



# Intel<sup>®</sup> IT Director

## User's Guide

Document number: 320205-003US

Revision 1.5

[Legal Information](#)

## Quick Links

[Start Here](#)

[What's New](#)

[www.intel.com/go/ITDirector](http://www.intel.com/go/ITDirector)

# Table of Contents

Introduction .....	3
What's New .....	5
System Configuration .....	7
Security.....	9
Network Status.....	11
Settings.....	13
Settings Tab: Overview .....	13
Setting User Privileges .....	13
Manageability Capability .....	13
About the Manageability Capability .....	13
Manageability Capability System Prerequisites.....	14
Setting Up the Manageability Capability.....	14
Retrieving the Manageability Admin Password .....	15
My Computer Settings.....	15
Monitoring Your Network.....	17
Monitoring Your Network: Overview .....	17
Computers without Intel(R) IT Director .....	18
Hardware and Software Asset Monitor .....	18
System Details Page .....	19
Software Health Monitor .....	19
Violations and Warnings .....	20
Warning Messages .....	20
Configuring Your Network .....	22
Configuring Your Network: Overview.....	22
Configuring Subnets .....	22
Configuring Hard Drive Backup and Restore Requirements .....	23
Configuring Software Health Monitor – Basic Mode .....	23
Configuring Hard Drive Free Space Requirements .....	24
Configuring Your Computer .....	27
Configuring Your Computer: Overview .....	27
Importing Settings.....	27
Exporting Settings .....	28
Enabling Hard Drive Backup and Restore.....	28
Configuring the Software Health Monitor-Advanced Mode .....	29

Blocking USB Devices.....	30
Blocking USB Devices: Overview .....	30
Enabling and Disabling USB Device Blocking .....	31
USB Device Types .....	32
Configuring the Power-on Monitor .....	33
Troubleshooting .....	35
Troubleshooting .....	35
Troubleshooting: Manageability Capability.....	38
Retrieving the Manageability Admin Password.....	40
Configuring Norton Internet Security* .....	40
Configuring McAfee Security Center* .....	43
Configuring Kaspersky Internet Security* .....	44
Configuring Trend Micro Internet Security Pro* .....	45
Configuring Microsoft Windows* Small Business Server .....	47
Index .....	49

## 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](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) 2008-2009, Intel Corporation. All rights reserved.

## Introduction

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

### To set up Intel(R) IT Director:

1. On each computer, [set user privileges](#) on Intel(R) IT Director.
2. On each computer, [configure Intel\(R\) 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(R) 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(R) 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](#)

## What's New

Intel(R) IT Director 1.5 introduces support for manageability capability on computers with Intel(R) vPro(TM) Technology, Intel(R) Standard Manageability, and Level III Manageability Upgrade.

Intel(R) IT Director 1.5 uses the manageability capability for the Software Health Monitor-Advanced Mode, to remotely monitor whether important software is running. It also uses the manageability capability to monitor the hardware and software assets information for each computer.

Intel(R) IT Director 1.5 also introduces changes to the [Violations and Warnings](#) shown in the My Network tab.

## See Also

[About the Manageability Capability](#)

[Violations and Warnings](#)

[Monitoring Your Network: Overview](#)

## System Configuration

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

This tool automatically opens the first time you use Intel(R) IT Director.

### See Also

[Getting Started Guide](#)

## Security











Intel(R) IT Director uses manageability capability for the Advanced Software Health Monitor feature. Intel(R) IT Director sets up manageability in Basic Mode (formerly Small Business Mode), which does not encrypt communications. Because these communications are not encrypted, you can more easily use third-party applications in conjunction with the manageability capability. Intel(R) IT Director does encrypt communications for all features that do not use the manageability capability.

### See Also

[About the Manageability Capability](#)

## Network Status

You can monitor your network status through the Intel(R) IT Director icons that resides in the system tray of your computer.

Icon	Access to My Computer Tab	Access to My Network Tab	Notes
	No	Yes	Fully compliant
	No	Yes	Scanning the network
	No	Yes	There is violation in the network
	No	Yes	There is warning in the network
	No	No	Being monitored only
	Yes	Yes	Fully compliant
	Yes	Yes	Scanning the network
	Yes	Yes	There is violation in the network
	Yes	Yes	There is warning in the network
	Yes	No	Being monitored only

# Settings

## Settings Tab: Overview

The Settings tab includes the following sections:

- [User Privilege Settings](#)
- [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](#).

### See Also

[Setting User Privileges](#)

[My Computer Settings](#)

[My Network Settings](#)

[Importing Settings](#)

[Exporting Settings](#)

## Setting User Privileges

The user logged on when you first access Intel(R) IT Director has access to all features of Intel(R) IT Director.

When you first use Intel(R) IT Director, set which features other users with Windows\* Administrator privilege can access. Set access privileges from **Settings** > **User Privilege Settings**.

You have two options:

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

### See Also

[Introduction](#)

[Settings tab](#)

## Manageability Capability

### About the Manageability Capability

The manageability capability enables you to remotely monitor whether software is properly running on computers. Intel(R) IT Director uses the manageability capability for the Advanced [Software Health Monitor](#) feature.

