Ivanti Device and Application Control 5.3

Application Control User Guide

ivanti | Endpoint Security
powered by HEAT

Notices

Version Information

Ivanti Device and Application Control Application Control User Guide - Ivanti Device and Application Control Version 5.3 - Published: March 2021

Document Number: 02_104_5.3

Table of Contents

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.

Chapter 1

Application Control Overview

In this chapter:

- Product Overview
- Application 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.

Product Overview

Ivanti Device and Application Control software 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 Application Control solution are:

- The Application 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 Management Console, which provides the administrative user interface for the Application Server.
- The Application Control client, which is installed on each computer, either endpoint or server, that you want to protect.

The following figure illustrates the relationships between the Ivanti Device and Application Control components.

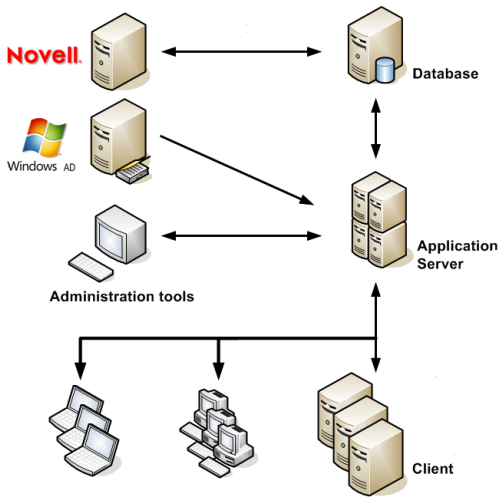


Figure 1: Application Control Component Relationships

Application 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 Application Servers, database, and clients when using Application Control.

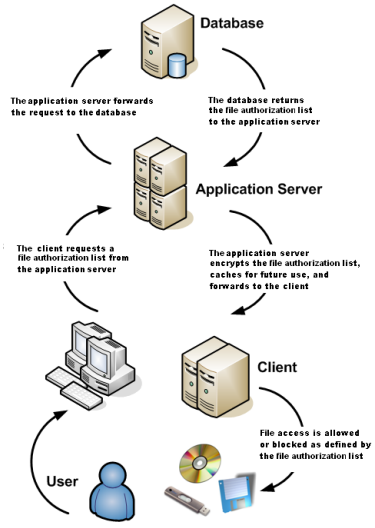


Figure 2: Application Control Process Flow

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.

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 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 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

Chapter 2

Using Application Control

In this chapter:

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 file authorization data from the database. The data is sent from the server to a client, thereby establishing application control on the client. The Management Console provides direct access to system management, configuration, file authorization, reporting, and logging functions.

Getting Started with Application Control

Get started with Application Control by installing the application, which includes all server and database components, the Management Console, and the client. Then you use the Management Console to define user access permissions and file authorization rules.

You must begin the installation process with a clean machine that fulfills the minimum software and hardware requirements. You must resolve all hardware and software conflicts prior installing 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 installing Application Control.

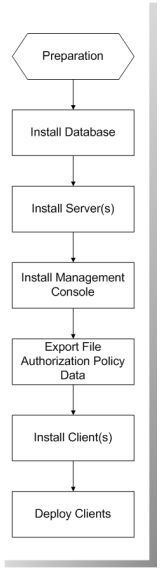
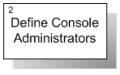


Figure 3: Ivanti Device and Application Control Installation

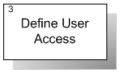
The File Authorization Setup Process

After successfully installing Application Control, an administrator uses the Management Console to configure and define user access permissions and file authorization rules required in a Ivanti Device and Application Control environment that specify which executable files, scripts, and macros each user can use, as described by the following process flow.

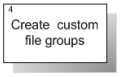
You can use standard Microsoft file definitions to quickly build a central file authorization list for executable files, macros, and scripts.



You can assign administrator access rights using the **User Access** tool. An *Administrator* has restricted access to the Management Console and can be assigned various administrative roles by an *Enterprise Administrator*.

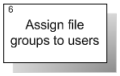


After defining *Administrator* roles, you can use the **User Access** tool to assign the defined roles to *Administrators*.

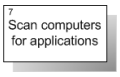


File groups simplify the process of administering large numbers of executable, script, and macro files for users. Instead of individually authorizing files, you can group files together logically by creating file groups.

Ivanti Device and Application Control verifies which file group is associated with an executable, script, or macro and whether the user has access permission for the file group. You can assign specific permissions to local users and user groups. Only authorized applications and scripts assigned to a user or a user group can run on the client.

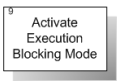


After creating the file groups and parent-child relationships you want to use, you can assign file groups to users or user groups.



You can create a template and scan a target computer running the client. You can scan all files on a computer, or you can create a template to scan selected directories or specific file types for example, *.exe, *.com, *.dll, *.ocx, *.sys, *.drv, *.cpl, *.vbs, *.js, to reduce the scan time required.

After you create the necessary file groups and required parent-child relationships, you can assign executable files, scripts, and macros to file groups.



Activating **Execution blocking** prohibits user access to unauthorized files. Local authorization is permitted only for the administrators and LocalSystem account.

Once you identify all your files, categorize them into file groups, and assign the file groups to users or user groups, these files are centrally authorized and immediately available to be run by all allowed users.

When a user wants to run an executable, script, or macro, the following actions take place automatically:

- A file that is identified as an executable, script, or macro, by the operating system is stored in the Ivanti Device and Application Control database ready for execution (but not actually executed).
- A file is identified by Ivanti Device and Application Control as an executable, script, or macro, has the entire file content checked to determine its digital signature (hash) before being allowed to execute by the operating system.
- The digital signature is compared to the digital signatures (stored in a central file authorization list) for files that are authorized to run.
- If, and only if, the file signature corresponds exactly to a file signature in the central file authorization list, in other words, the digital signatures are identical and the file is authorized for execution for the user or computer requesting authorization, can the file run.

Note: When an executable file is launched by the user, Application Control will identify and determine the digital signature (hash) of that executable regardless of the current mode (blocking or non-blocking). Although rarely detected by the user, this process of identifying the executable and determining the hash could result in a noticable delay on some systems.

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.
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.

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.

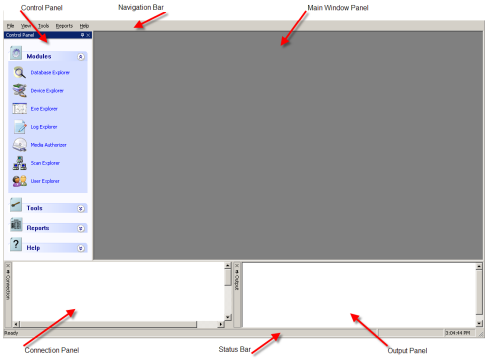


Figure 4: Management Console

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.

Screen Feature	Function
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.	

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

   Step Result: The ***Choose Columns*** dialog opens.

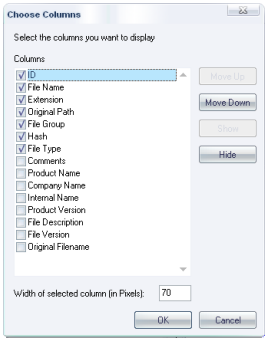


Figure 5: Choose Columns Dialog

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.

Using the Tools Menu

The **Tools** menu displays a list of tasks for performing user and database administration.

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

Table 11: Tools Menu

Menu Item	Description
Synchronize Domain Members	Updates the Ivanti Device and Application Control 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 Ivanti Device and Application Control *Enterprise Administrators* and *Administrators* by allowing you to assign access rights for setting permissions and viewing audit information for administrator actions.
Default Options	Changes the default option settings for users and computers.
Path Rules	Uses file paths and trusted owners to define which applications can run. Additional information can be found in the online help.
Spread Check	Prevents the spread of self-propagating code by disabling suspicious executables that have been locally authorized on multiple 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.

Menu Item	Description
Send Updates to	Transmits the latest setting and permission changes to specific computers on the network.
Import Standard File Definitions	Imports files and associated digital signatures for Windows operating systems supported by the Ivanti Device and Application Control application.
Export Settings	Places file authorization settings in an external file that can be sent to Ivanti Device and Application Control 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 Ivanti Device and Application Control clients.

Using the Reports Menu

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

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

Table 12: Reports Menu

Menu Item	Description
File Groups by User	Shows one or more users and groups the assigned files groups assigned to file groups.
Users by File Group	Shows one or more file groups assigned to users and groups.
User Options	Shows all the user options defined in the system.
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.

Using 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.

Note: There is no **Explorer** menu for the **User Explorer** module.

Table 13: Database Explorer Module Menu

Menu Item	Description
Assign	Changes the file group assignment.
Manage File Groups	Adds, renames, or deletes a file group.
Choose Columns	Organizes the panels columns.

Table 14: Exe Explorer Module Menu

Menu Item	Description
Map Network Drive	Assigns a drive letter to a shared resource on a network.
Disconnect Network Drive	Removes the drive letter assigned from any shared resource on a network to prevent users from browsing without credentials.
Assign	Changes the file group assignment.
Manage File Groups	Adds, renames, or deletes a file group.
Choose Columns	Organizes the panels columns.

Table 15: Log Explorer Module Menu

Menu Item	Description
Fetch log	Obtains the latest log data from a client.
Manage File Groups	Adds, renames, or deletes a file group.

Table 16: Scan Explorer Module Menu

Menu Item	Description
Perform Scan	Scans a computer to identify executable files, scripts and macros to be authorized.
Select Scans	Provides the option to compare two scans.
Assign	Changes the file group assignment.

Menu Item	Description
Manage File Groups	Adds, renames, or deletes a file group.
Choose Columns	Organizes the panel columns.

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 17: 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 18: 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.

Application Control Modules

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

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

Table 19: Application Control Modules

Module	Icon	Description
Database Explorer		Shows the list of executable files, scripts, and macros that are stored in the Ivanti Device and Application Control database and manages file assignment details.
Exe Explorer		Builds a list of executable files, scripts, and macros that are allowed to run on Ivanti Device and Application Control clients, and assigns files to file groups.
Log Explorer		Shows logs of applications, scripts, and macros that were run, files for which access was denied, and files authorized locally.
Scan Explorer		Scans a computer or domain to identify executable files, scripts, and macros to be authorized, and assigns files to a file group using templates.
User Explorer		Links users or user groups with file groups, granting permission to use the files assigned to file groups.

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

Expiration Period	Warning Message	Frequency
More than 60 days	No message.	Not applicable

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

Chapter 3

Using the Authorization Wizard

In this chapter:

- Working with the Authorization Wizard

The Authorization Wizard tool is used for performing an initial inventory of existing software applications that can be authorized for use.

Ivanti Device and Application Control allows the operating system determine whether a file is executable and then checks the digital signature against the central file authorization list. Ivanti Device and Application Control provides several strategies for authorizing executable files, scripts, and macros including:

- Central authorization using digital signatures.
- Central authorization using file paths and trusted owners.
- Local authorization providing local users limited rights to authorize executable files, scripts, and macros to run on a specific user computer.

Scripts and macros are more difficult to identify than executables files. Ivanti Device and Application Control recognizes and centrally manages the following types of scripts and macros:

- VBScripts and JScripts that are interpreted by the Windows Script Host that have the `.vbs` or `.js` extension.
- Scripts interpreted by `cscript.exe` and `wscript.exe`.
- Visual Basic scripts that run within Microsoft Office and other host applications.

The ***Authorization Wizard*** Wizard is an administrative tool that you can use to build an initial list of centrally authorized application files.

Working with the Authorization Wizard

The ***Authorization Wizard*** tool is used for performing an initial inventory of existing software applications that can be authorized for use.

The ***Authorization Wizard*** tool provides a simple method for scanning existing files and directories on a computer to add files to the central authorization list. The wizard can automatically assign scanned files with existing digital signatures to file groups. Alternatively, scanned files without a digital signature can be processed manually to create digital signatures and then assign these files to file groups.
The wizard can also expand compressed files during the scanning process, identify or create digital signatures, and then assign these files to files groups.

The ***Authorization Wizard***:

- Searches for executable files from a specific source, as a computer hard drive, network share (UNC path), or CD/DVD-ROM.

Executable file sources include the following:

  - Windows operating systems, applications, and service packs
  - Self-extracting ZIP archives
  - RAR, MSI, MSP and Microsoft CAB files

- Creates digital signatures for selected files.
- Records the digital signatures in the Ivanti Device and Application Control database.

The ***Authorization Wizard*** does not scan for scripts or macros.

Restriction: The ***Authorization Wizard*** does not expand `setup.exe` files and classifies them as a single executable file instead of an auto-extraction file.

Authorizing Executable Files

You can use the ***Authorization Wizard*** to scan a reference computer to build an initial list of centrally authorized files.

1. Select Windows **Start** > **Programs** > **Ivanti** > **Ivanti Device and Application Control Management Console** > **Authorization Wizard**.

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

2. Click **Next**.
   The wizard advances to the ***Options - Authorization Wizard*** dialog.

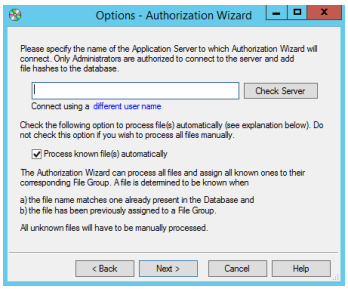


Figure 6: Options - Authorization Wizard Dialog

3. Enter the name of a computer to connect to the Application Server, using one of the following options:
   - Type the server name (`my_server`)
   - Type the server IP address (`192.168.1.1`)
   - Click **different user name** to use other server connection credentials (another dialog opens and you type the user name and password)

Attention: When you can only leave certain non-standard ports open in your firewall, you need to specify the server TCP port number between square brackets, for example: `server[1234]`.

   a) Click **Check Server** to verify the connection.

4. Select or clear the **Process known files automatically** check box as follows:

Option	Description
Select	Add existing files to the database that match an existing database entry with a different digital signature, and assign the files to existing file groups.
Clear	Identify unknown files and process them manually.

5. Click **Next**.
6. To browse to the root directory that you want to scan for executable files, select one of the following options, then click the ellipsis adjacent to the **Source** field.

Option	Description
Directory	If you are scanning from a directory
File	If you are scanning from a file or compressed archive file.

7. To select the temporary directory where the wizard can expand compressed files, click the ellipsis adjacent to the **Extract temporary files to:** field.

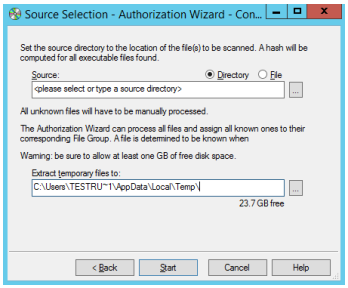


Figure 7: Options - Source Selection - Authorization Wizard - Connected Dialog

Caution: If the `Free space for extraction` falls below 100 MB, you receive a message prompting you to create more free disk space.

8. Click **Start**.

Step Result: The ***Assigning File(s) - Authorization Wizard - Connected*** dialog opens. The wizard searches the source directory or file and lists the number of files found.

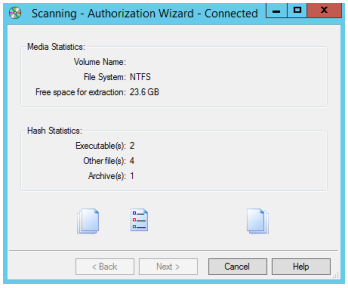


Figure 8: Assigning File(s) - Authorization Wizard - Connected Dialog

9. Click **Next**.

If you select the ***Process known files automatically*** option, the wizard processes all executable files and assigns them to corresponding file groups. If a matching filename exists in the database

and is assigned to a file group, the wizard assigns the new file definition to the same file group. The results are summarized as follows:

- Number of files processed
- Number of files assigned to file groups
- Number of files as duplicates of previously assigned files

Step Result: The ***Assigning Files - Authorization Wizard - Connected Summary*** dialog opens.

