

Intel(R) IT Director User's Guide

Table of Contents

Disclaimer and Legal Information	1
Introduction	3
To set up Intel IT Director:	3
See Also	3
System Configuration	5
See Also	5
Settings Page: Overview	7
See Also	7
Setting User Privileges	9
See Also	9
Disabling My Computer Settings.....	11
To disable your My Computer settings:	11
See Also	11
Monitoring Your Network.....	13
See Also.....	14
Computers Without Intel IT Director.....	14
See Also.....	14
Hardware and Software Asset Monitor	14
See Also.....	14
System Details Page	15
See Also.....	15
Violations and Warnings	15
See Also.....	16
Configuring Your Network	17
Configuring Subnets.....	17
Configuring Hard Drive Backup and Restore Requirements.....	17
Configuring Internet and Network Security Requirements	18
Configuring Hard Drive Free Space Requirements	19
Configuring Your Computer	21
See Also.....	21
Importing Settings	21

See Also.....	22
Exporting Settings.....	22
See Also.....	22
Enabling Hard Drive Backup and Restore	22
See Also.....	23
Blocking USB Devices	23
Disabling USB Blocking.....	24
USB Device Types.....	25
Configuring the Power-On Monitor	26
See Also.....	26
Troubleshooting.....	27
Configuring Norton 360*	30
Configuring McAfee Total Protection*	33
Configuring Trend Micro Internet Security*	34
Configuring Microsoft Windows* Small Business Server.....	37
Index	39

Disclaimer and Legal Information

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL(R) PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Atom, Centrino Atom Inside, Centrino Inside, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, IntelDX2, IntelDX4, IntelSX2, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skool, Sound Mark, The Journey Inside, Viiv Inside, vPro Inside, VTune, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.
Copyright (C) 2008, Intel Corporation. All rights reserved.

Introduction

Intel® IT Director enables you to configure and monitor system protection for computers in your network. It enables you to [monitor up to 25 client computers](#) on up to two [subnetworks \(subnets\)](#).

Before using Intel IT Director, configure your system as explained in the [Getting Started Guide](#).

To set up Intel IT Director:

1. On each computer, [set user privileges](#) on Intel IT Director.
2. On each computer, [configure Intel IT Director settings for that computer](#).
3. From computers you will use to monitor the network, [configure your network](#).

Once you finish these steps, you can start [monitoring your network](#).

The Intel IT Director interface includes the following tabs:

- **My Computer.** Configure protection and monitoring on client computers.
- **My Network.** Monitor your network.
- **Settings.** Set user privileges, disable My Computer settings, and configure your network.

For support and more information about Intel IT Director, see <http://support.intel.com/support/go/itdirector.htm>.

See Also

[Getting Started Guide](#)

[Setting User Privileges](#)

[Monitoring Your Network: Overview](#)

[Configuring Your Network: Overview](#)

[Configuring Your Computer: Overview](#)

[Blocking USB Devices: Overview](#)

[Configuring the Power-On Monitor](#)

[Troubleshooting](#)

System Configuration

Before using Intel IT Director, use the Intel IT Director Configuration Tool to configure your system, as explained in the Getting Started Guide.

Access this tool from **Start > All Programs > Intel(R) IT Director > Intel(R) IT Director Configuration Tool**.

The Intel IT Director Configuration Tool also enables you to re-configure your system after you have already configured it. See the Getting Started Guide for more information.

See Also

[Getting Started Guide](#)

Settings Page: Overview

The Settings page includes the following sections:

- [User Privilege Settings](#)
- [Disabling My Computer Settings](#)
- [My Network Settings](#)

You can configure settings manually, or you can [import the settings from a file](#). To use settings from the current computer on other computers, [export your settings to a file](#).

To switch log on accounts, click **Change Log On** from the **Settings** page. For the log-on box to automatically use the same username and password next time you log on, select **Save Username and Password**.

See Also

[Setting User Privileges](#)

[My Computer Settings](#)

[My Network Settings](#)

[Importing Settings](#)

[Exporting Settings](#)

Setting User Privileges

When you first use Intel IT Director on each computer, set which features users can access on that computer. Set access privileges from **Settings > User Privilege Settings**.

Choose from two options:

- **All users with Windows* administrator privilege can access all features.**
- **The current user (*username*) can access all features.**

If you choose **The current user (*username*) can access all features**, then you can also choose whether other users can access specific pages in Intel IT Director.

You can choose from:

- [My Computer](#) tab
- [My Network](#) tab

See Also

[Introduction](#)

[Settings Page](#)

Disabling My Computer Settings

Disabling My Computer settings:

- Disables access to the [My Computer tab](#).
- Disables USB Blocking and the Power-on Monitor
- Erases configuration of USB Blocking and Power-on Monitor.

To disable your My Computer settings:

1. From Intel IT Director on the client computer, go to **Settings > Disabling My Computer Settings**.
2. Select **Erase all Intel IT Director settings on this computer, and restore Intel IT Director to default**.
3. Click **Apply**.

After you disable My Computer settings, you can not enter the [My Computer tab](#) until you deselect **Erase all Intel IT Director settings on this computer, and restore Intel IT Director to default**.

