequisites:

You must select a template that displays query results in the *Log Explorer* window.

You can show additional information alongside predefined log entry columns, corresponding to additional information stored in the client activity logs.

1. Right-click the column header row to display the field names for the fields displayed in the **Results** panel.

   Step Result: A right-mouse menu appears showing all the column names.
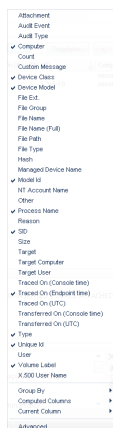
Figure 36: Columns Right-Mouse Menu

2. Select the **Computed Columns** option.

   The operations supported for computed columns are:

Table 34: Computed Columns Operations

Operation	Description
Count	Calculates the number of log entries for a value type, such as **Count (Device Class)** that shows how many log entries contain device information. **Count (Any)** shows the total number of log entries.
Min	Calculates the minimum value in a column for a set of results.
Max	Calculates the maximum value in a column for a set of results.
Sum	Calculates the sum of numerical data for a set of results; valid only for the **File Size** column.
Average	Calculates the numerical average of numerical data for a set of results; valid only for the **File Size** column.

Note: These operations do not apply to all columns.

ivanti

3. Select the type of calculation you want to perform from the ***Computed Columns*** sub menu.

Figure 37: Computed Columns Menu

4. Select the column shown in the ***Results*** panel that contains the data you want to calculate computed values for.

Result: The ***Log Explorer*** window shows the calculated column results.

Clear Columns Settings
You can reset columns to original values by clearing the sort and group filters.

1. Right-click the column header row to display the field names for the fields displayed in the ***Results*** panel.

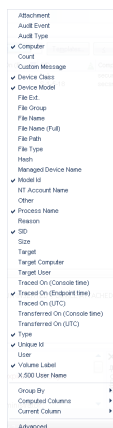> **Step Result:** A right-mouse menu appears showing all the column names.

Figure 38: Columns Right-Mouse Menu
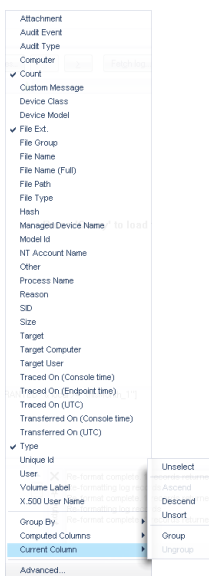
2. Select the **Current Column** option.

Figure 39: Reset Column Groups Headings

ivanti

3. Select **Unsort** or **Ungroup**.

Result: The selected column groupings are reset according to your selection.

Criteria/Properties Panel

The **Criteria/Properties** panel displays the criteria used in the template and the log entry information that corresponds to rows shown in the **Results** panel.

The **Criteria/Properties** panel has two tabs:

- The **Props** tab displays the log entry information corresponding to a selected results row in the **Results** panel. To copy the contents of the tab window to the Windows clipboard, you can select a row displaying log entry results and right-click in the **Props** tab, then select **Copy**.
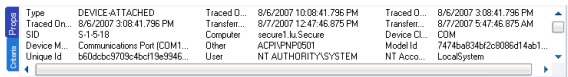
Figure 40: Props Tab

- The **Criteria** tab displays the criteria used in the template to select log entry results shown in the **Results** panel.
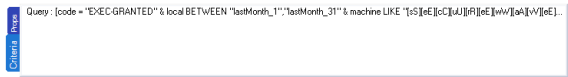
Figure 41: Criteria Tab

Results Panel/Custom Report Contents

The **Results** panel is the area of the **Log Explorer** window which displays and categorizes the template query results.

You can save the template query results as a Comma Separated Value (`*.csv`) file using the Management Console **Save as** command. When you generate scheduled custom reports the results, are sent to designated e-mail recipients or stored in a designated computer directory, rather than displayed in the **Log Explorer Results** panel.

Columns in Results Panel/Custom Report

You can control how column information for log entries is displayed in the **Results** panel from the **Template settings** dialog.

The following table describes the log entry information for columns in the **Results** panel and custom reports.

Note: Ellipses […] in the **Results** panel indicate hidden log entries. For example, if you group a set of results using the value in one column, then multiple values in other columns, the results are shown as […].

Table 35: Log Explorer Columns

Column	Description
Attachment	Shows that shadowed content is viewable.
Audit Event	Shows the type of event that triggered the audit log.
Audit Type	Shows the type of action the administrator performed.
Computer	Shows name of the computer where device access was requested.
Count	Shows how many log entries are hidden in a single row, accompanied by a grouping symbol displayed on the column header. Alternatively, this may be a computed column of data.
Device Class	Shows the name of the device class.
Device Model	Shows the manufacturer name for the device.
File Ext	Shows the type of file extension.
File Name	Shows the file name accessed on the device.
File Name (full)	Shows the full name (including path) of the file accessed on the device.
File Path	Shows the path to the file on the device.
File Type	Indicates whether the file relates to a script or an application, for example **Executable** or **Script**.
Hash	Shows the digital signature of the file, created by SHA-1 (Secure Hash Algorithm -1) that differentiate files with the same name.
Managed Device Name	Shows the device name defined in the Device Explorer module.
Model Id	Shows the device model that a user performed and action on.
NT Account Name	Shows the domain user name of the person who triggered the event, for example `MARVIN/johns` or `LocalSystem`.
Other	Shows information that may contain the access mask, DVD/CD serial number details, additional information, or parameters.

ivanti

Column	Description
Process Name	Describes the process used for device access.
Reason	Indicates whether device access was granted or denied. This can have a value of **No Permission**, **Granted** or **Denied**.
SID	Shows the secondary identifier for the user, for example `S-1-5-21-647365748-5676349349-7385635473-1645`. This is useful for tracing actions recorded in log files to users who have left an organization.
Size	Shows the size of the shadowed file.
Target	Shows the device for which the permissions were modified.
Target Computer	Shows the computer name that was the target of the administrator action.
Target User	Shows of the user or group name that the administrator action was applied to.
Traced On (Console time)	Records the date the event occurred on the console computer.
Traced On (Endpoint time)	Records the date the event occurred on the client computer.
Traced On (UTC)	Records the date (Coordinated Universal Time) the event occurred on the client computer.
Transferred On (Console)	Records the date the event record was transferred from the client computer to the Application Server.
Transferred On (UTC)	Records the date (Coordinated Universal Time) the event record was transferred from the client computer to the Application Server.
Type	Shows the type of event that triggered the log action such as the type of audit event.
Unique ID	Shows the serial number for the device the user performed an action on.
User	Shows the user name that triggered the event. For users removed from the Active Directory, this field also displays the *SID*, enabling identification of users who have left an organization.
Volume Label	Shows the volume tag for the event that is logged.

Column	Description
X.500 User Name	Shows the user name in Lightweight Directory Access Protocol format. This reflects the directory tree in which the user information is stored, for example, the X.500 user name may be `CN=John Doe, CN=Users, DC=Jane` and so forth.

Note: Columns names starting with **Count**, **Min**, **Max**, **Sum** and **Average** may also be displayed. These contain computed data based on the values in the columns specified for **Computed Columns**.

Log Explorer Templates

The operation of the ***Log Explorer*** module is based on templates that allow you to generate custom reports containing results that match specific criteria.

A template is a set of rules used for displaying audit and activity log data in the ***Log Explorer***. You can create your own templates or use predefined ones created by Ivanti.

Note: The list of predefined templates depends upon your license type.

Predefined Templates

Ivanti provides a set of predefined templates used by the ***Log Explorer,*** based on commonly used audit queries.

You can use the following predefined templates:

Table 36: Log Explorer Predefined Templates

Template Name	Shows	Prerequisite
Audit by Administrator 'adm'	All actions performed by a specific administrator.	You must change the `adm` user to an actual administrator in the ***Template Settings*** dialog. The result is classified by user.
Audit for PC xyz	Audit trace for a specific computer.	You must change the `xyz` computer to an actual computer name in the ***Template Settings*** dialog.
Audit for user 'abcd'	Audit trace for a specific user.	You must change the `abcd` user to an actual computer name in the ***Template Settings*** dialog.
Audit today	Daily audit trace.	No action is required.
CD-DVD in use this month	Monthly DVD/CD usage.	You must enable the **Device Log** option.
Copy limit met this week	Weekly copy limit rules that have been met or exceeded.	You must define a **Copy Limit** rule.

ivanti

Template Name	Shows	Prerequisite
Denied device acc. this week	Weekly list of device access denials.	You must enable the **Device Log** option.
Devices connected this month	Monthly list of device connections.	You must enable the **Device Log** option.
Devices denied/user this month	Monthly list of denied device access classified by user.	You must enable the **Device Log** option.
Devices often used this month	Monthly list of devices used most often.	You must enable the **Device Log** option.
Everything today	Everything that happened today.	No action is required.
Files DVD/CD->PC/user this month	Monthly list of all files transferred from DVD/CDs to PCs classified by user.	You must define a **Shadow** rule.
Files Floppy->Pc/user this month	Monthly list of all files transferred from floppy disks to PCs classified by user.	You must define a **Shadow** rule.
Hardening violations this month	All client hardening violations detected this month.	You must first configure the **Client Hardening** option.
Keylogger this week	All key logging violations and intrusions detected this week.	You must first configure the **USB Key Logger** option.
Medium Encrypted by User	All media encrypted by users.	You must define permissions for removable devices.
Medium Encrypted this month	Monthly list of all media encrypted by users.	You must define permissions for removable devices.
PC->DVD/user this month	Write granted by DVD/CD device, PC, and user for the month.	You must enable the **Device Log** option.
PC->Floppy/user this month	Write granted by floppy disk device, PC, and user for the month.	You must enable the **Device Log** option.

Template Name	Shows	Prerequisite
PC->Remove/user this month	Read granted by removable storage device, PC, and user for the month.	You must enable the **Device Log** option.
Remove->PC/user this month	All read operations from removable storage devices for the month, classified by user.	You must define a **Shadow** rule.
Shadow by file type for this month	A shadow copy of the file name or the entire file. for all files copied for the month. classified by file type.	You must define a **Shadow** rule.
Shadow by user per month	A shadow copy of the file name or the entire file. for all files copied for the month. classified by user.	You must define a **Shadow** rule.
Shadow exp by size dsc this month	A shadow copy of the file name or the entire file, for all files copied to an external device for the month, classified by size.	You must define a **Shadow** rule.
Shadow files >10 MB this month	A shadow copy of the file name or the entire file. for all files copied to an external device larger than 10 MB. for the month.	You must define a **Shadow** rule.
Shadow imp by size dsc this month	A shadow copy of the file name or the entire file. for all files copied from an external device for the month. classified by size.	You must define a **Shadow** rule.
Shadow mp3. mp4 by user	A shadow copy of the file name or the entire file. for all music and video files copied for the day. classified by user.	You must define a **Shadow** rule.

ivanti

Template Name	Shows	Prerequisite
Shadowing today	A shadow copy of the file name or the entire file, for all files copied for the day.	You must define a **Shadow** rule.
Users denied device this week	All device permissions denied by user for the week.	You must enable the **Device Log** option.

Create New Template

The *Log Explorer* provides extended capability for creating custom audit query templates.

You can createe customized templates that represent specific query criteria.

1. From the Management Console, select **View** > **Modules** > **Log Explorer** > **Template**.

Step Result: The *Select and edit templates* dialog opens.

Figure 42: Select and Edit Templates Dialog

2. Click **New**.

   Step Result: The *Templates settings* dialog opens, which consists of three tabs:

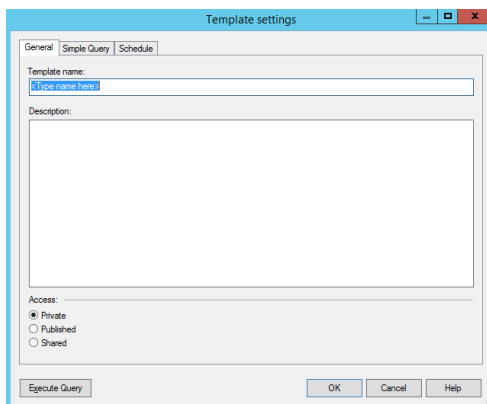   - *General* tab
   - *Simple Query* tab
   - *Schedule* tab

Figure 43: Template Settings Dialog

3. Select the *General* tab.
4. Enter a name for the new template in the **Template name** field.
5. Type a brief description of the template in the in the **Description** field.
6. Select one of the following options:

Option	Description
Private	The new template will only be accessible to the owner and *Enterprise Administrators*.
Published	The template can be: • accessed and used by any user, • edited, and saved by the owner and *Enterprise Administrators*, • edited but not saved by *Administrators*.
Shared	The template can be accessed, used, and edited by any user.

7. Select the *Simple Query* tab to specify your query columns and criteria.

   These criteria determine which log entries are shown as results in the Log Explorer report, and the information that is displayed.

ivanti

To select log entries that match certain criteria, select the column to which the criteria apply, by selecting the appropriate check box, clicking ⬚ (ellipsis) in the **Criteria** column, and specifying the criteria you want to match.

You can choose which information to display for each entry, the display size of the columns and how the results are grouped or sorted in particular ways.

> **Note:** If you select the **Count** column then the results are automatically grouped.

8. Click **Execute Query**.

   If you click **OK**, the window closes and then you will need to click **Execute** from the *Select and Edit Templates* dialog.

   Step Result: The *Template settings* dialog closes and you see the results in the Log Explorer window.

Result: The template is stored when you execute the query.

Select and Edit Templates Dialog

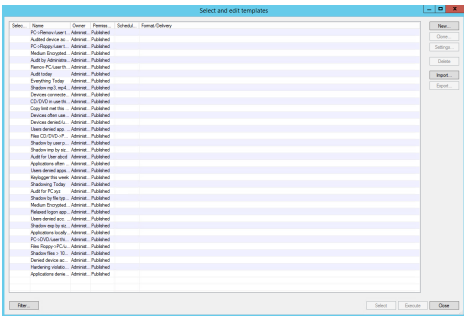The *Select and edit templates* dialog is used to select, add, edit, import, export, schedule, and run templates.

Figure 44: Select and Edit Templates Dialog

The *Select and edit templates* columns are described in the following table:

Column	Description
Name	Lists all existing templates that you can access.
Selected	Indicates whether the template is currently selected.
Owner	The template owner with full rights to use and edit the template.
Permissions	Indicates whether the template can be viewed or changed by users other than the **Owner**.
Scheduled	Indicates whether the template is used to create automatic reports periodically.

Column	Description
Format Delivery	Indicates whether schedule reports are e-mailed or where the reports are stored.

When you right-click the main panel of the **Select and edit templates** dialog, the **Templates** right-mouse menu is shown:
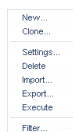

Figure 45: Templates Menu

Note: The options available in the **Templates** menu depend on whether you have a template selected when you opened the menu.

You can use the **Templates** menu to:

- Create a new template or clone an existing template.
- Change the settings of a selected template.
- Delete a selected template.
- Import templates in XML format or legacy format (`*.tmpl`) from the registry.
- Export a selected template to an XML file.
- Execute a query to retrieve all log entries that match the criteria defined in the currently selected template, and display these in the Log Explorer window.
- Filter the templates shown in the **Select and Edit Templates** dialog.

Filtering Templates
You can create subsets of the templates listed in the **Select and Edit Templates** dialog.

You can select multiple filtering criteria to narrow the focus of template sets shown, thereby reducing the number of templates that are listed.

1. From the Management Console, select **View** > **Modules** > **Log Explorer** > **Templates**.

   Step Result: The **Select and Edit Templates** dialog opens.

2. Click **Filter**.
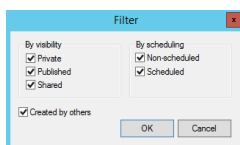
   Step Result: The **Filter** dialog opens.

Figure 46: Filter Dialog

ivanti

3. Select one or more of the following options:

Option	Description
Private	Shows templates visible only to the template owner and *Enterprise Administrator*.
Published	Shows templates visible to all Management Console users within your system that can be: • accessed and used by any user, • edited, and saved by the owner and *Enterprise Administrators*, • edited but not saved by *Administrators*.
Shared	Shows templates viewed and changed by any Management Console users within your system.
Non-scheduled	Shows templates used to generate specific reports.
Scheduled	Shows templates automatically run periodically to generate regular reports. These are saved in a shared folder on your network or e-mailed to specified recipients.
Created by others	Shows templates created by users other than the *Enterprise Administrator*.

4. Click **OK**.

Result: A subset of all available templates is shown.

Template Settings Dialog

The ***Template settings*** dialog is used to define the settings used for a new template, or a template selected from the ***Select and edit templates*** dialog:

You can use the ***Template settings*** dialog to:

- Name a new template using the ***General*** tab and specify who is allowed to use and edit the template by selecting the **Private**, **Published**, or **Shared** options.
- Choose whether the template is used to generate reports automatically on a periodic basis by setting the parameters in the ***Schedule*** tab and selecting **Generate scheduled reports**.
- Specify complex selection and display settings for the template by using the **Advanced View** with the ***Query & Output*** tab.
- Schedule the production of periodic reports using a template using the ***Schedule*** tab.
- Define the format of scheduled reports using the ***Schedule*** tab.
- Choose who you want the reports to be e-mailed to using the ***Schedule*** tab.
- Execute the query specified by the template and display the results in the main ***Log Explorer*** window.
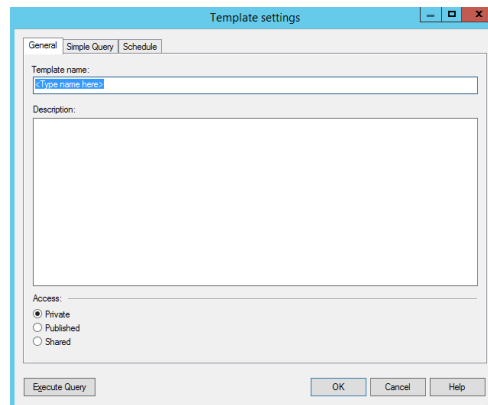- Save the changes made to the template settings.

Figure 47: Template Settings Dialog

General Tab

The ***General*** tab is displayed by default when the ***Template settings*** dialog opens and is used to define general template use conditions.

You can use the ***General*** tab to:

- Define the template name in the **Template name** field.
- Describe the template in the **Description** field.
- Define the user access type as:

    - **Private** - Template can be used only by the **Owner** and *Enterprise Administrators*.
    - **Published** - Template can be used by any user but can only be edited by the **Owner** and *Enterprise Administrators*.
    - **Shared** - Template can be used and edited by any user.

Simple Query Tab

The **_Simple Query_** tab is displayed by default when the **_Template settings_** dialog opens and is used define simple template query conditions.

Using the **_Simple Query_** tab,you can:

- Show/hide columns by selecting or deselecting the column names in the **Columns** list.

  Step Result: The column name moves to the top section of the list when you check it.

- Change the display size of a column by:

  a) Selecting a row.
  b) Clicking **Size**.
  c) Typing a new size.