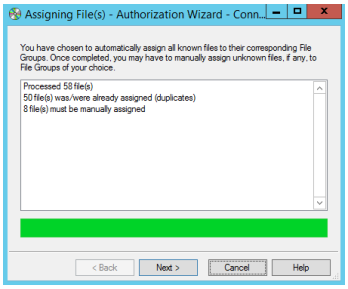


Figure 9: Assigning File(s) - Authorization Wizard - Connected Dialog

10. Click **Next**.

Step Result: The ***Assigning Files - Authorization Wizard - Connected*** dialog opens. The wizard lists files that are not assigned to file groups because they do not match existing filenames in the database or cannot be processed automatically.

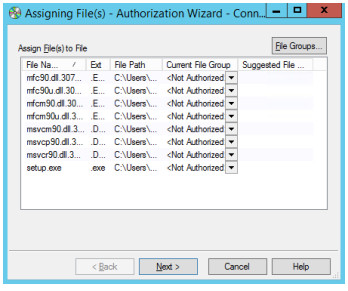


Figure 10: Assigning File(s) - Authorization Wizard - Connected Dialog

11. To manually assign the unknown file(s) to a file group, select one or more file names from the ***File Name*** list.

12. Click the ***Suggested File Group*** drop-down list or **File Groups** to select a file group for assignment.

13. Click **Next**.

Step Result: The new file definitions are added to the database.

14. Click **Finish**.

You may select the ***Restart the wizard to add more files or CDs*** option.

Result: The selected files are assigned to file groups.

After Completing This Task:

You may need to update user access permissions to enable users or user groups to run newly authorized applications.

Chapter 4

Using Modules

In this chapter:

- Working with Scan Explorer
- Working with the Exe Explorer
- Working with User Explorer
- Working with Database Explorer
- Working with Log Explorer

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

Depending on the task, you may use one of the following modules in the Management Console ***Control Panel***:

- **Exe Explorer** to explore a few directories or files.
- **Database Explorer** to explore previously authorized files already stored in the database.
- **User Explorer** to manage user and user group assignments to file groups.
- **Scan Explorer** to explore a computer using a predefined scanning template.
- **Log Explorer** to explore and analyze user activity logs.

Working with Scan Explorer

Using the ***Scan Explorer*** module you can create a template and scan a target computer that runs the client.

A scanning template provides a foundation for you to quickly build a centrally authorized list from the files scanned on a client computer, using a reference computer, and authorize applications.

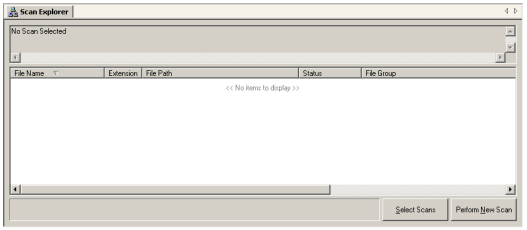


Figure 11: Scan Explorer Main Window

Creating a File Scanning Template

You can create a template to identify new file authorization changes to make when new software is installed.

You can scan for files by creating a template with the following rules:

- Scan all executables matching the pattern `*.exe` or `*.dll` in the `%SYSTEMROOT%` directory and subdirectories.
- Scan all files matching the pattern `*.exe` or `*.dll` in the `%PROGRAMFILES%` directory and subdirectories.

1. From the Management Console, select **View** > **Modules** > **Scan Explorer** > **Perform New Scan** > **Create New Template**.

   Step Result: The ***Create New Template*** dialog opens.

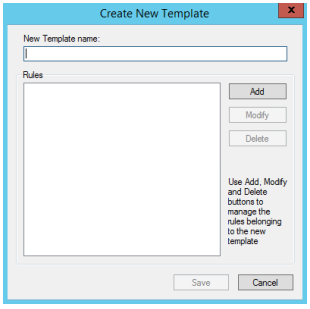


   Figure 12: Create New Template Dialog

2. In the **New Template name:** field, enter the name for the new template.
3. Click **Add**.

   Step Result: The ***New Rule*** dialog opens.

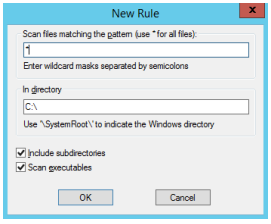


   Figure 13: New Rule Dialog

4. In the **Scan files matching the pattern (use * wildcard for all files)** field, enter the name patterns to use for scanning.

   Caution: When you specify wildcard masks, for example: `*.com`, you can miss scanning for files that do not use standard file extensions such as: `*.exe`, or `*.dll`, and so forth. The result is that these types of files will not be authorized, which means that these applications will not work or work properly.

5. In the **In directory** field, enter the path name for the directory you want to scan.
6. Select one or more of the following options:

Option	Description
Include subdirectories	Scan subdirectories of the root directory.
Scan executables	Scan for executable files and ignore all other file types. The scan also searches for 16-bit executables. **Attention:** If you do not select the **Scan Executables** option, you must specify the `*.exe` and `*.sys` for the matching pattern to scan for these types of files.

7. Click **OK**.

   Step Result: The ***New rule*** dialog closes and the rules you define appear on the ***Rules*** box.

8. Click **Save**.

Result: The ***Perform New Scan*** dialog lists the new template in the ***From Template*** drop-down list.

Scanning Files on a Client Computer

You can scan all files on a computer, or you can create a template to scan selected directories or specific file types for example, *.exe, *.com, *.dll, *.ocx, *.sys, *.drv, *.cpl, *.vbs, *.js, to reduce the scan time required.

Prerequisites:

Before you scan a computer, create a file scanning template.

Important: If you are using Application Control with Device Control enabled, you must set the following Device Control permissions before performing a scan on a secondary hard drive.

Device Class: **Removable**

User: **LocalSystem**

Permissions: **Read**

Encryption: **Unencrypted (Unencrypted or unknown encryption type)**

Bus: **All**

Drive: **Hard Drive**

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

   Step Result: The ***Scan Explorer*** window opens.

2. Click **Perform New Scan**.

   Step Result: The ***Perform New Scan*** dialog opens.

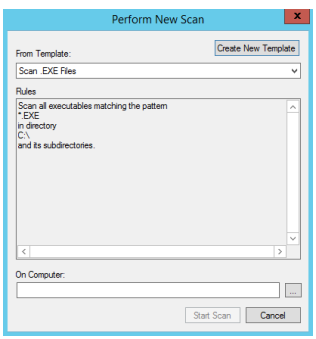


Figure 14: Perform New Scan Dialog

3. In the **From Template** field, select a template from the drop-down list.
4. Click the ellipsis ... adjacent to the **On Computer** field.

   a) Type the computer name.

b) Click **Search** or **Browse**.
c) Select the computer from the list.
d) Click **OK**.

You can type the computer name directly or use wildcard, such as * and ?.

Step Result: The ***Select Computer*** dialog opens.

5. Click **Start Scan**.

Step Result: The ***Perform New Scan*** dialog opens.

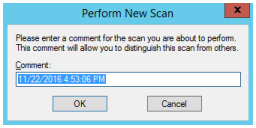


Figure 15: Perform New Scan Dialog - Comment

6. Enter a name or comment to distinguish this scan in the **Comment** field.
7. Click **OK**.

Result: Ivanti Device and Application Control scans the specified file directories, calculates digital signatures for all executable files, scripts, and macros, and adds these digital signatures to the database. The results are shown in the ***Scan Explorer*** main window as follows.

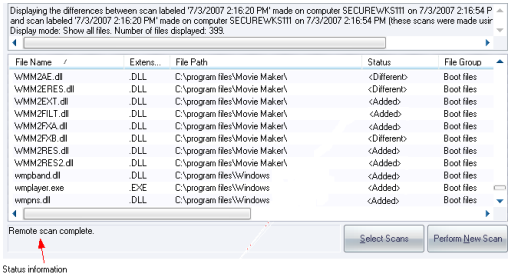


Figure 16: Scan Explorer Window

Comparing Scans

You can compare a scan, performed before installing a new application, to a scan performed after the installation process is complete. Alternatively, you can compare different scans to identify files associated with separate applications.

Prerequisites:

Before you can compare two scans, you must perform at least two separate scans.

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

Step Result: The ***Scan Explorer*** window opens.

2. Click **Select Scans**.

   Step Result: The ***Select Scans*** dialog opens.

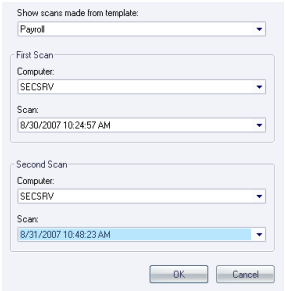


Figure 17: Select Scans Dialog

3. In the **Show scans made from template** field, select a template from the drop-down list.
4. In the ***First Scan*** panel:
   a) Select a computer name from the drop-down list.
   b) Select the name of your first scan from the drop-down list.
5. In the ***Second Scan*** panel:
   a) Select a computer from the drop-down list.
   b) Select the name of for your second scan from the drop-down list.
6. Click **OK**.

Result: The system compares the two scans and lists the results in the ***Scan Explorer*** window. Each file is assigned a status as follows:

- **Added** - The file was added between the first and second scans.
- **Different** - The file has been modified since the previous scan. The file has the same filename but a different digital signature and may be a newer version.
- **Original** - The file remains unchanged from the previous scan. This output only shows when comparing the same scan.

Modifying File Authorization

After scanning a computer to identify executable files, scripts, and macros, or comparing two scans to identify updates, you can change file assignment details so users can work with a new or upgraded application.

The purpose of the scan is to identify changes made when installing a new application, so you can assign new or modified files to a specific file group, or remove them.

Tip: You can use the right-click menu to filter a scan and show only **<Not Authorized>** files or **Show all files**.

1. Select the files.

2. Right-click the list.
3. From the shortcut menu shown, select own the following options.
   - ***Assign to File Group***
   - ***Remove from File Group***

Result: After changing the file group assignment, the applications use is denied or allowed, depending of the action specified in the ***User Explorer*** module.

Local Authorization

Local authorization allows users to locally authorize executable files, scripts, and macros that are not in the central authorization list. Then, the user can then use the software locally, providing users with the flexibility to run specific software applications without first requesting central authorization. You should limit use of this feature to avoid compromising the central network protection policy provided by Application Control.

Prerequisites:

- Using **Tools** > **Default Options**, verify that:
  - On the ***Computer*** tab, the **Local Authorization** default option is **Enabled**.

    Tip: You can also use this option to disable local authorization on all computers.

  - On the ***User/User Group*** tab, **Execution Blocking** default option is set to: **Ask user for *.exe only**, for the **Blocking mode**. The user is prompted to authorize the executable only. After the executable file is authorized, any DLLs or other executable files used by the authorized file will automatically be authorized.

    Tip: You may type a customized user notification message in the **Notification Text** field, such as `Do you want to authorize this file locally?`

- On the ***User Explorer*** module ***File Groups by User*** tab, the users and user groups permitted to use local authorization are listed.

1. Log in to a Ivanti Device and Application Control client computer using a locally authorized user or user group account.

2. Select an executable file, script, or macro to run that is not centrally authorized.

   Step Result: The ***Ivanti Device and Application Control - Unauthorized Application Detected*** dialog shows detailed information about the application that is about to run.

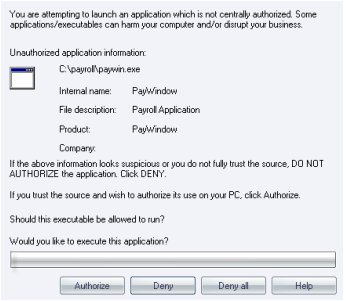


Figure 18: Ivanti Device and Application Control - Unauthorized Application Detected

3. Select one of the following options:

Option	Description
Deny	Denies local authorization of the specific executable file, script, or macro. The user is notified the next time an attempt is made to run the software application.
Deny All	Denies local authorization of all executable file, scripts, and macros.
Authorize	Authorizes the program locally only for that specific computer.

Result: A progress bar appears at the bottom of the dialog. The ***Ivanti Device and Application Control - Unauthorized Application Detected*** dialog closes and the authorized application runs or is denied, based on the option selected.

Note: The file is automatically denied and the dialog closes, if you do not respond within the time-out period.

Working with the Exe Explorer

You can use the ***Exe Explorer*** module to create a list of executable files, scripts, and macros that you want to authorize.

Use **Exe Explorer** for a newly configured reference computer to ensure that only clean (uncompromised) files are authorized. The reference computer does not have to be the same computer that the Management Console is installed on. You can browse the network and select any available computer as your reference. You may manually assign macros and scripts to the central file

authorization list using the **Exe Explorer** module, although Ivanti recommends that you do this using the **Log Explorer** module.

Before using the **Exe Explorer** module, you must set up the default options for this module. The default options determine the way Ivanti Device and Application Control searches computer directories and how results are displayed. When you choose the root directory of a computer, the search process creates a list of all executable files, scripts, and macros on the computer. This process can be slow and is typically done when you want to check all the applications installed on a computer.

Restriction: Only administrators with defined user access rights can use the **Exe Explorer** module.

Setting Up the Exe Explorer Default Options

The ***Exe Explorer*** searches computer directories for executable files, scripts, and macros.

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

   Step Result: The ***Exe Explorer*** window opens.

2. From the Ivanti Device and Application Control ***Control Panel***, select **Tools** > **Default Options**.

   Step Result: The ***Default Options*** dialog opens.

3. Select the ***Exe Explorer*** tab.

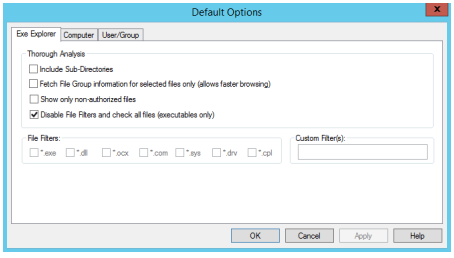


Figure 19: Default Options Dialog - Exe Explorer Tab

4. Select or clear one or more of the following check boxes:

Option/button	Description
Include SubDirectories	Defines the directories to search. Select to search for files from a named directory and sub-directories.
Fetch File Group information for selected files only (allows faster browsing)	Displays the file group information for all files or only selected files. Select search only for files with standard file extensions and display file group information only for files you select.
Show only non-authorized files	Displays previously authorized files. Select to filter previously authorized files and show the remaining files.

Option/button	Description
Disable file filters and check files (executable only)	Checks for all files or files with specific extensions. Select to search for files with standard file extensions.

5. To search for files with:
   - One or more non-standard file extensions, deselect the **Disable File Filters and check all files (executables only)** check box and enter the custom file extension(s) in the **Custom Filter(s)** field. Separate entries using semi-colons with no spaces.
   - Specific file extensions, deselect the **Disable File Filters and check all files (executables only)** check box and select the file extensions from the ***File Filters*** panel.

Result: The ***Exe Explorer*** module window changes to reflect the default options you select.

Adding a File Group

File groups simplify the process of administering large numbers of executable, script, and macro files for users. Instead of individually authorizing files, you can logically group files together logically by creating file groups.

1. In the Management Console, select **View** > **Modules** > **Exe Explorer** > **Explorer** > **Manage File Groups**.

   Step Result: The ***File Group Management*** dialog opens.

2. Click **Add File Group**.

   Step Result: The ***Add File Group*** dialog opens.

3. Enter the name of the file group in the **File Group** field.
4. Click **OK**.

   Step Result: The file group is added to the **File Groups** list.

5. Click **Close**.

Result: The file group is added to the list. You can now assign files to the new file group.

> **Note:** You must grant dedicated accounts such as `LocalSystem` the right to use the appropriate file groups containing services. For example, if you create a `Windows File Group` where you place all operating system executable files (including Windows services that run with the `LocalSystem` account), you should grant `LocalSystem` the right to use this Windows file group.

Renaming a File Group

You can rename an existing file group.

1. In the Management Console, select **View** > **Modules** > **Exe Explorer** > **Explorer** > **Manage File Groups**.

   Step Result: The ***File Group Management*** dialog opens.