See Also


[Settings Page](#)

[Configuring Your Computer: Overview](#)

Monitoring Your Network

Intel IT Director enables you to monitor status, statistics and warning messages for client computers on your network. You monitor computers on your network from the **My Network** page.




The bottom of the **My Network** page shows two rows of computers:

- The top row includes computers to which Intel IT Director has finished trying to connect. If Intel IT Director failed to connect, it shows a picture of the computer with the  icon on top of it. See [Troubleshooting](#) for possible reasons.
- The second row includes computers to which Intel IT Director is trying to connect. Once Intel IT Director connects to those computers, they move to the second row.

The **My Network** page monitors the following features:

- USB Blocking
- Hard Drive Backup and Restore
- Security Center
- Power-on Monitor
- Hard Drive Free Space

The My Network section can display the following icons in feature heading bars:

-  denotes Intel IT Director has recorded [violations or warnings](#) for the feature.
-  denotes all computers comply with the requirements for the feature.
-  denotes Intel IT Director does not detect any computer supporting this feature.

When you expand a section, you see a list of all computers with warnings or violations for that section. If you click on a computer from that list, the [System Details](#) page opens with details about that computer.

To see details about the [hardware and software assets on a computer](#), mouse over the icon of that computer from anywhere in the **My Network** page.

Note

To configure requirements that apply to all computers on your network, go to **Settings** > [My Network Settings](#). To configure monitoring and protection specific to a single computer, go to the [My Computer page](#) on Intel IT Director at that computer.

See Also

[Violations and Warnings](#)

[Configuring Your Network: Overview](#)

[Configuring Your Computer: Overview](#)

[Blocking USB Devices: Overview](#)

[Enabling Hard Drive Backup and Restore](#)

[Configuring Hard Drive Free Space Requirements](#)

[Configuring Internet and Network Security Requirements](#)

[Configuring the Power-on Monitor](#)

Computers Without Intel IT Director

For Intel IT Director to monitor a computer, remote queries must be configured on that computer. For more details, see the Getting Started Guide.

On computers that do not have Intel IT Director installed, you can monitor:

- [Internet and network security](#)
- [Free hard drive space](#)
- [Hardware and software assets](#)

You monitor computers without Intel IT Director in the same way as you monitor computers with Intel IT Director.

See Also

[Monitoring Your Network: Overview](#)

Getting Started Guide

Hardware and Software Asset Monitor

Intel IT Director monitors the hardware and software assets of computers on your network. You can see the list of hardware and software assets in two ways:

- By mousing over the icon of a computer from anywhere in the **My Network** page.
- From **System Details > Hardware and Software Assets**.

Intel IT Director monitors the following information about hardware and software assets for each computer:

- Computer System (manufacturer and model number)
- Processor
- Operating system

See Also

[Monitoring Your Network: Overview](#)

[System Details](#)

System Details Page

When you click a computer icon on the **My Network** page, the **System Details** page opens with the details of the computer you selected.

The System Details page shows all [violations and warnings](#) Intel IT Director has recorded for computers on your network. Once you acknowledge seeing a message, that message no longer appears in the list of warning messages.

The System Details page shows the details of the computer for the following features:

- [USB Device Blocking](#)
- [Hard Drive Backup and Restore](#)
- [Security Center](#)
- [Hardware and Software Asset](#)
- [Power-on Monitor](#)
- [Hard Drive Free Space](#)

See Also


[Monitoring Your Network](#)

[Configuring Your Network: Overview](#)

[Violations and Warnings](#)

Violations and Warnings


If Intel IT Director has recorded any violations or warnings for a feature, it shows the

 icon in the relevant feature heading bar in [My Network](#). The following table shows the possible violations and warnings for each feature:

Note

Warning messages are displayed in the [System Details Page](#). Once you acknowledge a warning message on the System Details page, the message is no longer displayed.

Feature	Violations and Warnings
USB Blocking	Violation: USB Blocking has not been configured Warnings: <ul style="list-style-type: none"> • A blocked USB device was connected. • USB Blocking stopped working.

<p>Hard Drive Backup and Restore</p>	<p>Violation: Intel® Matrix Storage Manager is not installed on a computer. This violation applies only if you choose to monitor hard drive backup and restore.</p> <p> Note</p> <p>Intel Matrix Storage Manager uses RAID to perform hard drive backup and restore. If the chipset does not support RAID, or if the RAID drivers are not installed on a computer, that computer will be listed in My Network as not supporting backup and restore through Intel Matrix Storage Manager. If the chipset is configured as AHCI mode, the RAID drivers cannot be installed.</p>
<p>Security Center</p>	<p>A feature monitored by the Security Center does not meet the Security Center requirements.</p>
<p>Power-on Monitor</p>	<p>Violation: The Power-on Monitor has not been configured</p> <p>Warnings:</p> <ul style="list-style-type: none"> • A computer was powered on for more than one hour outside of office hours in a given day. • The Power-on Monitor stopped working.
<p>Hard Drive Free Space</p>	<p>Free space on a hard drive dropped below the required threshold.</p> <p>If a hard drive has multiple partitions, Intel IT Director treats the entire hard drive as if it were only one partition. The percentage of free space is calculated as the total free hard drive space divided by the total hard drive space.</p>

See Also

[Monitoring Your Network: Overview](#)

[System Details Page](#)

Configuring Your Network

You configure requirements to apply across your network from **Settings > My Network Settings**.

