Ivanti Device and Application Control 5.2

Setup Guide

ivanti | Endpoint Security
powered by HEAT

Notices

Version Information

Ivanti Device and Application Control Setup Guide - Ivanti Device and Application Control Version 5.2 - Published: July 2020

Document Number: 02_102_5.2

Copyright Information

Table of Contents

Preface

About This Document

This Setup 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

Planning Your Installation

Planning for your software installation requires knowledge of the minimum system requirements necessary to support Application Control and Device Control coupled with recommendations for network security rules that can enhance the security state of your environment.

To assist in gathering the information required for a smooth installation, Ivanti recommends that you use the Installation Checklist on page 18.

Recommended Security Rules

Ivanti recommends that you define certain administrative security rules before installing Ivanti Device and Application Control.

The recommended security settings are specific to Microsoft® Windows® and complement operation of Ivanti Device and Application Control.

Table 2: Recommended Security Rules

Security Rule	Description
Hard Disk Encryption	Encrypts computer disk drives to prevent unauthorized user access to the computer hard disk drive.
Password Protect the BIOS	Prevents administrative user access when using a CMOS reset jumper, in combination with password protection for the BIOS and seal/chassis intrusion protection.
Seal/Chassis Intrusion Protector	Uses seal and/or chassis intrusion protection hardware to prevent administrative user access using an external boot device to bypass workstation security software.
Administrative Rights	Remove local users from the local *Administrators* group to prevent unrestricted local user computer access.
Power Users	Remove local users from the *Power Users* group to prevent users from tampering or bypassing standard Windows security policies.

Security Rule	Description
Access Policy	Restrict network and file access as much as possible, including use restriction only to *NTFS* partitions.
NTFS Partition	Use of *NTFS* partitioning is required for installation of Ivanti Device and Application Control product solutions.
Recovery Console	Password protect user access to the ***Recovery Console***, which is available for the Windows *DVD/CD-ROM* or *MSDN* subscription.
Service Pack and Hot Fixes	Always install the latest service packs and hot fixes for the operating system supported by Ivanti Device and Application Control product solutions.
Firewalls	Use traditional perimeter-based security systems, like firewalls, to complement Ivanti Device and Application Control product solutions.
Password Policies	Maintain strong password security policies.
Private and Public Key Generation	Deploy Ivanti Device and Application Control product solutions using secure public and private key pairs.

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 3: 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 4: 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) • Windows Embedded Standard 7 SP1 (32-bit and 64-bit) • 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

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 5: 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 6: 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 7: 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

Licensing Ivanti Device and Application Control Products

The following types of licenses are available for Ivanti Device and Application Control product solutions:

- An *Evaluation License* provides you with a fully functioning Ivanti Device and Application Control product solution for a limited time.
- A *Perpetual License* provides full capacity for an unlimited period.
- A *Subscription License* provides full capacity for the time period specified by the terms of your license.

Chapter 2

Installing Ivanti Device and Application Control Components

Ivanti Device and Application Control component installation requires that you follow a series of interdependent tasks in a prescribed order. Before you begin, you must have a valid license key for each software application(s) that your are installing.

Successful installation of Ivanti Device and Application Control requires you to install components in the following order:

1. Install the database.
2. Generate and save a public and private key pair. This action is not required, however, Ivanti strongly recommends the use of a public-private key pair to provide the highest level of security.
3. Install the Application Server(s).
4. Install the Management Console.
5. Install and deploy the client.

Installation Overview

Ivanti Device and Application Control component installation requires that you follow a series of interdependent tasks in a prescribed order. Before you begin, you must have a valid license key for each software application(s) that your are installing.

Use the following process to identify tasks for installing components installing Ivanti Device and Application Control, for your convenience this process refers to the Installation Checklist on page 18.

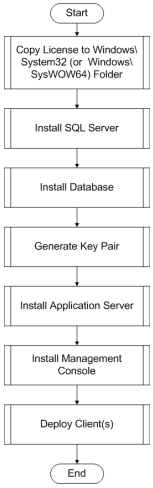

Figure 1: Ivanti Device and Application Control Product Solution Installation Process Flow

Installation Checklist

The installation checklist outlines the detailed tasks that you must perform when installing the Ivanti Device and Application Control solutions.

This checklist guides you through the installation process.

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.

To begin your installation:

1. Copy the Ivanti Device and Application Control license file to the `\\Windows\System32` or `\ \Windows\SysWOW64` folder, and rename the file to `endpoint.lic`. The license file may be installed after installing the database, however, the license file must installed before installing the Application Server.
2. Download the Ivanti Device and Application Control application software from the Self-Service Portal.
3. Create a device, media, or software application inventory which lists the items that you want Ivanti Device and Application Control to control.
4. Document company policy that defines:
   - Device permissions.
   - Shadowing requirements.
   - Device encryption requirements.
   - Ivanti Device and Application Control administrators and their roles.
   - Global domain groups for Ivanti Device and Application Control administrators.
5. Plan your Ivanti Device and Application Control network architecture, based on capacity requirements, that list the Application Server host names and IP addresses.
6. Create a dedicated Application Server domain user rights service account and set the following:
   - **User cannot change password**.
   - **Password never expires**.

   The domain account must have local administration rights when you plan to use the TLS communication protocol for client- Application Server and inter- Application Server data transfers.
7. Create **Impersonate a client after authentication** user rights for the Application Server. See Impersonate a Client After Authentication (http://support.microsoft.com/kb/821546) for additional information about impersonating a client after authentication user rights.
8. Verify that the Application Server domain account has **Log on as a service** user rights. See Add the Log on as a service right to an account (http://technet.microsoft.com/en-us/library/cc739424(WS.10).aspx) for additional information about logging on as a service user rights.
9. Install Microsoft® *Internet Information Services* on the same computer as the certification authority, otherwise the enterprise root certificate cannot be generated. See Internet Information Services (IIS) (http://www.iis.net) for additional information about installing *Internet Information Services*.
10. Install a Microsoft enterprise root certification authority to enable removable device encryption for Device Control. See Install a Microsoft enterprise root certification authority (http://technet.microsoft.com/en-us/library/cc776709.aspx) for additional information about installing an enterprise root certificate.
11. Install a Microsoft SQL Server® . See Getting Started with SQL Server (http://msdn.microsoft.com/en-us/sqlserver/default.aspx) for additional information about installing a SQL server.
12. Complete Installing the Database on page 20.
13. To install multiple Application Server s, create a shared file directory on a file server to share the Datafile directory component. This action is only required if you will be using more than one Application Server.
14. Complete Generating a Key Pair on page 23. This action is recommended, but not required.

15. Complete Installing the Application Server on page 25.

Important: The Application Server service account must have database owner (DBO) rights to the Ivanti Device and Application Control database.

16. Complete Installing the Management Console on page 32.
17. Complete Installing the Client on page 35.
18. Test your Ivanti Device and Application Control product solution installation for functionality.

Installing the Database

The Ivanti Device and Application Control database is the first component that you install. The database serves as the central repository for device permissions rules and executable file authorizations.

Prerequisites:

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.

Caution: When installing SQL server updates, ensure SQL server restarts properly as this may prevent SXS server from starting as the database will be unavailable.

Before you can successfully install the Ivanti Device and Application Control database, you must:

- Verify that you satisfy the minimum hardware and software system requirements.
- If you will be using a database cluster, you must specify an alternate *TDS* port during *SQL* server setup. See Creating a Server Alias for Use by a Client (SQL Server Configuration Manager) (http://msdn.microsoft.com/en-us/library/ms190445.aspx) for additional information about creating a server alias. You can install the Ivanti Device and Application Control database on a server cluster, where there are at least two servers in the cluster running SQL Server. For additional information regarding database clustering, see Microsoft Cluster Service (MSCS) Installation Resources (http://support.microsoft.com/kb/259267).

1. Log in to a computer as an administrative user with access to a Microsoft® SQL Server®.
2. Close all programs running on the computer.

3. From the location where you saved the Ivanti Device and Application Control application software, run the `\server\db\Db.exe` file.

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

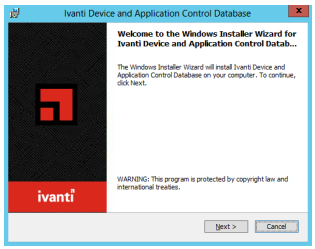

Figure 2: Welcome Page

4. Click **Next**.

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

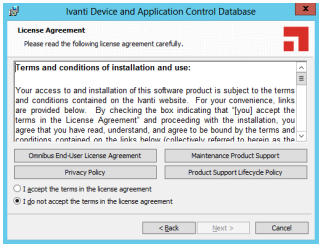

Figure 3: License Agreement Page

5. Review the license agreement and, if you agree, select **I accept the terms in the license agreement**.
6. Click **Next**.

   Step Result: The ***Destination Folder*** page opens.

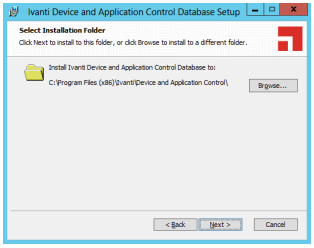

Figure 4: Destination Folder Page

7. You may choose an installation destination folder other than the default folder `C:\Program Files\Ivanti\Device and Application Control\`.

   a) Click **Change**

   Step Result: The ***Change Current Destination Folder*** page opens.

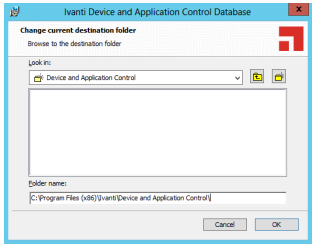

   Figure 5: Change Current Destination Folder Page

   b) Select a folder from the **Look in:** field.

   c) Click **OK**.