Intel(R) IT Director includes a tool for setting up manageability on your computer.

The manageability capability is supported on computers with Intel(R) vPro(TM) technology, Intel(R) Standard Manageability, and Level III Manageability Upgrade.

You can find more information from: <http://www.intel.com/technology/platform-technology/intel-amt/>

### See Also

## [Security](#)

### [Setting Up the Manageability Capability](#)

### [Troubleshooting: Manageability Capability](#)

### [Prerequisites for the Manageability Capability](#)

### [Software Health Monitor](#)

## **Manageability Capability System Prerequisites**

To set up the manageability capability, your system must be configured as follows:

- In the system BIOS, Intel(R) AMT must be enabled.
- In the Intel(R) Management Engine BIOS Extensions (Intel(R) MEBx), **Manageability** must be set to **Intel(R) AMT**.
- The manageability drivers for your chipset must be installed.
- The Local Management Service must be installed and running.
- The Intel(R) Management Engine Interface must be installed and enabled.

## **See Also**

### [Setting Up the Manageability Capability](#)

### [Troubleshooting: Manageability Capability](#)

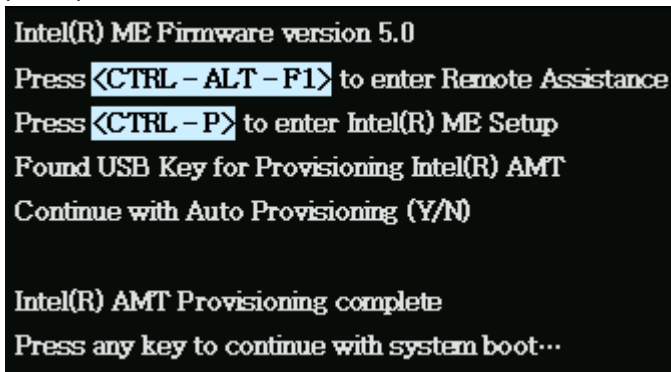
## **Setting Up the Manageability Capability**

Before setting up the manageability capability, verify that at least one other computer with Intel(R) IT Director is accessible on your network.

### **To set up the manageability capability:**

1. If your computer supports the manageability capability, Intel(R) IT Director asks you to open the manageability setup wizard the first time you open Intel(R) IT Director.
2. Select whether your manageability capability has been configured on this computer.
  - If yes, enter the manageability admin password from the previous setup.
  - If no or you do not know, follow the instructions on the screen.
3. Answer three password retrieval questions. To retrieve your password in the future, you will need to answer the questions as you do here. Click **Next**.
4. Select a connected USB drive on which to generate files needed for manageability setup, and click **Generate**. If your USB drive is not blank, all data on the drive will be erased.
5. Manageability setup requires a reboot. To continue, save and close all open files and click **Reboot now**. Leave the USB drive connected to the system, for use later in the process.

6. During reboot, the following screen will ask if you want to **Continue with Auto Provisioning**. At that screen, press **Y** and press any key when prompted.



7. If there was a problem with the files on the USB drive, you will see an error screen. Follow the instructions in the error screen.
8. After the system reboots, manageability setup continues. If you cancel manageability setup, you return to this page the next time you open the Manageability Setup Wizard.
9. Once manageability setup succeeds, click **Finish**.

## See Also

[Troubleshooting: Manageability Capability](#)

[Retrieving the Manageability Admin Password](#)

### Retrieving the Manageability Admin Password

To retrieve your manageability admin password:

1. In Intel(R) IT Director, go to **Settings > My Computer Settings**. Click **Retrieve Password**.
2. Answer the password retrieval questions as you answered them when you first set up the manageability capability.
3. If the answers are correct, a dialog box shows you the password. If your answers are not correct, a dialog box enables you to choose whether to try again or quit.

If you do not know your password and cannot answer the questions correctly, you cannot retrieve your manageability admin password. To reset the password, you must clear the CMOS settings. For more information, see the documentation for your motherboard.

## See Also

[About the Manageability Capability](#)

[Troubleshooting: Manageability Capability](#)

### My Computer Settings

From **Settings > My Computer Settings**, you can:

- Disable your changes to the My Computer tab, and prevent access to that tab.
- [Setting up the manageability capability.](#)
- Retrieve your manageability admin password.

**See Also**

[Settings tab](#)


[Configuring Your Computer: Overview](#)

## Monitoring Your Network

### Monitoring Your Network: Overview

Intel(R) 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** tab.





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

- The top row includes computers to which Intel(R) IT Director has finished trying to connect. If Intel(R) 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(R) IT Director is trying to connect. Once Intel(R) IT Director connects to those computers, they move to the first row.

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

- USB Blocking
- Hard Drive Backup and Restore
- Software Health Monitor
- Power-on Monitor
- Hard Drive Free Space

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

-  denotes Intel(R) IT Director has recorded [violations](#) for the feature.
-  denotes all computers comply with the requirements for the feature.
-  denotes Intel(R) IT Director has [warning](#) in the network, e.g. the feature is present, but has not been configured, has prevented prohibited usage, or has been changed or disabled.
-  denotes Intel(R) 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** tab.