My Network Settings enables you to configure:

- [Subnets](#)
- [Internet and Network Security Requirements](#)
- [Hard Drive Free Space Requirements](#)

See Also

[Monitoring Your Network](#)

[Settings Page](#)

Configuring Subnets

A subnetwork (or subnet) is a part of a larger network. Your network may have multiple subnets. Intel IT Director automatically searches for all computers on the local subnet. You can instruct Intel IT Director to search on an additional subnet.

To instruct Intel IT Director to search for computers on additional subnets:

1. Go to **Settings > My Network Settings**.
2. Select **In addition to the local PC subnet, scan the following subnet** and enter the subnet address.
3. Press **Apply**.

For Intel IT Director to find and monitor a computer, that computer must have remote queries configured.

See Also

[Monitoring Your Network: Overview](#)

[Configuring Your Network: Overview](#)

Configuring Hard Drive Backup and Restore Requirements

Intel® Matrix Storage Manager enables you to back up data to a second hard drive. It uses Serial Advanced Technology Attachment (SATA) to manage a Redundant Array of Independent Disks (RAID). For a computer to support Intel Matrix Storage Manager, the chipset must support RAID, and the RAID drivers must be installed.

You can choose to monitor whether Intel Matrix Storage Manager is installed on network computers. By default, Intel IT Director monitors Intel Matrix Storage Manager installation.

To start or stop monitoring whether Intel Matrix Storage Manager is installed on network computers:

1. Go to **Settings > My Network Settings**.
2. Check or uncheck the box next to **Monitor whether Intel Matrix Storage Manager is installed on network computers**.
3. Click **Apply**.

 **Note**

Intel Matrix Storage Manager uses RAID to perform hard drive backup and restore. If the chipset does not support RAID, or if the RAID drivers are not installed on a computer, that computer will be listed in [My Network](#) as not supporting backup and restore through Intel Matrix Storage Manager. If the chipset is configured as AHCI mode, the RAID drivers cannot be installed.

See Also

[Enabling Hard Drive Backup and Restore](#)

Intel® Matrix Storage Technology website:

http://www.intel.com/design/chipsets/matrixstorage_sb.htm

Configuring Internet and Network Security Requirements

Through the internet, your computer could be exposed to damage or unauthorized access. To increase your control over computer security, Intel IT Director monitors internet security settings on computers in your network. You can choose which of these settings to require. If a computer is missing a required setting, Intel IT Director records a [violation](#).

To select required internet security settings:

1. Go to **Settings > My Network Settings**.
2. Under **Choose which security features to monitor**, select any options from the following list:
 - Windows* Automatic Updates.
 - Firewall
 - Anti-Virus Software
 - Anti-Spyware Software
3. Press **Apply**.

The internet and network security settings are based on settings in the Windows Security Center*. For more information, see the Windows Security Center documentation.

Use the [My Network](#) tab to monitor the security features.

See Also

[Configuring Your Network: Overview](#)

[Monitoring Your Network: Overview](#)

[Violations and Warnings](#)

Configuring Hard Drive Free Space Requirements

Intel IT Director monitors free space on the hard drives on your network. You can choose to receive warnings if free space on a hard drive drops below a threshold.

To set a threshold for the free space on your hard drive:

1. Go to **Settings > My Network Settings**.
2. For **Hard Drive Free Space Threshold**, choose a percentage.
3. Click **Apply**.

See the free space on your hard drives and all warning messages in the [System Details](#) page.



Note

If a hard drive has multiple partitions, Intel IT Director treats the entire hard drive as if it were only one partition. The percentage of free space is calculated as the total free hard drive space divided by the total hard drive space.

See Also

[Configuring Your Network: Overview](#)

[Monitoring Your Network: Overview](#)

Configuring Your Computer

Configure protection and monitoring on a computer from the **My Computer** page in Intel IT Director on that computer.

The My Computer page includes the following features:

- [USB Blocking Policy](#)
- [Hard Drive Backup and Restore](#)
- [Power-on Monitor](#)

Once you configure features from the My Computer page, you can monitor those features from the [My Network](#) page.

See Also

[Monitoring Your Network: Overview](#)

[Configuring Your Network: Overview](#)

Importing Settings

Instead of separately configuring each Intel IT Director setting, you can import a group of settings from a file. You can import any of the following settings:

- Configurations in Settings Page:
 - [User Privileges](#)
 - [Local Computer Management](#)
 - [Additional Subnets](#)
 - [Security Center Required List](#)
 - [Hard Drive Free Space Threshold](#)
- Configurations in My Computer page:
 - [USB Blocking](#)
 - [Power-on Monitor](#)

Note

Importing settings overwrites the previous settings.

To import settings:

1. Go to **Settings**.
2. Click the **Import** button at the bottom of the window.
3. Choose whether to save your current settings to a file. Click **Next**.
4. Choose the file from which to import settings.
5. Choose the settings to import. Click on each setting to see how it is set.

