



1.6 TREND MICRO™ Endpoint Sensor

Update 5

Installation Guide

Next Generation Endpoint Security Against Targeted Attacks and
Advanced Threats

for Windows™



Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com/en-us/enterprise/trend-micro-endpoint-sensor.aspx>

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, and Trend Micro Endpoint Sensor are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2018. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM18552/181213

Release Date: December 2018

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Endpoint Sensor collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Preface	v
Documentation	vi
Audience	vii
Document Conventions	vii
Terminology	viii

Chapter 1: System Requirements

Server Installation Checklist	1-2
Server Requirements	1-2
Server Performance	1-5
Database Requirements	1-5
Agent Installation Checklist	1-6
Agent Requirements	1-7
Local Agent Installation Considerations	1-8
Network Considerations	1-9
Other Security Software	1-10
Integration with Deep Discovery Analyzer	1-11
Integration with Control Manager	1-11

Chapter 2: Trend Micro Endpoint Sensor Installation

Trend Micro Endpoint Sensor Server Installation	2-2
Database Server	2-11
Management Console	2-15
Server Identification	2-16
Server Communication	2-18
Certificate Import	2-19
Internal Proxy for Agent Connection to Server	2-20
About the Management Console Admin Account Password	2-22

Local Agent Installation	2-22
Local Agent Silent Installation	2-23
Trend Micro Endpoint Sensor Server Uninstallation	2-24
Local Agent Uninstallation	2-25
Local Agent Silent Uninstallation	2-25

Chapter 3: OfficeScan Integration

About Trend Micro OfficeScan Integration	3-2
About Plug-in Manager	3-2
Installing OfficeScan	3-3
Agent Installation Considerations When Using OfficeScan	3-4
Using the Trend Micro Endpoint Sensor Deployment Tool	3-4
Trend Micro Endpoint Sensor Deployment Tool Installation	3-5
Plug-in Program Management	3-6
Trend Micro Endpoint Sensor Deployment Tool Uninstallation ...	3-6
Deployment Tool Error Codes	3-7
Trend Micro Endpoint Sensor Agent Deployment Tasks	3-11
Downloading the Installation Package	3-11
Installing the Trend Micro Endpoint Sensor Agent	3-13
Monitoring Trend Micro Endpoint Sensor Agents	3-14
The OfficeScan Agent Tree	3-14
The OfficeScan Agent Tree	3-14
Agent Tree Specific Tasks	3-14

Chapter 4: Technical Support

Troubleshooting Resources	4-2
Using the Support Portal	4-2
Threat Encyclopedia	4-2
Contacting Trend Micro	4-3
Speeding Up the Support Call	4-4
Sending Suspicious Content to Trend Micro	4-4
Email Reputation Services	4-4

File Reputation Services 4-5

Web Reputation Services 4-5

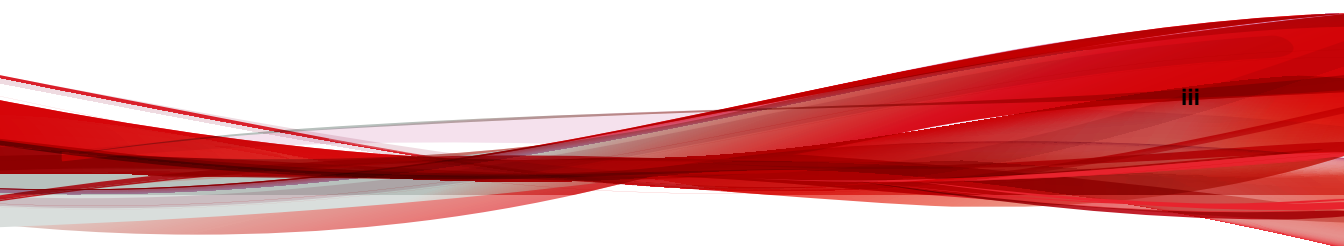
Other Resources 4-5

 Download Center 4-5

 Documentation Feedback 4-6

Index

Index IN-1



Preface

Preface

Welcome to the Trend Micro™ *Endpoint Sensor™ Installation Guide*. This document provides details related to the server and agent installation.



Note

Refer to the *Endpoint Sensor Administrator's Guide* or *Online Help* for product overview and configuration.

Topics include:

- *Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*
- *Terminology on page viii*

Documentation

The documentation set for Endpoint Sensor includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Endpoint Sensor , and explanations of Endpoint Sensor concepts and features.
Installation Guide	The Installation Guide discusses requirements and procedures for installing the Endpoint Sensor server and agent.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	The Online Help contains explanations of Endpoint Sensor components and features, as well as procedures needed to configure Endpoint Sensor .
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

<http://docs.trendmicro.com/en-us/home>

Evaluate this documentation at the following website:

<http://docs.trendmicro.com/en-us/survey.aspx>

Audience

The Endpoint Sensor documentation is written for network administrators, systems engineers, and information security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, which includes the following topics:

- Network topologies
- Server management
- Database management
- Incident response procedures
- Content security protection

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface

CONVENTION	DESCRIPTION
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Endpoint Sensor documentation:

TABLE 3. Endpoint Sensor Terminology

TERMINOLOGY	DESCRIPTION
Server	The Endpoint Sensor server
Agent endpoint	The host where the Endpoint Sensor agent is installed
Administrator (or Endpoint Sensor administrator)	The person managing the Endpoint Sensor server
Management console	The user interface for configuring and managing Endpoint Sensor server settings
Activation Code	Codes that enable all Endpoint Sensor features for a specified period of time.

TERMINOLOGY	DESCRIPTION
Agent installation folder	The folder on the host that contains the Endpoint Sensor agent files. If you accept the default settings during installation, you will find the agent installation folder at the following location: C:\Program Files\Trend Micro\ESE
Server installation folder	The folder on the host that contains the Endpoint Sensor server files. If you accept the default settings during installation, you will find the server installation folder at the following location: C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor

Chapter 1

System Requirements

This section provides an overview of the Endpoint Sensor server and agent installation, including key considerations.

Topics include:

- *Server Installation Checklist on page 1-2*
- *Agent Installation Checklist on page 1-6*
- *Other Security Software on page 1-10*

Server Installation Checklist

To ensure a successful installation of the Endpoint Sensor server, perform the following:

- Obtain the following from Trend Micro:
 - Endpoint Sensor server installer package
 - Full or trial version Activation Code

For details about the available Endpoint Sensor versions, refer to the Online Help or Administrator's Guide.

- Verify that all required hardware and software specifications have been met before installation.

For details, see [Server Requirements on page 1-2](#).

- Verify that a working IPv4 address has been assigned to the server.

Server Requirements

TABLE 1-1. Required Hardware and Software Components for Server Installation

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATIONS
CPU	At least 2GHz Intel Core2 Duo or compatible • AMD 64 processor • Intel 64 processor
RAM	• 4GB minimum • 16GB recommended
Available disk space	• 500GB minimum • 1TB recommended

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATIONS
Hardware	• Gigabit Network Interface Card (NIC) • Monitor that supports 1024 x 768 resolution at 256 colors or higher
Operating system	• Windows Server 2008 R2 • Windows Server 2012 R2 • Windows Server 2016 Build 14393
Database	• Microsoft SQL Server 2008 R2 Express • Microsoft SQL Server 2008 R2 (Standard or Enterprise Edition recommended) • Microsoft SQL Server 2012 Express • Microsoft SQL Server 2012 (Standard or Enterprise Edition recommended) • Microsoft SQL Server 2014 Express • Microsoft SQL Server 2014 (Standard or Enterprise Edition recommended) • Microsoft SQL Server 2016 Express • Microsoft SQL Server 2016 (Standard or Enterprise Edition recommended) Note Microsoft SQL Server may require the built-in .NET Framework 3.5.1 feature of IIS as a pre-requisite. Enable this feature before proceeding with the Endpoint Sensor installation. For details, see your IIS server documentation.

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATIONS
Web server	• Microsoft .NET Framework 4.5.1 • Microsoft Internet Information Services (IIS) 7.5, 8.5 or 10.0 with the following role services: • Static Content • Default Document • Directory Browsing • HTTP Errors • HTTP Redirection • ASP • CGI • ISAPI Extensions • ISAPI Filters • Request Filtering • IIS Management Console Additional role services for IIS 7.5: • .NET Extensibility • ASP.NET Additional role services for IIS 8.5: • .NET Extensibility 3.5 and 4.5 • ASP.NET 3.5 and 4.5 Additional role services for IIS 10.0: • .NET Extensibility 3.5 and 4.6 • ASP.NET 3.5 and 4.6

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATIONS
Web browser (for Endpoint Sensor management console access)	• Microsoft Internet Explorer 9 or later • The latest version of Google Chrome • The latest version of Mozilla Firefox

Server Performance

Enterprise networks require servers with higher specifications than those required for small and medium-sized businesses.

The number of agents that a single Endpoint Sensor server can manage depends on several factors, such as available server resources and network topology. Contact your Trend Micro representative for help in determining the optimal number of agents for your Endpoint Sensor server deployment.