   Step Result: The ***Change Current Destination Folder*** closes, and the ***Destination Folder*** page changes to reflect the new location.

8. Click **Next**.

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

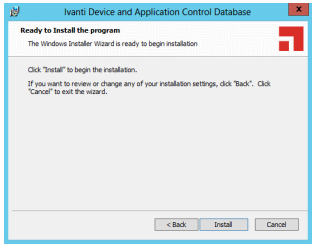

   Figure 6: Ready to Install the Program Dialog

9. Click **Install**.

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

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

10. Click **Finish**.

Result: Ivanti Device and Application Control setup runs the SQL installation scripts and creates the Ivanti Device and Application Control database for the SQL Server database instance that you specified.

Generating a Key Pair

The Application Server uses an asymmetric encryption system to communicate with a client, using a public-private key pair that you generate during installation.

The Application Server and Ivanti Device and Application Control clients contain a embedded default public and private key pair that should only be used with an evaluation license. Ivanti provides a *Key Pair Generator* utility, which generates a key pair for fully licensed application installations. The key pair ensures the integrity for communication between the Application Server and clients.

When an Application Server cannot find a valid key pair at startup, the event is logged and Ivanti Device and Application Control uses the default key pair.

Caution: When you are using Device Control, do not change the key pair:

- For media encrypted before exchanging a key pair, which will result in disabling password recovery for the previously encrypted media.
- During a Ivanti Device and Application Control upgrade installation which will result in the loss of access to media previously encrypted centrally and subsequent loss of data.
- During a Ivanti Device and Application Control upgrade installation when client hardening is enabled, which will cause Application Control and Device Control installations to fail.

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

   Step Result: The ***Key Pair Generator*** dialog opens.

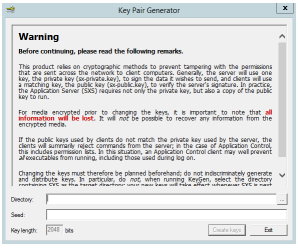

   Figure 7: Key Pair Generator Dialog

2. In the **Directory** field, enter the name of the temporary directory where you will save the key pair.
3. In the **Seed** field, type a random alphanumeric text string.

   This text is used to initiate the random number generator; the longer the text string the more secure the key pair.

4. Click **Create keys**.

   Step Result: The ***Key Pair Generator*** confirmation dialog opens.

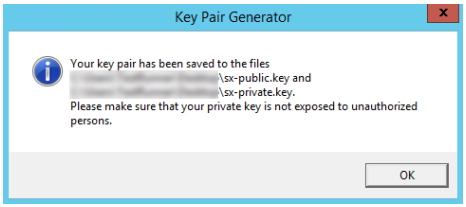

   Figure 8: Key Pair Generator Dialog

5. Click **OK**.

   Step Result: You return to the ***Key Pair Generator*** dialog.

6. Click **Exit**.

Result: The keys are saved as `sx-private.key` and `sx-public.key` files in the directory you specified.

After Completing This Task:

Distribute the key pair by copying the `sx-private.key` and `sx-public.key` files to `c:\windows\system32` (32-bit systems) or `c:\windows\syswow64` (64-bit systems) on the computer(s) where you are installing the Application Server. At startup, the Application Server searches all drive locations for a valid key pair, stopping at the first valid key pair.

Installing the Application Server

The Application Server processes Ivanti Device and Application Control client activities and is the only application component that connects to the database. One or more Application Servers communicate device and application control information between the Ivanti Device and Application Control database and Ivanti Device and Application Control client(s).

Prerequisites:

Before you can successfully install the Application Server, you must:

- Verify that a valid Ivanti Device and Application Control license file is listed in `c:\windows\system32` (32-bit systems) or `c:\windows\syswow64` (64-bit systems), and file name is `endpoint.lic`.

  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.

- Verify that you satisfy the minimum hardware and software system requirements.

- When using TLS protocol confirm TCP ports 33115 and 65229 are open. When not using TLS protocol open TCP port 65129. Depending upon how firewalls are setup in your environment, these ports may be closed.
- Configure the TCP/IP protocol to use a fixed IP address for the computer that runs the Application Server.
- Configure the Application Server host computer to perform fully qualified domain name (FQDN) resolution for the Ivanti Device and Application Control clients that the server manages.
- Ensure that the Application Server host computer account is configured to read domain information using the Microsoft® Windows® Security Account Manager. See Security Account Manager (SAM) (http://technet.microsoft.com/en-us/library/cc756748.aspx) for additional information about the Microsoft Windows Security Account Manager.
- 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.

1. Log in with administrative user access to the computer where you are installing the Application Server.

   Important: For Active Directory environments, log in using the dedicated Application Server domain user rights service account. The Application Server installation process configures the Application Server service account for access to the database.

2. Close all programs running on the computer.
3. From the location where you saved the Ivanti Device and Application Control application software, run `\server\sxs\Server.exe`.
4. Click **OK**.

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

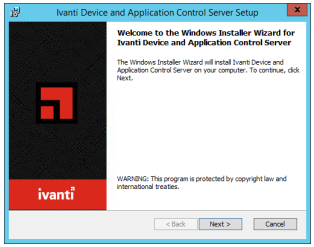

Figure 9: Welcome Page

5. Click **Next**.

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

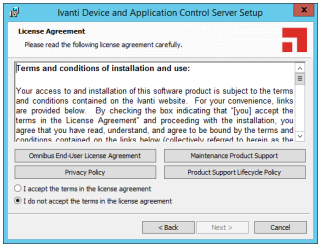

Figure 10: License Agreement Page

6. Review the license agreement and, if you agree, select **I accept the terms in the license agreement**.

7. Click **Next**.

   Step Result: The ***Setup*** dialog opens when the setup process detects an operating system that is subject to security changes concerning Remote Procedure Calls (RPC).

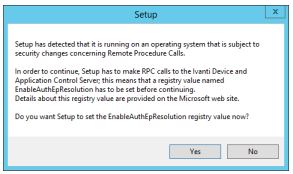

Figure 11: Setup Dialog

8. Click **Yes**.

   Step Result: A confirmation dialog opens after the registry value is reset.

Figure 12: The Setup Dialog

9. Click **OK**.

   Step Result: The ***Destination Folder*** page opens.

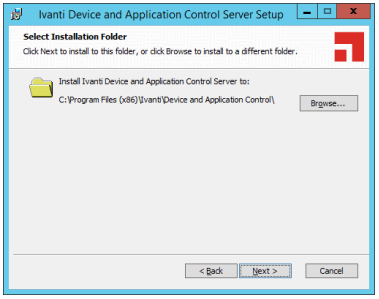

Figure 13: Destination Folder Page

10. You may choose an installation destination folder other than the Ivanti Device and Application Control default folder `C:\Program Files\Ivanti\Device and Application Control\`.

a) Click **Change**.

Step Result: The ***Change Current Destination Folder*** page opens.

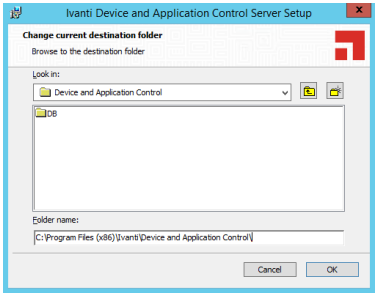

Figure 14: Change Current Destination Folder Page

b) Select a folder from the **Look in:** field.

c) Click **OK**.

Step Result: The ***Change Current Destination Folder*** closes, and the ***Destination Folder*** page changes to reflect the new location.

11. Click **Next**.

Step Result: The ***Service Account*** page opens.

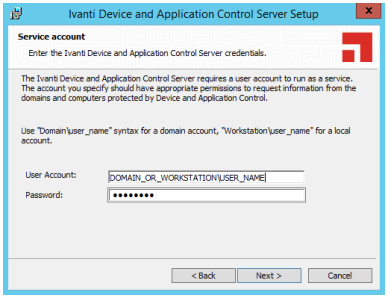

Figure 15: Service Account Page

12. Type the name of the user or domain in the **User Account** field for access to the Application Server.

Enter domain account information using the `Domain\User` format, and local account information using the `Computer\User` format. Ivanti Device and Application Control supports use of standard NetBIOS computer names up to fifteen (15) characters long.

Tip: This is the user name that you created when you configured the domain service account for the Application Server .

13. In the **Password** field, type the user account access password.

14. Click **Next**.

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

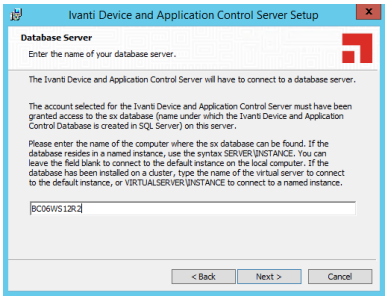

Figure 16: Database Server Page

15. Type the name of the database instance for the Application Server connection, using the `servername\instancename` format.

The default database instance is automatically populated, when installed on the same computer. Alternately, the `instancename` is not required if the database is installed in the default instance of Microsoft SQL Server.

16. Click **Next**.

Step Result: The ***Datafile directory*** page opens.

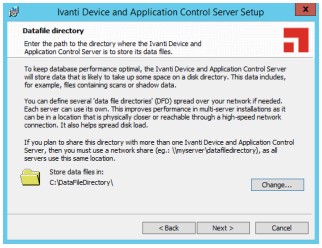

Figure 17: Datafile Directory Page

17. You may choose a folder other than the Ivanti Device and Application Control default folder, `C:\DataFileDirectory\`, where Application Server log, shadow, and scan files are stored.

Tip: Use a permanent network share when you are installing more than one Application Server or a dedicated file server. To improve performance for a multi-server installation, assign a separate data file directory to each server to provide load balancing; although more than one server can access the same data file directory. Use a `Universal\Uniform Name Convention` path name; do not use a mapped drive name.

a) Click **Change**.