6. Click **Finish** to import the settings.

See Also

[Configuring Your Network: Overview](#)

[Settings Page: Overview](#)

[Exporting Settings](#)

Exporting Settings

You can export your settings from Intel IT Director to a file. You can [import your settings](#) on other computers from this file.

You can export any of the following settings:

- Configurations in Settings Page:
 - [User Privileges](#)
 - [Local Computer Management](#)
 - [Additional Subnets](#)
 - [Security Center Required List](#)
 - [Hard Drive Free Space Threshold](#)
- Configurations in My Computer page:
 - [USB Blocking](#)
 - [Power-on Monitor](#)
- Intel IT Director Configuration Tool

To export settings:

1. Go to **Settings**.
2. Click the **Export** button at the bottom of the window.
3. Select the settings to export. Click **Next**.
4. Set the file name and directory path. Click **Next**.
5. Click **Finish** to export your settings to the file.

See Also

[Configuring Your Network: Overview](#)

[Settings Page: Overview](#)

[Importing Settings](#)


Enabling Hard Drive Backup and Restore

Your hard drive stores your electronic information. To prevent losing data in a hard drive crash, you should back up your hard drive and store the information in a separate location.

The Intel IT Director hard drive backup and restore feature uses the following applications:

- Intel® Matrix Storage Manager (default). Enables you to back up data to a second hard drive. Uses Serial Advanced Technology Attachment (SATA) to manage a Redundant Array of Independent Disks (RAID).
- Windows* Backup or Restore Wizard (if Intel® Matrix Storage Manager is not available). Helps you back up data, which you can then store elsewhere.

The  icon denotes that Intel® Matrix Storage Manager is not installed on your computer.

The  icon denotes that Intel® Matrix Storage Manager is not supported on your computer.

For more details, see [Configuring Hard Drive Backup and Restore Requirements](#).

To enable hard drive backup and restore on a computer:

1. From Intel IT Director on the computer, go to **My Computer > Hard Drive Backup and Restore**.
2. Click the Launch box to launch either Intel® Matrix Storage Manager or Windows* Backup or Restore Wizard.

Note

Intel IT Director only monitors whether or not you have configured a hard drive backup application. It does not monitor the actual configuration of that application.

See Also

[Monitoring Your Network: Overview](#)

[Configuring Hard Drive Backup and Restore Requirements](#)

Intel® Matrix Storage Technology website:

http://www.intel.com/design/chipsets/matrixstorage_sb.htm

Blocking USB Devices

Universal Serial Bus* (USB*) is a connection standard for many types of devices. In some situations, USB devices can pose risks to information security or computer stability. For example, someone could transfer classified information from your computer to a USB storage device.

Use Intel IT Director to block USB devices from accessing your computer. When you plug in a blocked USB device to your computer, Intel IT Director notifies you that you have tried to plug in a blocked device and prevents you from using that device.


 **Note**

For Intel IT Director to block USB devices, USB blocking must be [enabled](#).

You can block all or specific types of USB devices.

See [Troubleshooting](#) for what to do if a new device is blocked, and you think it should not be blocked.

 **Note**

The  icon denotes that USB Blocking either has not been configured or has stopped working.

To choose the USB device types to block on a computer:

1. From Intel IT Director on the computer, go to **My Computer > USB Blocking Policy**.
2. Under **Select USB Device Types to Block**, check the box next to device types you want to block.
3. Click **Apply**.

You can monitor the USB blocking feature on computers on your network from the [My Network](#) page.

See Also

[Disabling USB Blocking](#)

[USB Device Types](#)

[Troubleshooting](#)

Disabling USB Blocking

By default, Intel IT Director blocks the USB device types you selected to block. When you disable USB device blocking, Intel IT Director does not block any USB devices, even if you have selected devices to be blocked.

To activate USB device blocking on your computer:

1. From Intel IT Director on the computer, go to **My Computer > USB Blocking Policy**.
2. Check the box **Disable USB Blocking Policy**.
3. Press **Apply**.

If USB blocking is disabled on a computer, Intel IT Director records a warning message. Monitor USB Blocking through [My Network](#).

See Also

[Blocking USB Devices](#)

USB Device Types

Choose the USB device types to block from **My Computer** > [USB Blocking](#). Here are the device types you can block, along with examples of each:

Device Type	Example
Audio device	Headphones, speakers
Video device	Webcam
Digital camera	Digital camera
Joystick	Joystick or other controller
Mass storage drive	USB flash drive, mp3 player
Smart Card	A smart card
Network device	Printer, router
Wireless controller	Wi-Fi* adapter, Bluetooth* adapter
IrDA	Printer or camera using infrared communications
Printer	A device with printing capabilities
Content security	
Personal Healthcare	Heart rate monitor, blood pressure cuffs, exercise watch
Personal Data Assistant	Some handheld computers, smartphones

See Also

[Blocking USB Devices: Overview](#)

[Activating USB Device Blocking](#)

Configuring the Power-On Monitor

The Power-on Monitor tracks when computers in your network are turned on. This feature helps you monitor both energy usage and computer usage.

Note

When a computer is in a sleep state such as standby or hibernate, Intel IT Director considers it to be powered off.