2. Select a file group to rename.
3. Click **Rename File Group**.
4. Type a new file group name.
5. Click **OK**.
6. Click **Close**.

   Step Result: The ***File Group Management*** dialog closes.

Result: The file group is renamed.

Deleting a File Group

You can delete an existing file group.

1. In the Management Console, select **View** > **Modules** > **Exe Explorer** > **Explorer** > **Manage File Groups**.

   Step Result: The ***File Group Management*** dialog opens.

2. Select the file group you want to delete.
3. Click **OK**.

   Step Result: dialog closes**..** The File Group Management

4. Deleting a file group may remove parent-child dependencies for related file authorizations.
5. Click **Close**.

   Step Result: The ***File Group Management*** dialog closes.

Result: The file group is removed from the database.

> **Note:** Deleting a file group may remove parent-child dependencies for related file authorizations.

Working with User Explorer

You can use the ***User Explorer*** module to control user access to authorized software.

Many enterprises differentiate between types of users to control user access to software applications. Controlling user access to applications reduces the risk associated with malicious software applications. The **User Explorer** main window is divided in two tab pages where you can:

- Link users and user groups with the file groups containing files authorized for users, using the ***File Groups by User*** tab.
- Assign specific authorizations to users and groups, synchronize domains, and change options, using the ***Users by File Group*** tab.

About File Groups

Associating file groups with domain user groups reduces administrative burden because new user group members inherit application authorization assigned to the parent file group.

The users, groups, and computers assigned to each domain file group are defined within domain controllers as follows.

- You can authorize users directly or indirectly through a user group assignment.
- A user can be a member of more than one user group. A user group member is authorized to use the applications that are approved for the associated user groups.
- Users can have indirect authorization assignments resulting from creating parent-child relationships.
- When you assign a system group or system user a file authorization, the authorization is assigned to the associated users for every computer in your network.
- You can authorize a global user groups to use an application. Any member of a global user group is then indirectly authorized through domain user groups to use that application.

File Group by User Tab

You can use the ***File Group by User*** tab to group administrative actions based on user access.

Using the ***File Groups by User*** tab you can:

- Associate users and user groups to file groups.
- Change user, user group, and computer options.
- Send updates to computers.
- Synchronize local users, user groups, and domain member information.
- View indirect file group assignments.

The ***File Groups by User*** tab consists of the following panels:

- ***Users, Groups, Computers and Domains***
- ***File Groups***

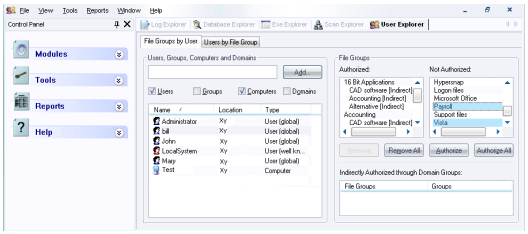


Figure 20: File Groups by User Tab

The following table describes the key elements in the **Users, Groups, Computers and Domains** panel:

Table 20: **Users, Groups, Computers and Domains** Panel

Name	Description
Users, Groups, Computers and Domains field	Type a name to add to the list of available users, groups, computers, and domains.
Add	Adds a name to the list of users, groups, computers, and domains names.
Users; **Groups**; **Computers**; **Domains** check box	Includes or excludes from the list of available users, groups, computers, and domains.
Users, groups, computers and domains list	Lists the selected users, groups, computers, and domains.

The following table describes the key elements in the **File Groups** panel:

Table 21: **File Groups** Panel

List Name	Description
Authorized	Lists authorized files groups for the user or user group selected from the list. This list may include indirect authorizations created by parent-child relationships.
Not Authorized	Lists files groups not authorized for the user or user group selected from the list.
Indirectly Authorized through Domain Groups	Lists file groups and domain user groups that specify the domain user groups that indirectly authorize other file groups to the user or user group selected from the list.

You can expand and collapse the hierarchy structure for an object in the **Name** column, to browse for the specific users or user groups that you want to create file group assignments for.

The following table describes the key elements in the ***Users, Groups, Computers and Domains*** list:

Table 22: ***Users, Groups, Computers and Domains*** List Columns

Column	Description
Name	The name of the user, user group, computer, or domain.
Location	Windows domain; only for computers or domains.
Type	Description of the list item like computer, global user, domain, and so on.

Assigning File Groups to Users

After creating file groups and parent-child relationships you want to use, you can assign file groups to users or user groups.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***File Groups by User*** tab.
3. In the **Users, Groups, Computers and Domains** panel, select a user or user group.
4. Select one or more file groups from the ***Not Authorized*** list.
5. Select one of the following options:

Command	Action
Authorize	Adds the selected file group to the list of file groups directly authorized for the selected user or user group.
Authorize All	Adds the names of file listed as **Not Authorized** to file groups directly authorized for the selected user or user group.

Note: Changes to file authorizations or user membership for a file group can remove users that are indirectly authorized for a file group.

Result: The user or user group is now assigned to the designated file group.

After Completing This Task:

You can send the updated authorization(s) immediately to the client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients, they automatically receive updates when they restart or at next user log in.

Removing File Groups from Users

You can remove file group assignments by user or user group.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***File Groups by User*** tab.
3. In the **Users, Groups, Computers and Domains** panel, select a user or user group.
4. Select one or more file groups from the ***Authorized*** list.
5. Select one of the following options:

Command	Action
Remove	Deletes the selected file group from the list of file groups directly authorized for the chosen user or user group.
Remove All	Deletes the file group names listed as **Authorized** from file groups directly authorized for the selected user or user group.

Result: The selected file group is no longer authorized for the chosen user or user group.

After Completing This Task:

You can send the updated authorization(s) immediately to the client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients, they automatically receive updates when they restart or at next user log in.

Changing the User Explorer Options

You can access the **Default Options** tool from the ***User Explorer*** using a shortcut menu.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***File Groups by User*** tab.
3. In the **Users, Groups, Computers and Domains** panel, right-click to select user, user group, or computer in the **Name** column.

   Step Result: A right-mouse menu appears.

4. Select **Options** from the shortcut menu.

   Step Result: The ***Default Options*** dialog opens.

Result: You have a shortcut to access the ***Default Options*** dialog directly from the **User Explorer** module to the**Control Panel** > **Tools** > **Default Options** for changing user, user group, and computer options.

Synchronizing Local Users and User Groups

An administrator must manually import and synchronize local user and user groups to add them to the database, when the users and groups are not part of the existing domain. This can be done through the User Explorer module (when Application Control is set up) or the Synchronize Domain Members tool.

Prerequisites:

You must ensure that:

- Application Control is set up and licensed.
- File groups are assigned for the target machine.

Restriction: Only an *Enterprise Administrator* can synchronize Novel Organization Units (OU) local user and user group domain information.

The Ivanti Device and Application Control database contains only domain users by default, therefore local users and groups must be added separately.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***File Groups by User*** tab.
3. In the **Users, Groups, Computers and Domains** panel, right-click to select a local computer on the **Name** column.

   Step Result: A context menu appears.

4. Select **Synchronize Local Users/Groups** from the context menu.

   The ***Ivanti Device and Application Control Management Console*** shows you an error message if the computer being synchronized is offline.

   Step Result: The operation result appears in the ***Output*** window.

(Alternative) Using the Synchronize Domain Members Tool to Synchronize Local Users and User Groups

Prerequisites:

You must ensure that:

- Remote Registry service is running on the target computer.
- File & Printer Sharing is enabled and opened in the firewall on the target computer.
- User you want to synchronize has admin permissions on the local machine and is able to access `c$` and `admin$` from the SXS.
- (Windows XP only) Simple File Share is disabled in Folder Options.
- User you want to import has password credentials.
- You know the domain the user belongs to.

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. Click the **Different user name** option to authenticate to the network as a different user.

   Step Result: The ***Connect As...*** dialog opens.

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 local user and user groups information is synchronized and imported to the database, confirmed by a message in the ***Output*** window of the Management Console.

The User by File Group Tab

You can use the ***User by File Group*** tab to group administrative actions based on file groups.

Using the ***Users by File Group*** tab you can:

- Associate file groups to users and user groups.
- View file group assignments.
- Change user and user group options.

The ***Users by File Group*** tab consists of the following panels:

- ***File Groups***
- ***Associated Users***

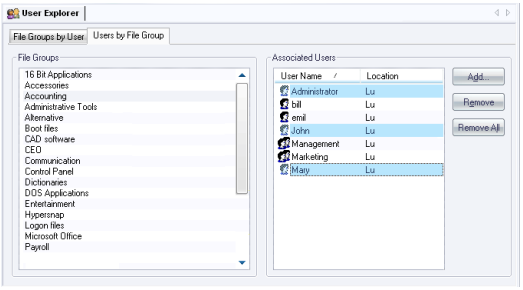


Figure 21: The **Users by File Group** Tab

The following table describes the key elements for the **Users by File Group** tab:

Table 23: **Users by File Group** Tab Elements

List Name	Description
File Groups	Lists the existing file groups including file groups imported when using the Standard File Definitions or file groups created by a Ivanti Device and Application Control administrator.
Associated Users	Shows the list of users or user groups directly or indirectly authorized to use the file group select from the ***File Groups*** list.

The following table describes the key elements in the ***Associated User*** list:

Table 24: Associated Users List Columns

Column	
Name	The name of the user, user group, computer, or domain.
Location	Windows domain; only for computers or domains.
Type	Description of the list item such as computer, global user, domain, and so forth.

Assigning Users to a File Group
You can assign specific permissions to local users and user groups. Only authorized applications and scripts assigned to a user or a user group can run on the client. Ivanti Device and Application Control verifies which file group is associated with an executable, script, or macro and whether the user has permission for the file group.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***User by File Group*** tab.
3. In the **File Groups** list, select a file group.
4. Click **Add**.

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

5. Click **Search**.

   Step Result: The **Name** column list the user group, user, local user group, and local user names.

6. Select one or more user or user group names from the list.
7. Click **OK**.

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

Result: The file group is assigned to the designated user or user group.

After Completing This Task:

You can send the updated authorization(s) immediately to the client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients, they automatically receive updates when they restart or at next user log in.

Removing Users from a File Group
You can remove individual users or groups of users from existing file groups.

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

   Step Result: The ***User Explorer*** window opens.

2. Select the ***User by File Group*** tab.
3. In the **File Groups** list, select a file group.
4. In the **Associated Users** list, select one or more users or user groups.

5. Select one of the following options:

Command	Action
Remove	Deletes the link for the file group assignment from the selected file group.
Remove All	Deletes the link for the file group assignment for users and user groups from the selected file group.

Result: The designated user or user group link is deleted from the file group assignment.

After Completing This Task:

You can send the updated authorization(s) immediately to the client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients, they automatically receive updates when they restart or at next user log in.

Working with Database Explorer

The ***Database Explorer*** module is the primary tool for viewing and managing database records as well as creating and maintaining file group relationships.

You can use the ***Database Explorer*** to:

- Administer file group assignments.
- Manage file groups.
- View database records.
- Administer file group relationships.

The Ivanti Device and Application Control database serves as the central repository of authorization information for:

- Authorized executable files, scripts, and macros.
- Digital signatures that uniquely identify the authorized files.
- File groups.
- File group parent-child relationships.
- Authorized users and user groups.

The **Database Explorer** module consists of two tab pages:

- The ***Files*** tab shows you all files stored in the Ivanti Device and Application Control database. You can assign files to file groups.
- The ***Groups*** tab allows you to manage file group relationships.

When working in either tab you can access the **Explorer** menu to manage file groups, and the **Tools** menu to do database maintenance.

On the ***Files*** tab page you can see the following columns and fields:

Table 25: Files Tab Column Descriptions

Column	Description
File Name	Object used to filter the result query for the **Database Explorer** main page, used in combination with the **File Group** field, which field accepts wildcard.
File Group	Field used to filter the result query in the **Database Explorer** main page to select the required file group from the list or use with `<All>`, and is used in combination with the **File Group** field.
ID	Unique system file identifier.
File Name	Full file name.
Extension	File extension.
Original Path	Full path from where the file was first scanned.
File Group	The assigned file group. <Not Authorized> if the file has not been assigned.
Hash	The calculated digital signature as stored in the database.
File Type	The file category: executable, macro, or script.

On the ***Groups*** tab page you can see the following panels and columns:

Table 26: Groups Tab Column Descriptions

Item	Description
File Groups	This panel shows the top-level file groups. File groups displaying a lock symbol cannot be deleted.
Relationships	This panel shows all available relationships.
Name	Shows the file group name in the ***File Group*** or ***Relationship*** panel.
Type	Shows the relationship type: `Child`, `Parent`, `Child (indirect)`, `Parent (indirect)`.

The Files Tab

The **Database Explorer** page shows the internal system ID, filename, extension, path, file group assignment, and parent-child relationships between file groups for each file on the ***Files*** tab.

The **Database Explorer** module displays a list of all the files stored in the Ivanti Device and Application Control database with a valid digital signature.

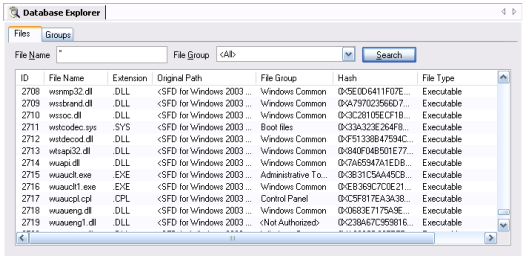


Figure 22: Database Explorer Files Tab

Assigning Files to File Groups

After you create the necessary file groups and required parent-child relationships, you can assign executable files, scripts, and macros to file groups.

1. In the Management Console, select **View** > **Modules** > **Database Explorer**.
2. Select the file(s) to assign to a file group.
3. Right-click the file selection.
4. Select the ***Assign to File Group*** option.

   Step Result: The ***Assign Files to a File Group*** dialog opens.

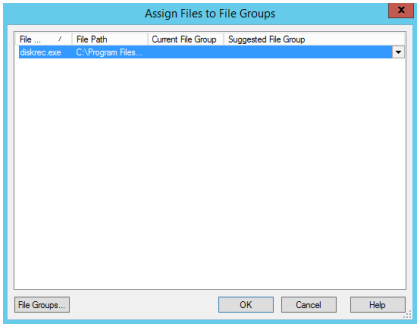


Figure 23: Assign Files to File Groups Dialog

Table 27: Assign Files to File Groups Columns

Column	Description
File	Name of the file including extension.
File Path	Complete file path name, including the drive.

Column	Description
Current File Group	The file group to which the file currently belongs. Files that are not assigned to a file group are designated as **<Not Authorized>**.
Suggested File Group	A proposed file group based on the file name. A file having the same name as another file in the database is suggested to belong to the same file group as the initial file.

5. Select a file group from the drop-down list in the **Suggested File Group** column.
6. Click **OK**.

Result: The file(s) are now assigned to the designated file group.

> **Note:** You can assign a script or macro to a file group as a script, as distinguished from an executable file.

Changing File Assignments

You can modify file lists and group assignments periodically.

You may need to modify your file lists or assignments when:

- New software has been installed on your protected endpoints, and you wish to permit users access to the new applications.
- Updated versions of existing software are provided, and you want users to use the new versions.
- An executable file, script, or macro has become corrupted or is no longer appropriate, and you want to prevent users from running the application.
- Multiple users are locally authorizing files that are centrally denied, as reported in the log files.

Viewing Database Records

The **Database Explorer** module displays a list of the executable, script, and macro files, digital signatures, and assigned file groups stored in the Ivanti Device and Application Control database.

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

   Step Result: The ***Database Explorer*** page opens.

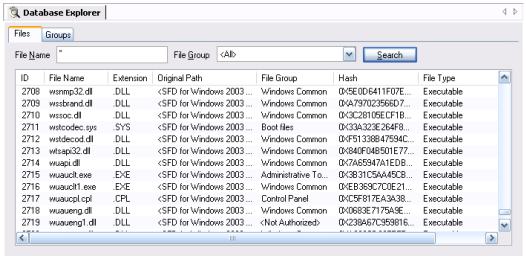


Figure 24: Database Explorer Module

2. Select the ***Files*** tab.
3. Type a file name in the ***File name*** field. You can use wild cards (* and ?).
4. Select a file group from the ***File Group*** list.
5. Click **Search**.