Step Result: The ***Select datafile directory*** page opens.

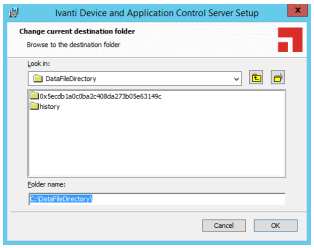

Figure 18: Select Datafile Directory Page

b) Type the name of the datafile directory in the **Folder name:** field.

c) Click **OK**.

18. Click **Next**.

Step Result: The ***Server communication protocol*** page opens.

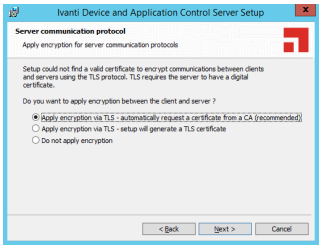

Figure 19: Server Communication Protocol Page

19. Select an encryption option.

Important: Do not select **Apply encryption via TLS - setup will generate a TLS certificate** as it is no longer supported.

Restriction: The server communication protocol options shown depend upon the client version supported and whether a certification authority digital certificate is installed.

20. Click **Next**.

Step Result: The ***Server communication protocol*** page opens.

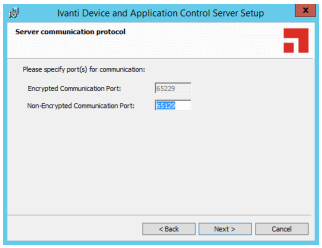

Figure 20: Server Communication Protocol Ports Page

21. Specify the communication port(s).

Restriction: The port field(s) shown depend upon the encryption communication protocol that you selected previously.

22. Click **Next**.

Step Result: The ***Syslog Server*** page opens.

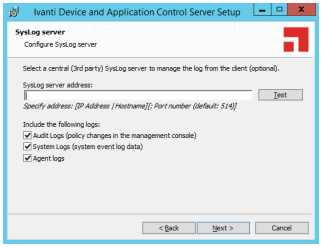

Figure 21: Syslog Server Page

23. Type the name or the IP address of the *SysLog* server in the **SysLog server address** field.

Important: This step is optional. You do not have to specify a *Syslog* server.

24. Select from the following options:

Option	Description
Audit Logs	Logs changes to policy administered through the Management Console .
System Logs	Logs system events.
Agent Logs	Logs events uploaded directly from the Ivanti Device and Application Control client.

25. Click **Next**.

Step Result: The ***Ready to Install Program*** page opens.

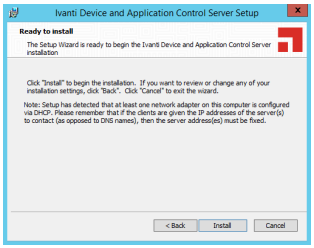

Figure 22: Ready to Install Program Page

26. Click **Install**.

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

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

27. Click **Finish**.

Result: The Application Server files are installed and the server establishes a connection to the Ivanti Device and Application Control database.

Installing the Management Console

The Management Console is the administrative tool that used to configure and run the Ivanti Device and Application Control software.

Prerequisites:

Before you can successfully install the Management Console, you must:

- Verify that you satisfy the minimum hardware and software system requirements.
- Install the Application Server.

1. Log in as an administrative user to the computer where you are installing the Management Console.
2. Close all programs running on the computer.

3. From the location where you saved the Ivanti Device and Application Control application software, run the `\server\smc\Console.exe`.

Attention: The Management Console requires the Microsoft® Visual C++ 2017 Redistributable Package for proper operation. You may receive a message prompting you to allow setup to trigger the redistributable package installation, if Visual C++ Libraries are not already installed. After the redistributable package installs, the Management Console resumes installation as follows.

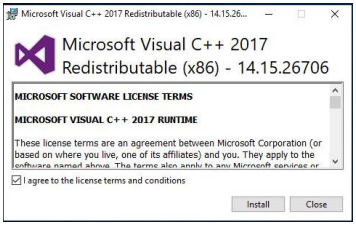

Figure 23: Microsoft Visual C++ 2017 Redistributable Package Setup

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

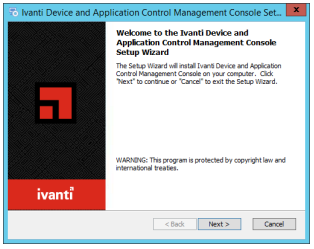

Figure 24: Welcome Page

4. Click **Next**.

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

Figure 25: License Agreement Page

5. Review the license agreement and, if you agree, select **I accept the terms in the license agreement**.

6. Click **Next**.

   Step Result: The ***Select Installation Folder*** page opens.

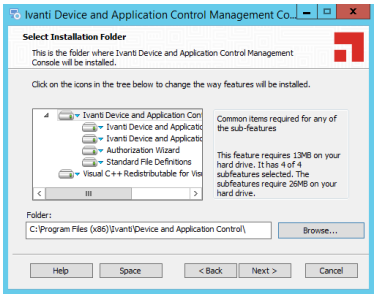

Figure 26: Setup Type Page

7. Select the features you want to install:

Note: The installation features shown depend upon the application you are licensed for.

a) Select the features that you want to install.

   The installation features shown depend upon the application that you are licensed for.

Feature	License Type(s)
Management Console	Device Control Application Control
Client Deployment Tool	Device Control Application Control
Standard File Definitions	Application Control
Authorization Wizard	Application Control

b) You may choose `C:\Program Files (x86)\Ivanti\Device and Application Control\` or change the destination folder.

8. Click **Next**.

   Step Result: The ***Ready to Install*** page opens.

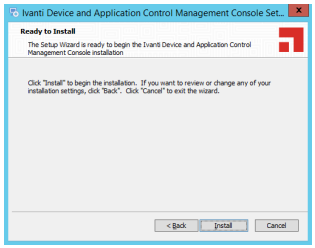

Figure 27: Ready to Install Page

9. Click **Install**.

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

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

10. Click **Finish**.

Result: The Management Console files are installed.

After Completing This Task:

Define Ivanti Device and Application Control administrator access as described in the Ivanti Device Control User Guide (https://help.ivanti.com) or the Ivanti Application Control User Guide (https://help.ivanti.com) depending upon your license type. By default, only users who are members of the *Administrators* group for the computer running the Management Console can connect to the Application Server.

Installing the Client

The Ivanti Device and Application Control client manages permissions for device access and user access to software applications for endpoint computers.

Prerequisites:

Before you can successfully install the Ivanti Device and Application Control client, you must:

- Verify that you satisfy the minimum hardware and software system requirements.
- Copy the `sx-public.key` file for the Ivanti Device and Application Control client to the `Client` folder located where you downloaded the Ivanti Device and Application Control software. The Ivanti Device and Application Control client installer detects the public key during installation and copies the key to the target directory (`%windir%\sxdata`).
- Install the Application Server.
- Install the Management Console.
- When installing Application Control, you must ensure that the **Execution blocking** default option is set to **Non-blocking mode**; otherwise the Ivanti Device and Application Control client computer will not restart after Ivanti Device and Application Control client installation because executable system files cannot run until they are centrally authorized from the Management Console.

1. Verify that the domain information in the Ivanti Device and Application Control database is synchronized as follows:

   a) From the Management Console, select **Tools** > **Synchronize Domain Members**.

   Step Result: The ***Synchronize Domain*** dialog opens.

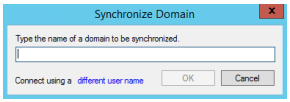

   Figure 28: Synchronize Domain Dialog

   b) Enter the name of the domain that you want to synchronize.

   Note: 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.

   c) Click **OK**.

2. Log in as an administrative user to the computer where you are deploying the Ivanti Device and Application Control client.
3. Close all programs running on the computer.
4. From the location where you saved the Ivanti Device and Application Control application software, run `\client\Client.exe` file.

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

5. Click **Next**.

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

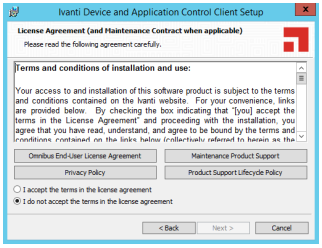

   Figure 29: License Agreement Page

6. Review the license agreement, and, if you agree, select **I accept the terms in the license agreement**.

7. Click **Next**.

   Step Result: The ***Encrypted Communication*** page opens.

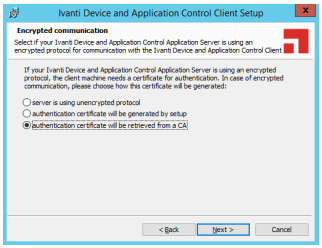

Figure 30: Encrypted Communication Page

8. Select one of the following options that matches the option you selected when installing the Application Server:

Important: Do not select **Apply encryption via TLS - setup will generate a TLS certificate** as it is no longer supported.

Option	Description
Server is using unencrypted protocol	Communication between the Application Server and Ivanti Device and Application Control client is not using the TLS communication protocol. Communication is not encrypted but is signed using the private key.
Authentication certificate will be retrieved from a CA	Communication between the Application Server and Ivanti Device and Application Control client uses the TLS communication protocol. Communication is encrypted and the digital certificate is retrieved automatically during installation.

Tip: Ivanti recommends that you use the automatic TLS retrieval option to deploy *Certificate Authority* infrastructure for issuing valid digital certificates.

Step Result: If you opt to manually generate a certificate during setup, the ***Client Authentication*** dialog opens.

