TREND MICRO™
Deep Discovery Endpoint Sensor™
Installation Guide
Next Generation Endpoint Security Against Targeted Attacks and Advanced Threats
for Windows™
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:

# 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 .................................................................................................................. 1-4 
  Database Requirements .......................................................................................................... 1-4

Agent Installation Checklist .......................................................................................................... 1-5 
  Agent Requirements ............................................................................................................... 1-6 
  Local Agent Installation Considerations .............................................................................. 1-6 
  Remote Agent Installation Considerations ............................................................................ 1-7

Other Security Software .............................................................................................................. 1-9

Integration with Control Manager .............................................................................................. 1-9

## Chapter 2: Deep Discovery Endpoint Sensor Installation

Deep Discovery Endpoint Sensor Server Installation ................................................................. 2-2 
  Database Server ....................................................................................................................... 2-11 
  Management Console .............................................................................................................. 2-14 
  Deep Discovery Endpoint Sensor Server Identification .................................................... 2-15 
  Server Communication Ports ................................................................................................. 2-17 
  Agent Communication Port ................................................................................................... 2-18 
  Internal Proxy for Server Connection to Agent .................................................................... 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
Remote Agent Installation ................................................................. 2-23
Deep Discovery Endpoint Sensor Server Uninstallation .................. 2-26
Local Agent Uninstallation ................................................................. 2-26
Remote Agent Uninstallation ................................................................. 2-27

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 Deep Discovery Endpoint Sensor Deployment Tool ........ 3-5
  Deep Discovery Endpoint Sensor Deployment Tool Installation . 3-5
  Plug-in Program Management ......................................................... 3-8
  Deep Discovery Endpoint Sensor Deployment Tool Uninstallation
  ........................................................................................................... 3-9
  Deployment Tool Error Codes ......................................................... 3-10
Deep Discovery Endpoint Sensor Agent Deployment Tasks .......... 3-13
  Configuring the Server and Downloading the Installation Package
  ........................................................................................................... 3-14
  Installing the Deep Discovery Endpoint Sensor Agent ............ 3-15
  Monitoring Deep Discovery Endpoint Sensor Agents .............. 3-16
Managing the Agent Tree ................................................................. 3-17
  The OfficeScan Agent Tree ........................................................ 3-17
  Agent Tree Specific Tasks .......................................................... 3-18

Chapter 4: Technical Support

Troubleshooting Resources ............................................................... 4-2
Contacting Trend Micro ................................................................. 4-3
Sending Suspicious Content to Trend Micro ............................... 4-4
Other Resources ............................................................................. 4-5
Index

Index .............................................................................................................. IN-1
Welcome to the Trend Micro™ Deep Discovery Endpoint Sensor™ Installation Guide. This document provides details related to the server and agent installation.

---

**Note**

Refer to the *Deep Discovery 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 Deep Discovery Endpoint Sensor includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Guide</td>
<td>The Installation Guide discusses requirements and procedures for installing the Deep Discovery Endpoint Sensor server and agent.</td>
</tr>
<tr>
<td>Readme</td>
<td>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.</td>
</tr>
<tr>
<td>Online Help</td>
<td>The Online Help contains explanations of Deep Discovery Endpoint Sensor components and features, as well as procedures needed to configure Deep Discovery Endpoint Sensor.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>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: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

View and download product documentation from the Trend Micro Online Help Center: [http://docs.trendmicro.com/en-us/home](http://docs.trendmicro.com/en-us/home)

Evaluate this documentation at the following website: [http://docs.trendmicro.com/en-us/survey.aspx](http://docs.trendmicro.com/en-us/survey.aspx)
Audience

The Deep Discovery 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 |
| **Italics** | 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 |
### Terminology

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

**TABLE 3. Deep Discovery Endpoint Sensor Terminology**

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The Deep Discovery Endpoint Sensor server</td>
</tr>
<tr>
<td>Agent endpoint</td>
<td>The host where the Deep Discovery Endpoint Sensor agent is installed</td>
</tr>
<tr>
<td>Administrator (or Deep Discovery Endpoint Sensor administrator)</td>
<td>The person managing the Deep Discovery Endpoint Sensor server</td>
</tr>
<tr>
<td>Management console</td>
<td>The user interface for configuring and managing Deep Discovery Endpoint Sensor server settings</td>
</tr>
<tr>
<td>Activation Code</td>
<td>Codes that enable all Deep Discovery Endpoint Sensor features for a specified period of time.</td>
</tr>
<tr>
<td>Terminology</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Agent installation folder   | The folder on the host that contains the Deep Discovery 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 Deep Discovery 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\Deep Discovery Endpoint Sensor |
Chapter 1