Result: You can view the files stored in the database including the digital signature and file group assignment.

Caution: Your request may process slowly when you have a large Ivanti Device and Application Control database.

Saving the Database Records

You can save database records as a Comma Separated Value `*.csv` files that you can use with third-party reporting tools.

1. Use the **File** > **Save as** command.

   Step Result: The Windows ***Save as*** dialog opens.
2. Select the file location and name.
3. Click **Save**.

Result: The records are saved as a Comma Separated Value `*.csv` file. You can import the file information to a third party reporting tool.

The Groups Tab

You use the ***Groups*** tab to manage parent-child relationships between file groups.

Creating Parent-Child Relationships

You administer parent-child relationships between file groups using the ***Database Explorer Groups*** tab.

Prerequisites:

You must create parent and child file groups before creating parent-child relationships.

Parent-child relationships may be direct or indirect. A direct relationship exists when a file group has a direct line of descendants between parent and child file groups. All other file group relationships are indirect relationships.

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

   Step Result: The ***Database Explorer*** page opens.
2. Select the ***Groups*** tab.
3. Select the desired group from the ***File Groups*** list.

4. To assign a relationship, by selecting a file group from the ***Relationships*** list and click one of the following:
   - **Add child**
   - **Add parent**
   - **Remove**

   Step Result: The **Type** column changes from `Available` to:
   - `Child`
   - `Parent`
   - `Child (Indirect)`
   - `Parent (Indirect)`

Result: The parent-child relationship associations are shown with one of the following icons indicating the relationship status:

Table 28: File Group Relationship Status Icons

Icon	Description
	The file group is a parent of the one selected in the ***File Groups*** panel.
	The file group is child of the one selected in the ***File Groups*** panel.
	The file group is an indirect parent of the one selected in the ***File Groups*** panel.
	The file group is an indirect child of the one selected in the ***File Groups*** panel.
	A file group created by a Ivanti Device and Application Control administrator that can be deleted or renamed.
	A file group created by the program that is blocked and cannot be deleted.

Note: You cannot delete indirect relationships, you must first proceed to the directly related file group and then remove the relationship.

The following examples demonstrate hierarchical parent-child file group relationships.

Example:

The file group `16 Bit Applications` is the parent of `Accessories`, and also has indirect child `Alternative` and `CAD software`:

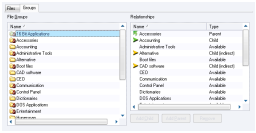


Figure 25: File Group Parent Relationship

The File Group `Accounting` is the child of `Marketing` who also has an indirect child `Payroll`:

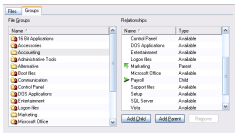


Figure 26: File Group Child Relationship

This is the consequence of the following parent-child assignments:

Figure 27: File Group Parent-Child Relationship

When assigning the file group `Payroll` to a user or user group; there is also an indirect assignment because of this relationship:

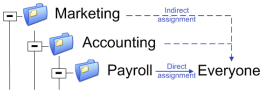


Figure 28: File Group Indirect Assignment

You can view indirect parent-child relationship assignments by using the ***File Groups by User*** tab of the ***User Explorer*** module.

Working with Log Explorer

Every endpoint protected by Ivanti Device and Application Control generates activity logs for administrator and user-defined client actions. The information in these logs is sent to the Application Server and can be viewed through the ***Log Explorer*** module of the Management Console.

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 granted or denied applications or administrator actions.
- Generate custom reports using templates.

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

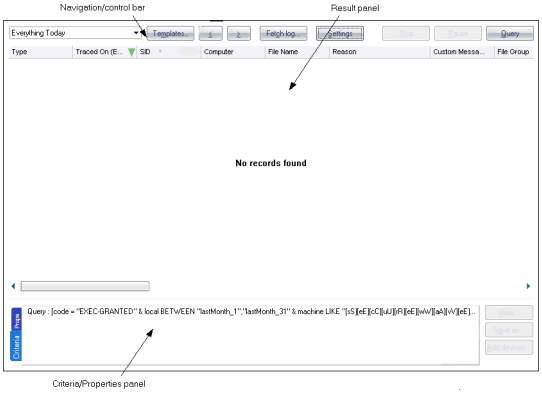


Figure 29: Log Explorer Window

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 29: 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.

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 30: 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.

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

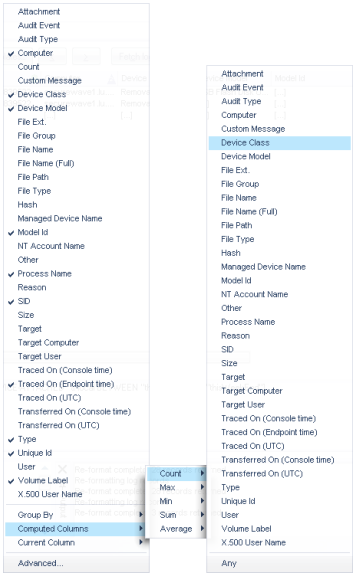


Figure 37: Computed Columns Menu

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.

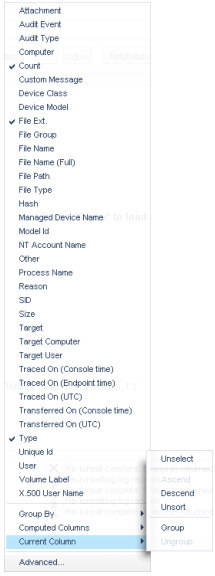


Figure 39: Reset Column Groups Headings

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

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

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 31: Log Explorer Predefined Templates

Template Name	Shows	Prerequisite
Applications denied today	All applications that have been denied for the day.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured.
Applications locally authorized today	All applications that have been locally authorized for the day.	This only applies to user for which the **Execution Blocking** option is properly configured. You must enable the **Local Authorization** option for each computer you want to audit.
Applications often denied this week	The most often denied applications for the week.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured.
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.

Template Name	Shows	Prerequisite
Audit for PC xyz	Audit trace for a specific computer.	You must change the "xyz" computer to an actual computer 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 in the ***Template Settings*** dialog.
Audit today	Daily audit trace.	No action is required.
Everything today	Everything that happened for the day.	No action is required.
Hardening violations this month	All client hardening violations detected for the month.	You must configure the **Client Hardening** option.
Relaxed logon apps this week	All relaxed logon applications done for the month.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured. You must configure the **Relaxed Logon** option for each user that you want to audit.
Users denied acc. to regedit this week	The user tried to run Windows regedit utility and access was denied.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured.
Users denied app. device this week	All applications and device denied this for the week.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured. You must enable the **Device Log** option.

Template Name	Shows	Prerequisite
Users denied apps this month	All applications denied by user for the month.	This only applies to user for which the **Execution Blocking** option is properly configured. Entries are only logged when the **Execution Log** option is properly configured.

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.

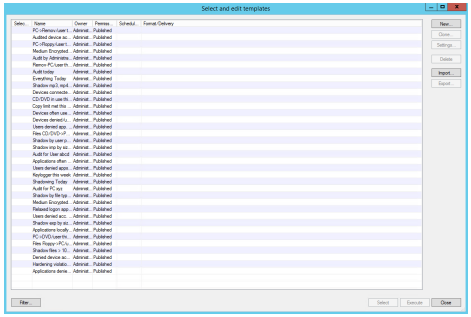


Figure 40: Select and Edit Templates Dialog

2. Click **New**.

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

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

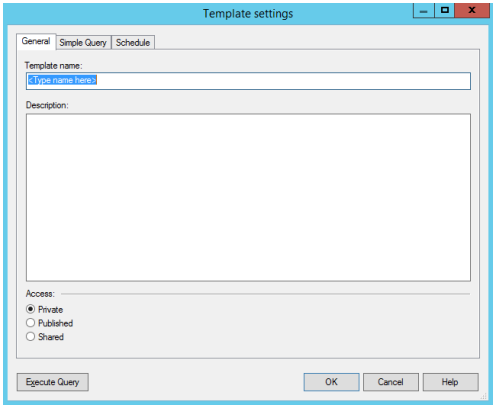


Figure 41: Template Settings Dialog

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.

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.

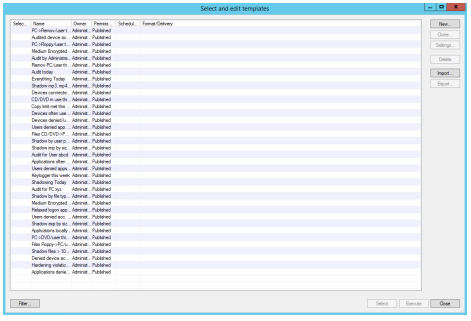


Figure 42: Select and Edit Templates Dialog

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:

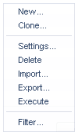


Figure 43: Templates Menu

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.

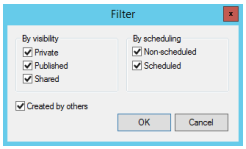


Figure 44: Filter Dialog

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.

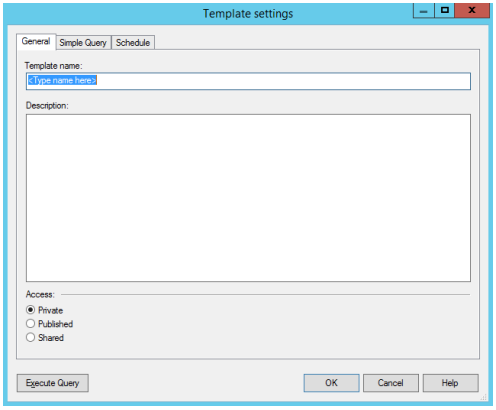


Figure 45: Template Settings Dialog

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**.

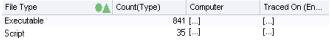


  Figure 46: Grouping Results in the Query

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

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.

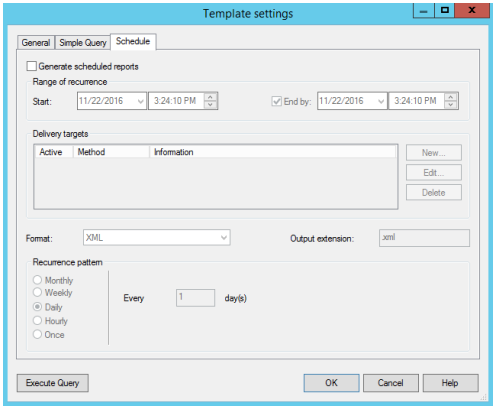


Figure 47: Schedule Tab

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.

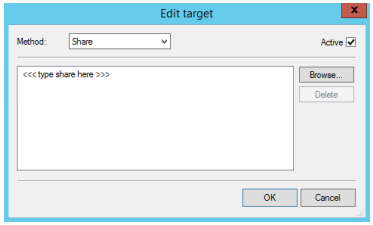


Figure 48: Edit Target Dialog

   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.

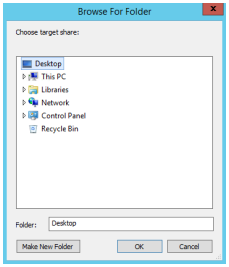


Figure 49: Browse for Folder

   d) Select a shared folder.
   e) Click **OK**.

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

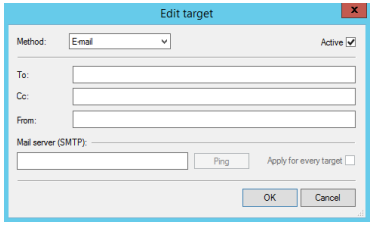


Figure 50: E-mail Options

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.

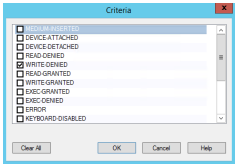


Figure 51: Criteria Dialog

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

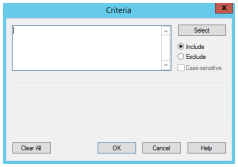


Figure 52: Free-text Criteria Dialog

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.

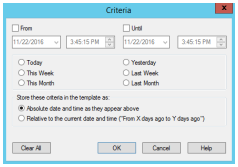


Figure 53: Time Criteria Dialog

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

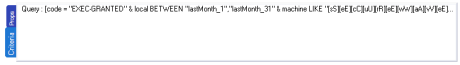


Figure 54: Example Criteria settings

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 32: 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.

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.

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.

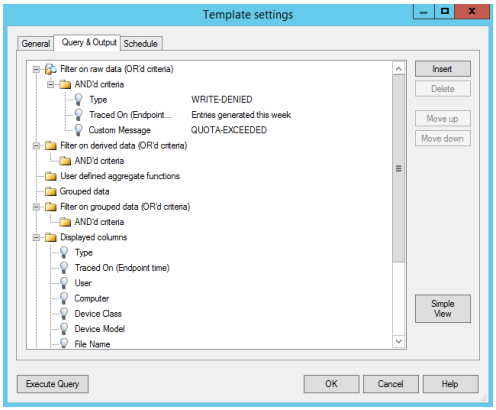


Figure 55: Query & Output Tab

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**.

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.

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 56: Props Tab

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

Figure 57: 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 33: Log Explorer Columns

Column	Description
Audit Event	Shows the type of event that triggered the audit log.

Column	Description
Audit Type	Shows the type of action the administrator carried out. The can be **Device Control**, **Application Control**, or **Unspecified**.
Computer	Shows the name of the computer where file access was requested.
Count	Shows the number of log entries hidden in a single row, accompanied by a grouping symbol displayed on the column header. Alternatively, The may be a computed column of data.
Custom Message	Indicates the reason the application is running or not running. For example, although authorized, the file may not run because the computer is in non-blocking mode or because there is a file path rule authorization.
File Ext	Shows the file extension.
File Group	Shows the file group the executable, script, macro, or file containing a VBA macro assignment. The can also be shown as **<Not Authorized>**.
File Name	Shows the file that access was authorized or denied for.
File Name (full)	Shows the full name (including path) of the file that access was authorized or denied.
File Path	Shows the file path for the file that access was authorized or denied.
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.
NT Account Name	Domain user name of the person who triggered the event, for example `MARVIN/johns` or `LocalSystem`.
Other	Shows additional information for an audit event, such as, when an administrator erases a scheduled permission. The column may also show parameters.
Reason	Indicates whether an action was granted or denied. Possible values: **GRANTED**, **DENIED**, **NOPERMISSIONS**, **LOCALAUTH**, **QUOTAEXCEED**, **NON-ENCRYPTED**, **SANCTUARY-ENCRYPTED**, **PGP-ENCRYPTED**, **OVERRIDESHADOW-CONFIGURED**.
SID	Shows the secondary identifier for the user, for example `S-1-5-21-647365748-5676349349-7385635473-1645`. The is useful when attributing actions recorded in log files to users who have left your organization.
Target	Shows the device name for which the permissions were modified.

Column	Description
Target Computer	Shows the name of the computer that was the target of the administrator action.
Target User	Shows the name of the user or group that the administrator action was applied.
Traced On (Console time)	Shows the date the event occurred on the console computer.
Traced On (Endpoint time)	Shows the date the event occurred on the client computer.
Traced On (UTC)	Shows the date (Coordinated Universal Time) the event occurred on the client computer.
Transferred On (Console)	Shows the date the event record was transferred from the client computer to the Ivanti Device and Application Control Application Server.
Transferred On (UTC)	Shows the date (Coordinated Universal Time) the event record was transferred from the client computer to the Ivanti Device and Application Control Application Server.
Type	Shows the cause of the event that triggered the log. The can be **Execution Granted**, **Execution Denied**, or the type of audit event.
User	Shows the name of the user who triggered the event. For users removed from the Active Directory, The field displays the SID, enabling the person who triggered an event to be identified after they have left your organization.
X.500 User Name	Shows the user name in Lightweight Directory Access Protocol format. The reflects the directory tree in which the user information is stored. For example, the X.500 user name may be `CN=John Smith, CN=Users,or DC=Marvin`.