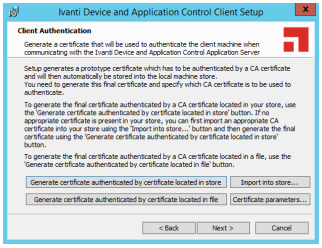

Figure 31: Client Authentication Dialog

9. To manually generate a certificate during setup specify the computer certificate location and parameters from the following options.

Option	Description
Generate certificate signed by certificate located in store	Generates a digital certificate during installation by using a signature certificate located in the local user store.
Generate certificate signed by certificate located in file	Generates a digital certificate during installation by using a signature certificate located in a specified file.
Import into store	Imports a signature certificate into the local user store.
Certificate parameters	Specifies the certificate parameters for the **Cryptographic service provider**, **Key length**, **Validity**, and **Signature**.

10. Click **Next**.

Step Result: The ***Ivanti Device and Application ControlApplication Server***s page opens.

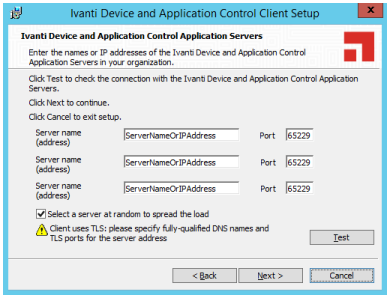

Figure 32: Application Server s Page

11. Specify up to three server names using fully qualified domain names (FQDN) or IP addresses that are managed from the Management Console.

Caution: Do not use IP address(es) when using the TLS communication protocol for encryption. You can only use FQDNs for when using the TLS communication protocol.

12. Verify that the Ivanti Device and Application Control client connects to the Application Server by clicking **Test**.

Caution: You can proceed with client installation if the Application Server is unavailable, by clicking **OK** in the following dialog. The client can establish a connection with the server later, when the server is available.

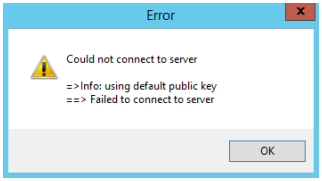

Figure 33: Error Dialog

Step Result: By default, Ivanti Device and Application Control connects with the first available server and retrieves default policy settings from the server.

13. If you are specifying more than one server, select or deselect the **Select a server at random to spread the load** option.

14. Click **Next**.

Step Result: The ***Destination Folder*** page opens.

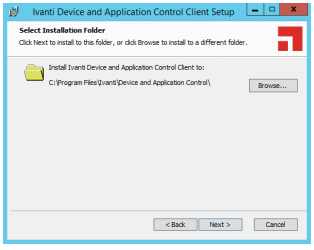

Figure 34: Destination Folder Page

15. You may choose an installation destination folder other than the Ivanti Device and Application Control default folder `C:\Program Files\Ivanti\Device and Application Control\`, by clicking **Change**.

Step Result: The ***Change Current Destination Folder*** page opens.

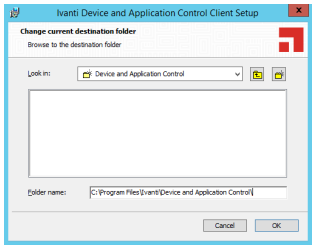

Figure 35: Change Current Destination Folder Page

16. Select a folder from the **Look in:** field.

17. Click **OK**.

Step Result: The ***Change Current Destination Folder*** closes, and the ***Destination Folder*** page changes to reflect the new location.

18. Click **Next**.

Step Result: The ***"Add or Remove Programs" list*** page opens.

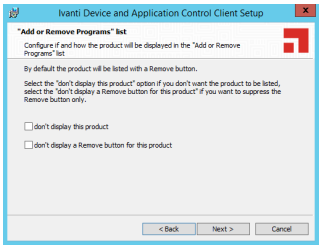

Figure 36: Add or Remove Programs List Page

19. You may select one of the following options, which are not required to proceed with installation:

Option	Description
Don't display this product	Does not display the Ivanti Device and Application Control component names in the **Add or Remove Programs** list in the Windows ***Control Panel***.
Don't display the Remove button for this product	Displays the Ivanti Device and Application Control component names in the **Add or Remove Programs** list in the Windows ***Control Panel*** without the **Remove** option.

20. Click **Next**.

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

> **Note:** NDIS enables Device Control to control 802.1x wireless adapters. If you do not need this protection, you may disable it here.

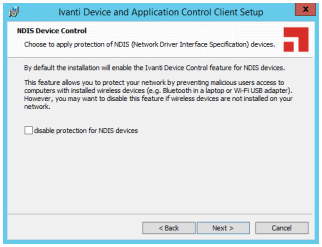

Figure 37: NDIS Device Control Page

21. Select the **disable protection for NDIS devices** check box to allow the use of wireless devices.

22. Click **Next**.

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

23. Click **Install**.

Step Result: A progress bar runs on the page, showing installation progress.

> **Attention:** The ***Setup*** dialog warning opens when there is an invalid, non-reachable server address and no policy file exists.

24. Select one of the following options.

Option	Description
Abort	Does not retrieve the policy file and cancels the installation process.
Retry	Attempts to retrieve the policy file and continue setup.
Ignore	Skips policy file retrieval and continues setup, creating the risk of blocking the computer from all device and executable file access.

> **Danger:** If you select **Ignore,** the Ivanti Device and Application Control suite installs with the most restrictive default file execution policy that denies use of all devices and/or executable files. This type of installation will deny you access to devices and software that you use on your computer, which can make the computer inaccessible. When you install a client offline for use with Application Control you must provide a policy settings file. Refer the Ivanti Application Control User Guide (https://help.ivanti.com) for more information about creating and exporting policy settings files.

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

25. Click **Finish**.

Result: The Ivanti Device and Application Control client is installed and connects to the Application Server.

After Completing This Task:

You must restart your computer system for the Ivanti Device and Application Control client configuration changes to become effective and enable the use of the Ivanti Device and Application Control client.

Chapter 3

Upgrading Ivanti Device and Application Control Components

You can use the installation software to upgrade previous versions Application Control and Device Control.

With Ivanti Device and Application Control, you can upgrade your Ivanti Device and Application Control product solution components that are versions 5.0 and higher.

Upgrade Overview

The Ivanti Device and Application Control upgrade process requires that you upgrade the primary software components, including the database, **Application Server**, **Management Console**, and client(s).

The following diagram illustrates the Ivanti Device and Application Control upgrade process.

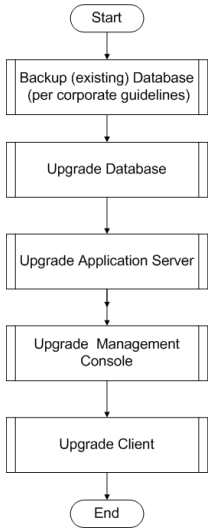

Figure 38: Ivanti Device and Application Control Component Upgrade Process

Danger: Do not change the key pair during an upgrade process when the **Client Hardening** mode is enabled, or the upgrade will fail.

Upgrading the Database

Using the Ivanti Device and Application Control installation software, the ***Installation Wizard*** upgrades the Ivanti Device and Application Control database, the first Ivanti Device and Application Control component that you upgrade.

Prerequisites:

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.

Note: Upgrade of the Ivanti Device and Application Control database does not require OLE automation or CLR to be enabled.

- Back-up your database before performing any upgrade.

  Please refer to the following for more information about database back-up and restore procedures for Microsoft SQL Server 2008.

  - See Backup Overview (http://msdn.microsoft.com/en-us/library/ms175477.aspx) for more information about backing up the database.
  - See Backing Up and Restoring How-to Topics (SQL Server Management Studio) (http://msdn.microsoft.com/en-us/library/ms189621.aspx) for more information about backing up and restoring the database.
  - See Backing Up and Restoring How-to Topics (Transact-SQL) (http://msdn.microsoft.com/en-us/library/aa337534.aspx) for more information about backing up and restoring the database.

1. Log in to the computer running the SQL server.

   Tip: If you are upgrading a database that was not installed on a SQL Server with the Ivanti Device and Application Control installation executable file, for example the database was moved to another server after initial installation or the database was installed using SQL script files, you must manually upgrade the Ivanti Device and Application Control database.

2. Close all programs running on the computer.

3. Open SQL Server Management Studio.

   During database migration, the size of the database may double. You must ensure enough disk space is available.

Caution: If a database size cap is set in SQL, database migration may fail.

a) Expand the **Databases** directory in the ***Object Explorer*** panel and right-click the target database.

Step Result: A right-mouse menu opens.

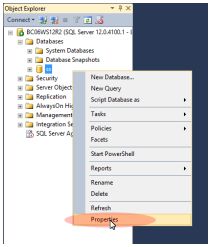

Figure 39: Right-Mouse Menu

b) Select **Properties** from the right-mouse menu.

Step Result: The ***Database Properties*** window opens.

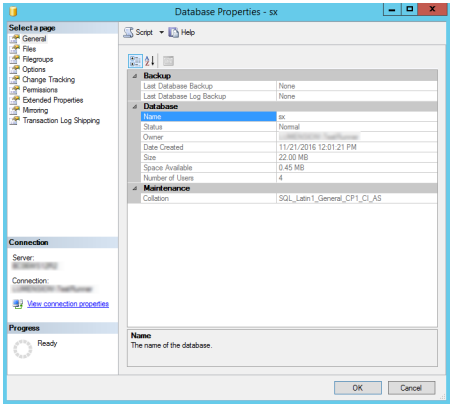

Figure 40: Database Properties Window

c) Select **Files**.

d) Click the ellipses [...] in **Autogrowth** column.

Step Result: The ***Change Autogrowth*** dialog opens.

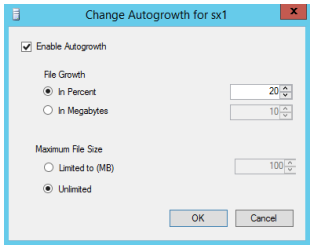

Figure 41: Change Autogrowth Dialog

e) Select **Enable Autogrowth**.

f) Select **Unrestricted File Growth**.