The Power-on Monitor does not physically limit computer usage. Instead, it tracks computer usage, and records a violation when a computer is powered on for more than one hour outside of office hours in a given day. Intel IT Director does not send any violation for a computer turned on during office hours. You can set the office hours for the Power-on Monitor.

For example:

You set the office hours to be Monday-Friday, 8:00 a.m. to 8:00 p.m. If the computer is on from 9:00 a.m. to 7:00 p.m. on Tuesday, no violation is recorded. However, if the computer is on from 6:00 a.m. to 7:01 a.m. Wednesday morning, a violation is recorded.

Note

The  icon denotes that the Power-on Monitor either has not been configured or has stopped working.

To set the office hours for the Power-on Monitor for a computer:

1. From Intel IT Director on the computer, go to **My Computer > Power-on Monitor**.
2. Select the days and hours to count as office hours.
3. Click **Apply**.

See the power-on statistics and violation messages in the [System Details](#) page.

See Also
[System Details](#)

[Configuring Your Computer: Overview](#)

[Monitoring Your Network: Overview](#)

Troubleshooting

Problem	Causes and Possible Solutions
Intel IT Director fails to monitor a client computer on your network.	<p>Several causes are possible:</p> <ul style="list-style-type: none">• The IP address is from a system not running Microsoft Windows* OS, such as a printer or router. You can only monitor systems with Microsoft Windows OS.• The client computer must be configured to support remote queries. For more details, see the Getting Started Guide.• Intel IT Director can monitor up to 25 client computers. Make sure you have 25 or fewer computers on your network.• For security reasons, the system times must be within 5 minutes of each other. Verify that the system time on the client computer is synchronized with the system time on the monitor computer.• A firewall on the client computer may be blocking remote queries. Configure the firewall to allow remote queries. Here are instructions for 3 firewalls:<ul style="list-style-type: none">• Norton 360*• McAfee Total Protection*• Trend Micro Internet Security*
You already set the USB devices to block on a client computer, but those devices are not blocked.	<p>USB blocking may be disabled on the client computer. To enable USB blocking:</p> <ol style="list-style-type: none">1. From Intel IT Director on the client computer, go to My Computer > USB Blocking.2. If checked, uncheck the box

	<p>Disable USB Blocking.</p> <p>3. Press Apply.</p>
<p>You cannot access the My Computer tab.</p>	<p>Multiple causes are possible:</p> <ul style="list-style-type: none"> • The My Computer tab may be disabled. For more information, see Disabling My Computer Settings. • You may not have permission to access the My Computer tab. For more information, see Setting User Privileges.
<p>You cannot access the My Network tab.</p>	<p>You may not have permission to access the My Network tab. For more information, see Setting User Privileges.</p>
<p>A new USB device is blocked, even though it is of an unblocked device type.</p>	<p>If USB Blocking is enabled and you connect a device whose type Intel IT Director cannot detect, the device is automatically blocked. To unblock the device:</p> <ol style="list-style-type: none"> 1. Disable USB Blocking 2. Install the drivers for the device 3. Verify that the type of device you want to use is not blocked. <p>You can now enable USB Blocking, while still using your USB device.</p>
<p>Intel IT Director does not work correctly in a network that uses Microsoft Windows* Small Business Server (SBS).</p>	<p>Intel IT Director adds ports to the Windows Firewall local programs exceptions list. If you have Microsoft Windows* Small Business Server (SBS) 2003 or 2008, your domain group policy may disable the ports added by Intel IT Director. See Configuring Microsoft Windows* Small Business Server.</p>
<p>On a system using Windows SBS 2003, entering the wrong username or password prevents Intel IT Director from monitoring other computers on the</p>	<p>In the default Windows SBS 2003 setting, users are locked out for 10 minutes after entering an incorrect username or password. Configure</p>

<p>network.</p>	<p>Windows SBS 2003 as follows:</p> <ol style="list-style-type: none"> 1. Go to Start > Run... and type <code>mmc</code> to open the Microsoft* Management Console. 2. On the File menu, click Add/Remove Snap-in. 3. Click Add. 4. In the Available Snap-ins list, click Group Policy Object Editor and then click Add. 5. In the Select Group Policy Object dialog box, click Browse and find the relevant policy to edit: <ul style="list-style-type: none"> • For Windows XP* OS: Small Business Server Lockout policy • For Windows Vista* OS: Small Business Server – Windows Vista Policy 6. Click Finish, click Close, and then click OK. Group Policy Object Editor opens the Group Policy object for you to edit. 7. Go to Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy > Account lockout threshold 8. Define the policy as 0 invalid logon attempts. You will no longer be locked out after entering an incorrect username or password.
<p>The first time you try launching Intel IT Director, launch is delayed.</p>	<p>Verify that your computer has a working internet connection.</p>
<p>Intel IT Director is unable to monitor a</p>	<p>Possible causes:</p>

<p>client computer on which Intel IT Director is not installed.</p>	<ul style="list-style-type: none"> • The client computer has not been configured. For configuration instructions, see the Getting Started Guide. • Even after you configure the client computer, Remote Windows Management Instrumentation* (WMI) may be still blocked. Reboot the client computer.
<p>A computer with Intel IT Director does not monitor itself.</p>	<p>The Intel IT Director service may not have started properly. Restart the service, as follows:</p> <ul style="list-style-type: none"> • Go to Start > Control Panel > Administrative Tools > Services. • From the list of services, select Intel(R) IT Director. • Click Restart the Service.