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

The **Custom Message** field displays one of the following values which are affected by the system-wide option settings for **Execution Blocking** and the logging mode:

Table 34: Custom Message Field Values

Value	Description
Authorized	The file is known, its digital signature is recorded in the Ivanti Device and Application Control database. If The file is assigned to a file group, The is also shown.

Value	Description
Denied	The file was not allowed to run because it was not centrally or locally authorized.
Logon	The file was allowed to run because **Relaxed logon** default option is enabled.
ok-dllDontCare	The `*.dll` execution was authorized because the **Execution Blocking** option was set to **Ask user for *.exe only**.
ok-hash	The file ran and the action was logged because the option to **Log Everything** is enabled. The option should only be set for a limited period, or else the system generates an unmanageable amount of data.
ok-localAuth	The file is not centrally authorized, but the user was prompted for local authorization.
ok-nonBlocking	The file ran because the **Non-Blocking** option was enabled.
ok-nonBlockUsr	The file is not centrally authorized, but ran because the **Non-Blocking** option was enabled for a user or group of users.
ok-pathRule	The file was allowed to run because it matched a path rule.

Interpreting Results

You can interpret ***Log Explorer*** results in several ways.

The primary reasons for not allowing file execution, resulting in the **Denied** value in the **Custom Message** field, are as follows.

- The file is unknown or is not centrally authorized. This means that either:
  - The program is not authorized and should remain so. This happens when the user tries to run an unauthorized application.
  - The software has not been yet authorized and should be evaluated for addition to the central file authorization list.
- The user does not have access to the file group that the file is assigned to. For example, the file may have been scanned and is on the central authorization list but belongs to a file group which is not accessible to the user. This means that either:
  - A user is trying to run a program to which the user has no rights.
  - The user, or one of the user groups to which the user belongs, should be granted access to the appropriate file group.

When a user has permission to locally authorize files and uses a particular file frequently, the file may be worth scanning and including it in a special file group to avoid having several users locally authorize the same application.

When you are using the ***Log Explorer*** module to monitor administrator actions the **Target** field may show a different set of information than you normally received for a file group when:

- A user access role has been modified.
- Options are changed.
- The names of the authorized files are changed.

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.

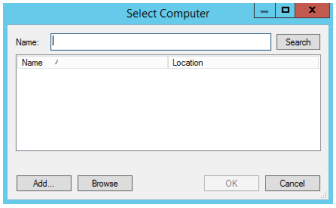


Figure 58: Fetch Logs - Select Computer

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.

Chapter 5

Using Tools

In this chapter:

The **Tools** module consists of administrative tools for administrators to manage database information.

The **Tools** module consists of a collection of administrative tools for performing Ivanti Device and Application Control application user, file group, file authorization and database administration actions.

User administrative actions include:

- Defining global system options.
- Defining Ivanti Device and Application Control administrators.
- Authorizing administrative users to disable Application Control using endpoint maintenance tickets.

File authorization administrative actions include:

- Authorizing file use with path rules.
- Creating an initial list of centrally authorized files by importing Standard File Definitions.
- Controlling the malicious spread of locally authorized files using a spread check tool.
- Exporting lists of authorized files to Ivanti Device and Application Control clients.
- Distributing file authorization updates to client computers.

Database administrative actions include:

- Managing the information retained in the Ivanti Device and Application Control database with a database cleanup tool.
- Adding computers to an existing workgroup by synchronizing domain information.

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.

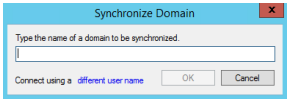


   Figure 59: Synchronize Domain Dialog

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.

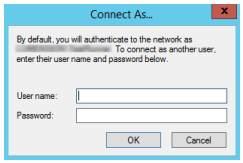


Figure 60: Connect As Dialog

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.

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.

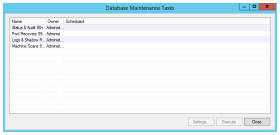


Figure 61: Database Maintenance Dialog

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 Ivanti Device and Application Control administrators:

- A Ivanti Device and Application Control ***Enterprise Administrator*** has full access to all management functions.

  Note: Initially, any member of the `Windows Administrators` group for an 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 ***Administrator*** group.

- A Ivanti Device and Application Control ***Administrator*** has restricted access to Management Console functions as defined by the *Enterprise Administrator*.

A Ivanti Device and Application Control *Enterprise Administrator* can delegate administrative rights to other administrators using Active Directory Organizational Units. These rights are described in the following table.

Table 35: 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

Administrative Rights	Administrator Type	Limitations	Ivanti Device and Application Control Application
Modify global-level device permissions	Enterprise Administrators	NA	Device Control
	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 for an administrator 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
Application Control= Application Control, Device Control= Device Control			

Initially, any administrator with password access to an Application Server and the Management Console can use the Management Console.

Before using Ivanti Device and Application Control, Ivanti recommends setting up Ivanti Device and Application Control 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 a Ivanti Device and Application Control 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.

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 36: 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

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

Ivanti Device and Application Control administrators can customize global system options for:

- Types of events logged.
- Types of notification users receive.
- Conditions that allow users to authorize unknown applications locally.

Default options can be set for:

- All computers.
- All users.
- Specific computers, users, or user groups.

Default Options Page

You can set global options that govern certain aspects of how protected clients interact with the Ivanti Device and Application Controlsystem. These settings apply to all servers or computers protected by Ivanti Device and Application Control.

The ***Default Options*** page consists of the following tabs:

- The ***Computer*** tab options apply to all client computers.
- The ***Users/Group*** tab options apply to all users and user groups.

Each tab page consists of the following columns and panels:

Table 37: 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.
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.

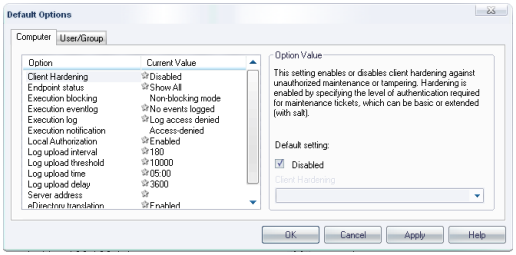


Figure 63: Default Options - Computer Tab

The following table describes the ***Computer*** tab default options and setting values.

Table 38: Default Options - 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 with **Endpoint Maintenance**.
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.

Option	Value	Description
Endpoint Status	**Do not Show**	Does not show the client in the Windows system tray and suppresses all event notifications except local authorization.
	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 policy information.
	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 policy information.
	Show Configured	Shows the client in the Windows system tray. Users can only view device status information for devices configured for the client.
	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.
Execution Blocking	**Blocking mode**	Denies local file authorization. This is the default value.
	Non-blocking mode	Allows local file authorization. Non-blocking mode applies only to executable files.

Option	Value	Description
Execution Eventlog	**No events logged**	Does not send a log entry to the Windows `Event Log` when a file access is denied. This is the default value.
	Access-denied logged	Sends a log entry to the Windows `Event Log` when file access is denied.
	Denied and non-blocked access	Sends a log entry to the Windows `Event Log` when a user requests access to an unauthorized file.
Execution Log	**Log everything**	Creates an Application Server log entry for every executable file access event.
	Log access denied	Creates an Application Server log entry for every denied executable file access event.
	Logging disabled	Does not creates Application Server log entries.
	Log Denied and Unmanaged Execution	Creates client log entries for every denied executable file access event and executable files and scripts which are executed but not expressly authorized, such as through local authorization.
Execution Notification	**No notifications**	Does not notify the user of file execution actions.
	Access-denied	Notifies the user when execution is denied. The user always receives an **Access Denied** message from Windows, there is no way to suppress this message.
	Denied and non-blocked access	Notifies the user when the system is in non-blocking mode or in blocking mode and file access is denied.
Local Authorization	**Enabled**	Local file authorization is allowed. This is the default value.

Option	Value	Description
	Disabled	Local file authorization is not allowed.
Log upload interval	**180**(Default)	Time, shown in seconds, that the client batches log entries. **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
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.
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.
Server Address	**Not configured** (Default)	Defines the IP address or fully qualified DNS name for the Application Server that the client connects to.
SysLog server address	**Not configured** (Default)	Defines the Syslog server address and, optionally, the port number to use.

User/Group Tab

The ***User/Group*** tab shows the user and user group default options that govern how clients interact with the Application Server.

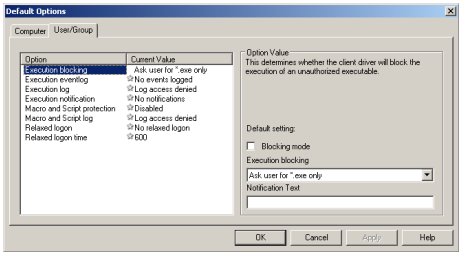


Figure 64: Default Options - User/Group Tab

The following table describes the ***User/Group*** tab default options and setting values.

Table 39: Default Options - User/Group Tab

Option	Value	Description
Execution Blocking	**Blocking mode**	Prohibits user access to unauthorized files. Local authorization is permitted only for the Administrators and `LocalSystem` account. This is the default value.
	Non-blocking mode	Allows user access to files that are not centrally authorized. Non-blocking mode applies only to executable files.
	Ask user for *.exe only	Prompts the user to locally authorize an *.exe file when a digital signature is not found in the database. The user is not prompted to authorize subsequent DLLs, scripts, or other executable files which the authorized executable file accesses.

Option	Value	Description
	Ask user always	Prompts the user to locally authorize the primary executable and control the loading of each additional module or ActiveX when a digital signature is not found in the database.
Execution Eventlog	**No events logged**	Does not create a Windows `Event Log` entry when a file access is denied. This is the default value.
	Access-denied logged	Creates a Windows `Event Log` entry when file access is denied.
	Denied and non-blocked access	Creates a Windows `Event Log` entry when a user requests access to an unauthorized file.
Execution Log	**Log everything**	Creates a client log entry for every executable file access event.
	Log access denied	Creates a client log entry for every denied executable file access event. This is the default value.
	Logging disabled	Does not creates client log entries.
	Log Denied and Unmanaged Execution	Creates client log entries for every denied executable file access event and script access requests from unauthorized users.
Execution Notification	**No notifications**	Does not notify the user of file execution actions. This is the default value.
	Access-denied	Notifies the user when execution is denied.

Option	Value	Description
	Denied and non-blocked access	Notifies the user when the system is in non-blocking mode or in blocking mode and file access is denied.
Macro and Script protection	**Disabled**	No script or macro protection is applied. All VBScripts, JScripts, and macros can run. This is the default value.
	Ask User	Only centrally and locally authorized VBScripts, JScript, or macros are automatically accessible. Ivanti Device and Application Control allows the local user the option to determine whether to access the unauthorized files.
	Deny All	Only centrally and locally authorized VBScripts, JScript, or macros are accessible.
Macro and Script log	**Log everything**	Creates a client log entry for every macro and script execution access event.
	Log access denied	Creates a client log entry for every denied macro and script execution access event. This is the default value.
	Logging disabled	Does not create client log entries.
	Log non whitelisted execution	Creates client log entries for any file execution which executes that is not centrally authorized.
Relaxed logon	**No relaxed logon**	No delay time before blocking is activated. This is the default value.
	Relaxed logon active	A delay time occurs before blocking is activated.

Option	Value	Description
Relaxed logon time	**600** (Default)	Time delay, shown in seconds, after logon during which the client operates in non-blocking mode. The relaxed logon time option only applies to executable files.

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.

User and User Group Precedence Options

Application Control establishes precedence rules for user and user group default option settings.

The user and user group options precedence rules are as follows:

1. An option value set for a specific user and supersedes all other option settings.
2. When no value is set for a specific user, and a value is set for the user group the user belongs to, the group option setting applies.
3. If no value is set for the user or any user groups to which the user belongs, the global default option settings in the ***User/Group*** tab apply.
4. If no global default option is set in the ***User/Group*** tab, the predefined Ivanti Device and Application Control system default settings apply.
5. When a specific user belongs to several user groups that have different option settings, the highest precedence option setting applies. The precedence that determines which option setting is used when a user belongs to multiple user groups having different values set for the same option, depends on a predefined precedence value. The predefined precedence value for certain options is shown in the following table:

Table 40: Option Precedence Values

Option	Value Precedence
Execution log	0 - Log everything 1 - Log access denied 2 - Logging disabled 3 - Log denied and unmanaged execution
Execution Blocking	0 - Blocking mode 1 - Non-blocking mode 2 - Ask user for *.exe only 3 - Ask user always

Option	Value Precedence
Execution Notification	0 - No notifications 1 - Access-denied 2 - Denied and non-blocking mode access
Execution Eventlog	0 - No events logged 1 - Access-denied logged 2 - Denied and non-blocking mode access
Macro and Script protection	0 - Disabled 1 - Ask user 2 - Deny all
The highest numerical value takes precedence. If the **Local Authorization** option is disabled, the **Ask user for *.exe only** and **Ask user always** values are ignored.	

The following flowchart outlines the users/groups precedence rules process.

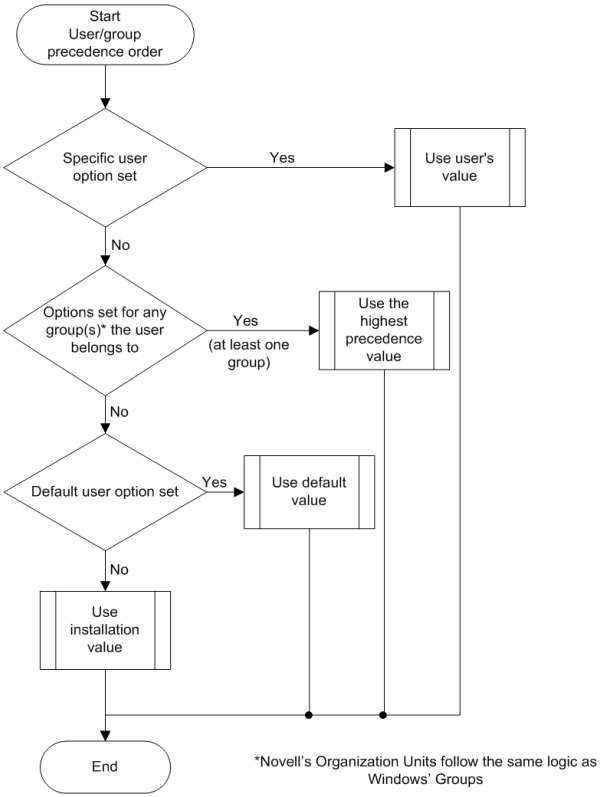


Figure 65: User/User Group Options Precedence

Computer Precedence Options

Application 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.
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.

The following flowchart outlines the computer options precedence rules process.

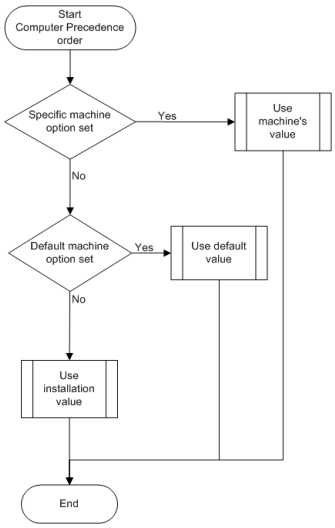


Figure 66: Computer Options Precedence

Global User/User Group Precedence Options

Application Control establishes precedence rules for global user and global user group default option settings.

Some options can be set at a global level or for user/user groups, using the ***Computer*** and the ***User/Group*** tabs. For the ***Execution eventlog***, ***Execution log*** and ***Execution notification*** options that are governed by user/user group options, the precedence rules follow in descending order:

1. Options set for a specific user take precedence over all other option settings.
2. Options set for a user group that a user is a member take precedence. If the user belongs to several groups that have different option settings, the highest precedence option setting applies.
3. Global settings from the ***User/Group*** tab of the ***Default Options*** dialog take precedence.
4. Predefined Ivanti Device and Application Control system default settings take precedence.