System Requirements

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

Topics include:

• Server Installation Checklist on page 1-2
• Agent Installation Checklist on page 1-5
• Other Security Software on page 1-9
• Integration with Control Manager on page 1-9
Server Installation Checklist

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

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

  For details about the available Deep Discovery Endpoint Sensor versions, refer to the Online Help or Administrator’s Guide available at:

- 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**

<table>
<thead>
<tr>
<th>Required Hardware/Software Component</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2 GHz minimum</td>
</tr>
<tr>
<td>RAM</td>
<td>• 4GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 16GB recommended</td>
</tr>
<tr>
<td>Available disk space</td>
<td>• 500GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 1TB recommended</td>
</tr>
<tr>
<td>Required Hardware/Software Component</td>
<td>Specifications</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Operating system                    | • Windows Server 2008 Service Pack 2 (32-bit and 64-bit)  
• Windows Server 2008 R2 (64-bit)  
• Windows Server 2012 R2 (64-bit) |
| Database                            | • Microsoft SQL Server 2008 Express  
• Microsoft SQL Server 2008 R2 Standard or Enterprise Edition recommended |
| Note                                | Installing Microsoft SQL Server requires the .NET Framework. Trend Micro recommends using Microsoft .NET Framework 3.5. |
| Web server                          | Microsoft Internet Information Services (IIS) 7 or 7.5 with the following role services:  
• Static Content  
• Default Document  
• Directory Browsing  
• HTTP Errors  
• HTTP Redirection  
• ASP.NET  
• ASP  
• CGI  
• ISAPI Extensions  
• ISAPI Filters  
• Request Filtering  
• IIS Management Console |
REQUISITED HARDWARE/ SOFTWARE COMPONENTS SPECIFICATIONS

| Web browser (for Deep Discovery 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 Deep Discovery 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 Deep Discovery Endpoint Sensor server deployment.

Database Requirements

Deep Discovery Endpoint Sensor stores data in an SQL database. When you install Deep Discovery 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.
Agent Installation Checklist

To ensure a successful installation of the Deep Discovery 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 Deep Discovery Endpoint Sensor agent on a pure IPv6 endpoint is not supported.

• Verify that the Deep Discovery Endpoint Sensor agent installer is available in the Deep Discovery Endpoint Sensor server installation folder (the default location is `C:\Program Files\Trend Micro\Deep Discovery Endpoint Sensor \Download\Agent\`).

• Verify that the agents meet the required hardware and software specifications. For details, see *Agent Requirements on page 1-6*.

• Use IIS Manager to check if the ports are correctly set. For details about the default ports, see *Agent Communication Port on page 2-18*.

• Verify that additional requirements needed for a local or remote installation of Deep Discovery Endpoint Sensor agents have been met. Refer to the following guidelines:

  • *Local Agent Installation Considerations on page 1-6*
  
  • *Remote Agent Installation Considerations on page 1-7*

• If you intend to install the Deep Discovery 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**

<table>
<thead>
<tr>
<th><strong>Required Hardware/Software Component</strong></th>
<th><strong>Specification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2 GHz minimum</td>
</tr>
</tbody>
</table>
| RAM| • 512MB minimum for Windows XP  
• 1GB minimum for other operating systems |
| Available disk space| • 3GB minimum  
• 4GB recommended |
| 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 2003 Service Pack 2 (32-bit and 64-bit)  
• Windows Server 2003 R2 Service Pack 2 (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) |

Local Agent Installation Considerations

To ensure a successful local installation of the Deep Discovery Endpoint Sensor agent, perform the following:
• The agent installer, EndpointSensor.exe, found at <Deep Discovery Endpoint Sensor server installation path>\Download\Agent\, has been shared or copied to the target endpoint.

• Check that your firewall program allows Deep Discovery Endpoint Sensor to communicate using the correct ports. The default port is 8081. Otherwise, use the value specified during installation.

• Confirm that the endpoint has an IPv4 address.

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

Remote Agent Installation Considerations

Remote installation launches the agent Setup program from one endpoint to install a Deep Discovery Endpoint Sensor agent on another endpoint. When performing a remote installation, Setup checks if the target endpoint meets the requirements for agent installation.

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

• Verify that target endpoints meet the Deep Discovery Endpoint Sensor agent system requirements.

  For details, see Agent Requirements on page 1-6.

• List each target endpoint's host name and logon credentials (user name and password with administrator access).

• Enable the administrative shares on target endpoints. \<endpoint's host name or IP address>\admin$ should be accessible.