Configuring Norton 360*

Configuring Norton 360* version 2.0 on a client computer enables Intel IT Director to remotely monitor that computer.

You need to complete three general steps:

- For computers with Intel® Core™2 Processor with vPro™ Technology, with the Intel® Q45 Express Chipset: [Make sure itdirector.exe and itdirectorsservice.exe are in the Program Rules list.](#)
- One of the following two steps:
 - For computers with Intel® Core™2 Processor with vPro™ Technology, with the Intel® Q45 Express Chipset: [Enable ISBNHUPort \(TCP: 17000\)](#)
 - For all other computers: [Enable Remote Procedure Calls \(RPC\) port \(TCP: 135\)](#)
- For all computers: [Enable ICMP incoming echo requests through the firewall](#)

To Make sure itdirector.exe and [itdirectorsservice.exe](#) are in the Program Rules list:

1. To open Norton 360, double-click the **Norton 360** icon on your desktop.

2. Mouse over **PC Security**. From the **PC Security** menu, choose **Manage Firewall**. The **Firewall Protection Settings** page opens.
3. Click the **General Settings** tab. Under **General Settings**, check **Turn on Firewall**.
4. Click the **Program Rules** tab. Under **Program Rules**, check whether the files `itdirector.exe` and `itdirectorservice.exe` are listed.
5. If `itdirector.exe` and `itdirectorservice.exe` are not listed, click **Add...**
6. Navigate to the location of the files `itdirector.exe` and `itdirectorservice.exe`. By default, they install to `C:\Program Files\Intel\IntelITDirector`. Select one file and click **Open**.
7. In the **Program Control** dialog, select **Allow** from the drop down list and press **OK**.
8. Repeat steps 5-7 for the second file.

To enable ISBNHUPort (TCP:17000):

1. To open Norton 360, double-click the **Norton 360** icon on your desktop.
2. Mouse over **PC Security**. From the **PC Security** menu, choose **Manage Firewall**. The **Firewall Protection Settings** page opens.
3. Click **Traffic Rules** tab. Click **Add** to add a rule.
4. When asked **Do you want to block, allow, or monitor a new connection?**, select **Allow** and click **Next**.
5. Select **Connections to and from other computers** and click **Next**.
6. Select **Any computer** and click **Next**.
7. For **The protocol you want to allow**, select **TCP**.
8. Select **Only communications that match all types and ports listed below**, and click **Add** to add a port. Set as follows:
 - Under **Filter by:**, select **Individually specified ports**.
 - Under **Locality:**, select **Local**.
 - For the port number, enter **17000**.
9. Click **OK** to return to the **Add Rule** page. Click **Next**.
10. On the page with options for **When a connection matches a rule**, click **Next** without changing the settings.
11. Set the name as `ISBNHUPort(17000)` and click **Finish**.
The port is now enabled.

12. The new rule **ISBNHUPort(17000)** is added at the bottom of the **Firewall Traffic Rules** list. select this rule and click **Move up** to move it to the top of the **Firewall Traffic Rules** list.
13. For Intel IT Director to monitor the computer, restart the computer.

To enable Remote Procedure Calls (RPC) port (TCP:135):

1. To open Norton 360, double-click the **Norton 360** icon on your desktop.
2. Mouse over **PC Security**. From the **PC Security** menu, choose **Manage Firewall**. The **Firewall Protection Settings** page opens.
3. Click **Traffic Rules** tab. Click **Add** to add a rule.
4. When asked **Do you want to block, allow, or monitor a new connection?**, select **Allow** and click **Next**.
5. Select **Connections to and from other computers** and click **Next**.
6. Select **Any computer** and click **Next**.
7. For **The protocol you want to allow**, select **TCP**.
8. Select **Only communications that match all types and ports listed below**, and click **Add** to add a port. Set as follows:
 - Under **Filter by:**, select **Individually specified ports**.
 - Under **Locality:**, select **Local**.
 - For the port number, enter **135**.
9. Click **OK** to return to the **Add Rule** page. Click **Next**.
10. On the page with options for **When a connection matches a rule**, click **Next** without changing the settings.
11. Set the name as `Remote Procedure Calls (RPC) Port(135)` and click **Finish**.
The port is now enabled.
12. The new rule `Remote Procedure Calls (RPC) Port(135)` is added at the bottom of the **Firewall Traffic Rules** list. Select this rule and click **Move up** to move it to the top of the **Firewall Traffic Rules** list.
13. For Intel IT Director to monitor the computer, restart the computer.