### 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](#) tab on Intel(R) 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 Software Health Monitor - Basic Mode](#)

[Configuring the Power-on Monitor](#)

## Computers without Intel(R) IT Director

For Intel(R) 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(R) IT Director installed, you can monitor:

- [Software health monitor - basic mode](#)
- [Free hard drive space](#)
- [Hardware and software assets](#)

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

**See Also**

[Monitoring Your Network: Overview](#)

[Getting Started Guide](#)

## Hardware and Software Asset Monitor

Intel(R) 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** tab.
- From **System Details > Hardware and Software Assets**.

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

- ITD ID
- Computer System (manufacturer and model number)
- Processor
- Operating system
- For computers with manageability capability:
  - Manageability (manageability type)
  - Memory

- Hard drive
- Battery

**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(R) 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](#)
- [Software Health Monitor](#)
- [Power-on Monitor](#)
- [Hard Drive Free Space](#)
- [Hardware and Software Asset](#)

**See Also**

[Monitoring Your Network: Overview](#)

[Configuring Your Network: Overview](#)

[Violations and Warnings](#)

## Software Health Monitor

Intel(R) IT Director monitors whether the following important software is installed and running on network computers:

- Intel(R) IT Director Service
- Microsoft Windows Automatic Updates
- Firewall
- Anti-virus software
- Anti-spyware software

To see the status of this software, go to **My Network > Internet and Network Security > Software Health Monitor**, and click on a computer to see the **System Details** for that computer.

The System Details page includes two columns for each application. The left column shows the type of software, and the right column shows the status, which can be OK, [Warning, or Violation](#).





**See Also**

[Configuring Network Software Health Monitor - Basic Mode](#)

[Configuring the Software Health Monitor - Advanced Mode](#)[Violations and Warnings](#)

## Violations and Warnings

In [My Network](#), Intel(R) IT Director shows the status of each feature. Here are the status definitions:

Symbol	Definition
 Not Present	The feature is not present on the system.
 Warning	The feature is present, and has one of these warnings: <ul style="list-style-type: none"> <li>• The feature has not been configured.</li> <li>• The feature has prevented prohibited usage.</li> <li>• Configuration of the feature has been changed or disabled.</li> </ul>
 Violation	The feature is present, but a violation has occurred.
 Normal	The feature is working normally.

**See Also**

[Monitoring Your Network: Overview](#)


[System Details Page](#)

[Warning Messages](#)

## Warning Messages

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 stopped working. Warnings: <ul style="list-style-type: none"> <li>• A blocked USB device was connected.</li> <li>• USB Blocking has not been configured</li> <li>• Configuration of the feature</li> </ul>

	has been changed or disabled
Hard Drive Backup and Restore	<p>Violation: Intel(R) Matrix Storage Manager is not installed on a computer. This violation applies only if you choose to <a href="#">monitor hard drive backup and restore</a>.</p> <p> <b>Note</b></p> <p>Intel(R) 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 <a href="#">My Network</a> as not supporting backup and restore through Intel(R) Matrix Storage Manager. If the chipset is configured as AHCI mode, the RAID drivers cannot be installed.</p>
Software Health Monitor	<p>Violation: A required application is not installed, not enabled, or not running.</p> <p>Warning: Software has not been configured.</p>
Power-on Monitor	<p>Violation:</p> <ul style="list-style-type: none"> <li>• A computer was powered on for more than one hour outside of office hours in a given day.</li> <li>• The Power-on Monitor stopped working.</li> </ul> <p>Warning: The Power-on Monitor has not been configured</p>
Hard Drive Free Space	<p>Violation: Free space on a hard drive dropped below the <a href="#">required threshold</a>.</p> <p>If a hard drive has multiple partitions, Intel(R) IT Director treats the entire hard drive as if it were only one</p>

partition. The percentage of free space is calculated as the total free hard drive space divided by the total hard drive space.

Warning: The feature has not been configured.

### See Also

[System Details Page](#)

[Violations and Warnings](#)

## Configuring Your Network

### Configuring Your Network: Overview

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

**My Network Settings** enables you to:

- Set which [Subnets](#) to scan.
- Choose whether to monitor installation of Intel(R) Matrix Storage Manager.
- Choose the software to be monitored in the Software Health Monitor.
- Set the [Hard Drive Free Space Threshold](#).
- Remove [warning messages](#).
- Change your Intel(R) IT Director Remote Monitoring Account password.
- Re-enter your Intel(R) IT Director Remote Monitoring Account password.

### See Also

[Monitoring Your Network](#)

[Settings tab](#)

### Configuring Subnets

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

#### To instruct Intel(R) 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(R) 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(R) 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(R) Matrix Storage Manager, the chipset must support RAID, and the RAID drivers must be installed.

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

### To start or stop monitoring whether Intel(R) 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(R) Matrix Storage Manager is installed on network computers**.
3. Click **Apply**.