The following flowchart outlines the global users/groups precedence rules process.

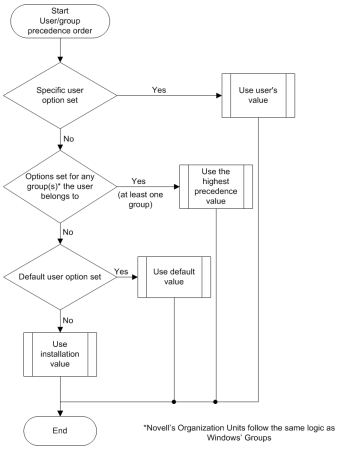


Figure 67: User/User Group Option Precedence

Execution Blocking Precedence Options

Application Control establishes precedence rules for execution blocking default option settings.

The **Execution Blocking** option follows a special rule pattern. When Ivanti Device and Application Control is installed, the `LocalSystem` account and `Administrators` group are automatically set up in **Non-blocking** mode to simplify routine administration, allowing you to install, scan, and authorize files. After you create a central file authorization list, you must manually change the option back to **Blocking** mode.

The Execution Blocking order of precedence is: **User** > **Group (including Everyone)** > **Global User Options** > **Machine** > **Global Machine**. The first explicit (no asterisk, *) in the order is the one that is used. Default settings with an asterisk (*) do not have an efefct on the order.

The following flowchart outlines the execution blocking precedence rules process.

Important: When the **Local Authorization** option is disabled, user access to all unauthorized applications is blocked, regardless of the **Execution Blocking** option value setting.

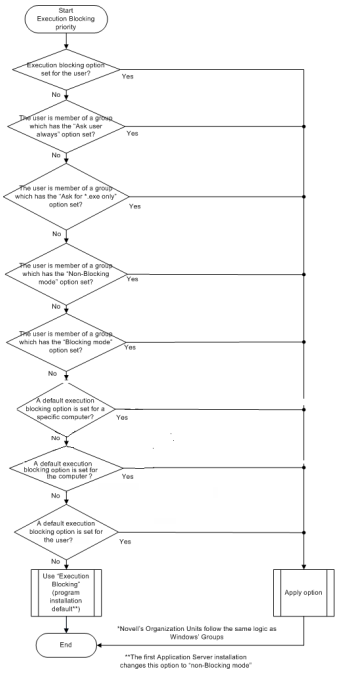


Figure 68: Execution Blocking Option Precedence

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*** and ***User/Group*** tabs to change or reset options for users, computers, user groups, and computer groups.

1. From the Management Console, select **Tools** > **Default Options**.

   Step Result: The ***Default Options*** dialog opens.

2. Select one of the following tabs:

   - ***Computer***
   - ***User/Group***

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.
Cancel	Closes the dialog without saving your changes.
Help	Shows the online help dialog.

After Completing This Task:

You can send the updated authorization(s) immediately to the client computers using the **Control Panel** > **Tools** > **Send Updates** option. If you do not send updates to protected clients, they automatically receive updates when they restart or at next user log in.

Managing Path Rules

For some applications, Application Control based on file signatures does not work. Ivanti Device and Application Control allows you to authorize executable files to run from a specified file path, without checking for authorization from a central listing.

A fundamental principle of authorization by path rules is that the path leads to a trusted source. You can add an additional layer of application control for file authorization by path rule; Ivanti Device and Application Control can verify the identity of the file owner and execute only files that belong to trusted owners. When you activate the **Ownership Check** for a path rule, Ivanti Device and Application Control only permits execution of files owned by a user who is a Trusted Owner.

You can assign path rules to:

- All users
- A specific user group
- A specific user

Column Definitions

The following table describes the columns in the ***Path Rules*** dialog.

Table 41: Path Rules Dialog Columns

Option	Description
Ownership Check	The path rule only applies if a user or user group is listed as a ***Trusted Owner*** in the ***Set Trusted Owner*** dialog.

Option	Description
Include subdirectories	The path rule applies to all files in subfolders of the root folder specified by the file path.
Log Execution	The path rule attempt is logged as ***EXEC-GRANTED*** when the ***Log everything*** option is set for the **Execution Log** default option.

Path Rules Conventions

Path rules are governed by conventions that allow you to select multiple files for path rule authorization, to reduce administrative burden.

A path name can be up to 900 characters long and consist of the following:

- Root specifier
- Path specifier
- Filename specifier

The root specifier can be a:

- Root token
- Drive letter
- Server or computer name

The path specifier is the file path name relative to the root token that must start and end with a backslash and cannot include wild cards.

The file specifier is the file name. The asterisk and question mark wild cards are allowed.

Caution: There is no warning notification when you specify a nonexistent file or directory that cannot be located.

Path Rules Precedence

The following rules apply to using path rules:

- You can adjust Windows NTFS path security properties.
- You can only authorize executable files using path rules.
- New path rules are effective after you send an update to the client computers.
- You can define a path rule that applies to all users and a second path rule that applies to a specific user that shares a subset of common files defined by the first path rule.
- Path rules are cumulative.
- A path rule assigned to a user group can not run an authorized file for a user that is not a group member.
- You can export one or more path rules to a `.csv` file to create a custom report.

Creating a Path Rule for All Users

You can authorize executable files from a specified location of all users and user groups, designated by path.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

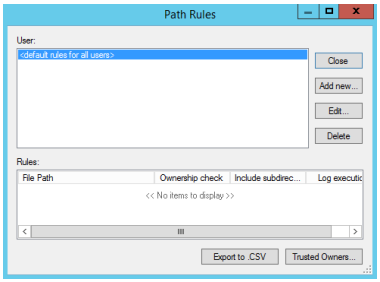


Figure 69: Path Rules Dialog

> **Note:** Using common Windows browser conventions, you can:
>
> - Maximize the dialog screen size
> - Sort columns by header row
> - Resize the width of columns

2. Select **<default rules for all users>**.
3. Click **Edit**.

   Step Result: The ***Edit Path Rules*** dialog opens:

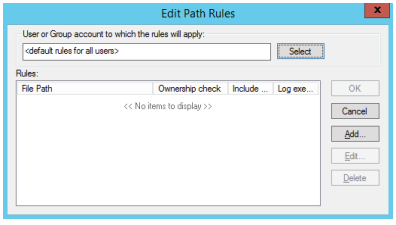


Figure 70: Edit Path Rules Dialog

4. Click **Add**.

   Step Result: The ***Path Rule*** dialog opens.

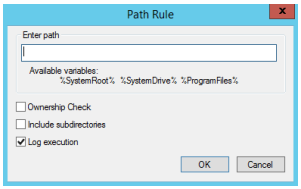


Figure 71: Path Rule Dialog

5. Type the full file path for the executable file.
6. Select one or a combination of the following options:

Option	Description
Ownership Check	The path rule only applies if a user or user group is listed as a ***Trusted Owner*** in the ***Set Trusted Owner*** dialog.
Include subdirectories	The path rule applies to all files in subfolders of the root folder specified by the file path.
Log execution	The path rule attempt is logged as ***EXEC-GRANTED*** when the ***Log everything*** option is set for the **Execution Log** default option.

7. Click **OK**.

   Step Result: The ***Path Rule*** dialog closes.

8. In the ***Edit Path Rules*** dialog, select one of the following options:

Option	Description
Add	Insert a new path for all users.
OK	Save the rule and close the dialog.
Cancel	Abandon the operation and close the dialog.
Edit	Change the selected path for the path rule.
Delete	Erase the selected path from the path rule.

9. Click **Close**.

   Step Result: The ***Path Rules*** dialog closes.

Result: All users are authorized to use the files specified in the path.

> **Note:** If you want to export a path rule, select the path rule and click **Export to .CSV**.

Creating a Path Rule for a User or User Group

You can authorize executable files from a specified location of specific users and user groups, designated by path.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

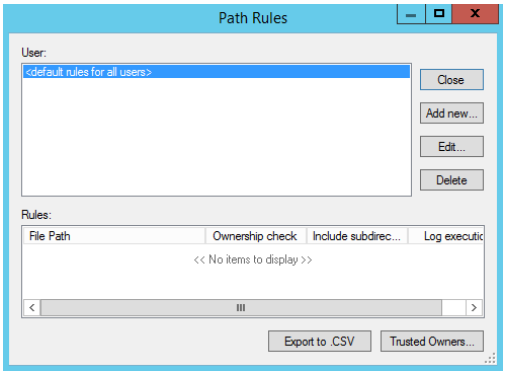


Figure 72: Path Rules Dialog

> **Note:** Using common Windows browser conventions, you can:
>
> - Maximize the dialog screen size
> - Sort columns by header row
> - Resize the width of columns

2. Click **Add new**.

   Step Result: The ***Edit Path Rules*** dialog opens:

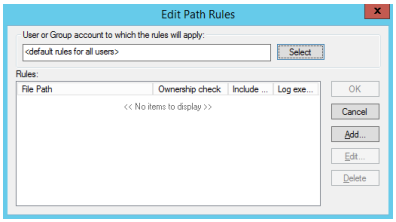


Figure 73: Edit Path Rules Dialog

3. Type the name of the user or user group that the path rule applies to.
4. Click **Add**.

   Step Result: The ***Path Rule*** dialog opens:

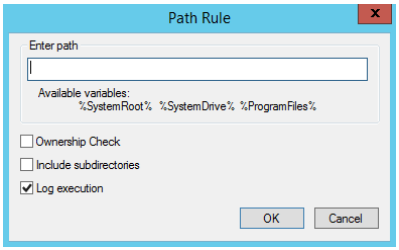


Figure 74: Path Rule Dialog

5. Type the full path for the path rule.
6. Select one or a combination of the following options:

Option	Description
Ownership Check	The path rule only applies if a user or user group is listed as a ***Trusted Owner*** in the ***Set Trusted Owner*** dialog.
Include subdirectories	The path rule applies to all files in subfolders of the root folder specified by the file path.
Log execution	The path rule attempt is logged as ***EXEC-GRANTED*** when the ***Log everything*** option is set for the **Execution Log** default option.

7. Click **OK**.

   Step Result: The ***Path Rule*** dialog closes.

8. In the ***Edit Path Rules*** dialog, select one of the following options:

Option	Description
Add	Insert a new path for all users.
OK	Save the rule and close the dialog.
Cancel	Abandon the operation and close the dialog.
Edit	Change the selected path for the path rule.
Delete	Erase the selected path from the path rule.

9. Click **Close**.

   Step Result: The ***Path Rules*** dialog closes.

Result: The specified user is authorized to use the files specified in the path.

> **Note:** If you want to export a path rule, select the path rule and click **Export to .CSV**.

Trusted Paths and Group Ownership
There are specific behaviors related to the use of a Group as a Trusted Owner.

- If a Trusted Path Rule is applied to a Group it will be applied to all Users within that Group.
- Security Identifiers in Trusted Ownership are a one to one match. This means that if a Group is a Trusted Owner it must be the owner of the file to be executed. It is not enough that a user who is a member of the group is the owner.

Modifying a Path Rule

You can edit a path rule assigned to a user or user group.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

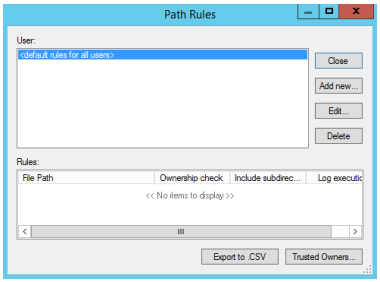


Figure 75: Path Rules Dialog

> **Note:** Using common Windows browser conventions, you can:
>
> - Maximize the dialog screen size
> - Sort columns by header row
> - Resize the width of columns

2. Select a user from the ***User*** panel.
3. Click **Edit**.

   Step Result: The ***Edit Path Rules*** dialog opens with the list of rules for the user.

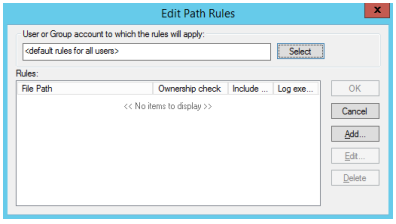


Figure 76: Edit Path Rules Dialog

4. Select a rule from the ***Rules*** panel.
5. Click **Edit**.

   Step Result: The ***Path Rule*** dialog opens.

6. Type a new path rule.

7. Select one or a combination of the following options:

Option	Description
Ownership Check	The path rule only applies if a user or user group is listed as a ***Trusted Owner*** in the ***Set Trusted Owner*** dialog.
Include subdirectories	The path rule applies to all files in subfolders of the root folder specified by the file path.
Log execution	The path rule attempt is logged as ***EXEC-GRANTED*** when the ***Log everything*** option is set for the **Execution Log** default option.

8. Click **OK**.

   Step Result: The ***Path Rule*** dialog closes.

9. In the ***Edit Path Rules*** dialog, select one of the following options:

Option	Description
Add	Insert a new path for all users.
OK	Save the rule and close the dialog.
Cancel	Abandon the operation and close the dialog.
Edit	Change the selected path for the path rule.
Delete	Erase the selected path from the path rule.

10. Click **Close**.

    Step Result: The ***Path Rules*** dialog closes.

Result: The path rule changes for the specified user.

Note: If you want to export a path rule, select the path rule and click **Export to .CSV**.

Deleting a Path Rule

You can delete a specific path rule for selected users or user groups.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

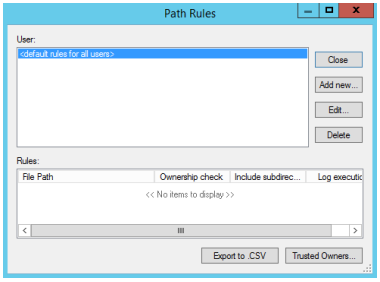


Figure 77: Path Rules Dialog

2. Select a user from the ***User*** panel.
3. Select a path rule from the ***Rules*** panel.

   If you do not select a path rule, then all of the path rules for the selected user or user group are deleted.

   Restriction: You cannot delete the **<default rules for all users>** user group, you can only remove individual rules.

4. Click **Delete**.

   Step Result: A confirmation dialog opens.

5. Click **Yes**.

   Step Result: The rule is removed from the path rule list.

6. Click **Close**.

   Step Result: The ***Path Rule*** dialog closes.

Result: The path rule for the selected user or user group is deleted.

Defining a Trusted Owner

You can identify file owners to execute files only from *Trusted Owners*.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

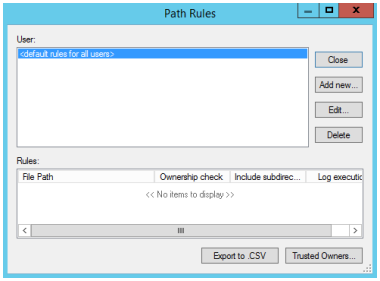


Figure 78: Path Rules Dialog

> **Note:** Using common Windows browser conventions, you can:
>
> - Maximize the dialog screen size
> - Sort columns by header row
> - Resize the width of columns

2. Click **Trusted Owners**.

   Step Result: The ***Set Trusted Owners*** dialog opens.

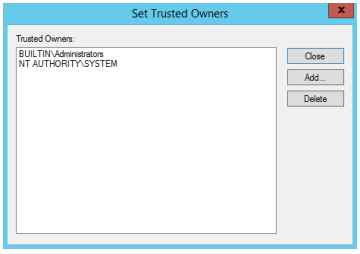


Figure 79: Set Trusted Owners Dialog

3. Click **Add**.

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

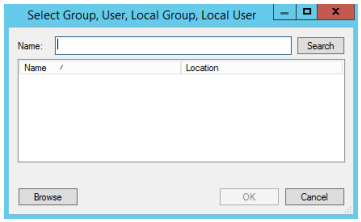


Figure 80: Select Group, User, Local Group, Local User Dialog

4. Click **Search**.
5. Select a user or user group from the ***Name*** column.
6. Click **OK**.

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

7. In the ***Set Trusted Owners*** dialog, click **Close**.

   Step Result: The ***Set Trusted Owners*** dialog closes.