To enable ICMP echo requests coming in through the firewall:

1. To open Norton 360, double-click the **Norton 360** icon on your desktop.

2. Mouse over **PC Security**. From the **PC Security** menu, choose **Manage Firewall**. The **Firewall Protection Settings** page opens.
3. Click **Traffic Rules** tab. Click **Add** to add a rule.
4. When asked **Do you want to block, allow, or monitor a new connection?**, select **Allow** and click **Next**.
5. Select **Connections from other computers** and click **Next**.
6. Select **Any computer** and click **Next**.
7. For **The protocol you want to allow**, select **ICMP**.
8. Under **Filter by:**, select **Known commands from list**. Select command **8**, named **echo-req**.
9. Click **OK** to return to the **Add Rule** page. Click **Next**.
10. On the page with options for **When a connection matches a rule**, click **Next** without changing the settings.
11. Set the name as `HVICMP-Incoming(echo request)` and click **Finish**.
The port is now enabled.
12. The new rule **HVICMP-Incoming(echo request)** is added at the bottom of the **Firewall Traffic Rules** list. select this rule and click **Move up** to move it to the top of the **Firewall Traffic Rules** list.
13. For Intel IT Director to monitor the computer, restart the computer.

Configuring McAfee Total Protection*

Configuring McAfee Total Protection* version 4.7 on a client computer enables Intel IT Director to remotely monitor that computer.

You need to complete one of two steps:

- For computers with Intel® Core™2 Processor with vPro™ Technology, with the Intel® Q45 Express Chipset: [Enable ISBNHUPort\(TCP:17000\)](#)
- For all other computers: [Enable Remote Procedure Calls \(RPC\) port 135](#)

To enable ISBNHUPort(TCP:17000):

1. Right click the McAfee Total Protection icon to open the menu.
2. Click **Settings**.
The **Firewall Settings** page opens.
3. Set the **Firewall Settings** page as follows:
 - a. Under **Select the status of your firewall service**, select **On**.
 - b. Under **Select the firewall's connection type**, select **Custom Settings** and click **Edit**.
The **Firewall Custom Settings** page opens.

4. Under the list of connections, click **Add**.
5. Set the **Incoming Connection** as follows:
 1. For the name, enter **ISBNHUPort**.
 2. For **Port(s)**, enter **17000 to 17000**.
 3. For **Protocol**, select **TCP**.
 4. Click **OK**.
6. Check **Specific address range**, and enter the range of IP addresses used by all computers on the network.
7. Click **OK**.

To enable Remote Procedure Calls (RPC) port 135:

1. Right click the McAfee Total Protection icon to open the menu.
2. Click **Settings**.
The **Firewall Settings** page opens.
3. Set the **Firewall Settings** page as follows:
 - a. Under **Select the status of your firewall service**, select **On**.
 - b. Under **Select the firewall's connection type**, select **Custom Settings** and click **Edit**.
The **Firewall Custom Settings** page opens.
4. Set the **Firewall Custom Settings** page as follows:
 1. Under **Allow**, select **Remote Procedure Calls (RPC) port 135**.
 2. Check **Specific address range**, and enter the range of IP addresses used by all computers on the network.
 3. Click **OK**.

Configuring Trend Micro Internet Security*

Configuring Trend Micro Internet Security* on a client computer enables Intel IT Director to remotely monitor that computer.

For computers with Intel® Core™2 Processor with vPro™ Technology, with the Intel® Q45 Express Chipset:

- [Set the firewall](#)
- [Add itdirector.exe and itdirectorservice.exe to the Program Control list.](#)
- [Add an ICMP incoming rule](#)
- [Add an ICMP outgoing rule](#)

- [Add an ISBNHUPort rule.](#)

For all other computers:

- [Set the firewall](#)
- [Add an ICMP incoming rule](#)

To set the firewall:

1. Double-click the Trend Micro Internet Security icon to open the application configuration window.
2. Click **Home Network & Firewall Controls > Personal Firewalls**. Set **Personal Firewalls** to **ON**.
3. Under **Personal Firewalls**, click **Settings**.
4. Set the **Personal Firewall Settings** as follows:
 1. Check **Activate the Personal Firewall**.
 2. Set the **Current Firewall Profile** to **Office Network**.
 3. Under **Security Level of Firewall Profile**, select **Medium**.

To add `itdirector.exe` and `itdirectorservice.exe` to the Program Control list:

1. Double-click the Trend Micro Internet Security icon to open the application configuration window.
2. Click **Home Network & Firewall Controls > Personal Firewalls**.
3. Under **Personal Firewalls**, click **Settings**.
4. Under **Security Level of Firewall Profile**, click **Advanced Settings**.
5. Click **Program Control**. If `itdirector.exe` is not listed, click **Add**.
6. Set the **Personal Firewall Profiles** page as follows:
 - Enter the Description as `IntelITDirector`.
 - For **Target**, select **Select a Program**. Browse to the file `itdirector.exe`. By default, it installs to: `C:\Program Files\Intel\IntelITDirector`.
 - For **Settings**, select **Simple**.
 - For **Firewall Response**, select **Allow**.
7. Repeat steps 5 and 6 for the file `itdirectorservice.exe`

To add an ICMP outgoing rule:

1. Double-click the Trend Micro Internet Security icon to open the application configuration window.
2. Click **Home Network & Firewall Controls > Personal Firewalls**.
3. Under **Personal Firewalls**, click **Settings**.
4. Under **Security Level of Firewall Profile**, click **Advanced Settings**.
5. Click **Network Protocol Control**. Click **Add**.
6. Set the **Personal Firewall Profiles** page as follows:
 - Enter the **Description** as **ICMP-Outgoing**.
 - Set the **Connection** as **Outgoing**.
 - For **Response**, select **Allow**.
 - For **Protocol**, select **ICMP (IPv4)**.
 - For **Type number**, select **All Types**.
 - For **Types**, set **IP address range (IPv4)**.
 - In the **From** and **To** fields, enter a range of IP addresses that covers all computers in the network.
7. Click **OK**.