Note

Trend Micro does not recommend installing Endpoint Sensor in a virtual machine. A Endpoint Sensor running in a virtual machine may not perform optimally. Additionally, if a virtual machine is reset to a previous state, this can lead to inconsistency of data between server and agent.

Database Requirements

Endpoint Sensor stores data in an SQL database. When you install Endpoint Sensor on a server that does not have access to a Microsoft SQL Server, Setup provides the option to install Microsoft SQL 2008 Express.

**Tip**

- Trend Micro highly recommends using Microsoft SQL Server Standard or Enterprise Edition. SQL Express is suitable for testing purposes but not for production environments. Due to the limitations of SQL Express, large networks require Microsoft SQL Server Standard or Enterprise Edition.

For details, see [Database Server on page 2-11](#).

- For enterprise environments, Trend Micro does not recommend installing the SQL server and the Endpoint Sensor server in the same physical machine.
-

Agent Installation Checklist

To ensure a successful installation of the Endpoint Sensor agent, perform the following:

- Use the ping command to check if the server can communicate with the agent.

If there is no ping response, verify that your firewall program allows network traffic between the server and agent. For details, check with your network administrator or refer to your firewall program documentation.

- Verify that the target endpoints have an IPv4 address.

Endpoints that are using IPv6 addresses must also have IPv4 addresses. Installing the Endpoint Sensor agent on a pure IPv6 endpoint is not supported.

- Verify that the Endpoint Sensor agent installer is available in the Endpoint Sensor server installation folder (the default location is `c:\Program Files\Trend Micro\Trend Micro Endpoint Sensor\Download\Agent\`).
- Verify that the agents meet the required hardware and software specifications. For details, see [Agent Requirements on page 1-7](#).
- Use IIS Manager to check if the ports are correctly set.
- Verify that additional requirements needed for a local installation of Endpoint Sensor agents have been met. Refer to the following guidelines:

For details, see [Local Agent Installation Considerations on page 1-8](#).

- If you intend to install the Endpoint Sensor agent on endpoints managed by OfficeScan, refer to *OfficeScan Integration on page 3-1*. In particular, see the guidelines found in *Agent Installation Considerations When Using OfficeScan on page 3-4*.

Agent Requirements

TABLE 1-2. Required Hardware and Software Components for Agent Installation

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATION
CPU	• 2GHz dual-core minimum for Windows 10 • 2GHz minimum for other operating systems
RAM	• 512MB minimum for Windows XP • 2GB minimum for Windows 10 • 1GB minimum for other operating systems
Available disk space	• 3GB minimum • 4GB recommended

REQUIRED HARDWARE/ SOFTWARE COMPONENT	SPECIFICATION
Operating system	• Windows XP Service Pack 3 (32-bit) • Windows Vista Service Pack 2 (32-bit and 64-bit) • Windows 7 Service Pack 1 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows Server 2008 Service Pack 2 (32-bit and 64-bit) • Windows Server 2008 R2 Service Pack 1 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit) • Windows Server 2016 (Long-Term Servicing Channel) • Windows 10 Redstone 2 and earlier (32-bit and 64-bit) • Windows 10 Fall Creators Update (Redstone 3) (32-bit and 64-bit) • Windows 10 April 2018 Update (Redstone 4) (32-bit and 64-bit) • Windows 10 October 2018 Update (Redstone 5) (32-bit and 64-bit)

Local Agent Installation Considerations

To ensure a successful local installation of the Endpoint Sensor agent, perform the following:

- The agent installer, `EndpointSensor.exe`, found at <Trend Micro Endpoint Sensor server installation path>\Download\Agent\, has been shared or copied to the target endpoint.
- Check that your firewall program allows Trend Micro Endpoint Sensor to communicate using the correct ports.

- Confirm that the endpoint has an IPv4 address.

Endpoints that are using IPv6 addresses must also have IPv4 addresses. Installing the Endpoint Sensor agent on a pure IPv6 endpoint is not supported.

**Note**

Trend Micro does not recommend installing Endpoint Sensor in a virtual machine. A Endpoint Sensor running in a virtual machine may not perform optimally. Additionally, if a virtual machine is reset to a previous state, this can lead to inconsistency of data between server and agent.

Network Considerations

Endpoint Sensor generates network traffic whenever communication occurs between server and agent, namely:

TABLE 1-3. Network Traffic

NETWORK TRAFFIC	DESCRIPTION
Heartbeat	Agent sends a periodic signal every 90 seconds to inform the server that the agent is online.
Reply investigation report	Agent investigates the endpoint and sends the report to the server.
Reply monitoring report	Agent finds a match during monitoring and sends a report to the server.
Endpoint status update	Agent sends an update to the server if endpoint settings have changed.
Download pattern	Agent receives pattern updates from an Endpoint Sensor server.
Deployment configuration	Server deploys configuration settings to agents.
Command polling	Agent checks the server to determine if a new command (for example, an investigation or a system update) has been requested.

To ensure optimal performance, network traffic should be an integral part in planning the Endpoint Sensor network.

Other Security Software

Endpoint Sensor is designed to be compatible with Trend Micro solutions with the exception of the following products:

TABLE 1-4. Software Incompatibilities

ENDPOINT SENSOR SOFTWARE	INCOMPATIBLE SOFTWARE
Server	• Trend Micro™ Safe Lock™ agent • Trend Micro™ Safe Lock™ Intelligent Manager
Agent	• Trend Micro™ Titanium™ • Trend Micro™ Internet Security • Deep Security 10.0 Update 2  Note Installation of a Trend Micro Endpoint Sensor agent and a Deep Security 10.0 Update 2 agent on one endpoint is supported only on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.



Important

Setup does not check for these incompatibilities, and will continue with the installation. The incompatible program may prevent Endpoint Sensor from functioning properly.

Integration with Deep Discovery Analyzer

Endpoint Sensor supports integration with Deep Discovery Analyzer™ 5.1 and later.

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration to augment or centralize the sandbox analysis of other Trend Micro products. The custom sandboxing environments created within Deep Discovery Analyzer precisely match target desktop software configurations, resulting in more accurate detections and fewer false positives.

For details, refer to the documentation available at:

<http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx>

Integration with Control Manager

Endpoint Sensor 1.6 Update 5 supports integration with Trend Micro™ Control Manager™. Control Manager manages Trend Micro products and services at the gateway, mail server, file server and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for products and services throughout the network. Use Control Manager to manage several Endpoint Sensor servers from a single location.

Endpoint Sensor supports the following Control Manager versions.

TABLE 1-5. Supported Control Manager versions

ENDPOINT SENSOR VERSION	CONTROL MANAGER VERSION
1.6 Update 5	• 6.0 SP3 Patch 3 • 7.0 Patch 1

For details, see the [Trend Micro Control Manager documentation](#).

Chapter 2

Trend Micro Endpoint Sensor Installation

This section provides details about the Endpoint Sensor server and agent installation procedures.



Note

For agent installation using OfficeScan, see [OfficeScan Integration on page 3-1](#).

Topics include:

- [Trend Micro Endpoint Sensor Server Installation on page 2-2](#)
- [Local Agent Installation on page 2-22](#)
- [Local Agent Silent Installation on page 2-23](#)
- [Trend Micro Endpoint Sensor Server Uninstallation on page 2-24](#)
- [Local Agent Uninstallation on page 2-25](#)
- [Local Agent Silent Uninstallation on page 2-25](#)

Trend Micro Endpoint Sensor Server Installation



Note

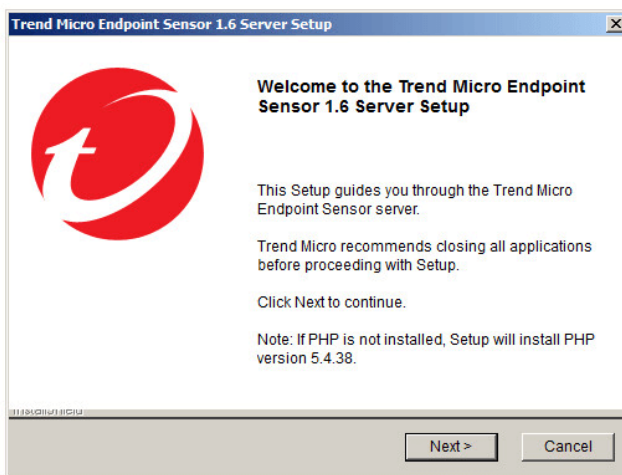
- Before installing the server, make sure you have performed all the steps necessary in *Server Installation Checklist on page 1-2*.
- Ensure that the installation is performed in a supported operating system. Setup does not check the operating system during installation, and will continue with the installation. Running in an unsupported operating system may prevent the Trend Micro Endpoint Sensor server from functioning properly.
- For existing installations running earlier versions of Endpoint Sensor , Trend Micro provides an upgrade tool that transfers the configuration of the existing server to a new Endpoint Sensor 1.6 server. For details, contact Trend Micro support.
- Enabling the FIPS compliant algorithm in Windows may prevent product activation from functioning properly. To prevent issues related to product activation, verify that the FIPS compliant algorithm is disabled in Windows before installing the Endpoint Sensor server.