- Sort ascending/descending:

  a) Click the **Sort/Group by** cell of the row corresponding to the appropriate results column (or highlight the row and click **Sort/Group By**).
  b) Choose either **Ascending** or **Descending** from the drop-down list options.
  c) If you want to sort the results of the query by the values in more than one column, select the multi-column sorting box and choose the columns that you want to sort your results by in turn.

- Group results according to the value in a particular column:

  a) Click the **Sort/Group by** cell of the row corresponding to the appropriate results column (or select the row and click **Sort/Group By**).
  b) Choose the **Group by** option from the drop-down list.

  When grouping results, all log entries in the Log Explorer **_Results_** panel/custom report are compiled into single entries corresponding to the unique values in the column. In the following figure, results are grouped according to their **File Type** value. The ellipses indicate hidden log entries and the **Count** column indicates how many log entries have the same **File Type**.

File Type		Count(Type)	Computer	Traced On (En...
Executable		841 [...]	[...]	
Script		35 [...]	[...]	

  Figure 48: Grouping Results in the Query

- Define the column display order using **Move up** and **Move down** commands.

ivanti

Schedule Tab

The **Schedule** tab is displayed by default when the **Template settings** dialog opens and is used scheduling report generation.

The **Schedule** tab is used to define the following:

- Start and end dates between which reports are automatically generated using the **Schedule** template.
- How often the report is generated and the pattern for production. For example, you can choose report generation on a daily or weekly basis for specific days, every few hours, or on a monthly basis.
- Who and where the information is sent, or stored, and the format.

Restriction: You cannot schedule a log report unless have the necessary administrative rights. If you do not have administrative rights, you will see that the options are grayed-out and you receive a warning message.
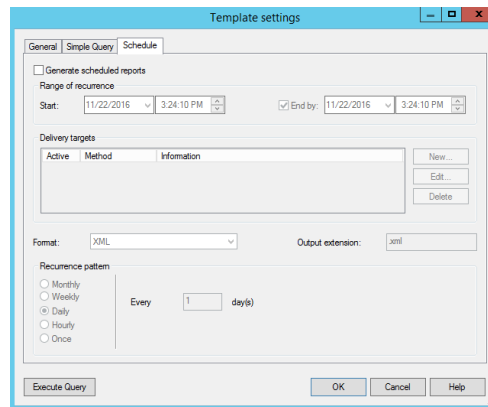

Figure 49: Schedule Tab

Scheduling a Report

Using a template, you can schedule automatic report generation by specifying the report frequency and report recipients.

1. From the Management Console, select **View** > **Modules** > **Log Explorer** > **Templates**.

    Step Result: The **Select and edit template** dialog opens.

2. Choose the template from the list.

3. Click **Settings**.

    Step Result: The **Template settings** dialog opens.

4. Select the **Schedule** tab.

5. Select the **Generate scheduled reports** option.

6. In the *Range of recurrence* panel:

    a) Select the starting date and hour.

    b) You may select the **End by** option and select and ending date and hour.

7. In the *Delivery targets* panel:

    a) Click **New**.

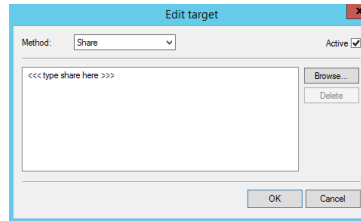   **Step Result:** The *Edit target* dialog opens.

Figure 50: Edit Target Dialog

    b) Select the **Method** from the drop-down list.

    c) If you select the **Share** method, click **Browse**.

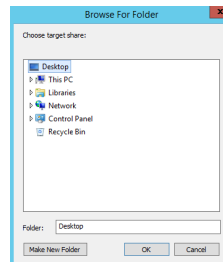   **Step Result:** The *Browse for Folder* dialog opens.

Figure 51: Browse for Folder

    d) Select a shared folder.

    e) Click **OK**.
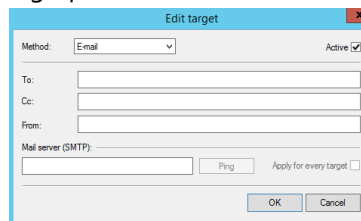
       Step Result: The *Edit target* dialog opens.

Figure 52: E-mail Options

ivanti

f) If you selected **E-mail** as method, specify the **To**, **Cc**, **From** recipients, and **Mail server (SMTP)** in the *Edit target* dialog.

g) Click **Ping** to test the connection.

h) If you select the **Apply for every target** option, the **Mail server** field for every delivery target changes and you lose any existing information. You must be careful when setting e-mail delivery options. If not correctly set, the report may be sent to the junk mail folder. The specified mail server should accept anonymous connections so that the reports delivery option works properly.

i) Click **OK**.

> **Step Result:** The *Edit target* dialog closes. The **Schedule** tab of the *Template settings* dialog opens. The **Schedule** tab is used to define whether reports are sent via mail or saved in a shared folder on the network.

8. In the **Format** field:

a) Select the file **Format** from the drop-down list.

b) Change the **Output extension**, as necessary.

9. In the **Recurrence pattern** panel:

a) Select a frequency option from the list shown.

> **Step Result:** The right panel changes to reflect your selection.

10. Click **OK**.

11. Click **Close**.

Result: The selected template is ready to generate a regularly schedule report that is archived on a shared folder or sent by e-mail as an attachment.

Criteria

You specify the criteria you want to use for a particular template using one or more context-dependent *Criteria* dialogs.

Criteria narrow the query results you. Typically, the more specific you are with your search criteria, the fewer results are returned.

Criteria choices range from a fixed value the *Criteria* dialog displays to a free text data field where you can use wild cards to delimit the criteria. Others dialogs contain **Select** or **Search** commands, for example, when specifying criteria involves matching one or more computers or users.

The *Criteria* dialog list is displayed when log entry fields contain one of a fixed set of values.
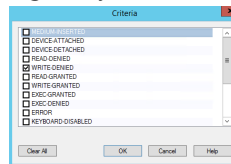

Figure 53: Criteria Dialog

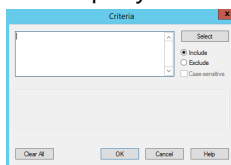The free-text **Criteria** dialog is used to filter the query results based on any text that you type in.

Figure 54: Free-text Criteria Dialog

The time **Criteria** dialog is used to search for log entries that were produced, or uploaded to the Application Server, at a certain date/time.
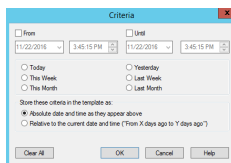

Figure 55: Time Criteria Dialog

As you define the criteria used in your template, they are displayed in the **Criteria** column of the **Template settings** dialog.
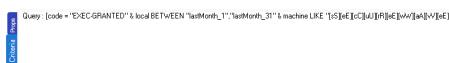
Figure 56: Example Criteria settings

Specify Criteria Type

You can view the device access event types by specifying log entry **Type** criteria.

The **Computer**, **Traced on**, and **Transferred on** fields are shown in the logs for every event associated with input/output device access, as described in the following table.

Table 37: Log Explorer Criteria by Type

Criteria by Type	Logged Event	Additional Information
MEDIUM-INSERTED	Occurs when a user inserts a CD/DVD in the computer drive or removable media reader.	**Device type** name of the device medium.
		Volume label is the medium tag.
		Medium hash is the hash number for the inserted medium.
		Other is the inserted medium serial number.
DEVICE-ATTACHED	Occurs when a device is connected to a computer.	None.

ivanti

Criteria by Type	Logged Event	Additional Information
DEVICE-DETACHED	Occurs when a device is disconnected from a computer.	None.
READ-DENIED	Occurs when a user attempts to access an unauthorized device.	**Device type** name of the device medium.
		Volume label is the medium tag.
		File Name is the name of the file the user attempted to read.
		User Name is the name of the user who attempted to access the device.
		Process Name is the application used to access the device.
		Other is the exact access mask, in hexadecimal format, used to access the device.
WRITE-DENIED	Occurs when a user attempts to write a file to a read-only device.	**Device type** name of the device medium.
		Volume label is the medium tag.
		File Name is the name of the file the user attempted to write to removable media.
		User Name is the name of the user who attempted to access the device.
		Process Name is the application used to access the device.
		Other is the exact access mask, in hexadecimal format, used to access the device.
READ-GRANTED	Occurs when a user accesses an authorized device.	None.
WRITE-GRANTED	Occurs when a user copies data to an authorized device.	None.

Criteria by Type	Logged Event	Additional Information
ERROR	Occurs for errors created when a user accesses or encrypts a device.	Error details specific to the user action are shown.
KEYBOARD-DISABLED	Occurs when the user keyboard is disabled because a keylogger may be present.	None.
KEYLOGGER-DETECTED	Occurs when a keylogger is detected.	None.
MEDIUM-ENCRYPTED	Occurs when removable storage medium is encrypted.	None.
ADMIN-AUDIT	Occurs when an administrator performs an action through the Management Console.	**User Name** is the name of the administrator.
		Audit Event is the type of action performed by the administrator.
		Target is the device that permissions were changed for.
		Target Computer is the name of the computer that the administrator changed permissions for.
		Target User is the user name that the administrator changed permissions.

ivanti

The Advanced View

You can use *Query & Output* tab to perform queries, with more complex criteria and specifications.

In the advanced view of *Query & Output* tab, you enter complex queries using a control hierarchy. The hierarchy representing the query has seven top-level nodes.
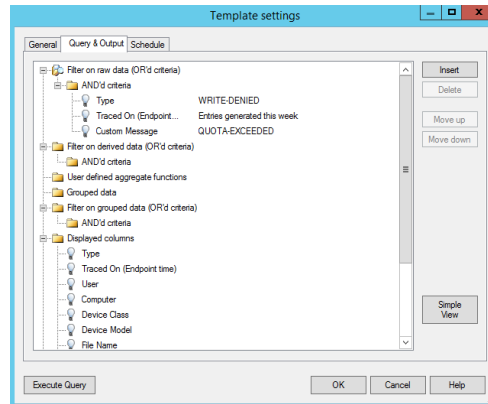

Figure 57: Query & Output Tab

The top level nodes are used to:

- **Filter on raw data (OR'd criteria)** to specify the criteria, based on information actually in the log entries, used to select results to be included in reports generated using the template.
- **Filter on derived data (OR'd criteria)** to specify the criteria, based on information derived from the Management Console, used to select results to be included in reports.
- **User defined aggregate functions** such as the sum, minimum, maximum, or average of values contained in the log entries.
- **Grouped data** to produce a single result corresponding to multiple log entries with the same value for a particular field.
- **Filter on grouped data (OR'd criteria)** to determine whether the report generated using the template displays only results where the values for the computed columns match specified criteria.
- **Displayed columns** to determine which columns are displayed and their order.
- **Sorting** to determine the order in which rows of results are displayed.
- **Insert** adds a new child node into the selected node of the tree. If the nodes in the group cannot be reordered then the new node is positioned below any existing nodes.
- **Delete** erases a selected child node from the tree.
- **Move up** and **Move down** exchanges a selected node for one place up or down.

When nodes representing columns are selected, a set of controls is displayed to the right. These controls can be used to select columns, criteria, and so forth.

If you are on the **Advanced View**, you can revert to a simple query by selecting **Simple View**.

Note: You cannot revert to the *Simple Query* tab after you have defined a complex query that cannot be represented correctly in the *Simple Query* tab. In this case, the **Simple View** is shown as disabled.

Create a Complex Query
You select **Advanced View** from the *Simple Query* tab to change the tab name to *Query & Output* and create complex queries.

You can create, save, and execute a complex query as follows.

1. From the Management Console, select **View** > **Modules** > **Log Explorer**.

   Step Result: The *Log Explorer* window opens.

2. Click **Template**.

   Step Result: The *Select and edit templates* dialog opens.

3. Select the *Simple Query* tab.

4. Click **Advanced View**.

   Step Result: The dialog changes to show the advanced view structure and the tab name changes to *Query & Output*.

5. Add the criteria you want to use to select results, as follows:

   a) Click the **AND'd criteria** node from the top-level node **Filter on raw data (OR'd criteria)**.
   b) Click **Insert**.
   c) Select **Type** from the drop-down list.
   d) Click the ellipsis ⬚ to select the column and the criteria you want from the drop-down list in the *Criteria* dialog.
   e) Click **OK** when you finish selecting your criteria.

      Step Result: The *Criteria* dialog closes.

   f) Repeat the preceding steps for derived data, by selecting criteria from the top-level node **Filter on derived data (OR'd criteria)**.

6. Select computed information you want to display, as necessary.

   Tip: For example, you may want to display a count, an average value, or a maximum value for a column when you group results. The computed information columns are named C1, C2, and so forth.

   To add a computed column:

   a) Click the top-level node *User defined aggregate functions*.
   b) Click **Insert**.
   c) Select the column and the calculated function, using the drop-down list.

7. Define how you want your results grouped, as necessary. To group results:

   a) Click the top-level node *Grouped data*.
   b) Click **Insert**.

ivanti

c) Select the column you want to group results, using the drop-down list.

> **Tip:** You can group results by values from several columns.

8. Specify that the values in your computed columns match particular criteria, as necessary.

    a) Click on the **AND'd criteria** node of the top-level node **Filter on grouped data (OR'd criteria)**.
    b) Click **Insert**.
    c) Select the computed column and criteria you want to use.
    d) Enter a corresponding value.

9. Choose the columns of information you want to display and the order. To select each column you want to display:

    a) Click on the top-level node **Displayed columns**.
    b) Click **Insert**.
    c) Select the column from the drop-down list.

> **Tip:** You can reorder the displayed columns by clicking **Move up** and **Move down**.

10. Specify how you want to sort the results in the report. To add a sorting level:

    a) Click on the top-level node **Sorting**.
    b) Click **Insert**.
    c) Select the column you want to sort by and how you want to sort, using the drop-down lists.

> **Tip:** You can sort results using several columns.

11. Click **Execute query**.

    Step Result: The **Template settings** dialog closes.

Result: You create, save, and execute a complex query.

Upload Latest Log Files

You may need to view the most current log information to help you quickly troubleshoot problems or verify that permissions or authorizations are set correctly.

Clients upload log information to the Application Server at the time specified when you define default options. You can use the Log Explorer to fetch log activity as needed, rather than waiting for the next log activity upload.

1. From the Management Console, select **View** > **Modules** > **Log Explorer**.

    Step Result: The **Log Explorer** window opens.

2. Click **Fetch Log**.

    Step Result: The *Select Computer* dialog opens and prompts you to specify the client computer to fetch the logs from.
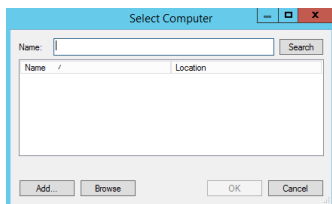

Figure 58: Fetch Logs - Select Computer

3. Click **Search** or **Browse** to select from a list.

4. Click **OK**.

Result: The computer logs are uploaded to the Application Server and stored in the database. Updated log files are shown in the **Log Explorer** window.

> **Restriction:** The time delay between retrieving the log entries from the client and the availability of the latest logs depends on the queue size and the database availability at the time of upload.

View Administrator Activity

You can use the **Log Explorer** module to monitor Ivanti Device and Application Control administrator activity.

Administrator activity includes changing user access rights, device permissions, and file authorizations. Access to audit log information depends upon administrative user access rights established when you define user access rights in the **Tools** module.

1. From the Management Console, select **View** > **Modules** > **Log Explorer**.

    Step Result: The *Log Explorer* window opens.

2. Select the **Audit by Admin** template.

> **Note:** You may also use a template that you create.

3. Click **Query**.

Result: A list of administrator audit log events is shown in the *Log Explorer* window.

ivanti

View Shadow Files

To view shadow files, you can use predefined templates. When a predefined template does not contain the type of data that you want to review, you can create your own template query to view shadow files.

Prerequisites:

To view shadow files, Ivanti recommends that you show only log entries that display attachments by filtering templates.

The file name, date, and administrator name are logged for every instance a shadowed file is accessed.

1. In the Management Console select **View** > **Modules** > **Log Explorer** > **Templates**.

   Step Result: The **Select and edit template** dialog opens.

2. Select a predefined shadow template from the list shown.

   Caution: Avoid opening files exceeding 350 MB unless sufficient resources are available.

3. Click **Select**.

4. Click **Query**.

5. To view shadow files using a custom query:

   a) Click **Settings**.
   b) Select **Attachment**.
   c) Click **Criteria**.
   d) Select **With**.
   e) Click **OK**.
   f) Click **Execute Query**.

      Step Result: The **Select and edit template** dialog closes and the query runs.

Result: When the **Shadow** rule is enforced, the entries listed show attached files that are exact copies of the shadowed files:

   - Copied to or from authorized devices
   - Read by users

   Depending on the selected fields, the date shown for shadow files are:

   - **Traced On** - when files were copied or read, to or from, the device
   - **Transferred On** - when a file was uploaded to the database

Device Control tracks the:

- User name for the copied file
- Computer name used for the copy action
- Filename
- Content
- Device name

After Completing This Task:

Once you list the files, right-click any attachment showing the `True` value, which indicates that the full content is shadowed, and select one of the following options:

Table 38: Shadow File Output Column Descriptions

Option	Description
View	Allows you to view the contents of the file in an internal binary viewer administered by Device Control.
Open	Opens the file with the associated application as defined in Windows Explorer®. If there is no association, this command is equivalent to Open With.
	Restriction: Only available for full shadowing and when selecting one log registry.
Open with	Allows you choose the application that opens the file.
	Restriction: Only available for full shadowing and when selecting one log registry.
Save as	Allows you to save the file to a local or network drive and use an external utility or program to open the file.

Forcing the Upload of Shadow Files from a Client Upon User Log Off

Use `scomc.exe` with the `fetch`, `dismount`, and `maxround` options in your client log off scripts to force the upload of shadow files to the server.

Upon user log off, the client will close any open shadow files and attempt to upload them to the server. If the client cannot complete the upload before the log off has finished, any remaining shadow files will be uploaded the next time the user logs in.

As the closing of shadow files in preparation for upload from the client to server can take time (dependent on file size and quantity), specifying the `maxround` option ensures the client checks for closed shadow files a sufficient number of times.

Syntax

```
scomc.exe -fetch -dismount -maxround <# of attempts>
```

ivanti

Options

-fetch	Specifies that shadow files are to be retrieved from the client.
-dismount	Dismounts removable media devices from the client.
-maxround	Specifies the maximum number of attempts to upload and remove shadow files from a client. Retry attempts accepted are 2 to 9 (no value or any value outside that range will result in no retry attempts).
	Important: The maxround option must be the last option specified in the command line.

Windows Event Log Entries Created by Device Control

Learn about the entries created in the Windows Event logs by Device Control actions.