Important: You must maintain these settings until the database migration is finished. Database migration begins the first time the Ivanti Device and Application Control starts after upgrading the application. Database migration can take several hours or days, depending on the size of the database.

g) Click **OK**.

Step Result: The ***Change Autogrowth*** dialog closes.

h) Click **OK**.

4. From the location where you saved the Ivanti Device and Application Control application software, run `\server\db\Db.exe`.

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

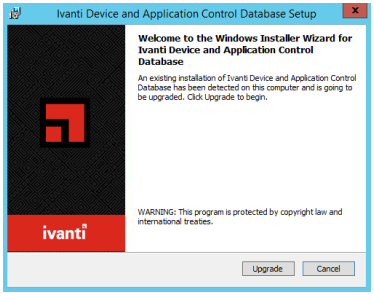

Figure 42: Welcome Page

5. Click **OK**.

6. Click **Upgrade**.

Step Result: The ***Ivanti Device and Application Control Database*** page opens showing a progress bar that indicates the installation status.

7. Click **Next**.

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

8. Click **Finish**.

Result: Ivanti Device and Application Control setup upgrades the existing Ivanti Device and Application Control database.

Upgrading the Application Server

Using the Ivanti Device and Application Control installation software, the ***Installation Wizard*** upgrades the Application Server, the second Ivanti Device and Application Control component that you upgrade.

Prerequisites:

- **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.

1. Log in to the computer that runs the Application Server.
2. Close all programs running on the computer.
3. Enter `net stop sxs` in a CMD prompt to stop the Application Server service.

   Note: If you are using several Application Servers, please stop their respective services manually before proceeding.

4. From the location where you saved the Ivanti Device and Application Control application software, run the `\server\sxs\Server.exe` file.
5. Click **OK**.

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

6. Click **Next**.

   Step Result: The ***Upgrade default Log Explorer templates*** page opens.

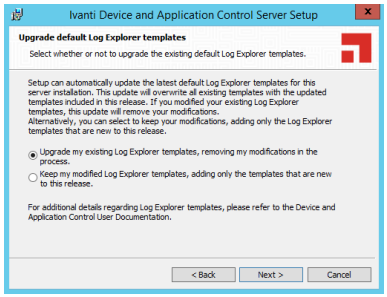

   Figure 43: Upgrade Default Log Explorer Templates Page

7. Select a ***Log Explorer*** template upgrade option.
8. Click **Next**.

   Step Result: The ***Server communication protocol*** page opens.

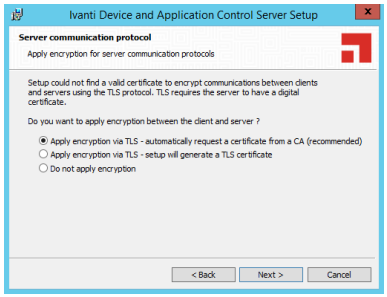

   Figure 44: Server Communication Protocol Page

9. Select an encryption option.

Restriction: The server communication protocol options shown depend upon the client version supported and whether a certification authority digital certificate is installed.

10. Click **Next**.

Step Result: The ***Server communication protocol*** page opens.

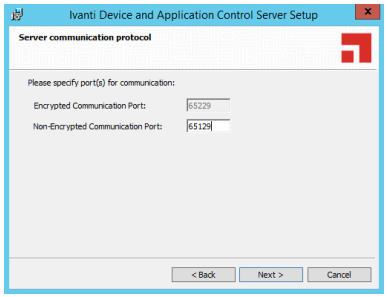

Figure 45: Server Communication Protocol Ports Page

11. Specify the communication port(s).

Restriction: The port field(s) shown depend upon the encryption communication protocol that you selected previously.

12. Click **Next**.

Step Result: The ***Syslog Server*** page opens.

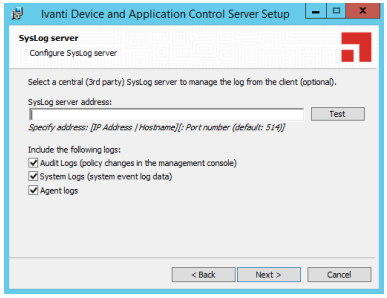

Figure 46: Syslog Server Page

13. Type the name or the IP address of the *SysLog* server in the **SysLog server address** field.

Important: This step is optional. You do not have to specify a *Syslog* server.

14. Select from the following options:

Option	Description
Audit Logs	Logs changes to policy administered through the Management Console.
System Logs	Logs system events.

Option	Description
Agent Logs	Logs events upload directly from the Ivanti Device and Application Control client.

15. Click **Next**.

Step Result: The ***Ready to Upgrade the Program*** page opens.

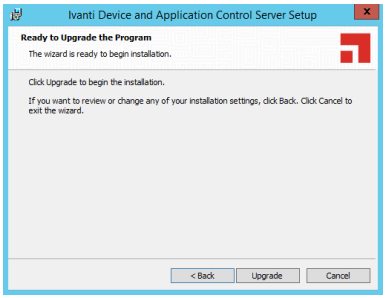

Figure 47: Ready to Upgrade Program Page

16. Click **Upgrade**.

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

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

17. Click **Finish**.

Result: Ivanti Device and Application Control setup upgrades and restarts the existing Application Server service.

Upgrading the Management Console

Using the Ivanti Device and Application Control installation software, the ***Installation Wizard*** upgrades the Management Console, the third Ivanti Device and Application Control component that you upgrade.

1. Log in to the computer where you are installing the Management Console.
2. Close all programs running on the computer.
3. From the location where you saved the Ivanti Device and Application Control application software, run the `\server\smc\Console.exe` file.

4. Click **OK**.

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

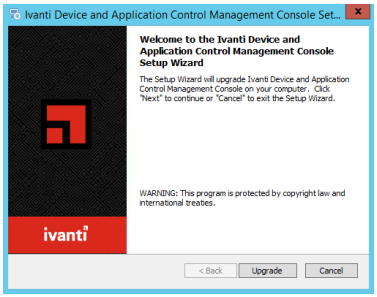

Figure 48: Welcome Page

5. Click **Upgrade**.

   Step Result: The ***Ivanti Device and Application Control Management Console*** page opens showing a progress bar that indicates the installation status.

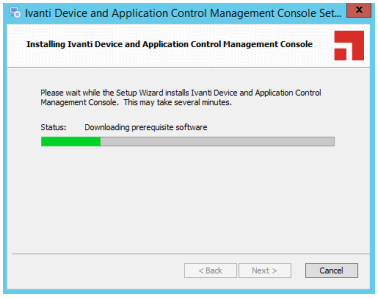

Figure 49: Installing Management Console Dialog

6. Click **Next**.

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

7. Click **Finish**.

Result: Ivanti Device and Application Control setup upgrades the existing Management Console.

Upgrading the Client

Using the Ivanti Device and Application Control installation software, the ***Installation Wizard*** upgrades the Ivanti Device and Application Control client, the fourth Ivanti Device and Application Control component that you upgrade.

Caution: When installing the client for Application Control, you may need to set the **Execution blocking** default option to **Non-blocking mode**. This is only necessary if the new client `.exe` and `.msi` files were not previously added to the central file authorization list and assigned to the corresponding file group. Otherwise, the Ivanti Device and Application Control client computer may not restart after Ivanti Device and Application Control client installation because executable system files cannot run until they are centrally authorized from the Management Console.

1. Log in to the computer that will run the Ivanti Device and Application Control client.
2. Close all programs running on the computer.
3. From the location where you saved the Ivanti Device and Application Control application software, run the `\client\Client.exe` file.

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

4. Click **Next**.

   Step Result: The ***Encrypted communication*** page opens.

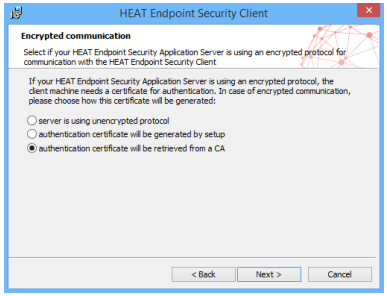

Figure 50: Encrypted Communication Page

5. Select one of the following options that matches the options you selected when you upgraded the Application Server.

Option	Description
Server is using unencrypted protocol	Communication between the Application Server and Ivanti Device and Application Control client is not using the TLS communication protocol. Communication is not encrypted but is signed using the private key.

Option	Description
Authentication certificate will be retrieved from a CA	Communication between the Application Server and Ivanti Device and Application Control client uses the TLS communication protocol. Communication is encrypted and the digital certificate is retrieved automatically during installation.

Tip: Ivanti recommends that you use the automatic TLS retrieval option to deploy *Certificate Authority* infrastructure for issuing valid digital certificates.

Step Result: If you opt to manually generate a certificate during setup, the ***Client Authentication*** dialog opens.

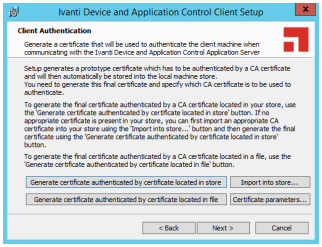

Figure 51: Client Authentication Dialog

6. To manually generate a certificate during setup specify the computer certificate location and parameters from the following options.

Option	Description
Generate certificate signed by certificate located in store	Generates a digital certificate during installation by using a signature certificate located in the local user store.
Generate certificate signed by certificate located in file	Generates a digital certificate during installation by using a signature certificate located in a specified file.
Import into store	Imports a signature certificate into the local user store.
Certificate parameters	Specifies the certificate parameters for the **Cryptographic service provider**, **Key length**, **Validity**, and **Signature**.