### Note

Intel(R) 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(R) 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(R) Matrix Storage Technology website:

[http://www.intel.com/design/chipsets/matrixstorage\\_sb.htm](http://www.intel.com/design/chipsets/matrixstorage_sb.htm)

### Configuring Software Health Monitor – Basic Mode

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

### To select required Software Health Monitor settings:

1. Go to **Settings > My Network Settings > Software Health Monitor - Basic Mode Settings**.

2. Under **Choose the application types to be monitored**, select any options from the following list:
  - Microsoft Windows Automatic Updates.
  - Firewall
  - Anti-Virus Software
  - Anti-Spyware Software
3. Press **Apply**.

 **Note**

If you set the network Software Health Monitor- Basic Mode from the Settings tab, those settings override the [Software Health Monitor-Advanced Mode](#) settings, which you set from the [My Computer](#) tab.

Use the [My Network](#) tab to view messages from the Software Health Monitor.

**See Also**

[Configuring Your Network: Overview](#)

[Monitoring Your Network: Overview](#)

[Violations and Warnings](#)

[Configuring the Software Health Monitor-Advanced Mode](#)

[About the Manageability Capability](#)

**Configuring Hard Drive Free Space Requirements**

Intel(R) 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(R) 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

## Configuring Your Computer: Overview

Configure protection and monitoring on a computer from the **My Computer** tab in Intel(R) IT Director on that computer.

### Tip

You can use **My Computer** to configure one computer, and then export the settings for use on other computers. For more information, see [Exporting Settings](#) and [Importing Settings](#).

The **My Computer** tab includes the following features:

- [USB Blocking](#)
- [Hard Drive Backup and Restore](#)
- [Software Health Monitor-Advanced Mode](#)
- [Power-on Monitor](#)

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

### See Also

[Monitoring Your Network: Overview](#)

[Configuring Your Network: Overview](#)

## Importing Settings

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

- Configurations in Settings tab:
  - [User Privileges](#)
  - [My Computer](#)
  - [Additional Subnets](#)
  - [Hard Drive Free Space Threshold](#)
  - [Software Health Monitor - Basic Mode settings](#)
- Configurations in My Computer tab:
  - [USB Blocking](#)
  - [Software Health Monitor- Advanced Mode](#)
  - [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(R) 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 tab:
  - [User Privileges](#)
  - [My Computer](#)
  - [Additional Subnets](#)
  - [Hard Drive Free Space Threshold](#)
  - [Software Health Monitor - Basic Mode settings](#)
- Configurations in My Computer tab:
  - [USB Blocking](#)
  - [Software Health Monitor- Advanced Mode](#)
  - [Power-on Monitor](#)

## 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(R) IT Director hard drive backup and restore feature uses the following applications:

- Intel(R) 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(R) Matrix Storage Manager is not available). Helps you back up data, which you can then store elsewhere.

The  icon denotes that Intel(R) Matrix Storage Manager is not installed on your computer.

The  icon denotes that Intel(R) 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(R) IT Director on the computer, go to **My Computer > Hard Drive Backup and Restore**.
2. Click the Launch box to launch either Intel(R) Matrix Storage Manager or Windows\* Backup or Restore Wizard.

#### Note

Intel(R) 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(R) Matrix Storage Technology website:

[http://www.intel.com/design/chipsets/matrixstorage\\_sb.htm](http://www.intel.com/design/chipsets/matrixstorage_sb.htm)

### Configuring the Software Health Monitor-Advanced Mode

You can only configure the Software Health Monitor on computers with Intel(R) Active Management Technology or Intel(R) Standard Manageability. The Software Health Monitor-Advanced Mode monitors whether important software is running properly.

### To set the Software Health Monitor for your local computer:

1. From the **My Computer** tab of Intel(R) IT Director, go to **Internet and Network Security**.
2. In the **Software Health Monitor - Advanced Mode** settings, you have two options:
  - **Monitor if Intel(R) IT Director service in Advanced Mode**
  - **Monitor if Intel(R) IT Director service and the following security software in Advanced Mode:** If you choose this option, you can then choose which specific software to monitor. Including:
    - Firewall
    - Anti-Virus software
    - Anti-spyware software

### **Note**

If you set the network [Software Health Monitor - Basic Mode](#) from the [Settings](#) tab, those requirements override the Software Health Monitor-Advanced Mode settings, which you set from the My Computer tab.

### **See Also**

[Configuring Software Health Monitor - Basic Mode](#)

[About the Manageability Capability](#)

[Setting up the Manageability Capability](#)

## Blocking USB Devices

### **Blocking USB Devices: Overview**

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



### **Note**

For Intel(R) 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 has stopped working. The  icon denotes that USB Blocking has not been configured.

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

1. From Intel(R) IT Director on the computer, go to **My Computer > USB Blocking**.
2. Choose to either **Allow all USB devices** or **Block the following USB devices on this computer**:
3. If you chose to block USB devices, check the box next to device types you want to block.
4. Click **Apply**.

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

#### See Also

[Enabling and Disabling USB Device Blocking](#)

[USB Device Types](#)

[Troubleshooting](#)

#### Enabling and Disabling USB Device Blocking

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

#### To disable USB device blocking on your computer:

1. From Intel(R) IT Director on the computer, go to **My Computer > Data and System Protection > USB Blocking**.
2. Check the box **Allow all USB devices**.
3. Press **Apply**.