Code	Message Name	Description
1	MSG_NO_VALID_KEY	SCC was unable to find a valid public key. It is currently using the default public key.
2	MSG_NO_VALID_KEY_WITH_LIST	SCC was unable to find a valid public key. It is currently using the default public key. For your reference
3	MSG_KEY_FOUND	SCC found a valid key in directory "%1" and is now using it.
4	MSG_WINSOCK_START_FAILURE	The Windows socket library could not be started.
5	MSG_PERMISSION_REMOVE_TIMEOUT	Unable to update permissions. Operation to remove old permissions timed out with error %1 on file "%2".
6	MSG_PERMISSION_REPLACE_TIMEOUT	Unable to update permissions. Operation to replace old permissions timed out with error %1 on file "%2".
7	MSG_ACCESS_DENIED	Application Control denied execution of the file "%1". For the full path and other details
8	MSG_ACCESS_NEARLY_DENIED	Application Control would have denied execution of the file "%1"
9	SWAVE_FSFILTER_ERROR_CANNOT_USE_SHADOW_DIRECTORY	The shadow directory does not exist or cannot be accessed. The floppy and removable drives will be disabled by the shadow driver.
10	SWAVE_UNSUPPORTED_CDBURNING	Unsupported CD/DVD burning mode
11	SWAVE_CDSHADOW_ERROR	Error during the processing CD/DVD shadow images

Code	Message Name	Description
12	MSG_NO_VALID_PUBLIC_KEY	SK was unable to find a valid public key. It is currently using a default key. You should
13	DWAVE_FSFILTER_ERROR_INTERNAL_ERROR	The shadow driver encountered an internal error that prevents normal operation. The drives will be disabled by the shadow driver.
14	SWAVE_FSFILTER_INFO_MEDIUM_INSERT	Action: Medium inserted%rVolume Name: %1%rSerial Number: %2 Encryption: %3
15	SWAVE_CDSHADOW_OVERRIDE	Unsupported CD/DVD burning mode
16	MSG_DEVICE_ATTACHED	Device "%1" (%2) attached to endpoint by user %3.
17	MSG_QUOTA_EXCEEDED	File copy quota has been reached.
18	MSG_READ_DENIED	Device Control denied read access for device "%1" (%2) accessing path "%3" by user %4 for reason %5 by process "%6".
19	MSG_WRITE_DENIED	Device Control denied write access for device "%1" (%2) accessing path "%3" by user %4 for reason %5 by process "%6".
20	MSG_WLAN_BLOCKED	Device Control device wlan blocked for %1. For the full path and other details
21	MSG_KEYLOGGER_DETECTED	Device Control detected a keylogger for device "%1" by user %2.
22	MSG_KEYBOARD_DISABLED	Device Control disabled keyboard "%1".
23	MSG_MEDIUM_ENCRYPTED	Device "%1" (%2) mounted as volume %4 was encrypted by user %3.
24	MSG_INVALID_PASSWORD	Invalid password entered for device "%1" (%2) by user %3.
25	MSG_WRITE_GRANTED	Device Control shadowed file "%1" from a write to device "%2" (%3) by user %4. For the full path and other details
26	MSG_READ_GRANTED	Device Control shadowed file "%1" from a read of device "%2" (%3) by user %4. For the full path and other details
27	MSG_DEVICE_DETACHED	Device "%1" (%2) detached from endpoint by user %3.
28	MSG_READ_AUDIT	Device Control audited a denied read access for device "%1" (%2) accessing path "%3" by user %4 for reason %5 by process "%6".

ivanti

Code	Message Name	Description
29	MSG_WRITE_AUDIT	Device Control audited a denied write access for device "%1" (%2) accessing path "%3" by user %4 for reason %5 by process "%6".

Reference_Body

Chapter

4

Using Tools

The **Tools** module consists of administrative tools for administrators to manage database information.

The **Tools** module administrative tools are used to maintain application user, file group, device permission, and database information.

User administrative actions include:

• Defining administrators.
• Defining global system options.
• Authorizing administrative users to disable Device Control using endpoint maintenance.

Device permission administrative actions include:

• Exporting permissions settings to clients.
• Distributing device permission updates by sending updates to computers.
• Providing temporary device permissions for users not connected to the network by authorizing temporary permissions.
• Recovering encryption passwords for users.

Database administrative actions include:

• Managing the information stored in the database by using database cleanup.
• Adding computers to an existing workgroup by synchronizing domains.

ivanti

Synchronizing Domains

You must regularly synchronize individual computers and Windows domain users with the domain controller to maintain accurate database user and domain information.

The database stores user, user groups, and computer and domain account information. To preserve the login performance experience, new user names are not resolved during login. Therefore, current user and domain name information must be synchronized by the adminstrator.

The synchronization process applies to protected computers that are in a domain or a file group. You can synchronize local users and user groups for one or more computers in a domain. This allows you to enforce policies for local users within a domain.

Synchronizing Domain Members

You can update the users and groups domain list in the Ivanti Device and Application Control database by using the **Synchronize Domain** tool.

When you enter a computer name that is a domain controller, the domain controller is used for synchronization. This is useful when replication between domain controllers is slow.

1. From the Management Console, select **Tools** > **Synchronize Domain Members**.

   Step Result: The *Synchronize Domain* dialog opens.

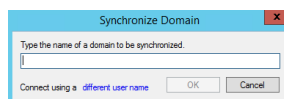
Figure 59: Synchronize Domain Dialog

2. Enter the name or IP address for the domain that you want to synchronize.

3. Click **OK**.

Result: The system updates the database list of domain users and groups.

> **Restriction:** The Windows XP Simple File Sharing feature can interfere with synchronizing a local computer running Windows XP. If you experience difficulty, turn off this option and retry.

Synchronizing Domain Users

When no domain controller exists to generate a user list for the **Synchronize Domain** task, you must add domain servers and computer users to the user list manually.

You can add workgroup computers to a domain by using the *Synchronize Domain Members* tool.

1. From the Management Console, select **Tools** > **Synchronize Domain Members**.

   Step Result: The *Synchronize Domain* dialog opens.

2. Enter the name of a domain.

3. To authenticate to the network as a different user, click the **Different user name** option.

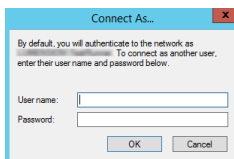**Step Result:** The *Connect As...* dialog opens.

Figure 60: Connect As Dialog

4. Enter the user name, including domain name, for the local user of the computer you want to synchronize with the domain.

5. Enter the password for the local computer user.

6. Click **OK**.

Step Result: The *Connect As...* dialog closes.

7. Click **OK**.

Step Result: The *Synchronize Domain* dialog closes.

Result: The user name for the specified is computer added to the database, so you can assign local user access rights. The synchronization results are shown in the *Output* panel of the Management Console.

Database Clean Up

You can use the **Database Maintenance** tool to remove obsolete database records that use storage capacity.

You can clean up the database to remove activity logs, scanning results, shadow files, and password recovery information records from the database. This function is limited to removing obsolete database records.

Caution: You cannot recover deleted database files. Ivanti advises that you create back-up files before deleting any data from the database.

ivanti

Deleting Database Records

Delete database records using the **Database Maintenance** tool.

1. From the Management Console, select **Tools** > **Database Maintenance**.
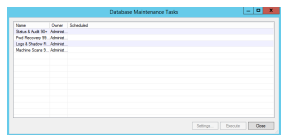
   Step Result: The *Database Maintenance* dialog opens.

   Figure 61: Database Maintenance Dialog

2. Select one of the pre-defined task templates:

Option	Description
Status & Audit 90+	Clears client status and admin audit logs 90 days old or older.
Pwd Recovery 999+	Clears out password recovery information as old or older than 999 days.
	Caution: Purging this data can result in the permanent loss of encrypted data in the case of a user forgetting their password.
Machine Scans 999+	Clears machine scan information as old or older than 999 days.
	Caution: Machine scan purging should not be conducted while scanning is in progress.
Log and Shadow Files 90+	Routine maintenance that clears client logs and shadow files 90 days old or older.

3. [Optional] Click **Settings** to change the parameters or schedule a recurring database maintenance task.

   How long should the DB maintenance task run for? let's you limit the the purge duration so, for example, it does not coincide with replication or import/export tasks. The purge stops when the minutes set expire and the system finishes the current batch it is purging. Depending on how long it takes your database to purge a batch, this can add several minutes to the actual purge duration.

4. Click **Execute**.

> **Important:** Verify that you have sufficient free disk space on the computer to generate the transaction logs that accompany database maintenance. If you get an error message indicating insufficient disk space, retry the process by selecting a shorter date range or less information.

Result: The selected data is deleted from the database and the Application Server data file directory.

> **Caution:** Deleting large volumes of files from the database usually results in engaging SQL server connectivity for long periods of time, during which the Management Console is unresponsive to the user. Also, exiting or cancelling the from the Management Console before database maintenance is complete can introduces errors and inconsistencies in the database.

Defining User Access

The Management Console can only be accessed by authorized network administrators.

To control user access to the Management Console, you can define two types of administrators:

- An *Enterprise Administrator* has full access to all management functions.

> **Note:** Initially, any member of the Windows `Administrators` group for a Application Server has the privileges of a *Enterprise Administrator*. After an *Enterprise Administrator* is designated, administrative privileges are automatically restricted for the members of the local `Administrators` group.

- An *Administrator* has restricted access to Management Console functions as defined by the *Enterprise Administrator*.

An *Enterprise Administrator* can delegate administrative rights to other administrators using Active Directory Organizational Units. These rights are described in the following table.

Table 39: Ivanti Device and Application Control Administrator Rights

Administrative Rights	Administrator Type	Limitations	Ivanti Device and Application Control Application
View all device permissions and file authorizations	All Ivanti Device and Application Control administrators	NA	Application Control; Device Control
Modify file authorizations	*Enterprise Administrators*	NA	Application Control
Modify global-level device permissions	*Enterprise Administrators*	NA	Device Control

ivanti

Administrative Rights	Administrator Type	Limitations	Ivanti Device and Application Control Application
	Members of the **Settings (Device Control)** role	Only users the administrator is allowed to manage	
Modify computer-level device permissions	*Enterprise Administrators*	NA	Device Control
	Members of the **Settings (Device Control)** role	Only for the computers that the administrator is allowed to manage	
Modify computer-group device permissions	*Enterprise Administrators*	NA	Device Control
	Members of the **Settings (Device Control)** role	Only if the administrator is allowed to manage all the computers in the computer group for all accounts	
Manage built-in accounts (Everyone, LocalSystem, and so forth)	*Enterprise Administrators*	NA	Application Control; Device Control

Initially, any administrator with password access to a Application Server and the Management Console can use the Management Console.

Before using Ivanti Device and Application Control, Ivanti recommends setting up administrators who have access to the Management Console. You can assign different roles to administrators, but you must define at least one *Enterprise Administrator*.

The following rules apply to administrative user roles:

- You must always designate one *Enterprise Administrator* before you modify the list of administrators.
- All Application Servers share the same database, so some administrative rights set for an administrator can be used for other Application Servers.
- Local computer users cannot manage the Management Console, even if assigned as an *Enterprise Administrator*, because they cannot connect to an Application Server.

Assigning Administrators

You assign administrator access rights using the **User Access** tool.

1. From the Management Console, select **Tools** > **User Access**.

   Step Result: The *User Access Manager* dialog opens.

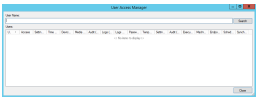

   Figure 62: User Access Manager Dialog

2. Click **Search** to generate a list of users and user groups.
   You can use wildcards (* or ?) in the **User name** field.

3. Select a user or user group from the **Users** list.

4. In the **Access** column, click the down arrow.

   Step Result: A drop-down menu listing administrative user access options appears.

5. Select one of the following options:

Option	Description
None	No user access.
Administrator	Restricted user access defined by the *Enterprise Administrator* .
Enterprise Administrator	Complete user access to the Management Console .

6. Click **Close** .

   Step Result: The *User Access Manager* dialog closes.

Result: Users or user groups can access Management Console features that the administrator type assigns for user access.

ivanti

Defining Administrator Roles

An *Administrator* has restricted access to the Management Console and can be assigned various administrative roles by an *Enterprise Administrator*.

Administrator access roles are described in the following table.

Table 40: Ivanti Device and Application Control Administrator Roles

Functions	Administrator Rights	Ivanti Device and Application Control Application
Settings (Device Control)	Change permissions and options for the user, user groups, computers, and devices that the Administrator has write privileges in the Active Directory. Can view the **Media Authorizer** module. Without this role assignment, *Administrator* can only view the users access permissions.	Device Control
Time based settings (Device Control)	Set temporary and scheduled device permissions. This function is a sub group of **Settings (Device Control)**.	Device Control
Devices (Device Control)	Add new devices to the database using **Manage Devices** and organize devices into groups.	Device Control
Media (Device Control)	Encrypt and authorize media using the **Media Authorizer** module and generate the **Media by User** and **Users by Medium** reports. This an optional function for subgroups of **Settings (Device Control)**.	Device Control
Audit (Device Control)	View and search **Audit Logs** and view *Administrator* actions, with the appropriate rights, using the **Log Explorer** module.	Device Control

Functions	Administrator Rights	Ivanti Device and Application Control Application
Logs (Device Control)	View central logging and access shadow files using the *Log Explorer* module and generating *Shadowing by Device* and *Shadowing by User* reports.	Device Control
Logs without File Access (Device Control)	View central logging without access to shadow file content. This option is a sub group of **Logs (Device Control)**.	Device Control
Key Recovery (Device Control)	Generate a passphrase for access to an encrypted device when the user has does not have a decentralized encryption password. **Tip:** Can be accomplished with a lower security risk when the user is connected to the network.	Device Control
Temporary Permissions Offline (Device Control)	Set only temporary permissions for users that are not connected to the Application Server and extend access permissions for a limited time.	Device Control
Settings (App. Control)	View and modify user, user group, and computer **Default Options** for which the administrator has write permissions in the Active Directory, and authorize applications using the **Authorization Wizard**.	Application Control
Audit (App. Control)	View and search audit logs of system activity using the *Log Explorer*.	Application Control

ivanti

Functions	Administrator Rights	Ivanti Device and Application Control Application
Execution Logs (App. Control)	View and search execution logs using the ***Log Explorer*** for users, user groups, and computers that the administrator has write permission in the Active Directory.	Application Control
Machine Scans (App. Control)	Use the ***Scan Explorer*** to scan target computers, build lists of authorized executable, script, and macro files, view scan results for computers that the administrator has write permission in the Active Directory, and create new scan templates.	Application Control
Endpoint Maintenance	Create tickets to update, delete, and install clients.	Application Control; Device Control
Scheduled Reports	Generate custom reports at pre-scheduled intervals between start and end dates.	Application Control; Device Control
Synchronize Computer	An *Administrator* can only synchronize computers, not domains. Only an *Enterprise Administrator* can synchronize domains and computers.	Application Control; Device Control

Assigning Administrator Roles

After defining *Administrator* roles, you use the **User Access** tool to assign the defined roles to *Administrators* .

1. From the Management Console, select **Tools** > **User Access**.

   Step Result: The ***User Access*** dialog opens.

2. Click **Search** to generate a list of users and user groups.
   You can use wild cards (* or ?) in the **User name** field.

3. Select the *Administrator* user or user group from the **Users** list.

4. Assign user access by selecting **Yes** or **No**.

5. Click **Close**.

    Step Result: The *User Access* dialog closes.

Result: The *Administrator* rights change based upon the selected user access role.

Defining Default Options

You can set global options that govern certain aspects of how protected clients interact with Ivanti Device and Application Control. These settings apply to all servers or computers protected by Ivanti Device and Application Control.

Administrators can customize global system options for:

- Logging the types of events.
- Defining the types of notification users receive.
- Rules governing detection and notification of USB key loggers.
- Displaying the client icon in the system tray.
- Defining the shadow directory.
- Generating certificates from the client.
- Sending endpoint maintenance tickets to clients.
- Detecting online and offline device usage.

Default options can be set for:

- All computers.
- Specific computers.

Default Options Page

You use the *Default Options* page in the *Tools* module to change or set global defaults option Device Control feature behaviour.

The *Default Options* page consists of the following tab:

- The **Computer** tab options apply to all client computers.

The tab page consists of the following columns and panels:

Table 41: Default Options Tab Layout

Name	Element	Descriptions
Option	Column	Lists available options for your license type.
Current Value	Column	List the current default option value. Default values are displayed with a star (⭐).
Option Value	Panel	Shows a brief description for the option selected in the **Option** column.
Default setting	Check box	Displays the default setting value.

ivanti

Name	Element	Descriptions
Default Option Values	Drop-down list	Lists available default option values.

Computer Tab

The **Computer** tab shows the computer default options that govern how clients interact with the Application Server.
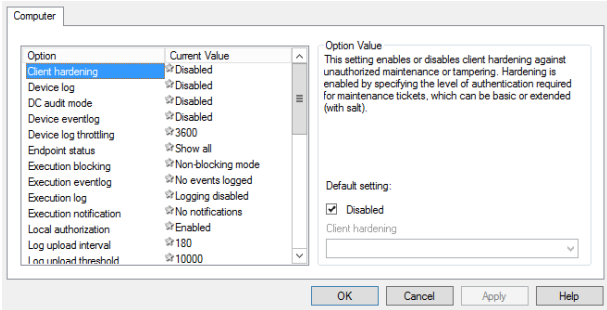

Figure 63: Default Options - Computer Tab

The following table describes the **Computer** tab default options and setting values.

Table 42: Computer Tab

Option	Value	Description
Client Hardening	**Disabled**	Feature is inactive. This is the default value.
	Basic	• Prevents users from deleting shadow files and log entries. • Allows an administrator to uninstall the client using **Endpoint Maintenance**.
	Extended	• Prevents users from deleting shadow files and log entries. • Allows an administrator to uninstall the client using the *Salt* value defined using **Endpoint Maintenance**.
Certificate generation	**Automatic**	A Certification Authority® (CA) digital certificate is generated automatically for media encryption, when a user does not have a certificate. This is the default value.

Option	Value	Description
	Disabled	When a user does not have a CA digital certificate, encrypted media cannot be used.
Clear unused space when encrypting	**Disabled**	The encryption process does not erase unused media disk space. This is the default value.
	Enabled	The encryption process automatically erases unused media disk space.
Device Log	**Disabled**	No device access or use events are logged. This is the default value.
	Enabled	All device access and use events are logged.
DC audit mode	**Disabled**	No device access or use events are logged. This is the default value.
	Enabled	Users have full acccess to all unmanaged devices. If no matching policy is configured for a given device, the client will provide logging information that can be used to create usage policies later. WRITE-AUDIT and READ-AUDIT events will be logged in sdcevent.log.
		Note: An endpoint is NOT secure while in Audit Mode.
Device Eventlog	**Disabled**	System does not send a log entry to the Windows Event Log when a device access or use event occurs. This is the default value.
	Enabled	System sends a log entry to the Windows Event Log when a device access or use event occurs.
Device Throttling	**3600**(Default)	Defines the period (in seconds) during which repeated attempts to log a previously logged event are ignored.

ivanti

Option	Value	Description
eDirectory Translation	**Disabled**	eDirectory user account information is not shown with the Windows account information. This is the default value.
	Enabled	eDirectory user account information is shown with the Windows account information.
Encryption Grace Period	**0** (Default)	Time, shown in hours, of the grace period for removable storage media encrypted without **Easy Exchange**, during which the media is accessible after attaching and removing the media, provided that the client has not yet logged an event.
Encryption Notification	**No Notification** (Default)	The user does not receive a custom encryption request notification when attaching an unencrypted removable storage device to a computer running the client.
		Note: This option applies only to a custom encryption notification message created by the administrator. It cannot be used to suppress the default notification.
	Encryption Notification	The user receives a custom encryption request notification when attaching an unencrypted removable storage device to a computer running the client. The notification request will include a custom message created by the administrator. With this option selected, the **Encryption Notification** field must contain a message to enable the notification property.