7. Click **Next**.

   Step Result: The ***Application Servers*** page opens.

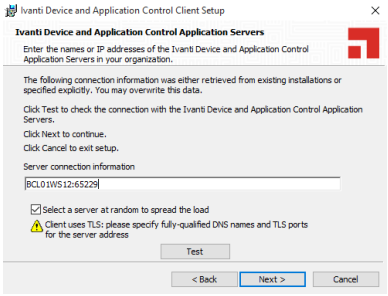

Figure 52: Application Servers Page

8. Specify up to three server names using fully qualified domain names (FQDN) or IP addresses that are managed from the Management Console.

Caution: Do not use IP address(es) when using the TLS communication protocol for encryption. You can only use FQDNs for when using the TLS communication protocol.

9. Verify that the Ivanti Device and Application Control client connects to the Application Server by clicking **Test**.

   Step Result: If the server name is correctly specified, the Application Server connects successfully with the client.

10. Click **Next**.

    Step Result: The ***"Add or Remove Programs" list*** page opens.

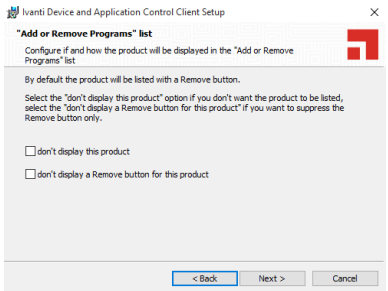

Figure 53: Add or Remove Programs List Page

11. You may select one of the following options, which are not required to proceed with the upgrade:

Option	Description
Don't display this product	Displays the Ivanti Device and Application Control product name in the **Add or Removes Programs** list in the Windows ***Control Panel*** with the **Remove** option.
Don't display the Remove button for this product	Displays the Ivanti Device and Application Control product name in the **Add or Removes Programs** list in the Windows ***Control Panel*** without the **Remove** option.

12. Click **Next**.

Attention: If NDIS was configured for the previously installed client version, the upgrade process may skip this step and proceed directly to the following step.

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

Note: NDIS enables Device Control to control 802.1x wireless adapters. If you do not need this protection, you may disable it here.

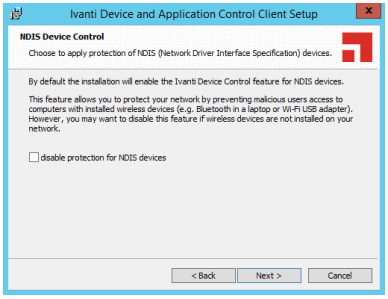

Figure 54: NDIS Device Control Page

13. Select the **disable protection for NDIS devices** check box to allow the use of wireless devices.

14. Click **Next**.

Step Result: The ***Ready to Upgrade the Program*** page opens.

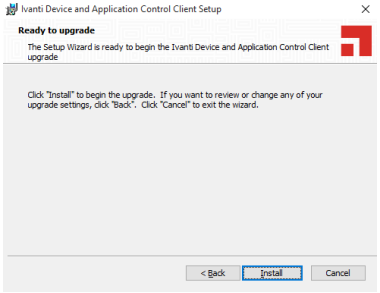

Figure 55: Ready to Upgrade the Program Page

15. Click **Upgrade**.

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

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

16. Click **Finish**.

Result: Ivanti Device and Application Control setup upgrades the existing Ivanti Device and Application Control client.

After Completing This Task:

You must restart your computer system as soon as possible, to prevent any existing file authorizations or device permission from becoming unstable and for the Ivanti Device and Application Control client configuration changes to become effective.

Chapter 4

Installation Checklist

To assist in gathering the information required for a smooth installation, Ivanti recommends that you use the following installation checklist.

The installation checklist identifies tasks necessary for installing the Ivanti Device and Application Control product solution.

Installation Checklist

The installation checklist outlines the detailed tasks that you must perform when installing the Ivanti Device and Application Control solutions.

This checklist guides you through the installation process.

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.

To begin your installation:

1. Copy the Ivanti Device and Application Control license file to the `\\Windows\System32` or `\\Windows\SysWOW64` folder, and rename the file to `endpoint.lic`. The license file may be installed after installing the database, however, the license file must installed before installing the Application Server.
2. Download the Ivanti Device and Application Control application software from the Self-Service Portal.
3. Create a device, media, or software application inventory which lists the items that you want Ivanti Device and Application Control to control.
4. Document company policy that defines:
    - Device permissions.

- Shadowing requirements.
- Device encryption requirements.
- Ivanti Device and Application Control administrators and their roles.
- Global domain groups for Ivanti Device and Application Control administrators.

5. Plan your Ivanti Device and Application Control network architecture, based on capacity requirements, that list the Application Server host names and IP addresses.
6. Create a dedicated Application Server domain user rights service account and set the following:

   - **User cannot change password**.
   - **Password never expires**.

   The domain account must have local administration rights when you plan to use the TLS communication protocol for client- Application Server and inter- Application Server data transfers.
7. Create **Impersonate a client after authentication** user rights for the Application Server. See Impersonate a Client After Authentication (http://support.microsoft.com/kb/821546) for additional information about impersonating a client after authentication user rights.
8. Verify that the Application Server domain account has **Log on as a service** user rights. See Add the Log on as a service right to an account (http://technet.microsoft.com/en-us/library/cc739424(WS.10).aspx) for additional information about logging on as a service user rights.
9. Install Microsoft® *Internet Information Services* on the same computer as the certification authority, otherwise the enterprise root certificate cannot be generated. See Internet Information Services (IIS) (http://www.iis.net) for additional information about installing *Internet Information Services*.
10. Install a Microsoft enterprise root certification authority to enable removable device encryption for Device Control. See Install a Microsoft enterprise root certification authority (http://technet.microsoft.com/en-us/library/cc776709.aspx) for additional information about installing an enterprise root certificate.
11. Install a Microsoft SQL Server® . See Getting Started with SQL Server (http://msdn.microsoft.com/en-us/sqlserver/default.aspx) for additional information about installing a SQL server.
12. Complete Installing the Database on page 20.
13. To install multiple Application Server s, create a shared file directory on a file server to share the Datafile directory component. This action is only required if you will be using more than one Application Server.
14. Complete Generating a Key Pair on page 23. This action is recommended, but not required.
15. Complete Installing the Application Server on page 25.

    Important: The Application Server service account must have database owner (DBO) rights to the Ivanti Device and Application Control database.

16. Complete Installing the Management Console on page 32.
17. Complete Installing the Client on page 35.
18. Test your Ivanti Device and Application Control product solution installation for functionality.

Chapter 5

Using Client Deployment

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***

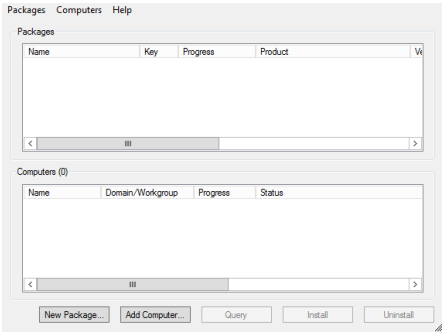

Figure 56: Client Deployment Dialog

Packages Panel

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

Table 8: 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 9: 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 10: 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 11: 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 `LESClient.msi` or `LESClient64.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.

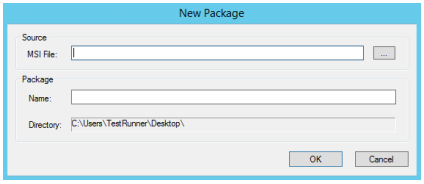

   Figure 57: New Packages Dialog

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.

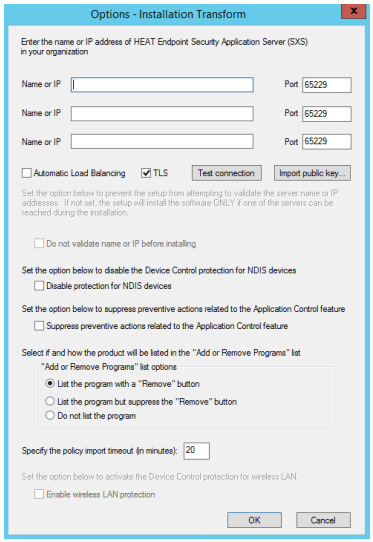

Figure 58: Options - Ivanti Device and Application Control Installation Transform Dialog

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 `LESClient.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.

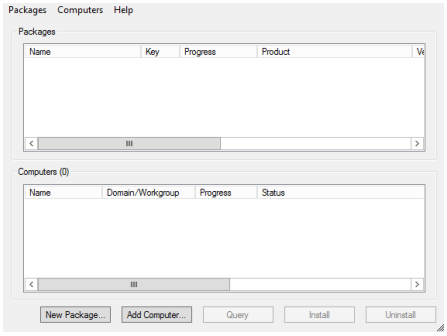

Figure 59: Client Deployment Dialog

2. Click **Add Computer**.

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

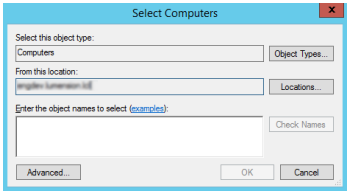

Figure 60: Select Computers Dialog

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.

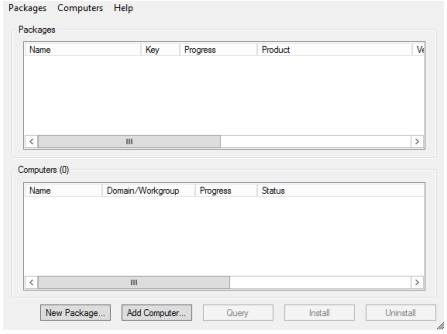

Figure 61: Client Deployment Dialog

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.