#### To enable USB device blocking on your computer:

1. From Intel(R) IT Director on the computer, go to **My Computer > Data and System Protection > USB Blocking**.
2. Check the box **Block the following USB devices on this computer**.
3. Select the USB devices that you need to block:
  - You can check the box **All USB Device Type**, all USB devices will be blocked on this computer
  - You also can choose the USB devices to be blocked, including:
    - Entertainment USB Devices
    - Storage Devices

- o Office Devices
- o Other Devices

You can click the arrow icon beside each USB device type to extract the device list

4. Press **Apply**.

If USB blocking is disabled on a computer, Intel(R) 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	Biometric reader
Personal Healthcare	Heart rate monitor, blood pressure cuffs, exercise watch
Personal Data Assistant	Some handheld computers, smartphones

## See Also

[Blocking USB Devices: Overview](#)

[Enabling and Disabling 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(R) 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(R) 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 has stopped working. The  icon denotes that the Power-on Monitor has not been configured.

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

1. From Intel(R) IT Director on the computer, go to **My Computer > Power-on Monitor**.
2. Select **Monitor system power usage and notify me if the system is on outside of office hours** option.

3. Select the days and hours to count as office hours.
4. 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

### Troubleshooting

Problem	Causes and Possible Solutions
Intel(R) IT Director fails to monitor a client computer on your network.	<p>Several causes are possible:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• The client computer must be configured to support remote queries. For more details, see the <a href="#">Getting Started Guide</a>.</li><li>• Intel(R) IT Director can monitor up to 25 client computers. Make sure you have 25 or fewer computers on your network.</li><li>• 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.</li><li>• A firewall on the client computer may be blocking remote queries. Configure the firewall to allow remote queries. Here are instructions for the firewalls:<ul style="list-style-type: none"><li>• <a href="#">Norton Internet Security*</a></li><li>• <a href="#">McAfee Security Center*</a></li><li>• <a href="#">Kaspersky Internet Security*</a></li><li>• <a href="#">Trend Micro Internet Security Pro*</a></li></ul></li></ul>

<p>You already set the USB devices to block on a client computer, but those devices are not blocked.</p>	<p>USB blocking may be disabled on the client computer. To enable USB blocking:</p> <ol style="list-style-type: none"> <li>1. From Intel(R) IT Director on the client computer, go to <b>My Computer</b> &gt; <b>USB Blocking</b>.</li> <li>2. If checked, uncheck the box <b>Disable USB Blocking</b>.</li> <li>3. Press <b>Apply</b>.</li> </ol>
<p>You cannot access the <b>My Computer</b> tab.</p>	<p>Multiple causes are possible:</p> <ul style="list-style-type: none"> <li>• The <b>My Computer</b> tab may be disabled. For more information, see <a href="#">Disabling My Computer Settings</a>.</li> <li>• You may not have permission to access the <b>My Computer</b> tab. For more information, see <a href="#">Setting User Privileges</a>.</li> </ul>
<p>You cannot access the <b>My Network</b> tab.</p>	<p>You may not have permission to access the <b>My Network</b> tab. For more information, see <a href="#">Setting User Privileges</a>.</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 type that Intel(R) IT Director cannot detect, the device is automatically blocked. To unblock the device:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Disable USB Blocking</a></li> <li>2. Install the drivers for the device</li> <li>3. <a href="#">Verify that the type of device you want to use is not blocked</a>.</li> </ol> <p>You can now enable USB Blocking, while still using your USB device.</p>
<p>Intel(R) IT Director does not work correctly in a network that uses Microsoft Windows* Small Business Server (SBS).</p>	<p>Intel(R) 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</p>

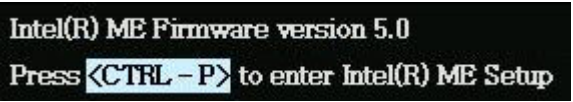
	<p>group policy may disable the ports added by Intel(R) IT Director. See <a href="#">Configuring Microsoft Windows* Small Business Server</a>.</p>
<p>On a system using Windows* SBS 2003, entering the wrong username or password prevents Intel(R) IT Director from monitoring other computers on the network.</p>	<p>In the default Windows* SBS 2003 setting, users are locked out for 10 minutes after entering an incorrect username or password. Configure Windows* SBS 2003 as follows:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Start &gt; Run...</b> and type <code>mmc</code> to open the Microsoft* Management Console.</li> <li>2. On the File menu, click <b>Add/Remove Snap-in</b>.</li> <li>3. Click <b>Add</b>.</li> <li>4. In the <b>Available Snap-ins</b> list, click <b>Group Policy Object Editor</b> and then click <b>Add</b>.</li> <li>5. In the <b>Select Group Policy Object</b> dialog box, click <b>Browse</b> and find the relevant policy to edit: <ul style="list-style-type: none"> <li>• For Windows XP* OS: <b>Small Business Server Lockout policy</b></li> <li>• For Windows Vista* OS: <b>Small Business Server Windows Vista Policy</b></li> </ul> </li> <li>6. Click <b>Finish</b>, click <b>Close</b>, and then click <b>OK</b>. Group Policy Object Editor opens the Group Policy object for you to edit.</li> <li>7. Go to <b>Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Account Policies &gt; Account Lockout Policy &gt; Account lockout threshold</b></li> <li>8. Define the policy as 0 invalid</li> </ol>