For details, refer to the documentation available at:

<https://support.microsoft.com/en-us/help/811833/>

Procedure

1. Launch the Endpoint Sensor server Setup program (EndpointSensorSetup.exe).

**Note**

The server Setup program installs PHP version 5.4.38 and modifies the IIS handler to instruct all PHP related files or folder to use this version. The PHP version is installed at the following location:

C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor\PHP

2. The Setup program checks for existing components, and then displays the **License Agreement** screen.

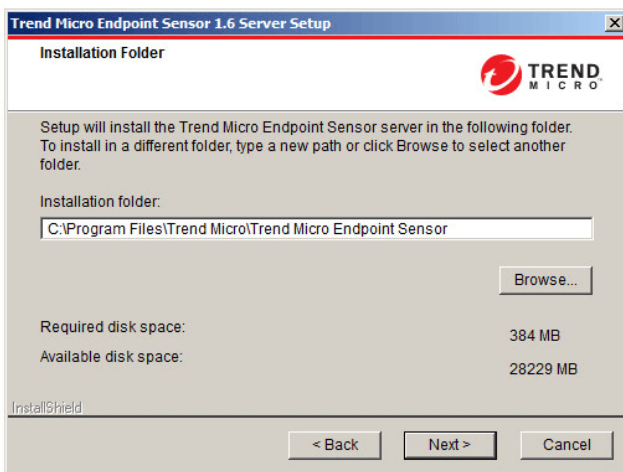


3. Specify the location where the Endpoint Sensor server program will be installed.

The default server installation path is:

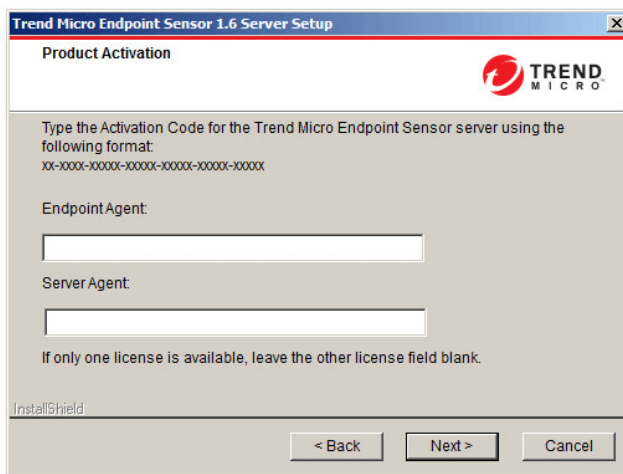
`C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor\`

Specify a new installation path or use the default path.



4. Type the full or trial Activation Code for Endpoint Sensor .

For details about the available Endpoint Sensor versions, refer to the Online Help or the Administrator's Guide.



Note

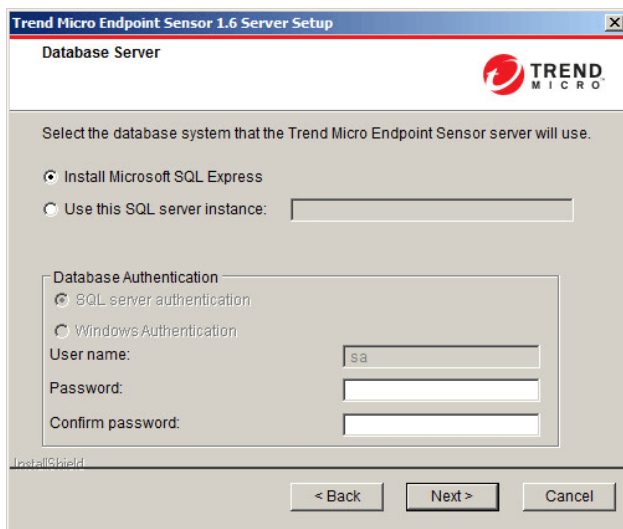
Enabling the FIPS compliant algorithm in Windows may prevent product activation from functioning properly. To prevent issues related to product activation, verify that the FIPS compliant algorithm is disabled in Windows before installing the Endpoint Sensor server.

For details, refer to the documentation available at:

<https://support.microsoft.com/en-us/help/811833/>

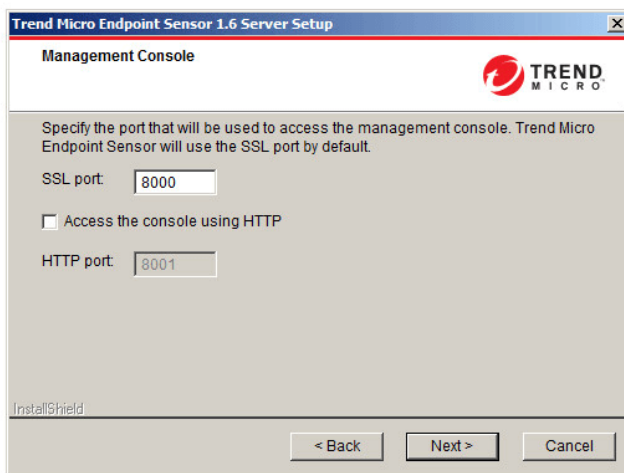
5. Specify the Endpoint Sensor server settings.
 - a. Configure the settings for the database server.

For details, see *Database Server on page 2-11*.



- b. Configure the settings for the management console.

For details, see [Management Console on page 2-15](#).



- c. Specify the Endpoint Sensor server name.

For details, see [Server Identification on page 2-16](#).

The screenshot shows the 'Server Identification' window of the 'Trend Micro Endpoint Sensor 1.6 Server Setup' wizard. The window has a title bar with the text 'Trend Micro Endpoint Sensor 1.6 Server Setup' and a close button. The main area is titled 'Server Identification' and contains the instruction: 'Specify the host address of the server that will host the Trend Micro Endpoint Sensor Server.' There are two radio buttons: 'Fully qualified domain name (FQDN) or host name:' (which is selected) and 'IP address:'. Below the first radio button is a text input field. Below the second radio button is a dropdown menu. At the bottom left, the 'InstallShield' logo is visible. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

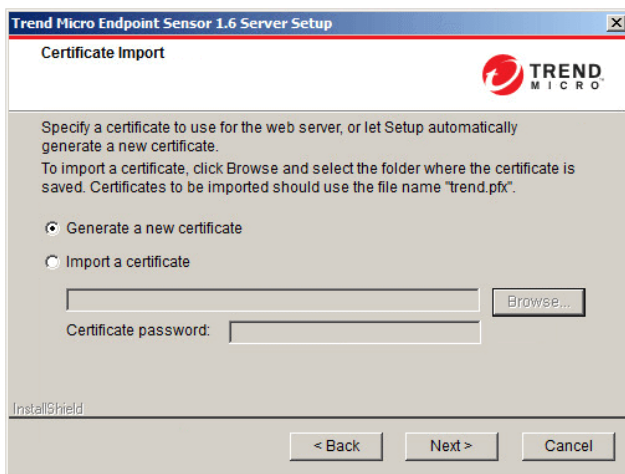
- d. Specify the ports the server uses for incoming agent communications.

For details, see [Server Communication on page 2-18](#).

The screenshot shows the 'Server Communication' window of the 'Trend Micro Endpoint Sensor 1.6 Server Setup' wizard. The window has a title bar with the text 'Trend Micro Endpoint Sensor 1.6 Server Setup' and a close button. The main area is titled 'Server Communication' and contains the instruction: 'Specify the ports that will be used for incoming agent communications.' There are two text input fields: 'Fast port:' with the value '8002' and 'Slow port:' with the value '8003'. At the bottom left, the 'InstallShield' logo is visible. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- e. Specify a certificate to use with the server by either importing an existing certificate or generating a new one.

For details, see [Certificate Import on page 2-19](#).



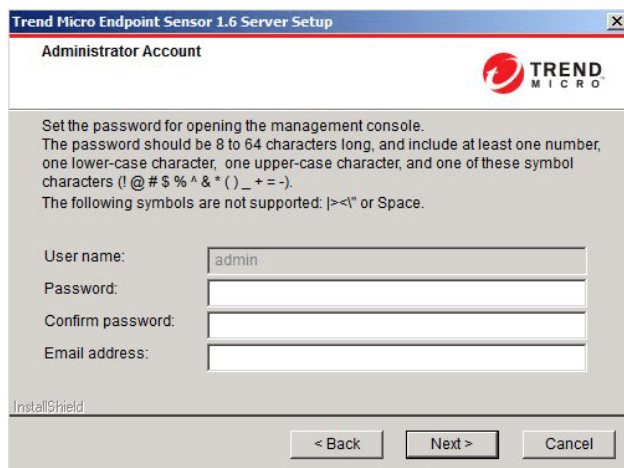
- f. Configure the Endpoint Sensor proxy settings for agent-to-server communication.

For details, see [Internal Proxy for Agent Connection to Server on page 2-20](#).



6. Set the “admin” account **password** that you will use to log on to the management console.

For details, see [About the Management Console Admin Account Password on page 2-22](#).



The screenshot shows the 'Administrator Account' screen of the 'Trend Micro Endpoint Sensor 1.6 Server Setup' window. The window has a blue title bar and a red border. The Trend Micro logo is in the top right corner. The main text area contains instructions for setting the password for the management console. Below the instructions are four input fields: 'User name' (containing 'admin'), 'Password', 'Confirm password', and 'Email address'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is in the bottom left corner.