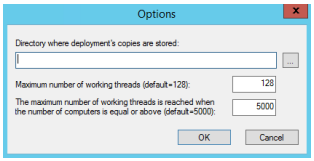

Figure 62: Options Dialog

   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 `setup.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.

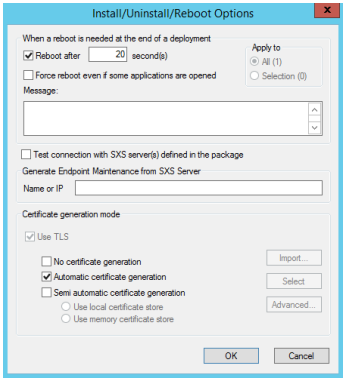

Figure 63: Install/Uninstall/Reboot/Options Dialog

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

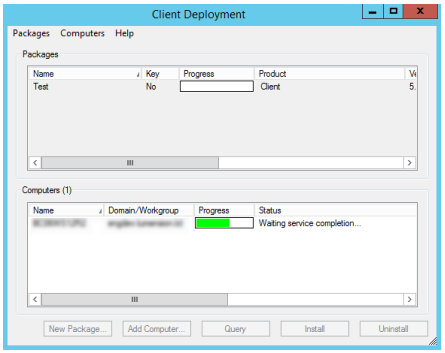

Figure 64: Dialog - Computer Progress

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.

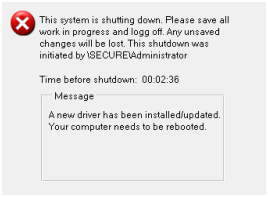

Figure 65: System Shutdown Dialog

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.

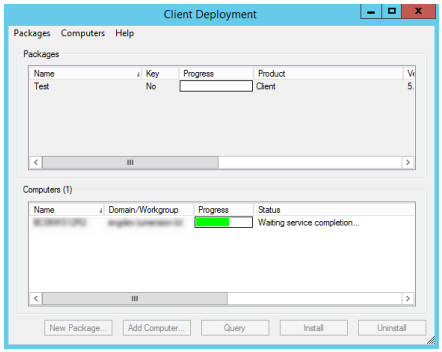

Figure 66: Client Deployment Dialog

Appendix
A

Configuring DCOM Settings for the Application Server

The Distributed Component Object Model (DCOM) is a Microsoft® technology that supports communication among software components distributed across networked computers, such as the Ivanti Device and Application Control Application Server and Management Console.

The ***Log Explorer*** module uses the Microsoft® Distributed Component Object Model (DCOM) protocol to retrieve log entries from the Management Console that is connected to theApplication Server. The other Management Console modules use Remote procedure calls (RPC) for network communication. If you intend to install the Management Console on a different computer or server than the Application Server, the network administrator must:

1. Configure the DCOM settings for the Application Server.
2. Set the security permissions for the computer-wide access control lists (ACLs) that govern access to all call, activation, or launch requests on the server, using Microsoft Group Policy to manage computer-wide DCOM access restrictions.

Note: DCOM does not work across non-trusted domains, especially when using workgroups.

Setting Up Distributed Component Object Model (DCOM)

The network administrator(s) that are responsible for using the Management Console must have the security access permissions set in Windows Component Services for DCOM properties.

1. Select **Start** > **Run**.

2. Type `dcomcnfg` in the **Open:** field.

   Step Result: The ***Component Services*** dialog opens.

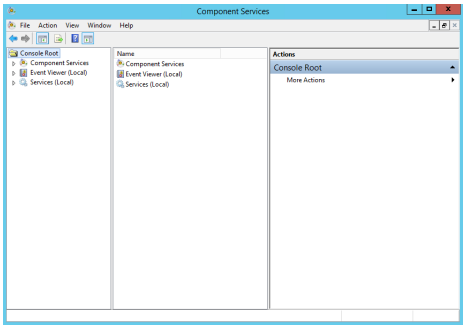

Figure 67: Component Services Dialog

> **Attention:** The steps described in this procedure are based on using a Windows® Server 2003 SP1 operating system (OS). If you are using a different Windows OS, the steps and step results may vary.

3. Double-click **Component Services**.
4. Double-click **Computers**.

   Step Result: **My Computer** is listed in the right pane.

5. Right-click **My Computer**.

6. Select **Properties**.

   Step Result: The ***My Computer Properties*** dialog opens.

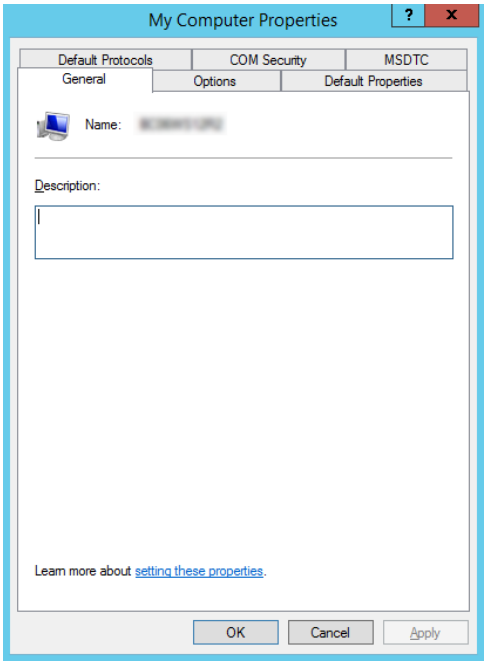

Figure 68: My Computer Properties Dialog

7. Select the ***COM Security*** tab.

8. In the ***Access Permissions*** panel, click **Edit Default**.

   a) Click **No**, for any warning screens that appear.

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

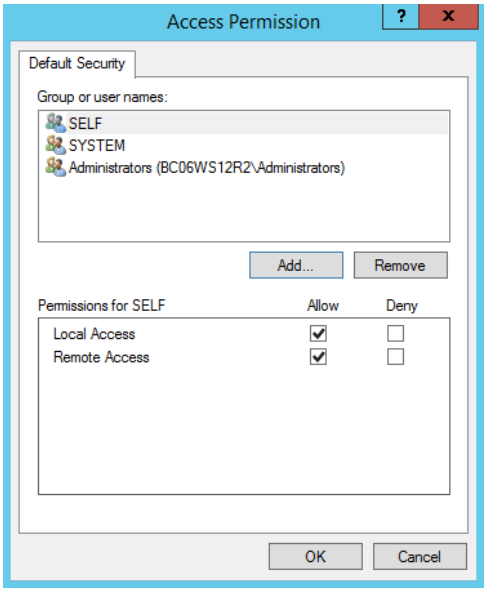

Figure 69: Access Dialog

9. Verify that:
   - SELF (the logged in user) is listed.
   - SYSTEM is listed.
   - The ***Permissions for SELF (and SYSTEM)*** **Allow** check boxes are selected for **Local Access** and **Remote Access**.

10. To create a new profile with the necessary permissions, click **Add**.

    Step Result: The ***Select Users or Groups*** dialog opens.

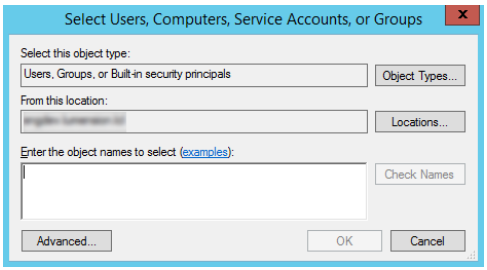

Figure 70: Select Users or Groups

11. In the **Select this object type** field, verify that at least **Users** is entered. If not:

a) Click **Object Types** and select **Users**.
b) In the **From this location** field, verify your computer name is entered.
c) Or, click **Locations** and select your computer name.
d) In the **Enter objects name to select** field, type a new object.
e) Click **OK**.
f) In the ***Access*** dialog, select the new object.
g) Select the **Allow** check box.

12. Click **OK**.

13. Click **OK**.

14. Close the ***Component Services*** dialog.

Set Access Control List Security Permissions

The network administrator(s) that are responsible for using the Management Console must have Access Control List (ACL) permissions configured for network Distributed Component Object Model (DCOM) security.

1. Select **Start** > **Run**.
2. Type `gpedit.msc` in the **Open:** field.

   Step Result: The ***Group Policy Object Editor*** dialog opens.

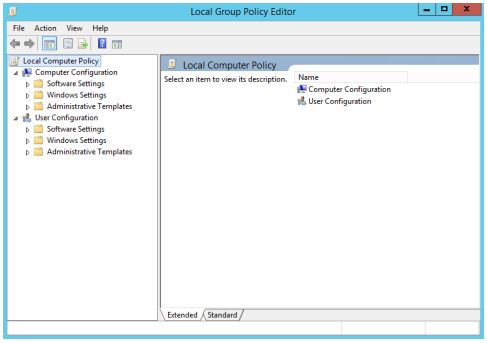

Figure 71: Group Policy Object Editor Dialog

3. Select **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

   Step Result: The right pane refreshes, listing the **Policy** settings.

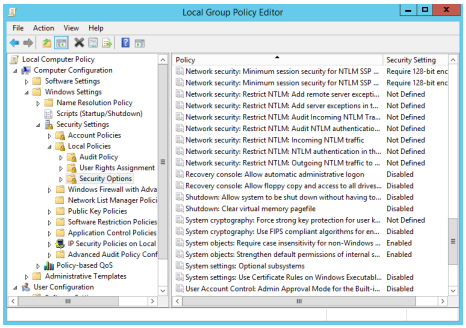

Figure 72: Group Policy Object Editor - Security Settings

4. Double-click **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax** from the **Policy** column in right pane.
5. Click **Edit Security**.
6. Add users and/or groups.
7. Select any or all of the following options for each user or group:
   - **Local Access**
   - **Remote Access**
8. Click **OK**.
9. Double-click **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax** from the **Policy** column in the right pane.
10. Click **Edit Security**.
11. Add users and/or groups.
12. Select any or all of the following options for each user or group:
    - **Local Launch**
    - **Remote Launch**
    - **Local Activation**
    - **Remote Activation**
13. Click **OK**.
14. Close ***Group Policy Object Editor*** dialog.
15. Select **Start** > **Run**.