8. In the ***Path Rules*** dialog, click ***Close***.

   Step Result: The ***Path Rules*** dialog closes.

Result: The `Trusted Owner` is assigned to the path rule.

Deleting a Trusted Owner

You can remove `Trusted Owner` assignments from path rules.

1. From the Management Console, select **Tools** > **Path Rules**.

   Step Result: The ***Path Rules*** dialog opens.

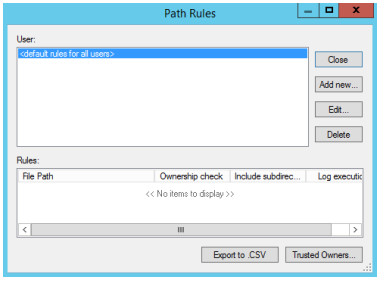


Figure 81: Path Rules Dialog

2. Click **Trusted Owners**.

   Step Result: The ***Set Trusted Owners*** dialog opens.

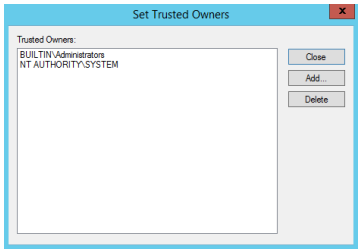


   Figure 82: Set Trusted Owners Dialog

3. Select the user or user group from the ***Trusted Owner*** list.
4. Click **Delete**.

   There is no confirmation dialog.
5. Click **Close**.

   Step Result: The ***Set Trusted Owners*** dialog closes.
6. Click **Close**.

   Step Result: The ***Path Rules*** dialog closes.

Result: The `Trusted Owner` assignment is removed from the path rule.

Defining Spread Check

Ivanti Device and Application Control provides a spread check tool to prevent the malicious spread of locally authorized files.

When Ivanti Device and Application Control detects an unknown executable, script, or macro that is locally authorized on numerous servers or computers during a specific period, Application Control immediately disables the locally authorized files and any self-propagating viruses and worms.

Note: If you have more than one Application Server in your network, only one server should be configured to perform spread checking.

Enabling Spread Check

With the spread checking tool you can specify the frequency for checking and the number of users that trigger the spread checking function.

1. From the Management Console, select **Tools** > **Spread Check**.

   Step Result: The system displays the ***Spread Check*** dialog.

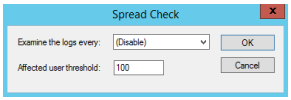


   Figure 83: Spread Check Dialog

2. Select a spread checking frequency from the **Examine the logs every** drop-down menu.
3. Enter the number of users in the **Affected users threshold** field.

   This number represents the number of users, set to 100 by default, that trigger the ***Spread Check*** rule.
4. Click **OK**.

Result: The spread check rule is applied at the frequency you specify. After the administrator investigates the condition that triggered the spread check rule, local authorization can be re-enabled.

Sending File Authorization Updates to Computers

You must send file authorization changes to servers and computers protected by Application 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.
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.

Working with Standard File Definitions

You can use Standard File Definitions (SFD) to simplify the task of building a central file authorization list.

Standard File Definitions (SFDs) contain digital signatures corresponding to standard executable files that are distributed with Microsoft Windows operating systems.

Using SFDs:

- Simplifies initial setup.
- Includes information necessary to automatically allocate files to predefined file groups and assign files to well-known user and user groups.
- Minimizes the risk of authorizing tampered versions of operating system files.
- Simplifies operating system upgrades because Ivanti Device and Application Control recognizes the standard files, and respective default file groups. Ivanti Device and Application Control automatically saves upgraded file definitions to the same locations as the originals.

The following table describes the system users/groups that can access the default SFD file groups.

Table 42: Standard File Definition File Groups and System Users/Groups

File Group Name	Users/Groups Assigned
16 Bit Applications	Administrators (group)
Accessories	Administrators (group), Everyone (group)
Administrative Tools	Administrators (group)
Boot files	Local Service (user), LocalSystem (user), Network Service (user)
Communication	Administrators (group)
Control Panel	Administrators (group)
DOS Applications	Administrators (group)
Entertainment	Administrators (group)
Logon files	Everyone (group)
Ivanti Device and Application Control support files	Administrators (group), Everyone (group)
Setup	Administrators (group)
Windows Common	Everyone (group)

Importing Standard File Definitions

You can use standard Microsoft file definitions to quickly build a central file authorization list for executable files, macros, and scripts.

1. From the Management Console, select **Tools** > **Import Standard File Definitions**.

   Step Result: The ***Import Standard File Definitions*** dialog opens.

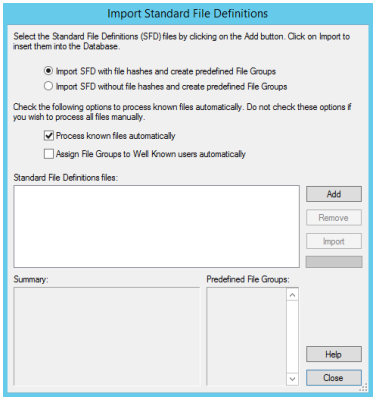


   Figure 84: Import Standard File Definitions Dialog

2. Click **Add**.

   Step Result: The ***Open*** dialog opens and displays files with an `.sfd` extension.

   Tip: You can import standard file definitions from the Self-Service Portal by downloading to a local computer and unzipping the archived files.

3. Select the standard definition file(s) to import.
4. Click **Open**.

   Step Result: The file(s) are shown in the ***Add*** window.

5. Select one or more of the following options:

Option	Description
Assign File Groups to Well Known Users Automatically	Assigns the executable files, scripts, and macros found in the scan to the system users/groups.
Process Known Files Automatically	The wizard adds the file to the database if they have the same name but different digital signature.
Import SFD with file hashes and create predefined File Groups:	Ivanti Device and Application Control automatically imports standard file definition digital signatures, then creates and assigns the files to predefined file groups.

Option	Description
Import SFD without file hashes and create predefined File Groups:	Predefined file groups for standard file definitions are created but no digital signatures are imported. Ivanti Device and Application Control partially assists you by identifying file names and proposing file groups for authorization during scanning.

6. Click **Import**.
7. After importing standard file definitions, click **OK**.
8. Click **Close**.

Result: The designated standard file definitions are now authorized and assigned to respective predefined file groups and system users/groups.

Caution: When you import standard file definitions, you should authorize logon and boot files. If these are not authorized, the system will not work properly. This is especially important for system updates.

After Completing This Task:

Assign the imported predefined file groups to users/groups, if you did not select the **Assign File Groups to Well Known User Automatically** option.

Exporting File Authorization Settings

You can export file authorization settings lists to a target computer.

You can use the file authorization export feature for a computer not connected to the network that needs updated file authorizations. The source computer authorization rules apply to the target computer that the authorized files are copied to.

Note: Exported authorization 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.

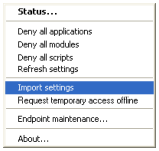


Figure 85: Ivanti Device and Application Control Client Menu

> **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.
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.

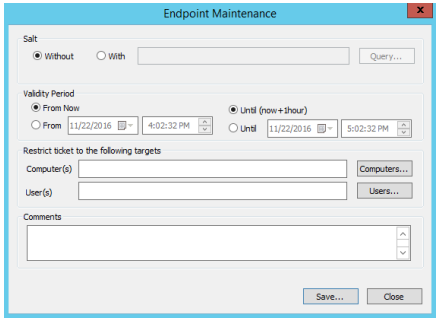


Figure 86: Endpoint Maintenance Dialog

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.
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.

CPA Compliance Mode Configuration Window

Use this window to configure all endpoints assigned Application Control policies to meet the UK CESG's Computer Product Assurance (CPA) compliance requirements for Endpoint Lockdown and Control.

A fully CPA compliant configuration blocks and logs the execution attempts of executables, macros, and scripts that are not centrally authorized. Learn how to to build a central file authorization list.

Statuses

Your environment's CPA compliance status is displayed at the top of the dialog:

CPA Compliance mode enabled	All options required to achieve CPA compliance are set for Computers and Users/Groups in your environment.
Partial CPA Compliance mode enabled	At least one option required to achieve CPA compliance is not set for Computers or Users/Groups in your environment. You will be in this mode when preparing to enable full compliance (for example, ensuring that settings do not disrupt the functioning of endpoints).
CPA Compliance mode is disabled	You are not enforcing CPA compliance requirements in your environment.
Enable CPA Compliance mode settings	Select to start enforcing the option settings required for CPA compliance in your environment. You will be unable to change option settings required for compliance in **ToolsDefault Options**, with the exception of `Client Hardening` (to Extended) and `Execution Log` (to Log Access Denied). **Important:** Test the required option settings in your environment before applying CPA compliance mode.

Computer Options

These options apply the settings required for CPA compliance to all endpoints protected by Application Control.

Execution Blocking is set to Blocking mode	Select to block the execution of unauthorized executable files.
Local Authorization is set to Disabled	Select to prevent users from locally authorizing files to execute.

Client Hardening is set to Basic as a default	Select to prevent users with administrative priviledges from uninstalling the Ivanti Device and Application Control agent, as well as deleting local shadow files and log entries. You can remain CPA compliant by setting the more restrictive `Extended` option (valid salt value required to deactivate the agent) in **Tools** > **Default Options** > **Computer tab**.
Execution Log is set to Log Everything as a default	Select to log every application-related execution event. The volume of logged events produced by this CPA Software Execution Control characteristic can overwhelm your database in very large deployments. You can, with the approval of your company's certification authority, change this logging option to the less detailed `Log Access Denied` in **Tools** > **Default Options** > **Computer tab**. You will remain CPA compliant and reduce the logged events to only those applications which are blocked; please be aware you are no longer capturing the allowed application executions.

User/Group Options

These options apply the settings required for CPA compliance to all users and groups protected by Application Control.

Execution Blocking is set to Blocking mode	Select to block the execution of all unauthorized executable files.
Execution Log is set to Log Everything as a default	Select to log every application-related execution event. The volume of logged events produced by this CPA Software Execution Control characteristic can overwhelm your database in very large deployments. You can, with the approval of your company's certification authority, change this logging option to the less detailed `Log Access Denied` in **Tools** > **Default Options** > **Computer tab**. You will remain CPA compliant and reduce the logged events to only those applications which are blocked; please be aware you are no longer capturing the allowed application executions.
Macro and Script protection is set to Deny All	Select to prevent all VBScripts, JScript, or macros not centrally authorized from running.
Marco and Script log is set to Log Access Denied	Select to log every denied macro and script execution access event.
Relaxed Logon is set to No relaxed logon	Select to block without delay the running of unauthorized logon scripts.

Chapter 6

Using Reports

In this chapter:

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
Administrator, no option settings selected in the ***User Access Manager*** dialog.	***Client Status***, ***User Options***, ***File Groups by User***, ***User by File Group***, ***Machine Options***, and ***Server Settings***. These are the default options for all *Administrators*.

User Role	Available Reports
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

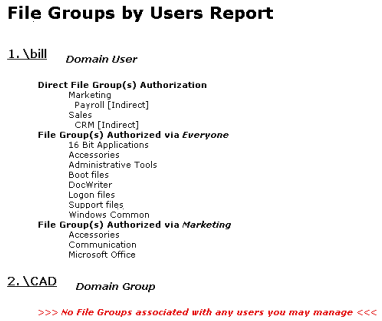
Using the **Reports** module you can generate the following Application Control reports.

Table 44: Available Reports

Report	Description
File Groups by User	Generates a report of file groups directly or indirectly associated with the user or user group you specify.
User by File Group	Creates a report of every user and user group associated, directly or indirectly, with every file group defined in the system.
User Options	Displays current user option settings that determine which activities are logged and whether users are allowed to locally authorize denied executables, scripts, and macros.
Machine Options	Generates a report of current computer option settings.
Server Settings	Shows options, registry values, and settings for installed Application Servers.
Client Status	Generates a report of the hardening options, client version, and log and file policy status.

File Groups by User

You can generate a report showing the file groups assigned to an individual user or users in a group.


File Groups by Users Report

1. \bill *Domain User*

Direct File Group(s) Authorization
Marketing
Payroll [Indirect]
Sales
CRM [Indirect]
File Group(s) Authorized via *Everyone*
16 Bit Applications
Accessories
Administrative Tools
Boot files
DocWriter
Logon files
Support files
Windows Common
File Group(s) Authorized via *Marketing*
Accessories
Communication
Microsoft Office

2. \CAD *Domain Group*

>>> No File Groups associated with any users you may manage <<<

Figure 87: File Groups by User Report

The following table describes the report rows.

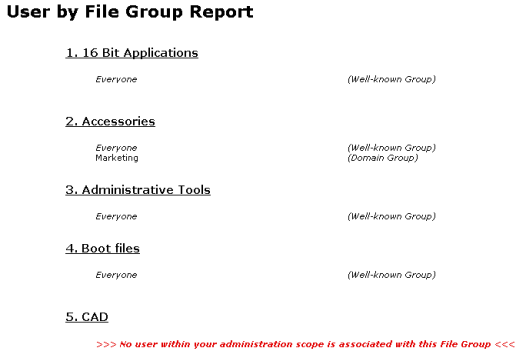
Table 45: File Groups by User Report Row Description

Row Name	Description
User Name	Full user name including domain.
User Group	Full user group name including domain.
Direct Group File Authorization	Group files directly authorized to the user or user group by the administrator.
Indirect Group File Authorization	Group files indirectly authorized to the user or user group through a parent-child relationship with file groups that are directly authorized for the user or user group.
Warning Message	Warns that you do not have permission to view the user or user group file group assignments selected.

User by File Group

You can generate a report showing the users assigned to each file group.

The report shows the users directly and indirectly assigned to the file group.



User by File Group Report

1. 16 Bit Applications

Everyone	(Well-known Group)

2. Accessories

Everyone	(Well-known Group)
Marketing	(Domain Group)

3. Administrative Tools

Everyone	(Well-known Group)

4. Boot files

Everyone	(Well-known Group)

5. CAD

>>> No user within your administration scope is associated with this File Group <<<

Figure 88: User by File Group Report

The following table describes the report rows.

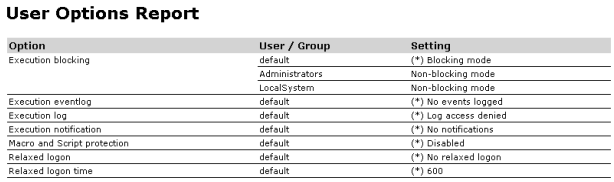
Table 46: User by File Group Report Row Description

Row Name	Description
Direct Group File Authorization	Group files directly authorized to the user or user group by the administrator.
Indirect Group File Authorization	Group files indirectly authorized to the user or user group through a parent-child relationship with file groups that are directly authorized to the user or user group.
User Name	Full user name including domain.
User Group	Full user group name including domain.
Warning Message	Warning that you do not have permissions to view the file group assignments selected.

User Options

You can generate a report showing the Ivanti Device and Application Control options settings status.

The report settings describe the types of Application Control activities that the user is permitted and that are monitored by Ivanti Device and Application Control.



User Options Report

Option	User / Group	Setting
Execution blocking	default	(*) Blocking mode
	Administrators	Non-blocking mode
	LocalSystem	Non-blocking mode
Execution eventlog	default	(*) No events logged
Execution log	default	(*) Log access denied
Execution notification	default	(*) No notifications
Macro and Script protection	default	(*) Disabled
Relaxed logon	default	(*) No relaxed logon
Relaxed logon time	default	(*) 600

Figure 89: User Options Report

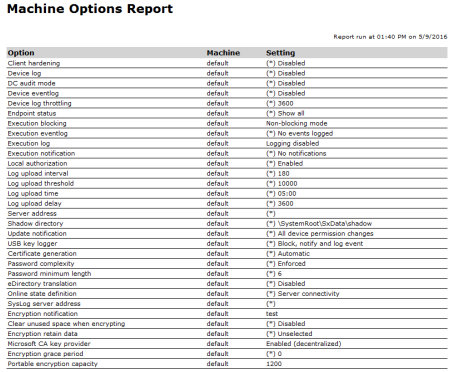
The following table describes the report columns.