Trend Micro Endpoint Sensor 1.6 Server Setup

Administrator Account

Set the password for opening the management console.
The password should be 8 to 64 characters long, and include at least one number, one lower-case character, one upper-case character, and one of these symbol characters (! @ # \$ % ^ & * () _ + = -).
The following symbols are not supported: | > < " or Space.

User name:

Password:

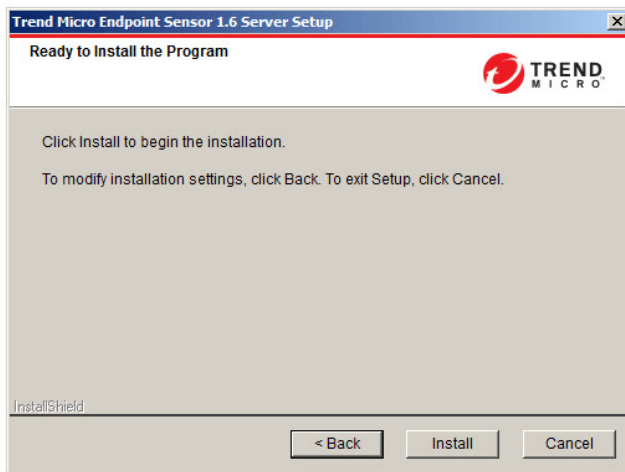
Confirm password:

Email address:

InstallShield

< Back Next > Cancel

7. Click **Install**.



The screenshot shows the 'Ready to Install the Program' screen of the 'Trend Micro Endpoint Sensor 1.6 Server Setup' window. The window has a blue title bar and a red border. The Trend Micro logo is in the top right corner. The main text area contains instructions to click 'Install' to begin the installation, and to click 'Back' to modify installation settings or 'Cancel' to exit Setup. At the bottom, there are three buttons: '< Back', 'Install', and 'Cancel'. The 'InstallShield' logo is in the bottom left corner.

Trend Micro Endpoint Sensor 1.6 Server Setup

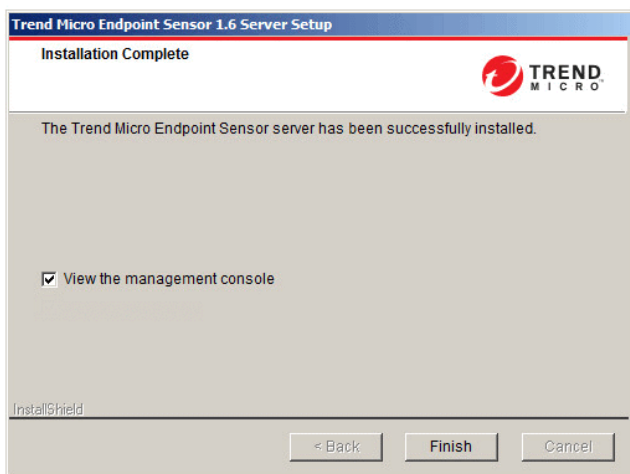
Ready to Install the Program

Click Install to begin the installation.
To modify installation settings, click Back. To exit Setup, click Cancel.

InstallShield

< Back Install Cancel

8. Click **Finish**.



Setup launches your default web browser, which allows you to access the Endpoint Sensor management console. The management console shortcut becomes available on the desktop.

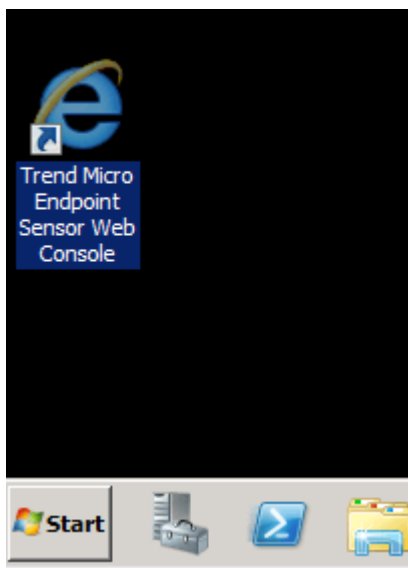


FIGURE 2-1. Management Console Shortcut

In addition, Setup displays the Endpoint Sensor readme file.

What to do next

Install the agents after verifying in the IIS configuration that the correct port is set for Endpoint Sensor server.

For details, see [Local Agent Installation Considerations on page 1-8](#).

Database Server

This screen sets the Endpoint Sensor database server used in investigations and agent configurations. The following options are available:

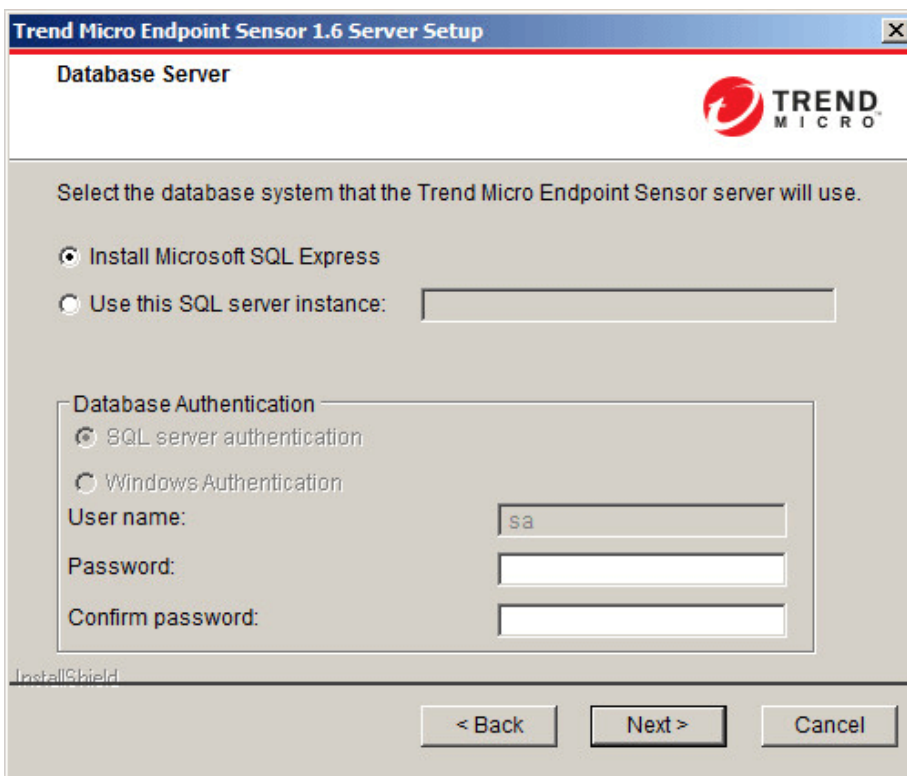


FIGURE 2-2. Configuring the Database Server

Select a database system:

- **Install Microsoft SQL Express:** If you do not have Microsoft SQL set up, the Setup program installs Microsoft™ SQL Server™ 2008 R2 SP2 - Express Edition.



Tip

Trend Micro highly recommends using Microsoft SQL Server Standard or Enterprise Edition. SQL Express is suitable for testing purposes but not for production environments. Due to the limitations of SQL Express, large networks require Microsoft SQL Server Standard or Enterprise Edition.

- **Use this SQL Server instance:** Type the SQL Server instance that you want to use. To specify another SQL server, identify the server using its FQDN, IPv4 address, or NetBIOS name.

**Note**

- A database from another Endpoint Sensor installation (or from a backup) can be used, as long as they are of the same version. However, ensure that the new environment matches exactly with the original environment of the database.
 - Restoring a database to a previous state can lead to inconsistency of data between server and agent.
-

Provide credentials to access the database server:

- **SQL Server Account**

By default, the user name is **sa**.

- **Windows Account**

Type the user name in this format: **domain name\user name**. The account should meet the following requirements:

- Belongs to the **Administrators Group**
- Assigned with the **Log on as a service** user rights
- Assigned with the **dbcreator** and **db_owner** database roles

**Note**

To use a Windows account, the ASP.NET Impersonation feature of the server's IIS installation must be enabled and configured to use the **Specific user** identity. See the IIS documentation for more information on the ASP.NET Impersonation feature.

Assign a secure password for the Endpoint Sensor database.

**Tip**

Follow the guidelines below to select a secure password:

- Use a long password. Trend Micro recommends using a password of at least 10 characters, but longer passwords are preferred.
- Avoid names or words in dictionaries.
- Use a combination of mixed-case letters, numbers, and other characters.
- Avoid simple patterns such as “101010” or “abcde.”