	<p>logon attempts. You will no longer be locked out after entering an incorrect user name or password.</p>
<p>The first time you try launching Intel(R) IT Director, launch is delayed.</p>	<p>Verify that your computer has a working internet connection.</p>
<p>Intel(R) IT Director is unable to monitor a client computer on which Intel(R) IT Director is not installed.</p>	<p>Possible causes:</p> <ul style="list-style-type: none"> <li>• The client computer has not been configured. For configuration instructions, see the <a href="#">Getting Started Guide</a>.</li> <li>• Even after you configure the client computer, Remote Windows Management Instrumentation* (WMI) may be still blocked. Reboot the client computer.</li> </ul>
<p>A computer with Intel(R) IT Director does not monitor itself.</p>	<p>The Intel(R) IT Director service may not have started properly. Restart the service, as follows:</p> <ul style="list-style-type: none"> <li>• Go to <b>Start &gt; Control Panel &gt; Administrative Tools &gt; Services</b>.</li> <li>• From the list of services, select <b>Intel(R) IT Director</b>.</li> <li>• Click <b>Restart the Service</b>.</li> </ul>

For more information, go to the Intel(R) IT Director Expert Center website: <http://communities.intel.com/docs/DOC-2675>

### Troubleshooting: Manageability Capability

<b>Problem</b>	<b>Causes and Possible Solutions</b>
<p>Manageability setup failed because Intel(R) IT Director did not detect another computer with Intel(R) IT Director on the network.</p>	<p>Verify that a computer with Intel(R) IT Director is connected. If it is, failure to find the other computer could have one of the following causes:</p> <ul style="list-style-type: none"> <li>• A firewall is blocking communication with the other computer.</li> <li>• The date or time on the two computers is not synchronized.</li> </ul>

	<ul style="list-style-type: none"> <li>• This computer did not have the correct user name or password to communicate with the other computer. The Intel(R) IT Director Remote Monitoring Account user name and password must be the same on all computers.</li> <li>• The Intel(R) IT Director service is not running on the other computer.</li> <li>• The other computer is running a previous version of Intel(R) IT Director.</li> </ul>
<p>There are not enough resources to create the Intel(R) vPro(TM)Technology watchdogs for Intel(R) IT Director.</p>	<p>Intel(R) vPr(TM) Technology or Intel Standard Manageability supports up to 16 watchdogs. Intel(R) IT Director will create 4 watchdogs to support the Software Health Monitor feature. If there are not enough resources to create the watchdogs, the feature is not supported.</p>
<p>The files for manageability setup cannot be generated on the USB drive.</p>	<p>Your USB drive may not be supported. For a list of supported and unsupported USB drives, see: <a href="http://communities.intel.com/docs/DOC-2675#USB_Provisioning">http://communities.intel.com/docs/DOC-2675#USB_Provisioning</a></p>
<p>Your computer supports manageability capability, but Intel(R) IT Director does not detect Intel(R) vPro(TM) technology or Intel(R) Standard Manageability.</p>	<p>Your system may not be configured correctly. For more, see <a href="#">Prerequisites for the Manageability Capability</a>.</p>
<p>You cannot find the manageability admin password.</p>	<p>See <a href="#">Retrieving the Manageability Admin Password</a>.</p>
<p>When you need to un-provision Intel(R) vPro(TM) technology or Intel(R) Standard Manageability</p>	<p>Un-provision Intel(R) vPro(TM) technology or Intel(R) Standard Manageability requires a reboot. Follow the steps:</p> <ol style="list-style-type: none"> <li>1. Save and close all open files and reboot the system.</li> <li>2. During reboot, screen will appear, press <b>CTRL-P</b> to enter Intel(R) MEBx screen.</li> </ol> 

3. Select **Intel(R) AMT (or Intel(R) Standard Manageability) Configuration > Un-provision > Full Unprovision**, press **Enter**.
4. System will automatically start un-provisioning process. Once finished, exit Intel(R) MEBx to reboot your system to OS.

## Retrieving the Manageability Admin Password

To retrieve your manageability admin password:

1. In Intel(R) IT Director, go to **Settings > My Computer Settings**. Click **Retrieve Password**.
2. Answer the password retrieval questions as you answered them when you first set up the manageability capability.
3. If the answers are correct, a dialog box shows you the password. If your answers are not correct, a dialog box enables you to choose whether to try again or quit.

If you do not know your password and cannot answer the questions correctly, you cannot retrieve your manageability admin password. To reset the password, you must clear the CMOS settings. For more information, see the documentation for your motherboard.

### See Also

[About the Manageability Capability](#)

[Troubleshooting: Manageability Capability](#)

## Configuring Norton Internet Security\*

Configuring Norton Internet Security\* on a client computer enables Intel(R) IT Director to remotely monitor that computer.