Option	Value	Description
Encryption Retain Data	**Unselected** (Default)	The check box in the **Encrypt Medium** dialog on the client is deselected.
	Forced Unselected	The check box in the **Encrypt Medium** dialog on the client is deselected. This option preset by the administrator and cannot be modified by the user.
	Selected	The check box in the **Encrypt Medium** dialog on the client is selected.
	Forced Selected	The check box in the **Encrypt Medium** dialog on the client is selected. This option preset by the administrator and cannot be modified by the user.
Endpoint Status	**Do not Show**	Does not show the client in the Windows system tray and suppresses all event notifications except local authorization (Application Control).
	Show All	Shows the client in the Windows system tray. Users can view all client status information. This is the default value.
	Show All without Shadow	Shows the client in the Windows system tray. Users can view all client status information, excluding shadow file policies.
	Show Allowed	Shows the client in the Windows system tray. Users can only view device status information for devices allowed for the client.
	Show Allowed without Shadow	Shows the client in the Windows system tray. Users can only view devices status information allowed for the client, excluding shadow file policies.
	Show Configured	Shows the client in the Windows system tray. Users can only view device status information for devices configured for the client.

ivanti

Option	Value	Description
	Show Configured without Shadow	Shows the client in the Windows system tray. Users can only view devices status information allowed for the client, excluding shadow file policies.
Compliance mode	**Enabled**	The Application Server uses **Compliance mode** algorithms for cryptographic services. This is the default value.
	Disabled	The Application Server does not use **Compliance mode** algorithms for cryptographic services.
DLC filter	**Not configured** (Default)	When configured this setting defines a filter string to be used against all MS Office and PDF documents contents. In order to work, DLP requires the Windows Search service to be configured propertly for all the given files. The filter string has to meet AQS requirements i.e.: • contents:"secret" • contents:(secret AND private) • contents:(secret OR private) • contents: secret AND tag: confidential
Log upload delay	**3600**(Default)	Random time, shown in seconds, that the client delays after the **Log upload time** before uploading the log to the Application Server log.
Log upload interval	**180**(Default)	Time, shown in seconds, that the client uploads the log to the Application Server log.
		Caution: Event logs do not upload from the client when the server or database are unavailable. Log upload will occur the next time the client connects to the server and/or database

Option	Value	Description
Log upload threshold	**10000**(Default)	Defines the number of lines written to the log before the client uploads the log to the Application Server log.
Log upload time	**05:00**(Default)	Time of day that the client uploads the log to the Application Server log.
Microsoft CA Key Provider	**Disabled**(Default)	Microsoft CA keys cannot be used for encryption.
	Enabled (Decentralized)	Microsoft CA keys can be used only for decentralized encryption.
	Enabled	Microsoft CA keys can be used for centralized and decentralized encryption.
Password Complexity	**Enforced** (Default)	Defines enforcement of password complexity. Enforcing complexity requires passwords to be at least 6 characters in length and contain at least 3 of the following: • uppercase letters (A-Z); • lowercase letters (a-z); • base 10 digits (0-9); • non-alphanumeric characters (e.g., !, $, #, %); • any other Unicode characters.
	Not enforced	Defines that passwords are not required to meet complexity requirements.
Password Minimum Length	**6** (default)	Defines the least number of characters that can make up a password. The value influences password complexity enforcement when Password Complexity is enforced. When allowing weak passwords, the minimum length can be set to 1.
Portable Encryption Capacity	**128 GB**	The maximum capacity of devices which may be encrypted using the Portable Encryption method. This value may be any number between 32 GB and 2000 GB (2 TB).

ivanti

Option	Value	Description
Online State Definition	**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.
Server Address	**Not configured** (Default)	Defines the IP address or fully qualified DNS name for the Application Server that the client connects to.
Shadow Directory	**Not configured** (Default)	Defines the local temporary directory where shadow and log files are stored before they are uploaded to the Application Server. The default directory is `\SystemRoot\sxdata\shadow\`. You cannot use a remote directory. **Note:** The specified shadow folder path must already exist.
SysLog server address	**Not configured** (Default)	Specifies the `SysLog` server address and the optional port to use.
Update Notification	**No messages**	No permissions change condition messages are displayed to the user.
	Temporary device permission changes	Displays a message when temporary permissions are changed, before the temporary permissions are to expire, and when temporary permissions are invalid.
	All device permission changes	Displays a message when any changes are made to permissions (permanent, scheduled, offline, online, and temporary) that affect the user. This is the default value.
USB Keylogger	**Disabled**	Does not detect keylogging activity.

Option	Value	Description
	Exclusive mode (Lock/ block, notify and log event)	Locks an endpoint, blocks further use and logs an event when an additional USB keyboard is detected, including keyboard emulation devices like Rubber Ducky. The user is notified about the connection change through a message box upon re-login. Immediately find and remove the detected device. If the device is a valid second keyboard, the warning can be ignored.

Default Option Precedence Rules

Default options can have different settings at the user, group, computer, or global level.

When default value option values conflict based on the type of user access defined by the administrator, a logical decision hierarchy determines which setting takes precedence.

Computer Precedence Options

Device Control establishes precedence rules for computer and computer group default option settings.

The computers options precedence rules are as follows:

1. An option value set for a specific computer supersedes all other option settings.

> **Important:** You must add computers to an existing domain or workgroup shown in the **Machine-specific settings** hierarchy of the **Device Explorer** module.

2. If no value is explicitly set for the computer, the global default option setting in the *Computer* tab applies.
3. If no global default option setting is defined for an option, the predefined Ivanti Device and Application Control system default settings apply.

ivanti

The following flowchart outlines the computer options precedence rules process.
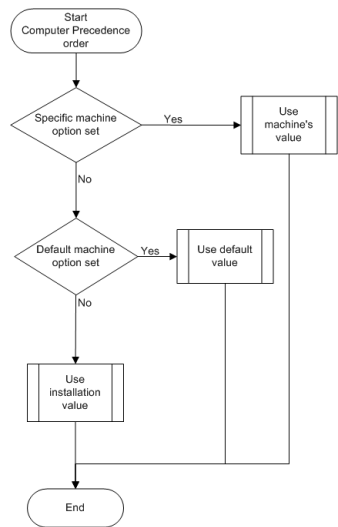
Figure 64: Computer Options Precedence

Changing Default Options

You can modify the default options settings to govern the interactions between the Application Server, database, and clients.

You can modify the option values shown in the **Computer** tab to change or reset options for computers and computer groups.

1. In the Management Console select **Tools** > **Default Options**.

    Step Result: The **Default Options** dialog opens.

2. Select the **Computer** tab.

3. In the **Option** column select the value to change.

4. In the **Option Value** panel, clear the **Default setting** check box.

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

6. In the **Option Value** panel, enter a message to be displayed to the user. This field is only available for some options, as indicated in the panel description.

7. Save the value as the default one by clicking:

Command	Description
OK	Saves the setting and close the **Default Options** dialog.
Apply	Saves the setting without closing the dialog. You can then repeat the process to change other default option settings.

Command	Description
Cancel	Closes the dialog without saving your changes.
Help	Shows the online help dialog.

After Completing This Task:

If you change a default option, send updates to all client computers for the option changes to take effect.

Sending Permissions Updates to Computers

You must distribute system setting changes to servers and computers protected by Device Control.

Updates can be sent manually by the administrator, or updates can be automatically downloaded whenever a computer or user logs in to the network.

Sending Updates to All Computers

After you define or update device permissions or file permissions, you can send the information to all client computers immediately. Otherwise, updated information will automatically upload the next time a user logs in or the computers are restarted.

1. From the Management Console, select **Tools** > **Send Updates to All Computers**.

   Step Result: The **Send updates to all computers** dialog opens.

2. Select one of the following options from the **Send updates to all computers** dialog.

Option	Description
Yes	Immediately updates connected computers. Ivanti Device and Application Control can take a long time to send updates depending on the number of computer connections. The Management Console dialog remains open until the Application Server finishes sending the updates.
No	Asynchronously updates connected computers. The Management Console dialog closes while the Application Server finishes sending the updates. You can continue working with the console while the update is done in the background.

ivanti

Option	Description
Cancel	Closes the ***Send updates to all computers*** dialog and halts the update process.

Result: Updates are distributed to all computers running the Ivanti Device and Application Control clients that are registered in the Application Server (s) online table(s). A message appears in the ***Output*** window when the updates are complete.

Remember: Any computer that is switched off, locked, or disconnected from the network receives the updates at the next network connection.

Sending Updates to a Single Computer

After you define or update device permissions or file permissions, you can send the information to a specific client computer immediately. Otherwise, updated information will automatically upload the next time a user logs in or the computer is restarted.

1. From the Management Console, select **Tools** > **Send Updates to...**.

   Step Result: The ***Select Computer*** dialog opens.

2. Click **Search**.

3. Select the computer you want to update from the list in the **Name** column.

4. Click **OK**.

   Step Result: The ***Select Computer*** dialog closes.

Result: The updates are sent to the specified computer. A message appears in the ***Output*** window showing you the update results.

Exporting Permissions Settings

You can export a permissions settings file to a target computer to transfer encryption keys and passwords when the client is not connected to theApplication Server.

You can use the device permissions export feature to update permissions settings for a computer that is not connected to the network. The source computer permissions rules apply to the target computer that the permissions settings file is copied to.

Note: Exported permissions settings data files are only valid for two weeks from the creation date.

Exporting Settings

You can export permission settings to files that can be imported to client computers.

1. From the Management Console, select **Tools** > **Export Settings**.

   Step Result: The Windows *Save as* dialog opens.

2. From the source computer, select the name of the file.

   > **Caution:** When you create file authorization settings (policy) file for deploying the client to computers that are not connected to the network (offline installation), you must name the settings file as `policies.dat` for the client setup process to work properly.

3. From the source computer, select the destination of the settings data file.

4. Click **Save**.

   Step Result: The Windows *Save as* dialog closes.

Importing Settings

You can import settings files to client computers for updates.

1. Copy the settings data file to the target computer.

2. On the target computer, right-click the client icon in the system tray.

   Step Result: A right-mouse menu opens.
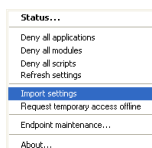
Figure 65: Ivanti Device and Application Control Client Menu

> **Note:** The right-mouse menu content varies according to the Ivanti Device and Application Control license type and hardware configuration.

3. Select *Import settings*.

   Step Result: The *Import Settings* dialog opens.

4. Select the source of the settings data file.

5. Select the settings data file.

ivanti

6. Click **Open**.

> **Step Result:** The ***Import Settings*** dialog closes.

Result: The settings are imported to the target computer.

Working with Endpoint Maintenance

The **Endpoint Maintenance** feature generates an endpoint maintenance ticket that provides provisional permission to modify, repair, or remove the client, registry keys, or special directories. The endpoint maintenance ticket is then sent to a specific computer or user.

When the client starts, a 15-byte random value key, called *Salt*, is generated. The *Salt* key is used to ensure that only authorized processes and users can perform endpoint maintenance. The *Salt* key works in conjunction with the **Client Hardening** default option value. To create an endpoint maintenance ticket when the **Client Hardening** value is set to:

- **Basic**, the *Salt* value is not required
- **Extended**, the *Salt* value is required

Endpoint Maintenance Ticket Rules

The following rules apply to creating and using endpoint maintenance tickets:

- You can only generate one endpoint maintenance ticket per client computer.
- You can define a validity period for the ticket.
    - If the ticket has not been accepted at the end of this period, the ticket is no longer valid for the client computer.
    - If a ticket is accepted, there is no expiration time limit.
- You must reboot a client computer to deactivate a valid ticket.
- A user must be logged in to accept an endpoint maintenance ticket generated specifically for the user. Otherwise, the ticket is rejected.
- If you choose to reduce the client hardening value by creating and using a maintenance ticket for a computer without choosing a user and another user logs into the same computer, the computer continues in a modified state until the next reboot.
- If the client computer is not connected to the network, you can always get the *Salt* value and hardening status of the client computer by right-clicking the client icon, located in the system tray, and selecting **Endpoint Maintenance** from the shortcut menu.
- When you create a relaxation ticket with a *Salt* value for a client computer that has a client hardening value set to **Extended**, and the client machine is running a different operating system than the administrator, the user specified must be `Administrators` because file ownership changes when files are copied to the ticket directory under different operating systems.

Creating Endpoint Maintenance Tickets

You must create endpoint maintenance tickets for clients to uninstall the Ivanti Device and Application Control application.

1. From the Management Console, select **Tools** > **Endpoint Maintenance...**.
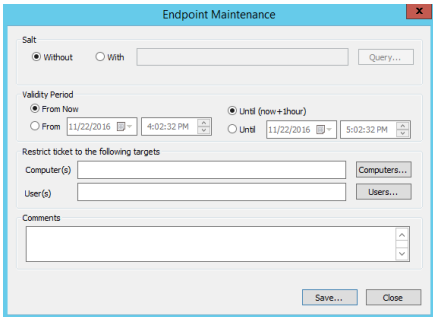
Step Result: The *Endpoint Maintenance* dialog opens.

Figure 66: Endpoint Maintenance Dialog

2. Select one of the following options from the *Salt* panel.

Option	Description
With	Creates an endpoint maintenance ticket with a *Salt* value.
Without	Creates an endpoint maintenance ticket without a *Salt* value.

3. If required, select one of the following options to obtain the *Salt* value:

- Click **Query** to obtain the *Salt* value directly from the client computer, when connected to the network.
- Right-click the **Ivanti Device and Application Control Client** icon to select **Endpoint Maintenance** for a computer that is not connected to the network.

4. In the *Validity Period* panel, specify the validity period for the ticket by selecting:

- **From Now** or **From**
- **Until(now +1 hour)** or **Until**

5. In the *Restrict ticket to the following targets* panel, select one or both of the following actions:

- Click **Computers** to select a client computer in the *Select Computer* dialog.
- Click **Users** to select a specific user in the *Select Group, User, Local Group, Local User* dialog.

6. Enter comments in the **Comments** field.

ivanti

7. Click **Save**.

> **Step Result:** The Windows *Save as* dialog opens.

8. Enter a file name in the **File name** field.

The default **Save as type** is `Maintenance Ticket.smt`.

9. Click **Close**.

> **Step Result:** The **Endpoint Maintenance** dialog closes.

10. Click **Save**.

> **Step Result:** The *Save as* dialog closes.

11. Click **Close**.

> **Step Result:** The **Endpoint Maintenance** dialog closes.

Result: Ivanti Device and Application Control saves the endpoint maintenance ticket.

After Completing This Task:

You must copy the maintenance ticket to the predefined ticket directory on the client computer. The ticket directory is specified by the `TicketDir` registry key during installation.

Authorizing Temporary Permission Offline

Administrators can create temporary permission for clients that do not have network or Internet access to the Application Server.

A key code is generated by the client and communicated by phone or e-mail to the administrator, who then enters the key code into the Management Console. When the temporary permissions request is approved through the system, the administrator provides a device unlock code for the user to enter into the client computer. The temporary permissions remain valid until the expiration date or the next time the computer connects the network.

Restriction: The **Temporary Permission Offline** tool is disabled when you are using Application Servers in **Compliance** mode.

Request Temporary Access Offline

A client user may request temporary permission from an administrator to access a device.

Users may need to temporarily modify encrypted device access permissions when they have no access the network or the Internet. For example, a user may need to read a file stored on a removable storage device or needs authorization to install a specialty software application for business use. A user communicates with an administrator to explain the required permissions and a provide device key code obtained from the client. The administrator enters this code in the Management Console and, after the request is approved, provides an unlock code to the user. The user enters the unlock code in the client.

The unlock code contains the necessary permissions for the user to access the encrypted device. The permissions are valid until they expire or the computer reconnects to the network.

1. In the Windows system tray, right-click the client icon.

2. From the right-mouse menu, select **Request temporary access offline**.

   Step Result: The **Request Temporary Access Offline** dialog opens with the **Input** page shown.

3. Select the **Device Class** from the drop-down menu.

4. Select the type(s) of permissions you are requesting from the following:

Option	Description
Read	User can read file information from the removable storage device.
Write	User can write file information to and from the removable storage device.
Encrypt	User can encrypt a removable storage device.
Decrypt	User can decrypt a removable storage device.
Export to File	Exports the public key used to encrypt the removable storage device to a file.
Export to Media	Exports the public key used to encrypt the removable storage device to the device itself.
Import	User can import data from an external encryption key.

5. In the **Lifetime of the Permissions** field, specify the following:
   - **Day(s)**
   - **Hour(s)**
   - **Minute(s)**

6. Choose a user type from the **For which user?** panel from the following:
   - **For you**
   - **For everyone**

   Note: You should use the **For everyone** option when logging the client computer in to a network that is unknown to the administrator.

7. Click **Next**.

   Step Result: The **Request Temporary Access Offline** dialog shows the **Output** page.

8. Provide the 27-character alphanumeric **Client Key** value to the administrator.

ivanti

9. Enter the 46-character alphanumeric **Unlock Key** value provided by the administrator in the **Unlock code** field.

> **Caution:** You are permitted 15 attempts to enter the correct **Unlock code** before triggering a lockout period.

10. Click **Next**.

> **Step Result:** The *Request Temporary Access Offline* dialog shows the *Finish* page.

11. Click **Finish**.

Result: The user receives a message shown in the Windows system tray that the device permission status is changed for a specified period.

Create Temporary Permission Offline

An administrator can create temporary offline permissions access for a client that cannot access the Application Server through a network connection.

Prerequisites:

The device user must request temporary offline permission access.

1. In the Management Console select **Tools** > **Temporary Permission Access Offline**.

> **Step Result:** The *Authorize Temporary Permission Offline* dialog opens.

Figure 67: Authorize Temporary Permission Offline Dialog

2. Select the **Device Class** from the drop-down menu.

3. Click **Permissions**, and choose one of the following options:

Option	Description
Read	User can read file information from the removable storage device.
Write	User can write file information to and from the removable storage device.
Encrypt	User can encrypt a removable storage device.
Decrypt	User can decrypt a removable storage device.
Export to File	Exports the public key used to encrypt the removable storage device to a file.
Export to Media	Exports the public key used to encrypt the removable storage device to the device itself.
Import	User can import data from an external encryption key.

4. In the **Lifetime of the Permissions** field, specify the following:
   - **Day(s)**
   - **Hour(s)**
   - **Minute(s)**

5. Click **Computers** and select the computer name from the list shown.

6. Click **Users** and select the user name from the list shown.

7. In the **Client Key** field, enter the alphanumeric value generated by the client.

   a) You may enter a comment in the **Comments** text field that will be shown in the associated audit log entry.