If you select **Install Microsoft SQL Express**, the following screen appears:

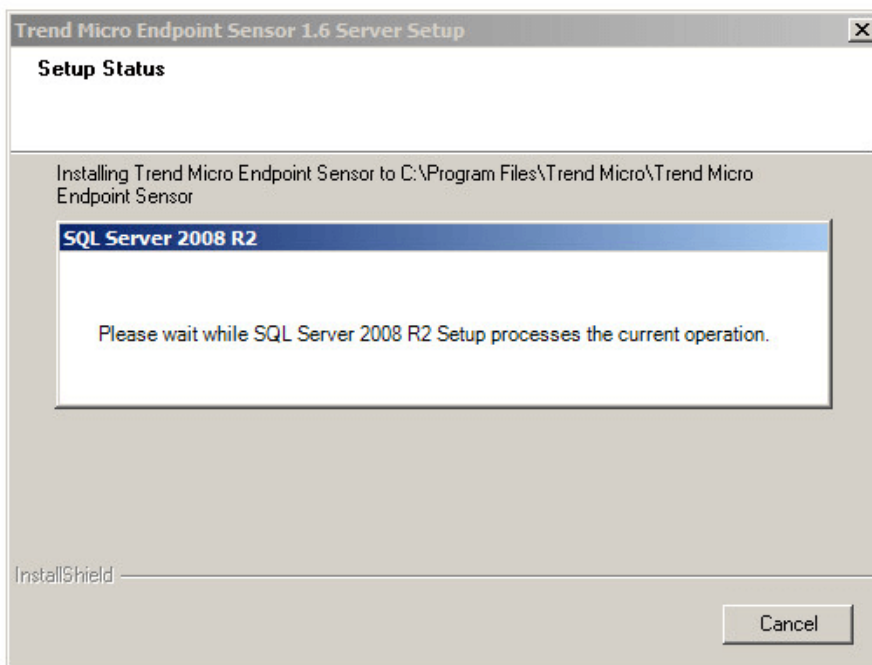


FIGURE 2-3. Installing Microsoft™ SQL Server™ 2008 R2 SP2 - Express Edition

Management Console

Confirm that the required IIS server and role services have already been installed.

For details, see [Server Installation Checklist on page 1-2](#).

This screen sets how the network connects to the Endpoint Sensor server management console. Accept the default settings or specify new ones. The following options are available:

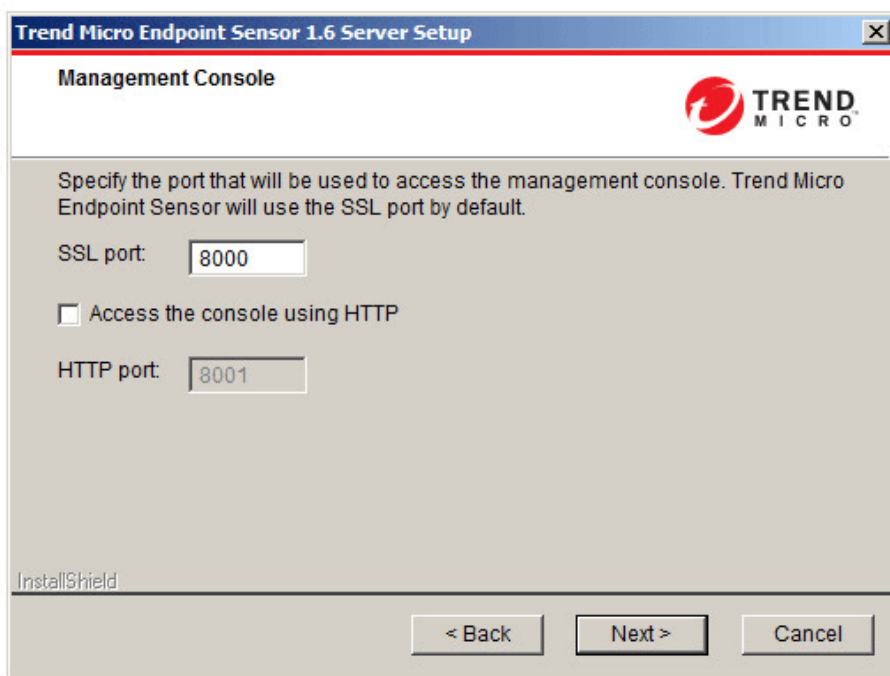


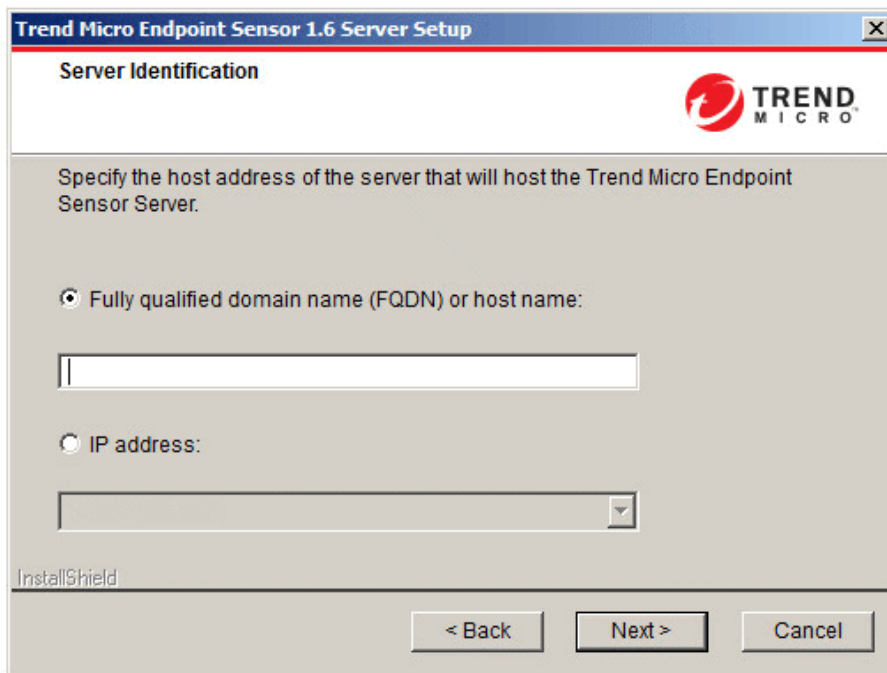
FIGURE 2-4. Configuring the Management Console Settings

- **SSL port:** Accept the default value (8000) or specify a new port. By default, the Endpoint Sensor management console is accessed using HTTPS.

- **Access the console using HTTP:** If the IIS server requires HTTP, select this option to enable the setting below.
 - **HTTP port:** Accept the default value (8001) or specify a new port number. If the port is changed, access the management console using the new port.

Server Identification

Specify the host address of the server where Endpoint Sensor is being installed. The host address functions as a server ID which agents will use to connect with the server. The following options are available:



The screenshot shows a Windows-style dialog box titled "Trend Micro Endpoint Sensor 1.6 Server Setup". The "Server Identification" tab is selected. The dialog contains the Trend Micro logo and the instruction: "Specify the host address of the server that will host the Trend Micro Endpoint Sensor Server." There are two radio button options: "Fully qualified domain name (FQDN) or host name:" (which is selected) and "IP address:". Below the first option is a text input field. Below the second option is a dropdown menu. At the bottom left, the "InstallShield" logo is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

FIGURE 2-5. Configuring the Server Identification

**Important**

Once the installation completes, the server identification specified on this screen becomes permanent. If there is a need to change the server identification at a later time, both the Endpoint Sensor server and all registered agents must be reinstalled.

- **Fully qualified domain name (FQDN) or host name:** Type the FQDN or host name of the Endpoint Sensor server.
- **IP address:** Select from the list of available IPv4 addresses.

Server Communication

This screen identifies the ports that the Endpoint Sensor server uses for incoming agent communications.

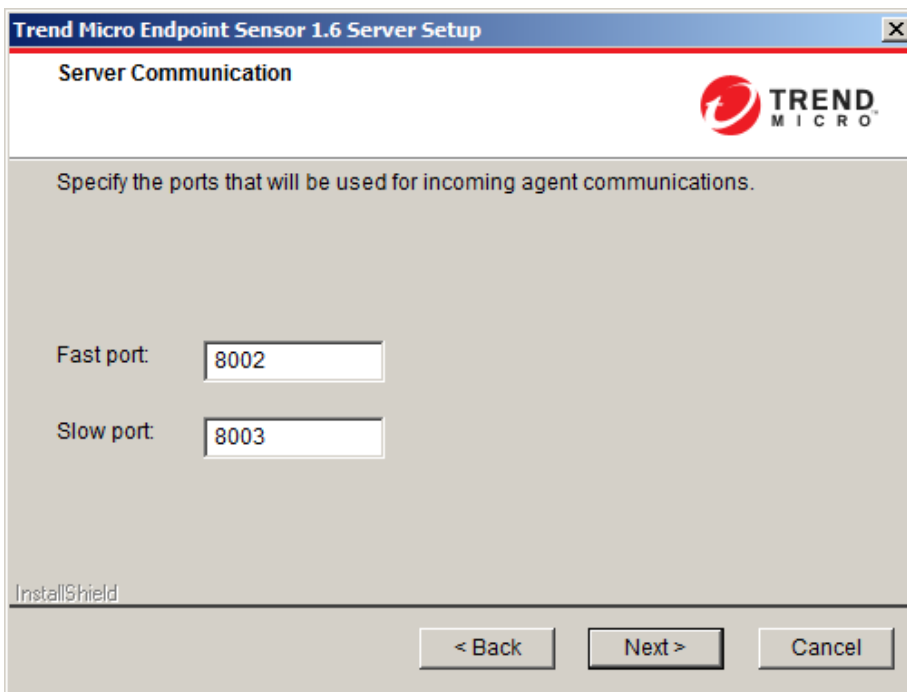


FIGURE 2-6. Server Communication

Endpoint Sensor uses HTTPS for server communication. The following options are available:

- **Fast port:** Default is 8002.
- **Slow port:** Default is 8003. Investigations using the System Process Audit method use the slow port for server communication.