To add an ISBNHUPort rule:

1. Double-click the Trend Micro Internet Security icon to open the application configuration window.
2. Click **Home Network & Firewall Controls > Personal Firewalls**.
3. Under **Personal Firewalls**, click **Settings**.
4. Under **Security Level of Firewall Profile**, click **Advanced Settings**.
5. Click **Network Protocol Control**. Click **Add**.
6. Set the **Personal Firewall Profiles** page as follows:
 - Enter the **Description** as **ISBNHUPort-Incoming**.
 - Set the **Connection** as **Incoming**.
 - For **Response**, select **Allow**.
 - For **Protocol**, select **TCP**.
 - For **Port**, select **Specific port(s)** and enter **17000**.
 - For **Types**, set **IP address range (IPv4)**.
 - In the **From** and **To** fields, enter a range of IP addresses that covers all computers in the network.
7. Click **OK**.

To add an ICMP incoming rule:

1. Double-click the Trend Micro Internet Security icon to open the application configuration window.
2. Click **Home Network & Firewall Controls > Personal Firewalls**.
3. Under **Personal Firewalls**, click **Settings**.
4. Under **Security Level of Firewall Profile**, click **Advanced Settings**.
5. Click **Network Protocol Control**. Click **Add**.
6. Set the **Personal Firewall Profiles** page as follows:
 - Enter the **Description** as **ICMP-Incoming**.
 - Set the **Connection** as **Incoming**.
 - For **Response**, select **Allow**.
 - For **Protocol**, select **ICMP (IPv4)**.
 - For **Type number**, select **All Types**.
 - For **Types**, set **IP address range (IPv4)**.
 - In the **From** and **To** fields, enter a range of IP addresses that covers all computers in the network.
7. Click **OK**.

Configuring Microsoft Windows* Small Business Server

For Intel IT Director to work correctly with Windows* Small Business Server (SBS), you must configure SBS on the client computer to enable local program exceptions in Windows* Firewall.

To configure SBS 2003 on a client computer with Windows XP* operating system, and SBS 2008 on both Windows XP and Windows Vista* operating systems:

1. Go to **Start > Administrative Tools > Server Management**.
2. On the left of the Server Management window, click the home page icon. Browse to **Advanced Management > Group Policy Management > Forest: *YourDomainName* > Domains > *YourDomainName* > Small Business Server Windows Firewall *YourServerName* Policy**
3. Click the Settings tab. Under **Administrative Templates**, go to **Network/Network Connections/Windows Firewall/Domain Profile**.
4. Right click on **Windows Firewall: Allow local program exception**, and click **Edit**.
5. In the **Group Policy Object Editor** window, browse to **Small Business Server Windows Firewall > Computer Configuration > Administrative**

- Templates > Network > Network Connections > Windows Firewall > Domain Profile.**
6. Under Domain Profile, double click **Windows Firewall: Allow local program exception**. In the dialog box, select **Enable**, click **Apply**, and click **OK**.
 7. Force the Group Policy settings to be applied, in one of two ways:
 - Restart the client computer.
 - From a command prompt with elevated privileges, run **gpupdate /force**.

To configure SBS 2003 on a client computer with Windows Vista* operating system:

1. Go to **Start > Administrative Tools > Server Management**.
2. On the left of the Server Management window, click the home page icon. Browse to **Advanced Management > Group Policy Management > Forest: *YourDomainName* > Domains > *YourDomainName* > Small Business Server - Windows Vista policy**
3. Right click **Small Business Server – Windows Vista policy** and click **Edit**.
4. In the **Group Policy Object Editor** window, go to **Small Business Server – Windows Vista policy *YourServerName* Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.
5. Under Domain Profile, double click **Windows Firewall: Allow remote administration exception**. In the dialog box, select **Enable**, click **Apply**, and click **OK**.
6. Force the Group Policy settings to be applied, in one of two ways:
 - Restart the client computer.
 - From a command prompt with elevated privileges, run **gpupdate /force**.

Index

A

Access 9

Asset monitor 14

C

Configuration 5

E

Export settings 22

G

Getting started 3

H

Hard drive backup and restore 22

Hard drive free space 19

I

Import settings 21

Internet security 18

M

Monitoring

Free hard drive space 19

Hard drive backup and restore 22

Hardware and software asset 14

Power 26

Security 18

N

Network security 18

P

Permissions 9

Power management 26

Power-on Monitor 26

Privileges 9

S

Security 18

Settings 7

Export 22

Import 21

Tab 7

Start up 3

Subnet 17

System details 15

U

USB device

Blocking activation 24

Types 25

User permissions 9

User privileges 9

V

Violation 15

W

Warning messages 15