Note: **Generate** is disabled until you enter all the information required in the *Authorize Temporary Access Offline* dialog.

Step Result: Ivanti Device and Application Control validates the value entered in the **Client Key** field and displays a validation message in the *Authorize Temporary Access Offline* dialog. Otherwise, a message is shown requesting that you re-enter the **Client Key** value.

8. Click **Generate**.

   Step Result: Ivanti Device and Application Control generates a 46-character alphanumeric value that is shown in the **Unlock Key** field.

9. Communicate the **Unlock Key** value to the user.

ivanti

10. Click **Close**.

Result: The administrator receivew a message that the temporary offline permission assigned to the user will be deleted when the user reconnects the network.

After Completing This Task:

To continue temporary permissions after the user reconnects to the network, you need to assign temporary permissions to users using the *Tools* module.

Recovering Encryption Key Passwords

An administrator can recover password encryption keys for users who forget the password for an encrypted storage medium or fail to enter the password successfully after five attempts.

The user contacts the administrator and provides the encrypted medium identity and security code generated by the client. The administrator uses this information to generate a passphrase so that the user can decrypt the storage medium and re-encrypt with a new password.

Request Password Recovery

You can request an administrator to recover a lost or forgotten password for an encrypted device.

Prerequisites:

You must contact an administrator to request a password recovery key.

You can use Windows Explorer on the client to create a password recovery key request for an encrypted removable storage device.

1. Attach the device to your computer.

2. Using **Windows Explorer**, right-click the name of the encrypted device.

3. Select **Unlock medium** from the right-mouse menu.

   Step Result: The *Unlock Medium* dialog opens.

4. Click **Recover Password**.

5. From the *Recover Password* dialog, provide the administrator with the 32-character alphanumeric **Encrypted Medium ID** and the 44-character alphanumeric **Security Code**.

6. Type the 52-character alphanumeric passphrase provided by the administrator in the **Enter passphrase received from administrator** field.

7. In the **New Password** field, type a new password.

8. In the **Confirm Password** field, retype the new password.

9. Click **OK**.

Result: You receive a message that the encrypted medium has been recovered.

Recover Password Key

A administrator can recover a password encryption key for a user that has access to the client and the encrypted storage medium.

Prerequisites:

You must complete the following actions before recovering a password encryption key:

- Generate a *Medium Encrypted by user* report using the predefined template in the *Log Explorer* module.
- From the *Medium Encrypted by user* report, verify the hash number provided by the user from the client *Recover Password* dialog is an exact match.
- Request the **Encrypted Medium ID** and **Security Code** values from the user that are shown in the client *Recover Password* dialog.

You can use the Password Recovery Wizard to generate a user passphrase that a user can use with the client to generate a new password for an encrypted removable storage device.

1. In the Management Console select **Tools** > **Password Recovery wizard**.

    Step Result: The *Password Recovery Wizard* dialog opens.
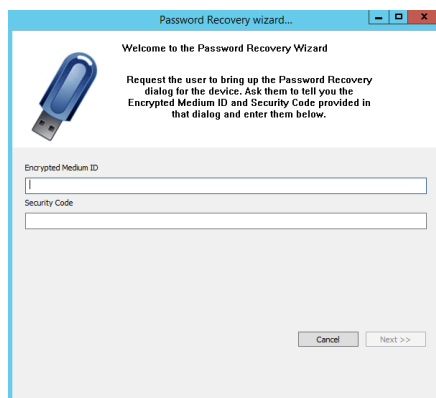
Figure 68: Password Recovery Wizard Dialog

2. Enter the 32-character alphanumeric value provided by the user in the **Encrypted Medium ID** field.

3. Enter the 44-character alphanumeric value provided by the user in **Security Code** field.

ivanti

4. Click **Next**.

> **Tip:**
> If any of the values are entered incorrectly, you will receive an error message. Re-enter the values and click **Next** again.

Step Result: The *Password Recovery Wizard* generates a 52-character alphanumeric passphrase, the device description, and the user name.

5. Communicate the **Passphrase** to the user.

6. Click **Finish**.

Result: The user can enter the passphrase in the client *Recover Password* dialog and create a new password to decrypt the encrypted storage medium.

Chapter

5

Using Reports

In this chapter:

- About Reports
- Reporting by User Role
- Working with Reports

Administrators use the **Reports** module to define and generate a variety of reports.

Reports provide a way to view current device permission policy information. Reports are generated as HTML files that are displayed in the main window of any module. You can be print, copy, convert, save, and modify as necessary. In addition to the standard reports, you can customize and generate your own reports, using the *Log Explorer* module.

About Reports

Reports are created provisionally and saved to the `Report` folder located in a temporary directory named `C:\%TEMP%`.

After saving a report, you can view it using any web browser that you system supports. You can change the date format for a report by selecting *Windows* **Control Panel** > **Regional and Language Options**. The regional options or settings vary according to the Windows operating system you are using.

Reporting by User Role

The types of reports that you can generate depend on whether you are an *Enterprise Administrator* or simply an *Administrator*.

The following table summarizes the types of reports that you can generate depending upon user role.

Table 43: Reports by User Role

User Role	Available Reports
Enterprise Administrator	All

ivanti

User Role	Available Reports
Administrator	***Client Status***, ***User Options***, ***User Permissions***, ***Device Permissions***, ***Computer Permissions***, ***Media by Users***, ***Users by Medium***, ***Shadowing by Device***, ***Shadowing by User***, ***Machine Options***, and ***Server Settings***. These are the default options for all *Administrators*.
Administrator, with **Scheduled Reports** setting of the ***User Access Manager*** dialog set to **Yes**.	All custom reports that are scheduled to run automatically using templates you have created or updated using the ***Log Explorer***.

Working with Reports

You can open, close, modify, save and print reports.

Ivanti Device and Application Control provides pre-defined reports designed to provide a comprehensive view of your computing environment for activities.

Opening a Report

You open a report by selecting a predefined report type listed in the **Reports** module.

1. From the Management Console, select **Reports**.

2. Select a report type from the list.

Result: The report you select is displayed as an HTML file in the ***Management Console*** main window.

Closing a Report

You may close a report after viewing the report that you generate.

1. Right-click the report title bar.

    Step Result: A right-mouse menu appears.

2. Click ***Close***.

Result: The report window closes. The data is saved in the temporary directory named `%Temp%` and can be archived for future reference.

Saving a Report

You may save a report that you generate.

1. From the Management Console, select **File** > **Save as**.

    Step Result: The ***Windows*** dialog for saving a web page opens.

2. Select the file path.

3. Type the file name.

4. Select the file type from the **Save as type** dropdown list.

5. Select an encoding method from the **Encoding** dropdown list.

6. Click **Save**.

    Step Result: The *Windows* dialog for saving a web page closes.

Printing a Report

You may print a report that you generate.

1. From the Management Console, select **File** > **Print**.

    Step Result: The standard Windows *Print* dialog opens.

2. Select a printer.

3. Click **Print**.

    Step Result: The Windows *Print* dialog closes.

Available Reports

Using the **Reports** module you can generate the following Device Control reports.

Table 44: Available Reports

Report	Description
User Permissions	Generates a report of the permission rules defined for each user or user group that you specify.
Device Permissions	Generates a report of all permissions rules assigned to the devices defined in the **Device Explorer** module.
Computer Permissions	Generates a report of the permissions rules defined for specific computers.
Media by Users	Generates a report of the permissions rules defined for users, classified by medium.
Users by Media	Generates a report of the permissions rules defined for removable media, classified by user.
Shadowing by Device	Generates a report summary of file data copied or read by users, for a specified date range.
Shadowing by User	Generates a report summary of file data copied or read by users of removable storage devices, classified by device class.

ivanti

Report	Description
Machine Options	Generates a report of current computer option settings.
Client Status	Generates a report of the hardening options, client version, and log and file policy status.
Server Settings	Generates a report of options, registry values, and settings for installed Application Servers.

User Permissions Report

You can generate a report that shows the permission rules defined for each user or user group that you specify. You may select one or more users to view report results for.

The name of the specific user you select is shown preceding the report results.

Figure 69: User Permissions Report

The following table describes the report columns.

Table 45: User Permissions Column Descriptions

Column	Description
Device	Shows the name of the device class or a specific device.
Computer	Shows whether default permission settings apply to all computers or computer-specific permission setting apply to a specific computer or groups of computers.

Column	Description
Permissions	Shows the type(s) of permission that applies to the device class.
Priority	Shows whether the permission is applied with a high or low priority. A low priority indicates that computer-specific exceptions to the permissions rules shown can be applied.
Details	Show whether the file shadowing and/or copy limit rules are applied to the permission rule.
User/Group Name	Shows the name of the user or user group assigned to the permission rule.

Device Permissions Report

You can generate a report that shows all permissions rules assigned to the devices defined in the **Device Explorer** module.

Figure 70: Device Permissions Report

The following table describes the report columns.

Table 46: Device Permissions Column Description

Column	Description
Device	Shows the name of the device class or a specific device.
Computer	Shows whether default permission settings apply to all computers or computer-specific permission setting apply to a specific computer or groups of computers.
User/Group Name	Shows the name of the user or user group assigned to the permission rule.

ivanti

Column	Description
Permissions	Shows the type(s) of permission that applies to the device class.
Priority	Shows whether the permission is applied with a high or low priority. A low priority indicates that computer-specific exceptions to the permissions rules shown can be applied.
Details	Show whether the file shadowing and/or copy limit rules are applied to the permission rule.

Computer Permissions Report

You can generate a report that shows the permissions rules defined for specific computers.

Computer Permissions

Computer	User / Group Name	Devices	Permissions	Priority	Details
COMPUTER 01	No users and/or computers you may manage have permissions set on this device				

Figure 71: Computer Permissions Report

The following table describes the report columns.

Table 47: Computer Permissions Column Description

Column	Description
Computer	Shows the name of the computer selected for the report.
User/Group Name	Shows the name of the user or user group assigned to the permission rule.
Device	Shows the name of the device class or a specific device.
Permissions	Shows the type(s) of permission that applies to the device class.
Priority	Shows whether the permission is applied with a high or low priority. A low priority indicates that computer-specific exceptions to the permissions rules shown can be applied.
Details	Show whether the file shadowing and/or copy limit rules are applied to the permission rule.

Media by User Report

You can generate a report that shows the permissions rules defined for users, classified by medium.
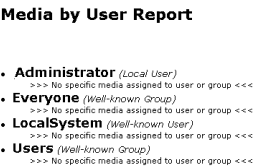

Figure 72: Media by User Report

The following table describes the report rows.

Table 48: Media by User Row Description

Row	Description
User Name	Name of the user or user group assigned to the permission rule.
Permission Rules	Removable storage medium permissions rules.

Users by Medium Report

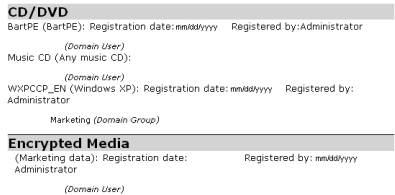You can generate a report that shows the permissions rules defined for removable media, classified by user.

Figure 73: User by Medium Report

The following table describes the report rows.

Table 49: User by Medium Row Description

Row	Description
Medium Name	Name of the removable storage medium.
User Name	Name of the user authorized to use the removable storage medium.

ivanti

Shadowing by Device Report

You can generate a report that shows a summary offline data copied or read by users, for a specified date range.

Shadowing by Device

Device	User Name	Computer Name	Total Size (MB)
Removable	administrator	abc.de.fgh	9.296148
Removable	bill	abc.de.fgh	2349.134
Removable	mary	abc.de.fgh	22.5
Removable	john	abc.de.fgh	135.3
Removable	jane	abc.de.fgh	19.29

Figure 74: Shadowing by Device Report

The following table describes the report columns.

Table 50: Shadowing by Device Column Description

Column	Description
Device	Shows the device class name.
User Name	Shows the name of the user assigned to the device.
Computer Name	Shows the name of the computer assigned to the device.
Total Size(MB)	Show the amount of file data copied or read by the device.

Shadowing by User Report

You can generate a report that shows a summary of file data copied or read by users of removable storage devices, classified by device class.

Shadowing by User

User Name	Computer Name	Device	Total Size (MB)
administrator(9.296148 MB)	com55.xx.xx	Removable	9.296148
bill(2349.134 MB)	sales.12.12	Removable	2349.134
mary(22.5 MB)	admin.14.14	Removable	22.5
john(135.3 MB)	admin.23.23	Removable	135.3
jane(19.29 MB)	admin.71.71	Removable	19.29

Figure 75: Shadowing by User Report

The following table describes the report columns.

Table 51: Shadowing by User Column Description

Column	Description
User Name	Shows the name of the user assigned to the device.
Computer Name	Shows the name of the computer assigned to the device.

Column	Description
Device	Shows the device class name.
Total Size(MB)	Show the amount of file data copied or read by the device.

Machine Options

You can generate a report that shows options settings status for Ivanti Device and Application Control default options.

Figure 76: Machine Options Report

The following table describes the report columns.

Table 52: Machine Options Column Description

Column	Description
Option	The name of the option shown in the **Default Options** dialog.
Machine	Complete computer name including domain. **Default** is the value configured for all computers and represents the default value.
Setting	The actual value of the option; the asterisk (*) indicates that the option is not configured and represents the default value.

ivanti

Client Status

You can generate different types of client status reports that show the hardening options, client version, and log and file policy status.

You can choose from the following report options.

- **All clients listed in the database**
- **Clients with outdated permissions**
- **Clients that are online**
- **Clients that are offline**
- **Select my own group of clients**

Client Status Report:: Server XY

Computer	Client Version	Client Hardening Status	Client Last Log Upload	Client Policy Date	Client Policy Status	Client Policy Source
user1.xy.com	4.4.0.0	disabled/inactive	mm/dd/yyyy hh/mm/ss	mm/dd/yyyy hh/mm/ss	Offline	Server: XY
user2.xy.com	pre 4.4.0	<not available>	<not available>	<not available>	Offline	Unknown
user3.xy.com	4.4.0.0	disabled/inactive	mm/dd/yyyy hh/mm/ss	<not available>	Offline	Unknown
user4.xy.com	pre 4.4.0	<not available>	<not available>	<not available>	Offline	Unknown

Figure 77: Client Status Report

The following table describes the report columns.

Table 53: Client Status Column Descriptions

Column	Description
Computer	Shows the complete computer name including domain. **Default** is the value configured for all computers and represents the default value.
Client Version	Shows the Ivanti Device and Application Control client version running for the computer(s).
Client Hardening Status	Shows the client hardening option running for the computer(s).
Client Policy Date	Show the date for the policy file that is applied to the computer(s).
Client Last Log Upload	Shows the last time that the client uploaded log events to the Application Server(s).
Client Policy Status	Shows the status of the current policy file. • `Unknown status`: The status is unknown. • `Offline`: The client has not connected to the server recently. • `Up-to-date`: The client connected to the server recently and has the latest policies. • `In-sync`: The client connected to the server recently, has the latest policies, but has not refreshed the policies. • `Obsolete`: The client connected to the server recently, but an issue occured while retrieving the most recently policies.

Column	Description
Client Policy Source	Shows the complete file for the policy file name running on the client name including file path. • `Illegal policy source`: Client policies are coming from an unknown database. • `Server`: Client policies are coming from a server. • `Import file`: Client policies are coming from a file. • `Unknown`: The source of client policies is unknown.
Compliance Mode	Shows the client's **Compliance Mode** status. • `Disabled`: The client is not in compliance mode. • `FIPS`: The client is operating in FIPS compliance mode (FIPS 140-2 Level 2). • `CPA`: The client is operating in CPA compliance mode. This column is only shown if Ivanti Device and Application Control is licensed for FIPS or CPA compliance mode.

Server Settings

You can generate a report that shows the Application Server configuration.

Server Settings Report

Setting	Machine	Value
commVer	secsrv.lu.Lu	2
DataFileDirectory	secsrv.lu.Lu	C:\DataFileDirectory\
DbConnectionCount	secsrv.lu.Lu	20
DbConnectionMaxCount	secsrv.lu.Lu	(*) 40
DbConnectionPoolTimeout	secsrv.lu.Lu	(*) 15
DbConnectionString	secsrv.lu.Lu	Provider=sqloledb;Data source=SECSRV\SQLEXPRESS;Initial Catalog=sx;Trusted_Connection=yes
DbConnectionTimeout	secsrv.lu.Lu	(*) 5
DbInitializationDelay	secsrv.lu.Lu	300
DbLossLatency	secsrv.lu.Lu	(*) 3600
DbPingPeriod	secsrv.lu.Lu	(*) 60
edrBatMaxDuration	secsrv.lu.Lu	(*) 30
edrBatMinEntries	secsrv.lu.Lu	(*) 10000
edrBatThreads	secsrv.lu.Lu	(*) 2
edrDspPause	secsrv.lu.Lu	(*) 0
edrDspPauseFail	secsrv.lu.Lu	(*) 60
edrDspRetryCount	secsrv.lu.Lu	(*) 5
edrDspThreads	secsrv.lu.Lu	(*) 1
edrQueLength	secsrv.lu.Lu	(*) 3
edrStaPeriod	secsrv.lu.Lu	(*) 43200
edrTmpTimeout	secsrv.lu.Lu	(*) 30
Log file name	secsrv.lu.Lu	sxs.log
Log to console	secsrv.lu.Lu	no
Log to dbwin	secsrv.lu.Lu	no
Log to file	secsrv.lu.Lu	no
MaxRpcCalls	secsrv.lu.Lu	(*) 50
MaxSockets	secsrv.lu.Lu	5000
Port	secsrv.lu.Lu	65129
Protocols	secsrv.lu.Lu	(*) ncacn_ip_tcp
RpcProtectionLevel	secsrv.lu.Lu	6
SecureInterSxs	secsrv.lu.Lu	no
ServerCertSerial	secsrv.lu.Lu	(*)
ServerName	secsrv.lu.Lu	(*)
SndPort	secsrv.lu.Lu	33115
SxdConnectAttempts	secsrv.lu.Lu	(*) 10
SxdConnectDelayBeforeRetry	secsrv.lu.Lu	(*) 500
SxdConnectTimeoutMSec	secsrv.lu.Lu	5000
SxdPort	secsrv.lu.Lu	33115
TLSCertFriendlyName	secsrv.lu.Lu	
TLSCertID	secsrv.lu.Lu	
TLSCertIssuer	secsrv.lu.Lu	
TLSCertName	secsrv.lu.Lu	
TLSMaxSockets	secsrv.lu.Lu	0
TLSPort	secsrv.lu.Lu	65229

Figure 78: Server Settings Report

ivanti

The following table describes the report columns.

Table 54: Server Settings Column Description

Column	Description
Setting	Shows the name of the **Default Options** setting or registry key value.
Machine	Shows the Application Server name including domain; `Default` is the value configured for all computers and represents the default value.
Value	The actual value of the option; the asterisk (*) indicates that the option is not configured and represents the default value.

Chapter

6

Using Client Deployment

In this chapter:

- Client Deployment Window
- Creating Deployment Packages
- Adding Computers
- Deploying Packages
- Querying Client Status

Ivanti Device and Application Control provides the Client Deployment tool that performs silent, unattended installation of the client to computers distributed throughout your network.