Certificate Import

This screen sets the certificate used by the web server.

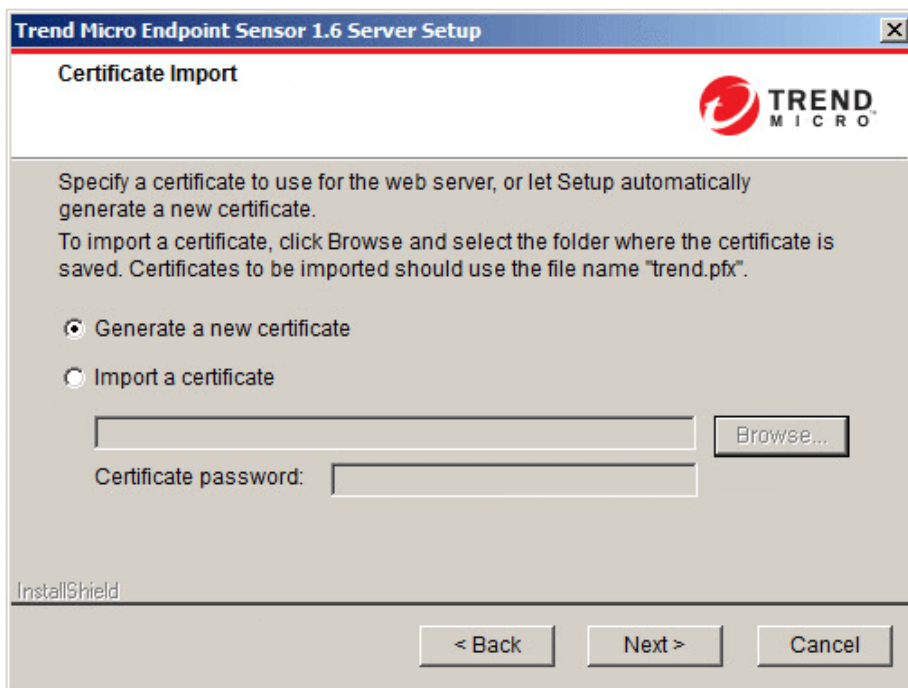


FIGURE 2-7. Configuring Certificate Import

The following options are available:

- **Generate a new certificate:** Endpoint Sensor automatically generates a new certificate for the web server during installation.
- **Import a certificate:** Import an existing certificate. Ensure that the certificate meets the following criteria:
 - The certificate is in *.pfx format.

- The certificate uses `Trend.pfx` as its file name.
- The certificate should be password-protected.

Internal Proxy for Agent Connection to Server

This screen defines the settings for agent-to-server communication through a proxy.



Important

These settings will be applied to all agent installation packages sent from the Endpoint Sensor server. After agents have been installed, the agent-to-server proxy settings cannot be changed from the Endpoint Sensor management console. The management console can only set proxy settings for new agents. Ensure that your agent-to-server proxy settings are correct before completing this step.

If you need to change agent-to-server proxy settings after agents have already been installed, contact Trend Micro support.

The screenshot shows a window titled "Trend Micro Endpoint Sensor 1.6 Server Setup" with a "Proxy Settings" tab. The window includes the Trend Micro logo and a description: "Specify proxy settings for agent-to-server communication." Inside a "Proxy settings" box, there is a checkbox "Use the following proxy settings when agents connect to the server". Below this, the "Proxy type" is set to "SOCKS5" (with "HTTP" also available). Fields for "Server name or IP address", "Port", "Authentication (optional)" (with sub-fields for "User name" and "Password") are present. The "InstallShield" logo is at the bottom left, and navigation buttons "< Back", "Next >", and "Cancel" are at the bottom right.

FIGURE 2-8. Setting the Proxy for Agent-to-Server Communication

The following options are available:

- **Use the following proxy settings when agents connect to the server:** Select to enable the proxy settings.
- **Proxy type:** Endpoint Sensor supports proxy connection over HTTP or SOCKS5 protocols.
- **Server name or IP address:** Specify the host name or IP address of the proxy server.
- **Port:** Specify the proxy server's port.
- **Authentication:** If the proxy server requires a user name or password, specify credentials here.

About the Management Console Admin Account Password

During the Endpoint Sensor server installation, setup creates the default "admin" account and prompts for a password for this account.

Endpoint Sensor uses the following criteria to check the password strength:

- The password is 8 to 64 characters long
- The password contains:
 - at least one number
 - at least one lower-case character
 - at least one upper-case character
 - at least one of these symbol characters (! @ # \$ % ^ & * () _ + = -)
- The password does not contain any of these unsupported symbols: | > < \ " or space



Tip

Follow the guidelines below to select a secure password:

- Use a long password. Trend Micro recommends using a password of at least 10 characters, but longer passwords are preferred.
 - Avoid names or words in dictionaries.
 - Use a combination of mixed-case letters, numbers, and other characters.
 - Avoid simple patterns such as "101010" or "abcde."
-

Local Agent Installation

Confirm that all installation requirements have been met. For details, see [Local Agent Installation Considerations on page 1-8](#).

Procedure

1. On the server, copy the file `EndpointSensor.exe`. By default, the file is located in the following folder:

```
C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor  
\Download\Agent\EndpointSensor.exe
```

2. On the target endpoint, paste the copied file in a local folder, and run `cmd.exe` as an administrator.
3. In the `cmd.exe` window, navigate to the folder where `EndpointSensor.exe` was pasted.
4. Issue the following command:

```
EndpointSensor.exe
```

`EndpointSensor.exe` installs the agent program in the background.

5. Log on to the Endpoint Sensor management console, and verify that the newly-installed agent is now listed in the **Endpoints** screen.



Note

If the agent is missing from the **Endpoints** screen, verify that your firewall program allows network traffic between the server and agent. If the problem persists, contact Trend Micro support.

Local Agent Silent Installation

If installation of the agent will be automated, a silent install may be performed. The installation process does not display messages or windows during its progress. A silent installation is ideal for a large-scale enterprise deployment.

Before continuing, confirm that all installation requirements have been met. For details, see [Local Agent Installation Considerations on page 1-8](#).

Procedure

1. On the server, copy the file `EndpointSensor.exe`. By default, the file is located in the following folder:

```
C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor  
\Download\Agent\Endpointsensor.exe
```

2. On the target endpoint, paste the copied file in a local folder, and run `cmd.exe` as an administrator.
3. Go to the folder where `EndpointSensor.exe` is copied.
4. Issue the following command:

```
EndpointSensor.exe /C:"agentsetuplauncher.exe -quiet -  
install"
```

`EndpointSensor.exe` installs the agent program in the background. The installation process does not display messages or windows during its progress.

5. Log on to the Endpoint Sensor management console, and verify that the newly-installed agent is now listed in the **Endpoints** screen.



Note

If the agent is missing from the **Endpoints** screen, verify that your firewall program allows network traffic between the server and agent. If the problem persists, contact Trend Micro support.

Trend Micro Endpoint Sensor Server Uninstallation

Procedure

1. On the server which hosts Endpoint Sensor, click **Control Panel > Programs and Features**. Locate and double-click "Endpoint Sensor."

2. Follow the on-screen instructions.

The server uninstallation program removes the server files. A confirmation message appears upon completion.

3. Click **Finish** to close the uninstallation program.
-

Local Agent Uninstallation

Procedure

1. On the target endpoint, run `cmd.exe` as an administrator.
2. Locate the folder where `EndpointSensor_Uninstall.exe` is installed
3. Issue the following command:

```
EndpointSensor_Uninstall.exe
```

The program uninstalls the agent program in the background.

Log on to the Endpoint Sensor management console. The **Endpoints** screen should no longer list the host name and other information related to the uninstalled agent.

Local Agent Silent Uninstallation

Procedure

1. On the target endpoint, run `cmd.exe` as an administrator.
2. Locate the folder where `EndpointSensor.exe` is installed
3. Issue the following command:

```
EndpointSensor_uninstall.exe /C:"agentsetuplauncher.exe -  
quiet -uninstall"
```

`EndpointSensor.exe` uninstalls the agent program in the background. The uninstallation process does not display messages or windows during its progress.

Log on to the Endpoint Sensor management console. The **Endpoints** screen should no longer list the host name and other information related to the uninstalled agent.

Chapter 3

OfficeScan Integration

The following content explains how to use the Trend Micro Endpoint Sensor Deployment Tool OfficeScan plug-in to deploy Endpoint Sensor across an enterprise with endpoints managed by OfficeScan.