Table 47: User Options Column Description

Column	Description
Option	The name of the option shown the ***Default Options*** dialog.
User/Group	The user or user group for which this option is set; **Default** is the value configured for all users and represents the default value.
Setting	The actual value of the option; the asterisk (*) indicates that the option is set to the default value.

Machine Options

You can generate a report that shows options settings status for Ivanti Device and Application Control default options.



Machine Options Report

Report run at 01:40 PM on 5/9/2016

Option	Machine	Setting
Client hardening	default	(*) Disabled
Device log	default	(*) Disabled
DC audit mode	default	(*) Disabled
Device eventlog	default	(*) Disabled
Device log throttling	default	(*) 3600
Endpoint status	default	(*) Show all
Execution blocking	default	Non-blocking mode
Execution eventlog	default	(*) No events logged
Execution log	default	Logging disabled
Execution notification	default	(*) No notifications
Local authorization	default	(*) Enabled
Log upload interval	default	(*) 180
Log upload threshold	default	(*) 10000
Log upload time	default	(*) 05:00
Log upload delay	default	(*) 3600
Server address	default	(*)
Shadow directory	default	(*) \SystemRoot\SxData\shadow
Update notification	default	(*) All device permission changes
USB key logger	default	(*) Block, notify and log event
Certificate generation	default	(*) Automatic
Password complexity	default	(*) Enforced
Password minimum length	default	(*) 6
eDirectory translation	default	(*) Disabled
Online state definition	default	(*) Server connectivity
SysLog server address	default	(*)
Encryption notification	default	test
Clear unused space when encrypting	default	(*) Disabled
Encryption retain data	default	(*) Unselected
Microsoft CA key provider	default	Enabled (decentralized)
Encryption grace period	default	(*) 0
Portable encryption capacity	default	1200

Figure 90: Machine Options Report

The following table describes the report columns.

Table 48: 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.

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**

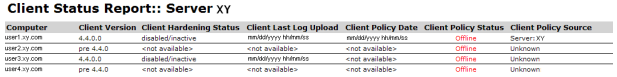


Figure 91: Client Status Report

The following table describes the report columns.

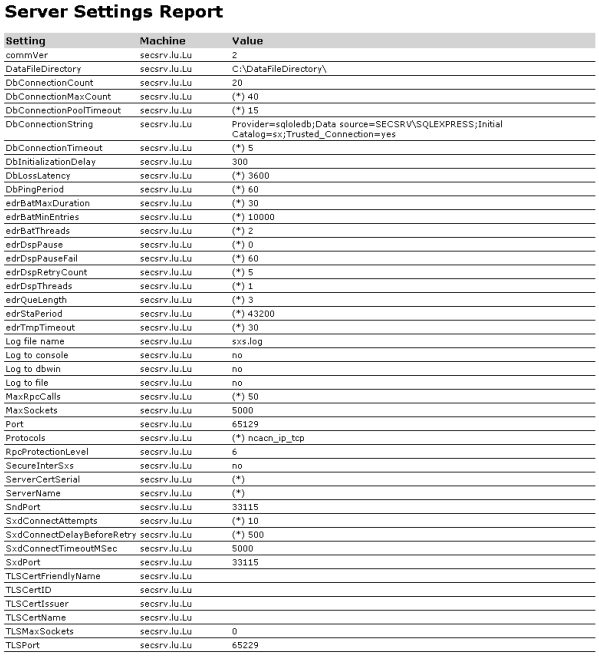
Table 49: Client Status Column Descriptions

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).

Column	Description
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.
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 92: Server Settings Report

The following table describes the report columns.

Table 50: 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 7

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***

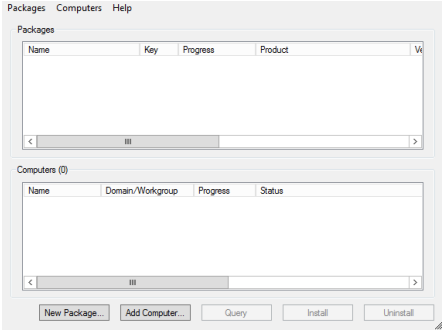


Figure 93: Client Deployment Dialog

Packages Panel

The following table describes the columns in the ***Packages*** panel.

Table 51: 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 52: 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 53: 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 54: 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.

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.

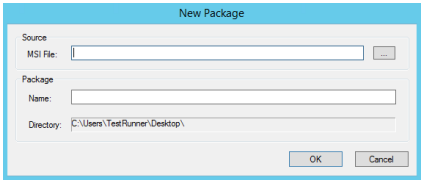


   Figure 94: New Packages Dialog

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.

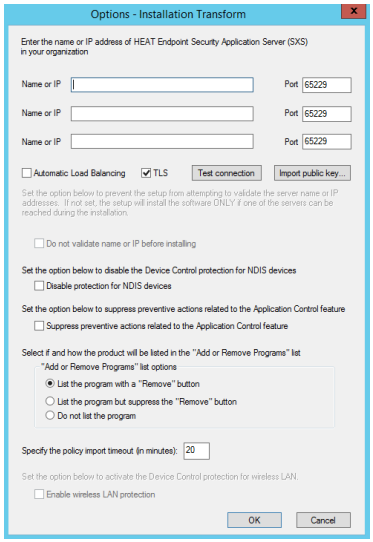


Figure 95: Options - Ivanti Device and Application Control Installation Transform Dialog

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.

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.

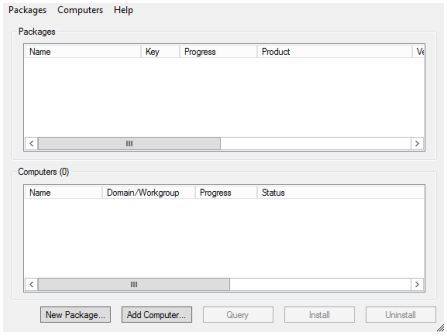


Figure 96: Client Deployment Dialog

2. Click **Add Computer**.

   Step Result: The ***Select Computers*** dialog opens.

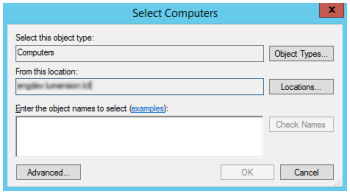


Figure 97: Select Computers Dialog

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.

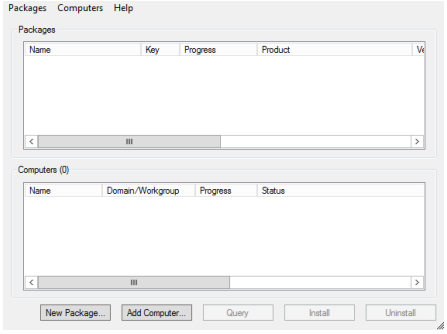


Figure 98: Client Deployment Dialog

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.

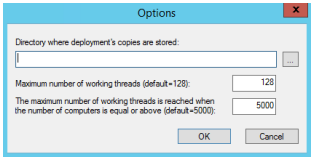


      Figure 99: Options Dialog

   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.

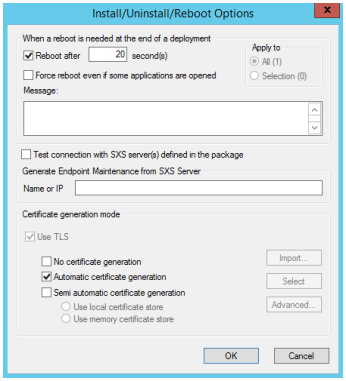


Figure 100: Install/Uninstall/Reboot/Options Dialog

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.

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

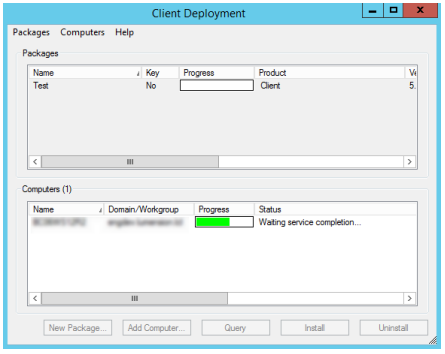


Figure 101: Dialog - Computer Progress

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.

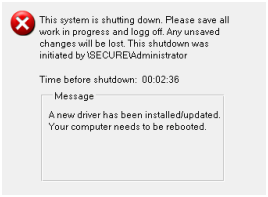


Figure 102: System Shutdown Dialog

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**.

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.

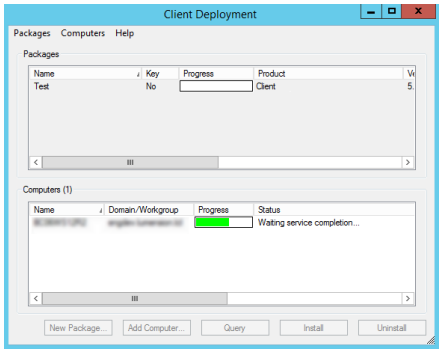


Figure 103: Client Deployment Dialog

Appendix
A

Administrative Tools

In this appendix:

- Using the Ivanti Device and Application Control Authorization Service Tool
- Scheduling Domain Synchronization
- Manage Administrator Rights
- Opening Firewall Ports
- Dynamic Script Support

Administrative utilities include automated authorization of trusted software upgrade sources, scheduling domain synchronization, and managing administrator rights.

The Ivanti Device and Application Control product solution suite provides administrative tools for the Ivanti Device and Application Control Enterprise Administrator to reduce administrative burden during installation of the Ivanti Device and Application Control product suite, for:

- Using the Ivanti Device and Application Control Authorization Service.
- Scheduling automatic domain synchronization.
- Managing Ivanti Device and Application Control administrator rights.
- Opening firewall ports for the Application Servers and clients.

Using the Ivanti Device and Application Control Authorization Service Tool

You can use the ***Ivanti Device and Application Control Authorization Service Tool*** to monitor approved and synchronized changes to executable file authorization policies using Microsoft® Update Services (SUS) and Windows® Server Update Services (WSUS).

The ***Ivanti Device and Application Control Authorization Service Tool*** service authorizes all approved Microsoft® updates and fixes, creates corresponding hash files, and updates the database.

1. From the location where you saved the Ivanti Device and Application Control application software, run the `\server\authsrv\AuthService.exe` file.

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

2. Click **Next**.

   Step Result: The ***License Agreement*** page opens.

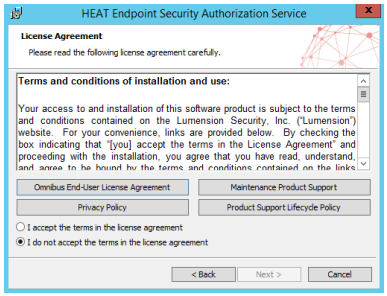


Figure 104: License Agreement Page

3. Review the license agreement and, if you agree, select **I accept the terms in the license agreement**.
4. Click **Next**.
5. From the ***Ivanti Device and Application ControlApplication Server*** dialog, enter an Application Server IP address in the corresponding field.
6. Click **Next**.

   Step Result: The ***Software Update Services*** dialog opens.

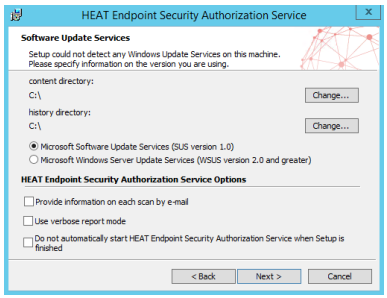


Figure 105: Software Update Services Dialog

7. Select one of the following options:
   - **Microsoft Software Update Services (SUS version 1.0)**
   - **Microsoft Windows Server Update Services (WSUS version 2.0 and greater)**

8. Select any of the following ***Ivanti Device and Application Control Authorization Service Options***.
   - **Provide information on each scan by e-mail**
   - **Use verbose report mode**
   - **Do not automatically start Ivanti Device and Application Control Authorization Service when Setup is finished**

   Step Result: If you choose to **Provide information on each scan by e-mail**, the ***E-mail configuration*** dialog opens. The ***Ivanti Device and Application Control Authorization Service*** tool does not support ***Outlook Express*** or ***Internet Information Server*** (IIS) as clients for sending email messages. If there is already an account for these types of clients, the SMTP IP address is transferred directly to the Ivanti Device and Application Control Authorization Service configuration.

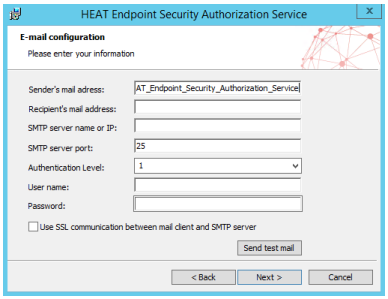


Figure 106: E-mail Configuration Dialog

> **Note:** If you select **Do not automatically start Ivanti Device and Application Control Authorization Service when Setup is finished**, the service will automatically start when one of the following events occurs:
>
> - A change is made by WSUS in the default update folder.
> - An administrator approves the SUS updates using the Management Console.
> - One hour elapses after installing the Ivanti Device and Application Control Authorization Service.

9. Click **Next**.
10. From the ***Destination Folder*** dialog, click **Change** to choose an installation destination folder other than the default folder `C:\Program Files\Ivanti\Device and Application Control\`.
11. Click **Next**.

    Step Result: The ***Ready to Install the Program*** dialog opens.

12. Click **Install**.

    A progress bar runs on the page, showing installation progress.

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

13. Click **Finish**.

Result: The Ivanti Device and Application Control ***Database Explorer*** window shows the specified installation directory(s) in the ***Files*** tab.

After Completing This Task:
After installing the ***Ivanti Device and Application Control Authorization Service Tool*** you must configure and synchronize WSUS. See Configure and Synchronize WSUS (http://technet.microsoft.com/en-us/library/cc708455.aspx) for more information about configuring WSUS or SUS.

You can modify ***Ivanti Device and Application Control Authorization Service Tool*** by rerunning the ***Authorization Service Tool***.

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.

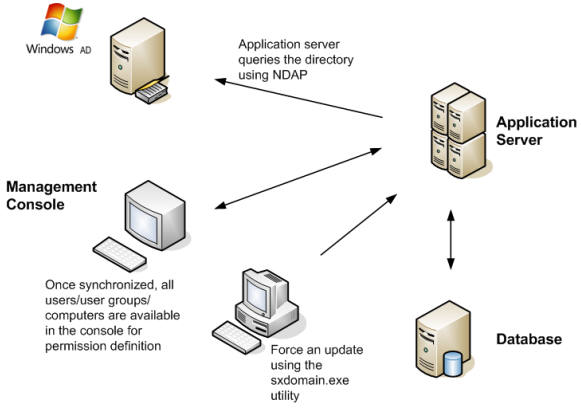


Figure 107: Synchronization Script Process

1. Navigate to `C:\Program Files\Ivanti\Device and Application Control\SXTools`.
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.

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**.
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.

Dynamic Script Support

You can specify, explicitly or with wildcards, one or more URLs that will permit the execution of non-whitelisted scripts within Microsoft Internet Explorer.

Note: This setting will apply to all users, and is only supported when using Microsoft Internet Explorer.

To enable script execution from a specific URL, you must use the **sxopt** command line utility to insert the URL into the Ivanti Device and Application Control database.

When specifying a URL, the following wildcards are available:

- `%` - the `%` character can be used to match zero or more characters, ending with the dot (`.`) character.

  For example, `http://%domain.com` would allow non-whitelisted scripts from `http://domain.com`, `http://www.domain.com`, or `http://subdomain.domain.com`, but scripts from `http://mydomain.com` would continue to be blocked.
- `*` - the `*` character can be used to match any number of characters.

  For example, `http://msdn.microsoft.com*` would allow any characters following the `.com`, such as `http://msdn.microsoft.com/en-us/library/ms143506.aspx`.

The following usage example will allow the execution of non-whitelisted scripts from any secure (https) Microsoft website.

```
sxopt <SXS> -ca -s 80 https://%microsoft.com*
```