16. Run `gpupdate.exe` from the command line.

Result: Group policy settings are refreshed with the DCOM settings that you specified.

Appendix
B

Installing the Client for Windows Embedded

Ivanti Device and Application Control provides a modular version of Application Control and Device Control for Microsoft Windows Embedded.

About Windows Embedded

Windows Embedded is an edition of Windows that contains a full feature set, but has restrictions on licensing that require the resulting device to boot directly into the original equipment manufacturer (OEM) application. When building the operating system (OS) image, the OEM chooses only necessary software components, which reduces the OS footprint. Component behavior is defined by component script and dynamic HTML.

Note: Windows Embedded is not the same as Windows CE, Windows Embedded targets a different set of devices with different functionality than Windows CE.

Windows Embedded is often used in the following devices:

- Thin Clients such as retail Point-of-Sale (POS) or Windows-based Terminals.
- Connected Clients such s Set-Top boxes, Gateways, Kiosks, ATMs, Industrial Control Systems, Office Automation, and Gaming Systems.

Refer to http://msdn.microsoft.com/embedded/ for additional information about Windows Embedded.

The Ivanti Device and Application Control Client for Windows Embedded

The Ivanti Device and Application Control Client for Windows Embedded is a modular application where the driver functionality is expressed as a set of properties, optional scripts, and resources.

Components are individually selectable pieces of functionality that can be included, or excluded, from an image. A component is comprised of properties, resources, and dependency information. Individual component behavior is defined by the components script and DHTML.

The following table defines the Ivanti Device and Application Control Client functionality supported within Windows Embedded:

Table 12: Windows Embedded Supported Functionality

Function	Windows Embedded Support
RTNotify	
RTNotify	Yes
Management Console Tools Menu	
Synchronize Domain	Yes
Send Updates to All Computers	Yes
Send Updates to	Yes
Purge Online Table	Yes
Offline Update	
Offline Update	Yes
Reports	
View reports	Yes
Device Control Default Options	
Device Control Status Window	Yes
Shadow Files Upload Delay or Time	Yes
Shadow Directory	Yes
Application Server Address	Yes
Encrypted Media Key Export	Yes
Encrypted Media Export Password	Yes
Certification generation	Yes
Centralized Device Control Logging	Yes
Suppress recurring log events	Yes
Device Explorer	
Default Settings	Yes
Manage Devices	Yes
Assigning Permissions	Yes

Function	Windows Embedded Support
Assigning Schedule Permissions	Yes
Assigning Temporary Permissions	Yes
Assigning Online and Offline Permissions	Yes
Shadow	Yes
Copy Limit	Yes
Computer Group	Yes
File Filtering	Yes
Media Authorizer	
Media Authorizer	Yes
Shadow Files Explorer	
View Shadowed Files	Yes
Encrypted communications (TLS protocol)	Yes
Ivanti Device and Application Control Client to **Application Server** and intra **Application Server** encrypted communications	Yes

The following table defines the devices supported by the Ivanti Device and Application Control Client on Windows Embedded.

Table 13: Windows Embedded Supported Devices

Device Group	Windows Embedded Support
Biometric devices	No Drivers *
COM/Serial Ports	No Drivers *
CD/DVD Drives	Yes
Floppy Disk Drives	Yes
Imaging Devices	No Drivers *
LPT/Parallel Ports	No Drivers *
Modems/Secondary Network Access devices	No Drivers *
Palm Handheld Devices	No Drivers *
Printers	No Drivers *

Device Group	Windows Embedded Support
PS/2 Ports	Not Applicable
Removable Storage Devices	Yes
RIM Blackberry Handhelds	No Drivers *
Smart Card Readers	No Drivers *
Tape Drives	No Drivers *
User Defined Devices	Not Applicable
Windows CE Handheld Devices	No Drivers *
Wireless NICs	No Drivers *
* Drivers for this device group are not automatically included in Windows Embedded. To enable support for this device group, you must manually install the necessary drivers.	

Install and Configure the Client

Using the Microsoft Target Designer, you can configure the Ivanti Device and Application Control Client for use on Windows Embedded.

Prerequisites:

- Verify that you satisfy the minimum hardware and software system requirements.
- Install the Application Server.
- Install the Management Console.

To install the Ivanti Device and Application Control Client, you must:

1. Create an image.
2. Install the image on the device.

This procedure will walk you through adding the Ivanti Device and Application Control Client to your image.

1. Import the Ivanti Device and Application Control Client `SLD` into the component database server using the **Import** functionality of the ***Microsoft Component Database Manager***.
2. Launch the ***Microsoft Target Designer***.
3. Add the Ivanti Device and Application Control Client `SLD` to your target image.
   a) Using the ***Microsoft Target Designer***'s search tool, search for the Ivanti Device and Application Control Client `SLD`.
   b) Once found, double-click the Ivanti Device and Application Control Client `SLD` to add it to your project.

4. Browse to and locate the Ivanti Device and Application Control Client Settings.
5. Enter the fully qualified domain name(s) or IP address(es) for the Application Server(s) installed in your environment.
   a) Within the **SXS name (or IP Address)** field, type the Application Server's IP Address or fully qualified domain name.
   b) Within the **Port** field, type the Application Server's port (Default = 65129).
6. Select the desired **Encrypted Communication** option.

Option	Description
Server is using unencrypted protocol	Communication between Application Server(s) and the Ivanti Device and Application Control Client and is not encrypted but is still signed using the private key. This is, essentially, a legacy communication protocol and not recommended for high security installations.
Authentication certificate will be copied manually (The certificate will have to be placed manually on the target image)	Manual mode using TLS communication: The administrator generates and provides the machine certificate used in all communications. All communication between Ivanti Device and Application Control Client and Application Server(s) is encrypted. This mode is used when there is no Certification Authority installed in the network or cannot be reached when doing the client installation. The machine certificate has to be created by a user (usually the administrator) who already possess a certificate good for issuance and trusted as a root or intermediate Certificate Authority by the Application Server. This authorized user has to be physically present at the machine to create this certificate.

Option	Description
Authentication certificate will be automatically retrieved from a CA	Automatic mode using TLS communication: The program asks for the certificate to one of the selected Certificate Authorities. This certificate must be good for issuance and trusted as a root or intermediate Certificate Authority by the Application Server. All communication between Ivanti Device and Application Control Client and Application Server(s) is encrypted. You do not need a Certificate Authority at this point, but it will be required when first starting the client(s) since the program request a machine certificate. The user who has the rights to create machine's certificates does not have to be physically present at the machine to do the installation if this mode is selected.

Note: You should use automatic mode when your organization has already deployed a Certificate Authority infrastructure and the Ivanti Device and Application Control servers and clients are part of it. Thus making the deployment of the Client using TLS completely transparent with no additional action required. When it is not possible to use this mode, then you should turn to the manual mode, as the semi-automatic mode is not available when installing the Client on Windows Embedded.

7. If desired, select the **Do not use NDIS Feature** option to disable NDIS support.

Note: NDIS enables Device Control to control 802.1x wireless adapters. If you do not need this protection, you may disable it here.

After Completing This Task:

- Continue using the ***Microsoft Target Designer*** to complete the image.
- When the image is complete, save the image and then mount the image to your target device.

Tip: Refer to http://msdn.microsoft.com/embedded/ for additional information.

Enhance Write Filter

Enhance Write Filter (EWF) is used to protect disk volumes by intercepting write requests and redirecting them to an overlay volume (such as RAM or another disk).

The Ivanti Device and Application Control Client running with EWF enabled is able to pick up all permissions, including managed devices and temporary permissions, from the server after a reboot. EWF can be activated or deactivated from within the Control Panel.

Enhance Write Filter provides the following functionality:

- Write protects one or more partitions on your system.
- Enables read-only media, such as CD-ROM or flash to boot and run.

Enhance Write Filter consists of two major components:

- **EWF Overlay**: EWF protects the contents of a volume by redirecting all write operations to an alternative storage location.
- **EWF Volume**: An EWF volume is created on the media in an un-partitioned disk space. This EWF volume stores configuration information about all EWF–protected volumes on the device

There are three different modes of EWF, depending upon the different configurations of the EWF Overlay and EWF Volume. These modes are as follows:

- **Disk on Disk**: Used to maintain the state of the system between reboots. The EWF volume is created on disk in an un-partitioned space.
- **RAM in RAM**: Utilized to discard any write information after reboot or to delay writing the overlay to the media. The EWF volume is created on disk in an un-partitioned space.
- **RAM Reg in RAM**: Similar to EWF RAM types, RAM Reg overlays stores information in RAM. However, the configuration information about EWF is not stored in a separate EWF volume, but within the registry.

Issues to Consider

When installing the Ivanti Device and Application Control Client on Windows Embedded, the following must be considered.

- User Notifications are displayed only within the Explorer Shell
- The RTNotify icon is only displayed in the Explorer Shell and only when the **Show Notification in Taskbar** setting is selected within the user interface.
- You cannot deploy the Ivanti Device and Application Control Client to Windows Embedded using Client Deployment tool. You must use the procedure defined within Install and Configure the Client on page 86.
- The public file key (`sx-public.key`) import must be done manually. This can be done by manually copying the file into the `%SystemRoot%\sxdata` directory of your image prior to deployment.
- In order to retrieve initial permissions, the Application Server must be running, and accessible from the client, when the client boots.