Topics include:

- *About Trend Micro OfficeScan Integration on page 3-2*
- *About Plug-in Manager on page 3-2*
- *Installing OfficeScan on page 3-3*
- *Agent Installation Considerations When Using OfficeScan on page 3-4*
- *Using the Trend Micro Endpoint Sensor Deployment Tool on page 3-4*
- *Trend Micro Endpoint Sensor Agent Deployment Tasks on page 3-11*
- *The OfficeScan Agent Tree on page 3-14*

About Trend Micro OfficeScan Integration

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

**Note**

For information about OfficeScan, see the supporting documentation at:

<http://docs.trendmicro.com/en-us/enterprise/officescan.aspx>

Use the OfficeScan Trend Micro Endpoint Sensor Deployment Tool plug-in to deploy Endpoint Sensor agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment.

After the Trend Micro Endpoint Sensor Deployment Tool plug-in deploys the Endpoint Sensor agent software, the Endpoint Sensor agent synchronizes to the Endpoint Sensor server specified in the plug-in. OfficeScan does not manage Endpoint Sensor agents or perform investigations. The OfficeScan agent and the Endpoint Sensor agent are independent on the same endpoint.

About Plug-in Manager

OfficeScan includes a framework called Plug-in Manager that integrates new solutions into the existing OfficeScan environment. To help ease the management of these solutions, Plug-in Manager provides at-a-glance data for the solutions in the form of widgets.

**Note**

None of the plug-in solutions currently support IPv6. The server can download these solutions but is not able to deploy the solutions to pure IPv6 Trend Micro Endpoint Sensor agents or pure IPv6 hosts.

Plug-in Manager delivers the following:

- **Native Product Features**

Some native OfficeScan features are licensed separately and activated through Plug-in Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection**.

- **Plug-in programs**

Plug-in programs are not part of the OfficeScan program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the OfficeScan web console. Examples of plug-in programs are **Trend Micro OfficeScan ToolBox** and **Trend Micro Security (for Mac)**.

- **Dashboard tabs and widgets**

The OfficeScan **Summary** screen requires Plug-in Manager to display the tabs and widgets used to monitor the OfficeScan server and agent protection status.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets. Refer to specific plug-in program documentation for details on configuring and managing the program.

Installing OfficeScan

For information about installing and configuring OfficeScan, see the documentation available at:

<http://docs.trendmicro.com/en-us/enterprise/officescan.aspx>

For information on how to prepare the OfficeScan Trend Micro Endpoint Sensor Deployment Tool before deploying agents, see the *Endpoint Sensor Installation and Migration Guide*.

Agent Installation Considerations When Using OfficeScan

When using OfficeScan to install the Endpoint Sensor agent, check that your environment meets the following criteria:

- The server must have one of the following versions of OfficeScan installed:
 - OfficeScan version 10.6
 - OfficeScan version 10.6 Service Pack 1
 - OfficeScan version 10.6 Service Pack 2
 - OfficeScan version 10.6 Service Pack 3
 - OfficeScan version 11
 - OfficeScan version 11 Service Pack 1
 - OfficeScan XG
- The server must have Microsoft Internet Explorer 9 or later installed.
- The OfficeScan installation must have Plug-in Manager installed.
- The OfficeScan installation must not be installed in an Apache HTTP Server environment. Endpoint Sensor does not support Apache HTTP Server environments.

Using the Trend Micro Endpoint Sensor Deployment Tool

This section outlines how to configure OfficeScan in order to install or uninstall the Trend Micro Endpoint Sensor Deployment Tool.

Topics include:

- *[Trend Micro Endpoint Sensor Deployment Tool Installation on page 3-5](#)*

- *Plug-in Program Management on page 3-6*
- *Trend Micro Endpoint Sensor Deployment Tool Uninstallation on page 3-6*
- *Deployment Tool Error Codes on page 3-7*

Trend Micro Endpoint Sensor Deployment Tool Installation

Plug-in programs display on the **Plug-in Manager** console. Use the console to download, install, and manage the programs. Plug-in Manager downloads the installation package for the plug-in program from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the installation, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program installation or management from the Trend Micro Control Manager single sign-on function.

Installing Trend Micro Endpoint Sensor Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the **Endpoint Sensor** plug-in section and click **Download**.

The size of the plug-in program package displays beside the **Download** button. Plug-in Manager stores the downloaded package to <OSCE server installation folder>\PCCSRV\Download\Product.

Monitor the progress or navigate away from the screen during the download.

3. Click **Agree** to install the plug-in program.

Monitor the progress or navigate away from the screen during the download.

After the installation, the current plug-in program version displays on the **Plug-in Manager** screen.

**Note**

- If OfficeScan encounters problems downloading or installing the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs > Server Update**.
 - Trend Micro recommends using Internet Explorer 9 to access Trend Micro Endpoint Sensor Deployment Tool.
-

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program's management console, which is accessible from each OfficeScan web console. Tasks include activating the program and deploying the plug-in program agent to endpoints. Consult the documentation of the specific plug-in program for details on configuring and managing the program.

Managing Trend Micro Endpoint Sensor Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
 2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.
-

Trend Micro Endpoint Sensor Deployment Tool Uninstallation

Uninstall a plug-in program in the following ways:

- Uninstall the OfficeScan server, which uninstalls Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the *OfficeScan Installation and Upgrade Guide*.
- Uninstall the plug-in program from the Plug-in Manager console.

**WARNING!**

Uninstalling the Trend Micro Endpoint Sensor Deployment Tool automatically uninstalls all agents listed in the agent tree. To ensure that all agents uninstall properly, use the agent tree to uninstall all agents first before uninstalling the Trend Micro Endpoint Sensor Deployment Tool.

For details, see [Uninstalling the Trend Micro Endpoint Sensor Agent on page 3-17](#).

Uninstalling Trend Micro Endpoint Sensor Deployment Tool from the Plug-in Manager Console

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Uninstall**.
3. Refresh the **Plug-in Manager** screen after the uninstallation.

The plug-in program is available for reinstallation.

Deployment Tool Error Codes

The following error codes may appear while using the Trend Micro Endpoint Sensor Deployment Tool. Use the following list for potential solutions to issues you may encounter.

TABLE 3-1. Deployment Tool Error Codes

ERROR CODE	DETAILS
-113	Endpoint Sensor is unable to obtain required Windows environment information. Endpoint Sensor cannot determine whether the environment uses x86 or x64 architecture. Contact your system administrator.
-114	Verification of the installation package or Endpoint Sensor program was unsuccessful. • If you were installing Endpoint Sensor , download the installation package again and retry installation. • If you were uninstalling Endpoint Sensor , check if the program files have been successfully removed from the endpoint. If files have not been removed, contact technical support.
-116	The Endpoint Sensor certificate or the certificate manager tool is either missing or corrupt. Download the installation package again and retry installation.
-151	Endpoint Sensor is unable to perform installation. This problem could be caused by a variety of reasons. Check the following and try again: • The user account may have insufficient permissions to install the program. • A previous Endpoint Sensor agent may not have been completely removed. • Another process or service may be interrupting installation. • The system may be busy or locked. If installation is still unsuccessful, download the installation package again and retry installation. If this problem persists, contact technical support.
-152	A Endpoint Sensor agent is already installed on the endpoint. If you were attempting to update the Endpoint Sensor agent version, uninstall the previous agent, and try again.

ERROR CODE	DETAILS
-153	Endpoint Sensor is unable to install requisite files. This problem could be caused by a variety of reasons. Check the following and try again: • The user account may have insufficient permissions to install the program. • Another process or service may be interrupting installation. • The system may be busy or locked. If installation is still unsuccessful, download the installation package again and retry installation. If this problem persists, contact technical support.
-154	The Endpoint Sensor service, TMESC, is unable to start. Either the service has timed out, or the system may be busy. Wait for a few minutes, and try again. If this problem persists, check the system logs through Event Viewer to find the cause or contact your system administrator.
-157	Endpoint Sensor is unable to write to the Windows registry. Check that the user account has sufficient permissions to edit the registry and try again.
-158	Endpoint Sensor is unable to read the Windows registry. Check that the user account has sufficient permissions regarding registry and try again.
-167	The configuration file is missing or corrupted, or your user account does not have sufficient privileges to read the configuration file. Check that the user account has sufficient permissions and try again. If this problem persists, contact technical support.

ERROR CODE	DETAILS
-170	Endpoint Sensor is unable to perform uninstallation. This problem could be caused by a variety of reasons. Check the following and try again: • The user account may have insufficient permissions to install the program. • Another process or service may be interrupting uninstallation. • The system may be busy or locked. If this problem persists, contact technical support.
-180	Endpoint Sensor is unable to extract files from the installation package. This problem could be caused by a variety of reasons. Check the following and try again: • The installation package may be corrupt. Download the installation package again and retry installation. • The endpoint or partition may have insufficient disk space to extract the required files. • The system may be busy or locked. If this problem persists, contact technical support.
-199	Endpoint Sensor is unable to move files from the temporary folder. This problem could be caused by a variety of reasons. Verify the following and try again: • The user account may have insufficient permissions to move files. • The endpoint or partition may have insufficient disk space to move the files. • The system may be busy or locked. If this problem persists, contact technical support.

Trend Micro Endpoint Sensor Agent Deployment Tasks

The following procedure explains how to install Endpoint Sensor agents.