Client deployment employs the Microsoft Installer (MSI) service that distributes installation packages that you create. After deployment is complete, you can monitor the computers and status of the client deployment packages throughout your network.

Client Deployment Window

The ***Ivanti Device and Application Control Client Deployment*** dialog is the primary administrative interface used for creating and deploying client installation packages.

The ***Ivanti Device and Application Control Client Deployment*** dialog consists of two panels:
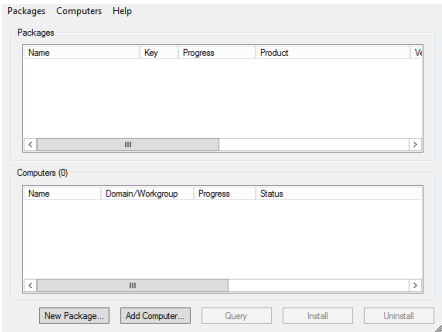
- ***Packages***
- ***Computers***

Figure 79: Client Deployment Dialog

ivanti

Packages Panel

The following table describes the columns in the **Packages** panel.

Table 55: Packages Panel Column Descriptions

Column	Description
Name	Shows the name of the deployment package.
Key	Indicates whether the public key is included in the deployment package.
Progress	Shows the installation progress of the deployment package for a computer.
Product	Shows the name of the Ivanti Device and Application Control product included in the deployment package.
Version	Shows the version of the Ivanti Device and Application Control product included in the deployment package.
Servers(s)	Shows the name of the server(s) that connect to the selected client computer.
Last deployment	Shows the date and time of the last client package deployment.
License	Shows the type of product licensed.
Policies	Shows whether permission policies are imported.
TLS	Shows whether the TLS communication protocol is in use.

Packages Menu

You can administer deployment packages from the **Packages** menu.

The following table describes the **Packages** menu.

Table 56: Packages Menu Options

Option	Description
New	Creates new deployment packages.
Delete	Deletes a selected deployment package.
Rename	Renames a selected deployment package.
Import public key	Copies the `sx-public.key` in to the deployment package directory folder.
Set Licenses	Adds a license to deployment package installed in the *serverless* mode.
Set Policies	Allows addition of an Application Server to retrieve the policy file (`*.dat`) for a specific deployment package.
Test Connection	Allows verification of connection with the Application Server for the specific deployment package, before deploying the package.

Option	Description
Install	Installs the selected deployment package.
Uninstall	Uninstalls the selected deployment package for the computers listed in the ***Computers*** panel.
Open last report	Displays a report describing the last install or uninstall, indicating the status of the install or uninstall activity.
Options	Allows modification of the directory where deployment packages are stored.

Computers Panel

The following table describes the columns in the ***Computers*** panel.

Table 57: Computers Panel Column Descriptions

Column	Description
Name	Shows the name of the computer associated with a deployment package.
Domain/Workgroup	Shows the domain or workgroup that a computer belongs to.
Progress	Shows the installation progress of the deployment package for a computer.
Status	Describes the attributes associated with the deployment package for a computer, including the: • Client operating system and version • TLS communication protocol used • Client hardening status

Computers Menu

You can administer deployment packages by computer from the **Computers** menu.

The following table describes **Computers** the ***Computers*** menu.

Table 58: Computers Menu Options

Option	Description
Add	Adds one or more computers to the list of computers for the specific deployment package.
Remove	Removes one or more computers from the list of computers for the specific deployment package.
Import	Imports a list of computers from an external ASCII or Unicode text file.

ivanti

Option	Description
Export	Exports a list of computers to an external ASCII or Unicode text file.
Change TLS mode	Allow changes to the TLS communication protocol used for specific computers.
Reboot	Forces specific computers to restart.
Query	Queries the client version and driver status for every computer listed.
Progress details	Displays the results of the install, uninstall, or query operation for specific computers.
Open last log	Opens the last installation log for specific computers.

Creating Deployment Packages

When you create a Ivanti Device and Application Control client deployment package, the Client Deployment tool copies the local client setup `.MSI` file and creates an `.MST` transform file that is linked to the `.MSI` file.

Prerequisites:

Before you can successfully create an Ivanti Device and Application Control client deployment package, you must:

- Have access to the `Client.msi` or `Client64.msi` file on the computer where you will deploy the client packages.
- If there is a firewall between the Client Deployment tool installed on the client computer and the targeted computer(s), you must verify that firewall ports are open.
- Synchronize the Application Server's system clock with the Ivanti Device and Application Control database server's system clock using the Microsoft Windows time service. See Time Service (http://support.microsoft.com/kb/816042) for details about using the Microsoft Windows time service.
- Start the Windows Remote Registry service on the remote client computer.
- Have a valid digital certificate on the client computer that deploys the client and test the TLS connection between the Application Server.

Important: In Windows Server 2008 operating systems there is a security setting which blocks access to the **admin$** share required for Client Deployment . When the following error message is `received failed to start the remote registry service. Access is denied` you must confirm the correct registry keys. Check the following registry keys:

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system \LocalAccountTokenFilterPolicy?` and change the DWORD entry to `1` to resolve the access to **admin$** share problem.
- If the **LocalAccountTokenFilterPolicy** registry entry does not exist then it has to be created.

The `.MSI` file contains the information necessary deploy the Ivanti Device and Application Control client to targeted computers.

1. From the *Ivanti Device and Application Control Client Deployment* dialog, click **New Package**.

   Step Result: The *New Packages* dialog opens.
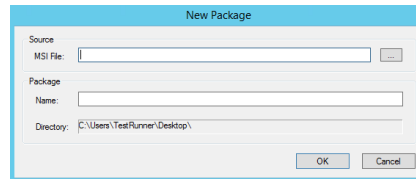

Figure 80: New Packages Dialog

2. To select deployment package, select the **ellipses** from the *Source* panel.
3. In the *Package* panel, enter a name for the deployment package in the **Name** field.

4. Click **OK**.

> **Step Result:** The *Options - Ivanti Device and Application Control Installation Transform* dialog opens.

Figure 81: Options - Ivanti Device and Application Control Installation Transform Dialog

> **Attention:** The shaded options are only valid when are installing versions client lower than 4.3. These options are:
>
> • **Do not validate name or IP before installing** - Provides an Application Server address or name that is not currently available but is accessible after deployment.
> • **Enable wireless LAN protection** - An option available in 2.8 clients lower that is now deprecated by permissions rules.

5. Click **Import public key**.

6. Select the `sx-public.key` file.

If there is no `sx-public.key` file in your client setup folder, then the installation continues using the default public key.

> **Step Result:** The Client Deployment tool copies the selected public key to the appropriated folder for client deployment.

7. In the **Name or IP** field(s), enter the fully qualified domain name(s) or IP address(es) for the Application Server (s) installed in your environment.

> **Tip:** You may enter alternative port numbers, as necessary. When you do not specify fully qualified domain name(s) or IP address(es), the Ivanti Device and Application Control clients are deployed in a *serverless* mode.

8. If Ivanti Device and Application Control is set up to use more than one Application Server, you may select the **Automatic Load Balancing** check box to allow clients to contact any available Application Server.

9. To specify that the Ivanti Device and Application Control client uses the TLS communication protocol, select the **TLS** check box.

10. To disable Device Control for NDIS devices, select the **Disable NDIS protection for devices** check box.

> **Note:** NDIS enables Device Control to control 802.1x wireless adapters. If you do not need this protection, you may disable it here.

11. To validate the fully qualified domain name(s) or IP address(es) for the Application Server (s), click **Test Connection**.

   Step Result: You will receive a confirmation message indicating whether the server connection is successful or not. If not, you follow the error resolution directions.

12. From the *"Add or Remove Programs" list options* panel, select one of the following options:

Option	Description
List the program with a "Remove button"	Displays the Ivanti Device and Application Control product name in the **Add or Remove Program** list in the Windows **Control Panel** with the **Remove** option.
List the program but suppress the "Remove button"	Displays the Ivanti Device and Application Control product name in the **Add or Removes Program** list in the Windows **Control Panel** without the **Remove** option.
Do not list the program	Does not display the Ivanti Device and Application Control product name in the **Add or Remove Program** list in the Windows **Control Panel**.

13. To suppress preventive actions associated with Application Control, select the **Suppress preventive actions related to the Application Control feature** check box.

14. In the **Specify the policy import time-out (in minutes)** field, enter a numerical value.

15. Click **OK**.

Result: The client deployment package files are copied to the specified directory. The new deployment package is listed in the *Packages* panel of the *Ivanti Device and Application Control Client Deployment* dialog.

After Completing This Task:
Verify the location of the `Client.mst` file created in the deployment package folder you specified, by selecting **Packages** > **Options** from the *Ivanti Device and Application Control Client Deployment* dialog.

ivanti

Adding Computers

You can add computers where the client is deployed with the Client Deployment.

1. Select **Start** > **Programs** > **Ivanti** > **Ivanti Device and Application Control Management Console** > **Ivanti Device and Application Control Client Deployment**.

   Step Result: The *Ivanti Device and Application Control Client Deployment* dialog opens.
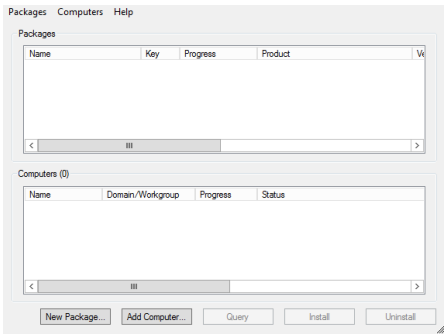

   Figure 82: Client Deployment Dialog

2. Click **Add Computer**.

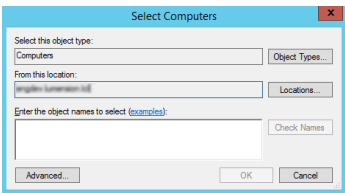   **Step Result:** The *Select Computers* dialog opens.

   Figure 83: Select Computers Dialog

3. In the **Enter the object names to select field**, select **ObjectName** to enter the names of the computers to add to the list.

   Note: ObjectName is the only format you can select to add computers.

Object Name	Example
Display Name	FirstName LastName
ObjectName	Computer1
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.

4. Click **OK**.

Result: The computer names are listed in the *Computers* panel of the *Ivanti Device and Application Control Client Deployment* dialog.

Deploying Packages

The **Ivanti Device and Application Control Client Deployment** tool silently deploys Ivanti Device and Application Control client for unattended installation, using deployment installation packages.

Prerequisites:

Before you can successfully deploy Ivanti Device and Application Control clients, you must:

- Create deployment packages.
- Be a member of the Local Administrators group for all targeted computers.
- If you will be deploying clients to computers that are not connected to the Application Server, you must import the policies.dat setting file to the same directory where the deployment packages that you create are saved.

1. Select **Start** > **Programs** > **Ivanti** > **Ivanti Device and Application Control Management Console** > **Ivanti Device and Application Control Client Deployment**.

Step Result: The *Ivanti Device and Application Control Client Deployment* dialog opens.
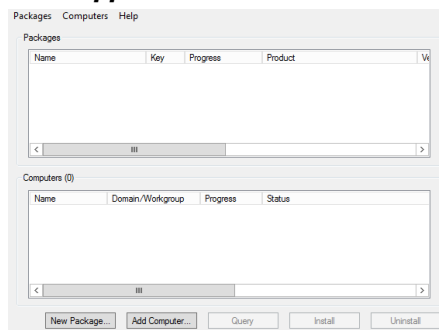
Figure 84: Client Deployment Dialog

ivanti

2. If you are deploying the client to computers that are not connected (offline) to the Application Server, you must first export the policy file `policies.dat` to the targeted computer(s), as follows.

a) Select **Packages** > **Options**.
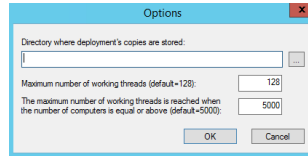
Step Result: The **Options** dialog opens.

Figure 85: Options Dialog

b) To select the directory to store deployment copies, click the **ellipses**.

You must specify a directory that is different than a system drive root directory or directory containing existing files. When the **Ivanti Device and Application Control Client Deployment** tool runs on different computers, you may want to specify a shared directory where all instances of the **Ivanti Device and Application Control Client Deployment** tool have access to the deployment packages.

Important: Installing a client using exported policies works well when `policies.dat` is placed locally in the same directory as `client.exe`. However if the policies.dat file is placed on a file share you must change the security of the share directory so that computer accounts are able to

access it must have access to it through `LocalSystem`.

c) Click **OK**.

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

3. To add computers for client deployment, select the computer name(s).

You can select multiple computers while pressing the CTRL key.

4. Click **OK**.

5. From the **Packages** panel, select a deployment package from the list.

a) From the **Computers** panel, you may also select a subset of targeted computers for package deployment.

6. Click **Install**.

    Step Result: Because deployment requires restarting the target computer(s), the ***Install/Uninstall/Reboot/Options*** dialog opens.
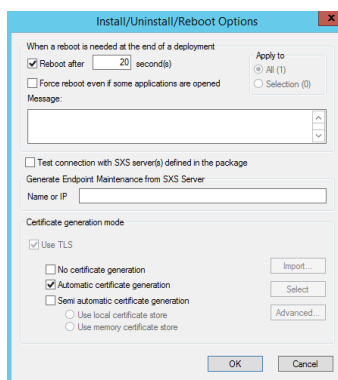

Figure 86: Install/Uninstall/Reboot/Options Dialog

7. From the ***When a reboot is needed at the end of a deployment*** panel, select the following options, as necessary:

Option	Description
Reboot after (x) second(s)	Restarts the target computer(s) after deployment, within the period that you specify.
Force reboot even if some applications are opened	Forces the target computer(s) to restart after deployment, regardless of open applications.
Apply to	Applies reboot options to **All** target computers or a **Selection** of computers, representing the subset chosen when selecting the deployment package.
Message	You can type a message that users receive when the target computer(s) restart.

8. To generate a certificate semi-automatically during setup, select the computer certificate location and parameters from the following options.

Option	Description
Use local certificate store	Generates a digital certificate during installation by using a signature certificate located in the local user store.
Use memory certificate store	Generates a digital certificate during installation by using a signature certificate located in a specified file.

ivanti

Option	Description
Import	Imports a signature certificate into the local user store.
Select	Allows you to select a signature certificate located in a specified file
Advanced	Specifies the certificate parameters for the **Cryptographic service provider**, **Key length**, **Validity**, and **Signature**.

9. Click **Next**.

10. Click **OK**.

> **Step Result:** The *Ivanti Device and Application Control Client Deployment* dialog reopens showing the deployment progress for the computer(s) added to the deployment package selected.
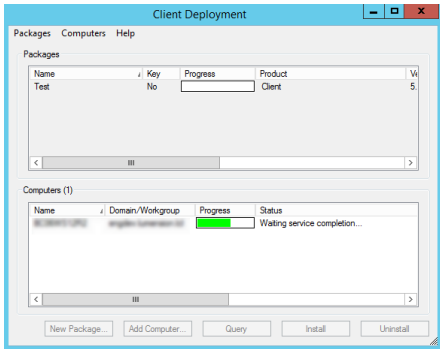>
> Client Deployment

Figure 87: Dialog - Computer Progress

> The **Progress** column in the *Computers* panel displays a progress bar showing the deployment status for each computer. The **Progress** column in the *Packages* panel displays a progress bar showing the overall deployment status the deployment package. The following table describes the status bar.

Color	Status Condition
Turquoise	Task completed successfully.
Green	Task in progress with no warning.
Yellow	Task in progress or completed with warnings.

Color	Status Condition
Red	Task in progress or stopped with an error.

Result: The deployment package is silently deployed the designated computer(s) or computer group(s).

After Completing This Task:

If you chose to restart the client after deployment is complete, the **System Shutdown** dialog displays with the message created when selecting the reboot option(s), as illustrated by the following example.
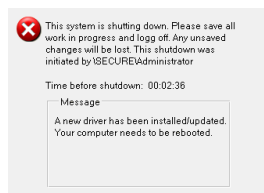

Figure 88: System Shutdown Dialog

Querying Client Status

You can use the Client Deployment **Query** for target computers to determine the operating system that is running, whether a client is installed and which version, whether hardening is enabled, and whether the Ivanti Device and Application Control components are running.

1. Select **Start** > **Programs** > **Ivanti** > **Ivanti Device and Application Control** > **Ivanti Device and Application Control Management Console** > **Ivanti Device and Application Control Client Deployment**.

   Step Result: The **Ivanti Device and Application Control Client Deployment** dialog opens.

2. Click **Query**.

ivanti

3. From the **Packages** panel, select a deployment package from the list.

Result: The **Computers** panel lists the computers where the deployment package(s) are installed. The **Status** column describes the client operating system and version, TLS protocol selection, and client hardening status.
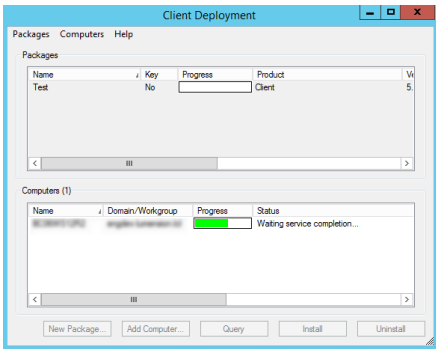

Figure 89: Client Deployment Dialog

Chapter

7

Using the Device Control Client

In this chapter:

- Device Control Client Menu
- About Encrypting Devices
- Using the Encrypt Medium Utility
- Transferring Encryption Keys

The 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 permission, copy limit, shadowing, and file filtering rules that apply to devices and device classes for the Device Control client user that is logged on.
Refresh Settings	Updates permission settings for the Device Control client.
Import Settings	Allows you to import a permission setting file from any external source to the computer running the Device Control client.
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.
Endpoint Maintenance	Allows the Device Control administrator to perform endpoint maintenance, as necessary, for the Device Control client.

ivanti

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:

- Open portable media.
- Decrypt encrypted removable storage devices.
- Manage user permissions for 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. See Defining Default Options for more information about using default options.

You can specify additional users by passphrase or 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. Select **My Computer**.

2. Right-click the CD/DVD label name to encrypt.

   Step Result: The CD/DVD encryption right-click menu opens.
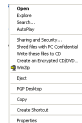

Figure 90: CD/DVD Encryption Menu

3. Click **Create an Encrypted CD/DVD...**

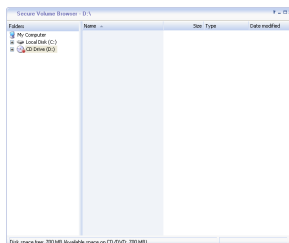   **Step Result:** The *Secure Volume Browser* dialog opens.

Figure 91: 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 right-click menu opens.