### To configure Norton Internet Security 2009\* to enable remote monitoring:

1. Open the Norton Internet Security application.
2. Under **Internet**, turn on **Smart Firewall**. Next to **Internet**, click **Settings**.

### For all computers with Intel(R) IT Director installed:

1. The Internet Settings page opens. At the bottom, go to **Smart Firewall > Program Control**, and click **Configure[+]**.

2. The **Program Control** page opens. Click **Add**. Select the file `itdirector.exe`.
3. When the dialog asks **What do you want to do?**, select **Allow**.
4. Repeat steps 4 and 5 for the `itdirectorconfig.exe`, `itdirectorservice.exe`, and `amtprovisiontool.exe` files.
5. From the bottom of the **Internet Settings** page, go to **Smart Firewall > Advanced Settings**, and click **Configure[+]**.
6. In the **Advanced Settings** page, go to **General Rules > Configure [+]**.
7. The **General Rules** page opens. At the bottom, click **Add**. Follow the **Add Rules** wizard:
  - For **Do you want to allow, block or monitor a connection**, select **Allow**, click **Next**
  - For **What type of connection do you want to allow**, select **Connection to and from other computers**, click **Next**
  - For **What computers or sites do you want to allow access to**, select **Any Computer**, click **Next**
8. For **The protocol you want to allow**, select **TCP**, click **Next**
9. 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**.
10. Click **OK** to return to the **Add Rule** page. Click **Next**. 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. In the **Add Rules** wizard, repeat Step 7 (a-c).
13. For **The protocol you want to allow**, select **TCP**, click **Next**
14. 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**.
15. Click **OK** to return to the **Add Rule** page. Click **Next**. On the page with options for **When a connection matches a rule**, click **Next** without changing the settings.
16. Set the name as `Remote Procedure Calls (RPC) Port(135)` and click **Finish**.

17. In the **Add Rules** wizard, repeat Step 9 (a-c).
18. For **The protocol you want to allow**, select **ICMP**.
19. Under **Filter by:**, select **Known commands from list**. Select command **8**, named **echo-req**.
20. Click **OK** to return to the **Add Rule** page. Click **Next**. On the page with options for **When a connection matches a rule**, click **Next** without changing the settings.
21. Set the name as `HVICMP-Incoming(echo request)` and click **Finish**.
22. The new rules are added at the bottom of the **General Rules** list. Select the rules and click **Move up** to move them to the top of the **General Rules** list.
23. For Intel(R) IT Director to monitor the computer, restart the computer.

**For all computers without Intel(R) IT Director installed:**

1. The Internet Settings page opens. At the bottom, go to **Smart Firewall > Advanced Settings**, and click on **Configure[+]**.
2. In the **Advanced Settings** page, go to **General Rules > Configure [+]**.
3. The **General Rules** page opens. At the bottom, click **Add**. Follow the **Add Rules** wizard:
  - For **Do you want to allow, block or monitor a connection**, select **Allow**, click **Next**
  - For **What type of connection do you want to allow**, select **Connection to and from other computers**, click **Next**
  - For **What computers or sites do you want to allow access to**, select **Any Computer**, click **Next**
11. For **The protocol you want to allow**, select **ICMP**.
12. For **What types of communication , or ports, do you want to allow**, select **Only communications that match all types and ports listed below**.
13. Click **Add**.
14. Under **Filter by:**, select **Known commands from list**. Select command **8**, named **echo-req**.
11. Click **OK** to return to the **Add Rule** page. Click **Next**.
12. Set the name as `HVICMP-Incoming(echo request)` and click **Next**.
13. Check the newly added rule information, click **Finish**.
14. The new rules are added at the bottom of the **General Rules** list. Select the rules and click **Move up** to move them to the top of the **General Rules** list.
15. For Intel(R) IT Director to monitor the computer, restart the computer.

## Configuring McAfee Security Center\*

Configuring McAfee Security Center\* on a client computer enables Intel(R) IT Director to remotely monitor that computer.

### To configure McAfee Security Center 2009\* to enable remote monitoring:

1. Right click the McAfee Security Center icon to open the menu.
2. Click **Common Tasks > Home**.  
The **Home** page opens.
3. Click **Internet & Network > Configure**. The **Internet & Network Configuration** page opens.
4. Set the **Internet & Network Configuration** page as follows:
  - a. Under **Firewall protection is enabled**, select **On**.
    - b. Under **Firewall protection is enabled**, click **Advanced...** The **Firewall Settings** page opens.

### For all computers with Intel(R) IT Director installed:

1. Click **Program Permissions**. The **Program Permissions** page opens.
2. For systems with Intel(R) IT Director only: Click **Add Allowed Program** and add the files `itdirector.exe`, `itdirectorconfig.exe`, `itdirectorservice.exe`, and `amtprovisiontool.exe` to the **Program Permissions** list.
3. Click **OK**.
4. Click **System Services**. The **System Services** page opens.
5. Click **Add**, to add a system service port. Set the System Service Port as follows:
  - a. For the name, enter **ISBNHUPort(TCP:17000)**.
    - b. For **Local TCP/IP Port(s)**, enter **17000**.
    - c. For **Open port to a computer or network that is**, select **Trusted, Standard, and Public**
    - d. For Description, enter **Intel(R) IT Director used TCP port**.
    - e. Click **OK**.
6. Click **OK**.