Procedure

1. Install and open the Trend Micro Endpoint Sensor Deployment Tool plug-in.
For details, see [Using the Trend Micro Endpoint Sensor Deployment Tool on page 3-4](#).
 2. Configure the Endpoint Sensor server and download the agent installation package.
For details, see [Downloading the Installation Package on page 3-11](#).
 3. Install the Endpoint Sensor agent program to selected endpoints.
For information on using Agent Tree to select domains and agents, see [Agent Tree Specific Tasks on page 3-14](#).

For information about agent installation, see [Installing the Trend Micro Endpoint Sensor Agent on page 3-13](#).

Once installation is complete, each OfficeScan agent acts independently of each Endpoint Sensor agent.
 4. On the **Summary** screen, verify that all agents have been installed.
For information about the **Summary** screen, see [Monitoring Trend Micro Endpoint Sensor Agents on page 3-14](#).
 5. Use the Endpoint Sensor management console to manage agents and perform investigations.
-

Downloading the Installation Package

Before you can deploy the Endpoint Sensor agents, you must specify the location where the Endpoint Sensor server downloads the agent installation package.

**Note**

At any time, if you want to change the current server URL or reset the proxy settings, click **Reset Trend Micro Endpoint Sensor Server URL and proxy server**.

Procedure

1. Go to **Administration > Server Setup**.
2. Specify the URL of the Endpoint Sensor server.

This is the same URL of the Endpoint Sensor server management console. Endpoint Sensor agents report to this server.

3. If you intend to download the agent installation package over a proxy, specify your proxy settings.

Endpoint Sensor can also use the same proxy server set in OfficeScan. To specify proxy settings for Endpoint Sensor, use the Trend Micro Endpoint Sensor Deployment Tool **Set Server** screen.

TABLE 3-2. Proxy Setting Requirements

FIELD	ACTION REQUIRED
Proxy settings toggle	Check the box to enable communication over a proxy.
Proxy protocol	Endpoint Sensor supports proxy over HTTP or SOCKS5 protocols.
Server name or IP address	Specify the IP address or URL of the proxy server.
Port	Specify the port of the proxy server.
User ID	If the proxy server requires authentication, specify the user name for authentication.
Password	If the proxy server requires authentication, specify the password for authentication.

4. Click **Set and Download**.

Endpoint Sensor tests the connection to the server, sets the server for Endpoint Sensor agent management, and then attempts to download the latest agent installation package from that server.

**Note**

After configuration, the screen changes to show which server has been set up. To download the latest agent installation package, click **Get latest package**.

Installing the Trend Micro Endpoint Sensor Agent

**Note**

You can install the Endpoint Sensor agent program to domains or individual agents but not to the root domain.

Procedure

1. Open the plug-in console and go to the **Agent Management** screen.
2. In the agent tree, select specific domains or agents.
3. Click **Deploy Agent**.

The **Deploy Agent** confirmation screen appears.

**Important**

Verify that the operating system of the endpoints where agents will be deployed is supported by Trend Micro Endpoint Sensor Deployment Tool, as the tool will skip installation on endpoints with unsupported operating systems. Trend Micro Endpoint Sensor will generate a list of the endpoints that the Endpoint Sensor agent was not installed on after installation. For details on supported operating systems, refer to the System Requirements section of the Installation Guide.

4. Click **Install**.

Endpoint Sensor begins deploying the agent to the selected endpoints.

If Endpoint Sensor agent installation was skipped on any endpoints, Endpoint Sensor generates a list of those endpoints.

5. Click **Close** to return to the **Agent Management** screen.
-

Monitoring Trend Micro Endpoint Sensor Agents

The **Summary** screen shows the installation status of the Endpoint Sensor agents.

The **Agent Installation Status** widget displays the number of endpoints with the Endpoint Sensor agent installed.



Note

Click the **Agents** hyperlink to view the agents in the **Agent Management** tree.

The OfficeScan Agent Tree

The OfficeScan agent tree displays all the agents grouped into domains that the server currently manages. Agents are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

The OfficeScan Agent Tree

The OfficeScan agent tree displays all the agents grouped into domains that the server currently manages. This allows administrators to configure, manage, and apply the same configuration to all domain members.

Agent Tree Specific Tasks

The agent tree displays when you access certain screens on the web console. Above the agent tree are menu items specific to the screen you have accessed. These menu items allow you to perform specific tasks, such as configuring agent settings or initiating agent tasks. To perform any of the tasks, first select the task target and then select a menu item.

The agent tree provides access to the following functions:

- **Search for computers:** Locate specific endpoints by typing search criteria in the text box.
- **Advanced Search:** Click the hyperlink to display the **Advanced Search** screen. Locate specific endpoints by using specific search criteria.

For details, see [Performing an Advanced Search on page 3-15](#).

- **Synchronize with OfficeScan:** Synchronize the plug-in program's agent tree with the OfficeScan server's agent tree.

For details, see [Synchronizing the Agent Tree on page 3-16](#).

- **Deploy Agent:** Install and deploy Endpoint Sensor agents to selected endpoints or upgrade existing Endpoint Sensor agents to the latest version.

For details, see [Installing the Trend Micro Endpoint Sensor Agent on page 3-13](#).

- **Uninstall:** Uninstall Endpoint Sensor agents from the selected endpoints.

For details, see [Uninstalling the Trend Micro Endpoint Sensor Agent on page 3-17](#).

Administrators can also manually search the agent tree to locate endpoints or domains. Specific computer information displays in the table on the right.

Performing an Advanced Search

Procedure

1. Open the plug-in program console. On the **Agent Management** screen, click the **Advanced Search** link.

The **Advanced Search** screen appears.

2. Search for agents by specifying the available criteria.

TABLE 3-3. Search Criteria

CRITERIA	DESCRIPTION
IPv4 range	Searching by IPv4 address range requires a portion of an IP address starting with the first octet. The search returns all endpoints with IP addresses containing that entry. For example, typing 10.5 returns all endpoints in the IP address range 10.5.0.0 to 10.5.255.255.
Host name	Search by host name.
Platform	 Note Endpoint Sensor supports both 32-bit and 64-bit platforms. For example, type <code>Windows Server</code> to return a list of all Windows Server platform endpoints available. Search by operating system.
Connection status	Search by agent connection status.
Installation status	Search by agent installation status.
Domain name	Search by agent domain name.
Build version	Search by agent version.

3. Click **Search**.
-

Synchronizing the Agent Tree

Before the plug-in program can deploy settings to agents, administrators need to synchronize the agent tree with the OfficeScan server.

Procedure

1. Open the plug-in console.
2. On the **Agent Management** screen, click **Synchronize with OfficeScan**.

A confirmation message screen appears.

3. Allow a few moments for the synchronization to complete.

After the synchronization completes, the message `The client tree has been successfully synchronized with the OfficeScan server` appears.

4. Click **Close** to return to the **Agent Management** screen.
-

Uninstalling the Trend Micro Endpoint Sensor Agent

Procedure

1. Open the plug-in console and go to the **Agent Management** screen.
2. In the agent tree, select specific domains or agents.
3. Click **Uninstall**.
4. Click **OK** to confirm the uninstallation.
5. Click **Close** in the confirmation dialog.
6. Monitor the uninstallation of the Endpoint Sensor agent in the **Installation Status** column of the **Agent Management** screen.



Tip

Allow some time for the uninstallation process to complete. Click the **Refresh** button periodically to view the updated status.

Chapter 4

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 4-2*
- *Contacting Trend Micro on page 4-3*
- *Sending Suspicious Content to Trend Micro on page 4-4*
- *Other Resources on page 4-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://ers.trendmicro.com/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<http://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<http://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Index

A

- about
 - OfficeScan, 3-2
- agent
 - install, 3-13
 - local installation, 2-22
 - monitoring, 3-14
 - silent installation, 2-23
 - silent uninstallation, 2-25
 - uninstall, 3-17
- agent tree, 3-14
 - about, 3-14
 - specific tasks, 3-14
 - synchronize, 3-16

C

- connection
 - agent connection to server, 2-20

D

- database server, 2-11
- documentation feedback, 4-6

I

- installation
 - agent, 3-13
 - local, 2-22
 - silent, 2-23
 - plug-in program, 3-5
 - server, 2-2
 - status, 3-14

M

- management console, 2-15
 - admin password, 2-22

O

- OfficeScan
 - synchronize, 3-16

P

- password, 2-22
- Plug-in Manager, 3-2
- plug-in program
 - installation, 3-5
 - uninstall, 3-7
- port
 - server communication, 2-18
- proxy
 - agent connection to server, 2-20

R

- requirements
 - agent, 1-7, 1-8
 - server, 1-2–1-5

S

- server
 - communication, 2-18
 - database, 2-11
 - identification, 2-16
 - installation, 2-2
 - listening port, 2-18
 - requirements, 1-2–1-5
 - uninstallation, 2-24
- server identification, 2-16
- SQL
 - Express, 2-12
 - screen, 2-14
 - Server, 2-13
- support

resolve issues faster, 4-4

U

uninstallation

agent, 3-17

local

silent, 2-25

local agent, 2-25

plug-in program, 3-7



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM18552/181213