Figure 92: CD/DVD Menu

6. Click **Burn the CD/DVD**.

   Step Result: After retrieving information for the logged in user, the **Add Passphrase** dialog opens.
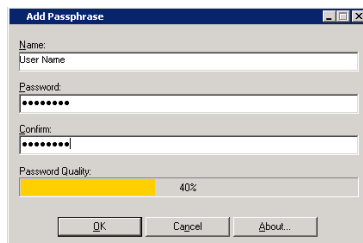

Figure 93: Add Passphrase Dialog

> **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.
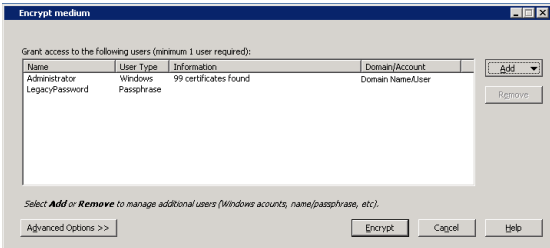

Figure 94: Encrypt Medium Dialog

9. You may add user access the device, by clicking **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 are shown in the right-mouse menu that opens.

Figure 95: Encrypt Medium Dialog - Add User
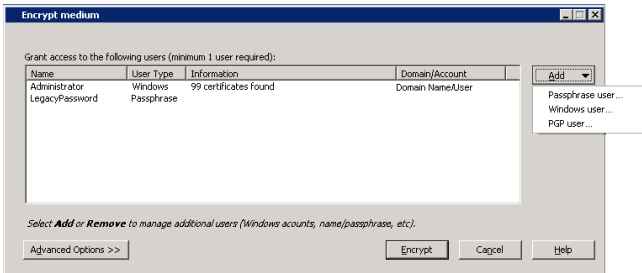
10. Select one of the following options:

These options depend upon your environment and configuration.

Option	Description
Passphrase user	Adds a user name with password access.
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.

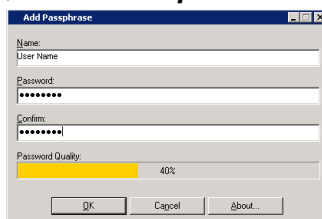If you select **Passphrase user**, the ***Add Passphrase*** dialog opens.

Figure 96: Add Passphrase Dialog

If you select **Windows user**, the ***Select Users or Groups*** dialog opens.
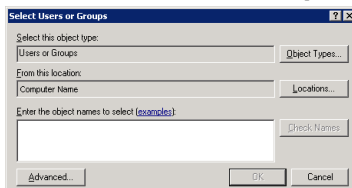
Figure 97: Select Users or Groups Dialog

11. Depending on the option you select, 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
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.

ivanti

14. When you finish adding users, click **Next**.

> **Step Result:** The ***Burning Encrypted Media*** dialog opens.
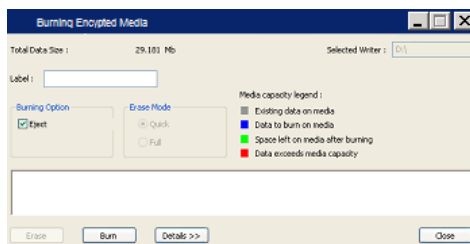
Figure 98: Burning Encrypted Media Dialog

> **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. To verify the users are added to the encrypted medium, refer to Managing Devices. 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.

> **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.`

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. Select **My Computer**.

2. Right-click the name of the device listed under ***Devices with Removable Storage***.

> **Step Result:** A right-mouse menu opens.

3. From the right-mouse menu, click **Manage Device**.

> **Step Result:** The *Manage Device* dialog opens.
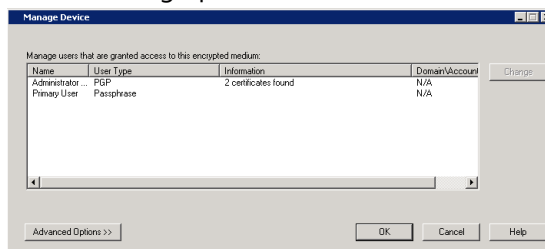
Figure 99: Manage Device Dialog

4. Select a user from the list shown.

5. 4. Click **Change**.

> **Step Result:** The *Change Password* dialog opens.
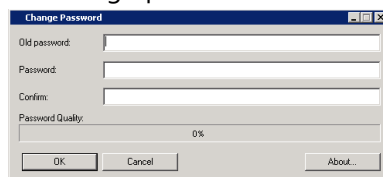
Figure 100: Change Password Dialog

6. Type your current password in the **Old Password** field.

7. Type a new password in the **Password** field.

8. Retype the new password in the **Confirm** field.

9. Click **OK**.

> **Step Result:** The *Change Password* dialog closes and you return to the *Manage Device* window.

10. 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.

The following steps describe how to change your password.

1. Click **Unlock**.

ivanti

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.

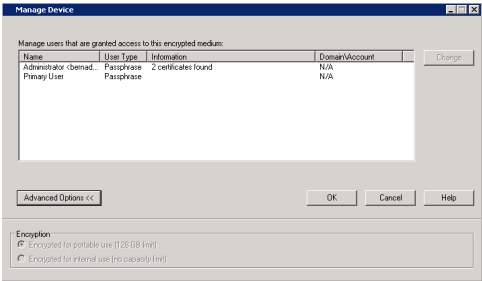| Option	Description
Encrypted for portable use (2 TB limit)	Allows use of an encrypted device on any computer running Microsoft® Windows®.
Encrypted for internal use (no capacity limit)	Allows use of devices only inside your network on computers that are managed by Device Control. There is no limit to the capacity for the encrypted device.

Step Result:

Figure 101: Advanced Options - Manage Device Dialog

7. Click **OK**.

Result: You receive a confirmation message 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 the Windows Explorer.

To unlock an encrypted removable storage device:

1. Select **Start** > **My Computer**.
2. Right-click the name of the device listed under ***Devices with Removable Storage***.
3. Click **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.

> **Note:** The message `Device Not Ready` may appear when a user attempts to access a CD/DVD or removable while logs are being fetched immediately after unlock.

Opening Portable Media

You can open encrypted removable storage devices as portable media using the Windows Explorer.

To open an encrypted removable storage device as a portable medium:

1. Select **My Computer**.

   Step Result: A right-mouse menu opens.

2. From the right-mouse menu, click 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.

Decrypt a removable storage medium using the Windows Explorer.

> **Caution:** Decrypting a medium is the same as formatting a medium and all data on the medium will be erased.

1. Select **My Computer**.
2. Right-click the name of the device listed under ***Devices with Removable Storage***.

   Step Result: A right-mouse menu opens.

ivanti

3. From the right-mouse menu, click **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:

- 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.
- Upgrade the encryption on devices encrypted using a Citrix virtual endpoint.

Setting Encrypt Medium Utility Options

The **Encrypt Medium** utility options that the user sees on the client are governed by the Device Control default options set by the administrator.

The **Encrypt Medium** utility requires an administrator to set the default options that govern the client behavior for the **Encrypt Medium** utility. These default options are shown when selecting the **Tools** > **Default Options** > **Computer** tab from the navigation bar in the Management Console. For more information about default options, see the Computer Tab section. Options which affect the behaviour of the **Encrypt Medium** utility include:

- Selecting an encryption access method that determines whether the device can be used outside of your network.
- Adding Windows® or password users that can access the device.
- Saving all existing data on the device during encryption.
- Erasing data from unused sectors of the device during encryption.

1. From the Management Console, select **Tools** > **Default Options** > **Computer** tab.

2. Set the default options described in the following table. See the Default Options Page for additional information about working with default options and the default settings for the options described in the following table.

The following table describes device encryption default options and the resulting behaviour for the **Encrypt Medium** utility.

Table 59: Setting Encrypt Medium Default Options

Default Option	Setting	Encrypt Medium Behavior
Encryption notification	Create message in the **Encryption Notification** field.	Prompts a user to encrypt a device attached to a computer running the client when launching the **Encrypt Medium** utility.
Encryption Grace Period	Enter a time value in seconds in the **Encryption Grace Period** field.	Allows a user a grace period to use a device encrypted without **Easy Exchange** to use the device after attaching and detaching the device from the client computer before the client uploads a log to the Application Server.
Encryption Retain Data **Attention:** If no data is stored on the device before encryption, the **Data Integrity** page is not visible during encryption.	**Selected**	The user can view the **Data Integrity** page and choose that data already stored on the device is saved during the encryption process. The check box in the **Encrypt Medium** dialog on the client is selected and can be deselected by the user.
	Forced Unselected	The check box in the **Encrypt Medium** dialog on the client is deselected. This option preset by the administrator and cannot be modified by the user.
	Unselected	The check box in the **Encrypt Medium** dialog on the client is deselected and can be selected by the user.
	Forced Selected	The check box in the **Encrypt Medium** dialog on the client is preselected. This option preset by the administrator and cannot be modified by the user.
Clear unused space when encrypting	**Enabled**	The user can view the **Secure Unused Space** page and choose that unused sectors on the device be wiped clean of data during the encryption process.
Microsoft CA Key Provider	**Enabled**	

ivanti

Default Option	Setting	Encrypt Medium Behavior
	Enabled (Decentralized)	The user can view the **User Access** and **Add Additional User** pages to add a Windows user with password access.

Important: The option to add a passphrase user is always visible to the user from the **Encrypt Medium** utility.

Result: You have configured the specific behaviour of the **Encrypt Medium** utility. For additional information about using encryption scenarios, see the following topics.

- Portable Device Encryption Permission
- Nonportable Device Encryption Permission
- Portable and Nonportable Device Encryption Permission

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:

You may set the **Password Attempts Limit** option for user password requirements, using the **Tools** > **Default Options** > **Computer** tab.

For detailed information about using default options, refer to Computer Tab on page 146.

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.

Computers that are served applications via Citrix XenApp (version 6 or higher) but do not have the Device Control Client installed, can use the **Secure Volume Browser** (SVolBro) to encrypt devices on the unmanaged endpoint.

Note:

- The **Secure Volume Browser** must already be installed on the computer or published to the user.
- Only up to 2 GB of space can be used on a portable device encrypted using Citrix SVolBro.

1. In the Management Console select **Tools** > **Default Options**.

   Step Result: The **Default Options** dialog opens.

2. Select the **Computer** tab.

3. In the **Option** column select the **Microsoft CA Key Provider** value.

    a) To allow a user to add other users to access the device, clear the **Default setting** check box in the **Option Value** panel.
    b) Select the **Disabled** value from the drop-down list.

4. In the Management Console select **View** > **Modules** > **Device Explorer**.

5. Right-click the **Removable Storage Devices** device class in the hierarchical structure at the **Default settings** (to activate decentralized encryption for all computers), **Machine-specific settings** level (to activate decentralized encryption for a specific computer), or at the individual computer group level.

6. Click **Add/Modify Permissions**.

    Step Result: The **Permissions** dialog opens. See Managing Permissions for additional information about assigning permissions for encryption.

7. To create permissions that force a user to encrypt a removable storage device, click **Add**.

    Step Result: The **Select Group, User, Local Group, Local User** dialog opens.

8. Click **Search** or **Browse**.

    a) Select a user or user group to assign user access permission rules.
    b) Click **OK**.

9. From the **Encryption** panel, select the **Unencrypted (Unencrypted or unknown encryption type)** option.

    Selection of this option forces a user or user group to encrypt all unencrypted devices attached to the client computer.

    Important: You must deselect the **Self Contained Encryption** **Encryption** option.

10. From the **Permissions** panel, select the following options:

    • **Encrypt**
    • **Export to media**

    Important: To allow a user to save existing data stored on the removable storage device, you must add the **Read** permission.

11. From the **Bus** and **Drive** panels, select any options you want to apply.

    For detailed information regarding **Bus** and **Drive** type options, see the Permissions Dialog.

12. Click **OK**.

ivanti

13. To create permissions that allow the user to access the encrypted device, click **Add**.

> **Important:** This step requires that you must add the same users <u>a second time</u> that you added in the previous steps. In the previous steps you created encryption permissions; in the following steps you are creating user access permissions for the device after encryption.

Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

14. Click **Search** or **Browse**.

    a) Select a user or user group to assign user access permission rules.
    b) Click **OK**.

15. From the *Encryption* panel, select the **Self Contained Encryption** option.

> **Important:** You must deselect the **Unencrypted (Unencrypted or unknown encryption type)** *Encryption* option.

16. Create permissions that allow a user to access an encrypted removable storage medium. From the *Permissions* panel, select one or any combination of the following options:

- **Read**
- **Write**
- **Decrypt**

17. From the *Bus* and *Drive* panels, select any options you want to apply.

For detailed information regarding *Bus* and *Drive* type options, see the Permissions Dialog.

18. Click **OK**.

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 show 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 issues 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 force users to encrypt devices for use only on computers running the Device Control client that are connected to the corporate network.

1. In the Management Console select **Tools** > **Default Options**.

    Step Result: The *Default Options* dialog opens.

2. Select the *Computer* tab.

3. In the **Option** column select the **Microsoft CA Key Provider** value.

    a) To allow a user to add other users to access the device, clear the **Default setting** check box in the *Option Value* panel.
    b) Select the**Enabled** value from the drop-down list.
        This configuration setting requires that a Microsoft Certificate Authority is available.

4. In the Management Console select **View** > **Modules** > **Device Explorer**.

5. Right-click the **Removable Storage Devices** device class in the hierarchical structure at the **Default settings** (to activate decentralized encryption for all computers), **Machine-specific settings** level (to activate decentralized encryption for a specific computer), or at the individual computer group level.

6. Click **Add/Modify Permissions**.

    Step Result: The *Permissions* dialog opens. See Managing Permissions for additional information about assigning permissions for encryption.

7. To create permissions that force a user to encrypt a removable storage device, click **Add**.

    Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

8. Click **Search** or **Browse**.

    a) Select a user or user group to assign user access permission rules.
    b) Click **OK**.

9. From the *Encryption* panel, select the **Unencrypted (Unencrypted or unknown encryption type)** option.

    Selection of this option forces a user or user group to encrypt all unencrypted devices attached to the client computer.

    Important: You must deselect the **Self Contained Encryption** *Encryption* option.

10. From the *Permissions* panel, select the following options:

    •   **Encrypt**

    Attention: To allow a user to save existing data stored on the removable storage device, you must add the **Read** permission.

ivanti

11. Click **OK**.

12. From the *Bus* and *Drive* panels, select any options you want to apply.

For detailed information regarding *Bus* and *Drive* type options, see the Permissions Dialog.

13. To create permissions that allow the user to access the encrypted device, click **Add**.

> **Important:** This step requires that you must add the same users a second time that you added in the previous steps. In the previous steps you created encryption permissions; in the following steps you are creating user access permissions for the device after encryption.

Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

14. Click **Search** or **Browse**.

  a) Select a user or user group to assign user access permission rules.
  b) Click **OK**.

15. From the *Encryption* panel, select the **Self Contained Encryption** option.

> **Important:** You must deselect the **Unencrypted (Unencrypted or unknown encryption type)** *Encryption* option.

16. Create permissions that allow a user to access an encrypted removable storage medium. From the *Permissions* panel, select one or any combination of the following options:

- **Read**
- **Write**
- **Decrypt**

17. From the *Bus* and *Drive* panels, select any options you want to apply.

For detailed information regarding *Bus* and *Drive* type options, see the Permissions Dialog.

18. Click **OK**.

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:** You may authorize additional users for the same type of device access using the *Media Authorizer*. For detailed information about using the *Media Authorizer*, see The Media Authorizer Window. Verify that additional 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 issues certificates to users for the purpose of encryption.
- You may set the **Password Attempts Limit** option for user password requirements, using the **Tools** > **Default Options** > **Computer** tab.

  For detailed information about using default options, refer to Computer Tab on page 146.

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 Management Console select **Tools** > **Default Options**.

   Step Result: The *Default Options* dialog opens.

2. Select the *Computer* tab.

3. In the **Option** column select the **Microsoft CA Key Provider** value.

   a) To allow a user to add other users to access the device, clear the **Default setting** check box in the *Option Value* panel.
   b) Select the**Enabled** value from the drop-down list.

4. In the Management Console select **View** > **Modules** > **Device Explorer**.

5. Right-click the **Removable Storage Devices** device class in the hierarchical structure at the **Default settings** (to activate decentralized encryption for all computers), **Machine-specific settings** level (to activate decentralized encryption for a specific computer), or at the individual computer group level.

6. Click **Add/Modify Permissions**.

   Step Result: The *Permissions* dialog opens. See Managing Permissions for additional information about assigning permissions for encryption.

7. To create permissions that force a user to encrypt a removable storage device, click **Add**.

   Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

8. Click **Search** or **Browse**.

   a) Select a user or user group to assign user access permission rules.
   b) Click **OK**.

ivanti

9. From the *Encryption* panel, select the **Unencrypted (Unencrypted or unknown encryption type)** option.

Selection of this option forces a user or user group to encrypt all unencrypted devices attached to the client computer.

> **Important:** You must deselect the **Self Contained Encryption** *Encryption* option.

10. From the *Permissions* panel, select the following options:

- **Encrypt**
- **Export to Media**

> **Attention:** To allow a user to save existing data stored on the removable storage device, you must add the **Read** permission.

11. Click **OK**.

12. From the *Bus* and *Drive* panels, select any options you want to apply.

For detailed information regarding *Bus* and *Drive* type options, see the Permissions Dialog.

13. To create permissions that allow the user to access the encrypted device, click **Add**.

> **Important:** This step requires that you must add the same users <u>a second time</u> that you added in the previous steps. In the previous steps you created encryption permissions; in the following steps you are creating user access permissions for the device after encryption.

Step Result: The *Select Group, User, Local Group, Local User* dialog opens.

14. Click **Search** or **Browse**.

a) Select a user or user group to assign user access permission rules.
b) Click **OK**.

15. From the *Encryption* panel, select the **Self Contained Encryption** option.

> **Important:** You must deselect the **Unencrypted (Unencrypted or unknown encryption type)** *Encryption* options.

16. Create permissions that allow a user to access an encrypted removable storage medium. From the *Permissions* panel, select one or any combination of the following options:

- **Read**
- **Write**
- **Decrypt**

17. From the *Bus* and *Drive* panels, select any options you want to apply.

For detailed information regarding *Bus* and *Drive* type options, see the Permissions Dialog.

18. Click **OK**.

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.

  Important: You may authorize additional users for the same type of device access using the **Media Authorizer**. For detailed information about using the **Media Authorizer**, see The Media Authorizer Window. Verify that additional users have **Read** and/or **Write** permissions for devices encrypted using **Self Contained Encryption**.

- 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 Controlclient. For example, you attach device that you decrypt and decide to re-encypt 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.

ivanti

1. Select **My Computer**.

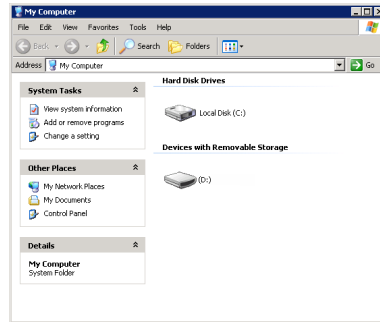   **Step Result:** The *My Computer* page opens.

Figure 102: My Computer Page

2. Right-click the name of the device listed under ***Devices with Removable Storage***.

    Step Result: A right-mouse menu opens.

3. From the right-mouse menu, click **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: Portable encryption is available for devices containing storage up to 2 TB.