### For all computers without Intel(R) IT Director installed:

1. Click **System Services**. The **System Services** page opens.
2. Click **Add**, to add a system service port.

3. From the **System Services** list, select **Remote Procedure Calls (RPC) port 135**.
4. Click **OK**.

## Configuring Kaspersky Internet Security\*

### To configure Kaspersky Internet Security 2009\* for use with Intel(R) IT Director:

#### For all computers with Intel(R) IT Director installed:

1. Open the Kaspersky Internet Security application.
2. Under **Protection** on the left, click **System Security**.
3. From the box in the middle, click **Settings**.
4. The **Rules Settings** page opens. Click **Trusted**, and click **Add Group...** from the bottom of the screen. Enter **INTEL** as the group name.
5. After adding the group **INTEL**, you return to the **Rules Settings** page. Select **INTEL**, and click **Add...**
6. Navigate to `c:\Program Files\Intel\IntelITDirector`, select `itdirector.exe`, `itdirectorconfig.exe`, `itdirectorservice.exe`, and `amtprovisiontool.exe`, and click **Open**.
7. Click **OK**.

#### For all computers without Intel(R) IT Director installed:

1. Open the Kaspersky Internet Security application.
2. Under **Protection** on the left, click **System Security**.
3. From the box in the middle, click **Settings**.
4. The **Rules Settings** page opens. Click on the **Network Packets** tab.
5. **At the bottom of the Network Packets** tab, click **Add**.
6. Under **Action**, select **Allow**. Under **Network Service**, click **Add**. For the Network Service, enter:
  - Name: ITD\_DCOM\_135
  - Direction: Inbound/Outbound
  - Protocol: TCP
  - Remote ports: (leave empty)
  - Local ports: 135
7. Click **OK**.

## Configuring Trend Micro Internet Security Pro\*

Configuring Trend Micro Internet Security Pro\* on a client computer enables Intel(R) IT Director to remotely monitor that computer.

### To configure Trend Micro Internet Security Pro 2009\* to enable remote monitoring:

1. Double-click the Trend Micro Internet Security Pro icon to open the application configuration window.
2. Click **My Computer > Personal Firewall Controls > Personal Firewalls**.
3. Under **Personal Firewall**, click **Settings**.
4. Set the **Personal Firewall Settings** as follows:
  1. Check **Activate the Personal Firewall**.
  2. Click **Change Profile**, select **Office Network**.
  3. Click **Activate selected profile**.
  4. Click **OK**.
  5. Under **Security Level of Firewall Profile**, select **Medium**.
  6. Click **OK**.
5. Under **Security Level of Firewall Profile**, click **Advanced Settings**.

### For all computers with Intel(R) IT Director installed:

1. Click **Program Control** tab. If `itdirector.exe` is not listed, click **Add**.
2. Set the **Personal Firewall Profiles** page as follows:
  - Enter the Description as `IntelITDirector`.
  - For **Target**, select **Select a Program**. Click **Browse** to select the file `itdirector.exe`. By default, it installs to: `C:\Program Files\Intel\IntelITDirector`.
  - For **Settings**, select **Simple**.
  - For **Firewall Response**, select **Allow**.
3. Repeat steps 3 and 4 for files `amtprovisiontool.exe`, `itdirectorconfig.exe` and `itdirectorservice.exe`.
4. As in step 5, 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.  
Click **OK**.
7. As in step 10, click **Network Protocol Control**. Click **Add**.
8. 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.  
Click **OK**.
9. As in step 10, click **Network Protocol Control**. Click **Add**.
10. 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.  
Click **OK**.

**For all computers without Intel(R) IT Director installed:**

1. Click **Network Protocol Control** tab. Click **Add**.
2. 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.  
Click **OK**.

## Configuring Microsoft Windows\* Small Business Server

For Intel(R) 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 ..... 13

Asset monitor ..... 18

### B

Block USB device ..... 30

### C

Configuration ..... 7

### E

Export settings ..... 28

### G

Getting started ..... 3

### H

Hard drive backup and restore ..... 28

Hard drive free space ..... 24

### I

Import settings ..... 27

Internet security ..... 23

### M

Monitoring ..... 17

    Free hard drive space ..... 24

    Hard drive backup and restore ..... 28

    Hardware and software asset ..... 18

    Power ..... 33

    Security ..... 23

    USB device blocking ..... 30

### N

Network security ..... 23

### P

Permissions ..... 13

Power management ..... 33

Power-on Monitor ..... 33

Privileges ..... 13

### S

Security ..... 23

Settings ..... 13

    Export ..... 28

    Import ..... 27

    Tab ..... 13

Start up ..... 3

Subnet ..... 22

System details ..... 19

### T

Troubleshooting ..... 35

### U

USB device ..... 30

    Blocking ..... 30

    Blocking activation ..... 31

    Types ..... 32

User permissions ..... 13

User privileges ..... 13

### V

Violation ..... 20

### W

Warning messages ..... 20