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- 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.
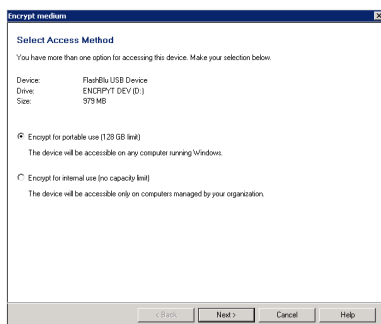

Figure 103: Select Access Method Page

Option	Description
Encrypt for portable use (2 TB limit)	Allows use of an encrypted device on any computer running Microsoft® Windows®. This encryption access method is called *Portable*.
Encrypted for internal use (no capacity limit)	Allows use of devices only inside your network on computers that run are managed by Device Control. There is no limit to the capacity for the encrypted device. This encryption access method is called *Non-portable*.

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.

ivanti

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. To create your own user name and password for device access:

   a) Type a user name in the **User name** field.

Figure 104: User Access to Device Page

> **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.

2. If you wish to add other users for access to the encrypted device, click **Add User**.

   Step Result: The *Add User* page opens.

3. 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 a minimum, one user who is allowed access to the encrypted device must be listed.

1. Select one of the following options:
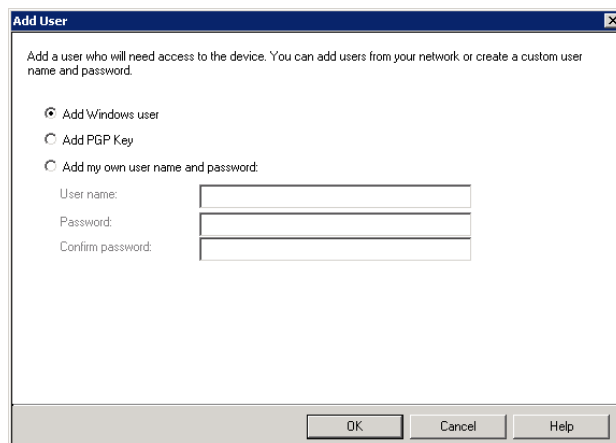

Figure 105: Add User Page

2. To add a Windows Active Directory user:

   a) Select **Add Windows user**.
   b) Click **OK**.

      Step Result: The *Select Users or Groups* dialog opens.
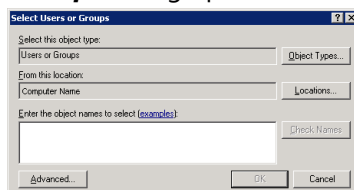
      Figure 106: Select Users or Groups Dialog

   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 60: 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.

ivanti

e) Click **OK**.

3. 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.
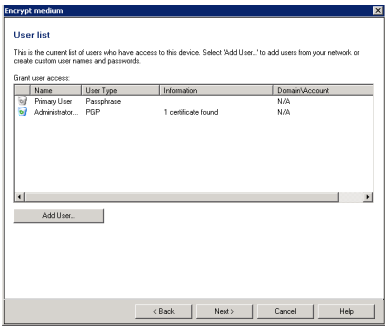

Figure 107: User List Page

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.
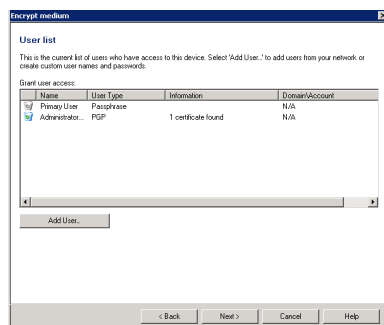
Figure 108: User List Page

1. Review the user access list on the *User List* page.
2. You may add more users by clicking **Add User**, as necessary.
3. You may remove users by clicking the **Recycle Bin** icon, as necessary.
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.

ivanti

1. Select one of the following options:
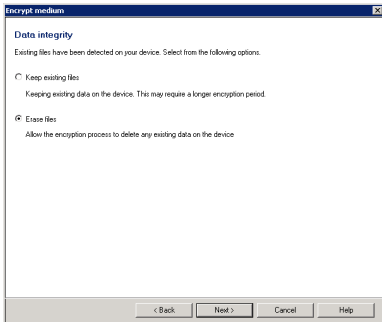
Figure 109: Data Integrity Page

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.
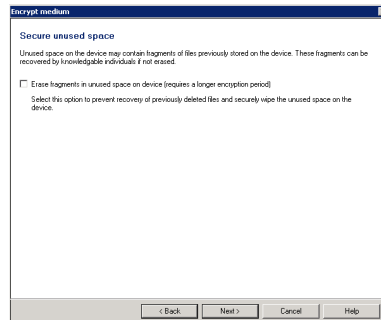
Figure 110: Secure Unused Space Page

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.

ivanti

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.

Figure 111: Start Encryption Page

2. When you are satisfied with the list of users allowed to access the device, click **Encrypt**.

Step Result: The **RTNotify** warning dialog opens.

Figure 112: RTNotify Dialog

3. Click **OK**.

Step Result: The **Encrypt Medium** dialog opens, showing a progress bar for the encryption process.

Figure 113: Encrypt Medium Dialog

4. Click **Close**.

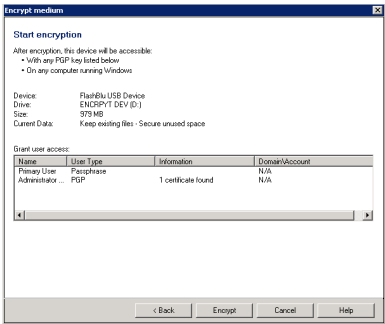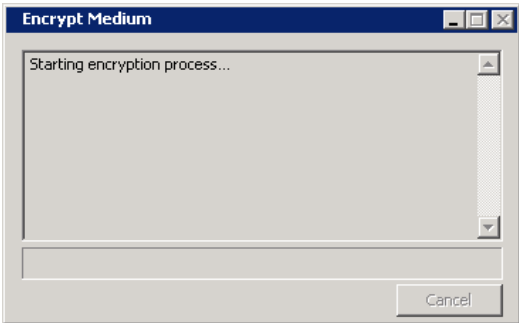**Result:** The device is encrypted for the users specified. To verify the users are added to the encrypted medium, refer to Managing Devices.

> **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 and Application Control administrators can export and import encryption keys for 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:

The following must be completed before you can successfully transfer an encryption key:

- An administrator must assign users access to the media.
- Am 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. Navigate to Windows Explorer®.
2. Right-click the device.
3. Select **Export medium key** from the right-mouse menu.

   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.

ivanti

Option	Description
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.

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:

The following must be completed before you can successfully import an encryption key:

- 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. Navigate to Windows Explorer®.

2. Right-click the device name.

3. Select **Unlock medium** from the right-mouse menu.

   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.

Option	Description
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®.

ivanti

Chapter

8

Accessing Encrypted Media without the Client

In this chapter:

- About Accessing Unauthorized Encrypted Media

Device Control is designed to allow local users to access authorized and unauthorized encrypted removable storage devices, when the user cannot access a Ivanti Device and Application Control client. A removable storage device is defined for Ivanti Device and Application Control purposes as any device declared in the Windows **Removable Storage Devices** class through the *plug-and-play* feature.

Users can access encrypted removable storage media by:

- Exporting an encryption key to the device or a separate file.
- Unlocking a device in Windows Explorer by importing an encryption key from a device or file.
- Using the ***Stand-Alone Decryption Tool*** (SADEC).
- Using Easy Exchange encryption.

About Accessing Unauthorized Encrypted Media

Encrypted media access without the client uses a separate utility that a user downloads to a non-Ivanti Device and Application Control computer.

You can access devices encrypted by Device Control from a computer that does not run the Ivanti Device and Application Control client by using the following methods:

- Install the Ivanti Device and Application Control *Stand-Alone Decryption Tool* and import an encryption key.
- Encrypt the device using the **Easy Exchange** encryption option in the ***Media Authorizer*** module.

Stand-Alone Decryption Tool

You can access a device encrypted by Device Control from a computer that does not run the client by installing the ***Stand Alone Decryption Tool*** (SADEC).

You must download the Ivanti Device and Application Control application software from the Self-Service Portal. After you install SADEC, you can import an encryption key to access the encrypted removable storage device with a password. SADEC is supported on the following Microsoft operating systems:

ivanti

- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2 (64 bit only)
- Microsoft Windows 7 (32- and 64-bit)

Restriction: SADEC cannot be installed on a computer that runs the client.

Easy Exchange

Using *Easy Exchange* encryption, you can access a device encrypted by Device Control from a computer that does not run the Ivanti Device and Application Control client.

The *Secure Volume Browser*, installed on the device during **Easy Exchange** encryption, allows you to access the device by:

- Entering a valid password, when the encryption key is stored on the device.
- Allowing you to import an encryption key and enter a valid password.

The encryption is done in a single file or multiple files (depending on removable media capacity) using a FAT structure.

Caution: You should use the **Safely Remove Hardware** feature in the Windows system tray when unplugging an encrypted device from the computer, to ensure that all your files are safely copied to the device.

Appendix

A

Ivanti Device and Application Control Administrative Tools

In this appendix:

- Scheduling Domain Synchronization
- Manage Administrator Rights
- Opening Firewall Ports
- Logging File Transfers to the Windows Event Log

Administrative utilities include scheduling domain synchronization, and managing administrator rights.

The Ivanti Device and Application Control product solution suite provides administrative tools for the Enterprise *Administrator* to reduce administrative burden for installation and maintenance of the Ivanti Device and Application Control product suite.

Scheduling Domain Synchronization

The SXDomain utility provides a method to automatically schedule domain synchronization, using the Windows *Task Scheduler*.

You can schedule domain synchronizations with a task scheduler, such as the Windows **Task Scheduler**. You create a batch file that contains a list domains to synchronize.
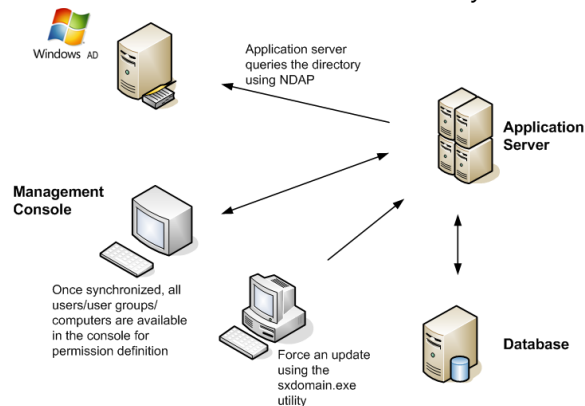

Figure 114: Synchronization Script Process

1. Navigate to `C:\Program Files\Ivanti\Device and Application Control\SXTools`.

ivanti

2. Create a batch file named `sxsync.bat` containing the following command line: `CMD/C SXDOMAIN-s SXS_Server -i -e <mydomains.txt> error_list.txt`.

3. Navigate to the Windows **Control Panel**, select **Scheduled Tasks**.

4. Select **Add Scheduled Tasks**.

    Step Result: The **Scheduled Task Wizard** dialog opens.

5. Click **Next**.

6. Select the `sxsynch.bat` file from files shown.

7. Click **Next**.

8. Type a name for your scheduled task at the prompt.

9. Select a schedule frequency from the options listed from **Perform this task**.

10. Click **Next**.

11. Select the day and time you want to perform the task.

12. Click **Next**.

    Step Result: A user name and password information dialog opens.

13. Type the user name in the **User Name** field.

14. Type the associated password in the **Password** and **Confirm Password** fields.

15. Click **Next**.

    Step Result: A dialog opens showing the name of the scheduled task and the date and time the task is scheduled to perform.

16. Click **Finish**.

Result: Domain synchronization is scheduled to perform according to your specifications.

Manage Administrator Rights

Initially, you can manage administrator rights allocated in the **Active Directory** (AD) to delegate roles and responsibilities using the Microsoft® Windows® Visual Basic® script provided with the Ivanti Device and Application Control installation software.

Prerequisites:

*   Install the Windows® Script Host (WSH) interpreter. See Script Host (http://msdn.microsoft.com/en-us/library/ec0wcxh3(VS.85).aspx) for additional information about the Windows Script Host.
*   Schedule domain synchronization.

When `ctrlacx.vbs` runs, the script creates a special entry in the permissions list of the AD organization unit named **Manage Ivanti Device and Application Control Settings**. This entry only affects Device Control administrators and the devices they control permissions for. If you assign this

setting to a specific user, who is also an *Administrator* defined using the **User Access Manager** dialog in the Management Console, this *Administrator* can only manage, directly from the Management Console, the designated users, user groups, and computers that the *Administrator* has assigned rights for. Administrator access rights are described by *Defining User Access* in the Ivanti Device Control User Guide (https://help.ivanti.com) or Ivanti Application Control User Guide (https://help.ivanti.com) .

1. Select **Start** > **Run**.

2. Type: `cscript ctrlacx.vbs [parameter from following list]>filename.txt`

3. Add any of the following optional parameters, individually or in combination, to the parameters list command line:

Parameter	Description
-	Shows a brief description for each available parameter.
-e	Lists all access control rights, with condensed output.
-v	Lists all access control rights, with detailed output.
-q cn	Shows control rights by canonical name.
-s	Shows **Manage Ivanti Device and Application Control Settings** rights.
-create	Creates or updates **Manage Ivanti Device and Application Control Settings** rights.
-delete	Deletes **Manage Ivanti Device and Application Control Settings** rights.

ivanti

4. Click **OK**.

Result: The delegation rights you create can be assigned to Active Directory organizational units (OUs).

> **Example:**
>
> To list all control access rights in condensed mode redirecting the output to MyFile.txt file, type:
>
> ```
> cscript ctrlacx.vbs -e > MyFile.txt
> ```
>
> To show the **Manage Ivanti Device and Application Control Settings** rights interactively, type:
>
> ```
> ctrlacx.vbs -s
> ```

After Completing This Task:

You can assign the delegation rights by using the *Windows Management Services and MMC* when you run the script with `-create` parameter. See Windows Management Services and MMC (http://technet.microsoft.com/en-us/library/bb742441.aspx#XSLTsection123121120120) for additional information about assigning delegation rights.

Opening Firewall Ports

Firewall settings may deny access to services and network ports which prevent the Ivanti Device and Application Control Client Deployment Tool from connecting to remote computers.

You need to open the listed ports on the computers where you want to deploy the Ivanti Device and Application Control client. The specific network communication ports that are required for Application Server-client communications are:

- UDP 137
- UDP 138
- TCP 139
- TCP 445

Open Ports by Firewall Exception

You must enable Windows **File and Printer Sharing** services to open the ports necessary to remotely deploy the client.

Ivanti Device and Application Control uses two configurable ports for full two-way communication between the client and Application Server components. To manually open network ports on each computer where the client is deployed:

1. From the Windows **Start** menu, select **Control Panel** > **Security Center** > **Windows Firewall** > **Exceptions** tab.

2. Select the **File and Printer Sharing** check box.

    a) If the computer resides on a remote IP subnet, select **Add Port** > **Change Scope** > **My Network (subnet) only**.

    b) Click **OK**.

3. Click **OK**.

Result: TCP ports 139 and 445 and UDP ports 137 and 138 are opened.

Open Ports by Active Directory Policy

You can open the ports necessary to remotely deploy the client in a large network, by centrally configuring the **Windows Firewall** using *Group Policy*.

Prerequisites:

Before you can successfully open ports using Windows *Group Policy* to deploy the Ivanti Device and Application Control client, you must:

- Have administrative user access to the computer where you are deploying the Ivanti Device and Application Control client.
- Install the Microsoft® Group Policy Management Console. See Installing Microsoft Group Policy Management Console (http://www.microsoft.com/windowsserver2003/gpmc/default.mspx) for additional information about installing the Microsoft Group Policy Management Console.
- Install Microsoft .Net Framework. See Installing Microsoft .Net Framework (http://www.microsoft.com/downloads/Search.aspx?displaylang=en#) for additional information about installing Microsoft .Net Framework.

As with other TCP-based services, the Application Servercannot establish full two-way communication with clients connecting through a firewall, unless the required ports are open. To open ports closed by firewall policy:

1. From the Windows **Start** menu, select **Run** `gpmc.msc`.

2. From the *Group Policy Management* window, select the **Forest** and **Domain** where you will create the **Windows Firewall** policy.

3. Right-click **Default Domain Policy**.

4. Expand the **Computer Configuration** hierarchy.

5. Navigate to **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profile**.

6. Right-click **Windows Firewall: Allow file and printer sharing exception**.

7. Select **Properties** > **Setting** tab.

8. Select **Enabled**.

ivanti

9. In the **Allow unsolicited incoming messages from** field, type `Localsubnet`.

> **Tip:** To enhance security, you can replace `Localsubnet` with specific IP addresses for the computers allowed to deploy the Ivanti Device and Application Control client.

10. Click **Apply**.

11. Click **OK**.

Result: TCP ports 139 and 445 and UDP ports 137 and 138 are opened, making the ports available on the same local IP subnet.

Logging File Transfers to the Windows Event Log

When the Secure Volume Browser (SVolBro) is installed on client computers, you can log file transfers to and from these devices using the Windows Event Log.

Enabling file transfer data to be recorded in the Windows Event Log requires the creation of registry subkeys.

1. Open the Windows registry on the client computer.

2. Navigate to one of the following subkeys within the Windows registry, depending on the operating system's architecture.

Operating System Architecture	Subkey Location
32-bit	`HKEY_LOCAL_MACHINE\SOFTWARE\Lumension Security\SubVolGUI`
64-bit	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Lumension Security\SubVolGUI`

3. Right-click in the subkey entries pane.

4. Select **New** > **String Value**.

Step Result: A new entry is created.

5. In the **Name** column for the new entry, type `Log Transfers to Windows Event Log`.

6. Press Enter.

7. Right-click the **Log Transfers to Windows Event Log** entry.

8. Select **Modify**.

9. Enter `yes` in the **Value data** field.

10. Click **OK**.

> **Step Result:** The value for the new registry entry is set.

11. Navigate to the following registry subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`
`\Services\Eventlog\Application\Lumension`.

12. Right-click in the subkey entries pane.

13. Select **New** > **Expandable String Value**.

> **Step Result:** A new entry is created.

14. In the **Name** column for the new entry, type `EventMessageFile`.

15. Press Enter.

16. Right-click the **EventMessageFile** entry.

17. Select **Modify**.

18. Enter the location of the Secure Volume Browser executable file in the **Value data** field.

> **Example:** `C:\Program Files\Ivanti\Device and Application Control\\Client`
> `\SVOLBRO.exe`

19. Click **OK**.

> **Step Result:** The value for the new registry entry is set.

20. Right-click in the subkey entries pane.

21. Select **New** > **String Value**.

> **Step Result:** A new entry is created.

22. In the **Name** column for the new entry, type `TypesSupported`.

23. Press ENTER.

24. Right-click the **TypesSupported** entry.

25. Select **Modify**.

26. Enter `0x1F` in the **Value data** field.

27. Click **OK**.

> **Step Result:** The value for the new registry entry is set.

Result: File transfers to and from the client computer will be recorded in the Windows Event Log.

ivanti