  For details, see Enabling Administrative Shares on page 1-8.

• Confirm that the target endpoints have an IPv4 address.

Endpoints that are using IPv6 addresses must also have IPv4 addresses. Installing the Deep Discovery Endpoint Sensor agent on a pure IPv6 endpoint is not supported.
• Check that your firewall program allows Deep Discovery Endpoint Sensor to communicate using the correct ports.

The remote agent uses ports 137, 139 and 445 for installation. The default server ports are 8002 (fast port) and 8003 (slow port). The default agent port is 8081. You can specify your own values during the server installation.

For other firewall-related concerns, check with your network administrator or refer to your firewall program documentation.

Enabling Administrative Shares

Procedure

• Windows XP

Change the local security policy from Network access: Sharing and security model for local accounts to Classic - local users authenticate as themselves.

• Windows 7

a. Enable File and Printer Sharing through Control Panel > Network and Internet > Network and Sharing Center.

b. Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \System.

c. Add a new DWORD (32-bit) Value with the following settings:
   • Name: LocalAccountTokenFilterPolicy
   • Value data: 1

d. Restart the computer.
Other Security Software

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

---

**Important**

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

---

**TABLE 1-3. Software Incompatibilities**

<table>
<thead>
<tr>
<th>DEEP DISCOVERY ENDPOINT SENSOR SOFTWARE</th>
<th>INCOMPATIBLE SOFTWARE</th>
</tr>
</thead>
</table>
| Server                                 | • Trend Micro™ Safe Lock™ agent  
|                                        | • Trend Micro™ Safe Lock™ Intelligent Manager |
| Agent                                  | • Trend Micro™ Titanium™  
|                                        | • Trend Micro™ Internet Security |

Integration with Control Manager

The following diagram illustrates a typical Deep Discovery Endpoint Sensor deployment.
Deep Discovery Endpoint Sensor 1.5 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 Deep Discovery Endpoint Sensor servers from a single location.

For details, see the Control Manager documentation.
Chapter 2

Deep Discovery Endpoint Sensor Installation

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

Note

For agent installation using OfficeScan, see *OfficeScan Integration on page 3-1.*

Topics include:

- *Deep Discovery Endpoint Sensor Server Installation on page 2-2*
- *Local Agent Installation on page 2-22*
- *Remote Agent Installation on page 2-23*
- *Local Agent Uninstallation on page 2-26*
- *Remote Agent Uninstallation on page 2-27*
Deep Discovery 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*.

**Procedure**

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

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

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

The default server installation path is `C:\Program Files\Trend Micro\Deep Discovery Endpoint Sensor\`. Specify a new installation path or use the default path.
4. Type the full or trial Activation Code for Deep Discovery Endpoint Sensor.

For details about the available Deep Discovery Endpoint Sensor versions, refer to the Online Help or the Administrator's Guide available at:


5. Specify the Deep Discovery 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 2-14.*

c. Specify the Deep Discovery Endpoint Sensor server name.
d. Specify the ports for server communications.

For details, see *Server Communication Ports on page 2-17.*

e. Specify the port for agent communications.
For details, see *Agent Communication Port on page 2-18.*

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

For details, see *Internal Proxy for Server Connection to Agent on page 2-19.*
g. Configure the Deep Discovery Endpoint Sensor proxy settings for agent-to-server communication.

For details, see *Internal Proxy for Agent Connection to Server on page 2-20.*

![Internal Proxy for Agent Connection to Server](image)

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.*
7. Click **Install**.

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

**Figure 2-1. Management Console Shortcut**
In addition, Setup displays the Deep Discovery Endpoint Sensor readme file.

**What to do next**

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

For details, see *Local Agent Installation Considerations on page 1-6.*

**Database Server**

This screen sets the Deep Discovery 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.

• 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**
    • Contains the **Log on as a service** and **Log on as a batch job** user rights
    • Contains the **dbcreator** and **db_owner** database roles

Assign a secure password for the Deep Discovery 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](image)

**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 Deep Discovery 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 Deep Discovery 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.

Deep Discovery Endpoint Sensor Server Identification

Specify the host address of the server where Deep Discovery 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:
**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 Deep Discovery 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 Deep Discovery Endpoint Sensor server.
- **IP address**: Select from the list of available IPv4 addresses.
Server Communication Ports

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

![Server Communication](image)

**Figure 2-6. Setting the Server Communication Ports**

Accept the defaults or specify new ports. The following options are available:

- **Fast port**: Default is 8002.
- **Slow port**: Default is 8003.
Note

Investigations using the System Process Audit method use the slow port for server communication. All other investigation methods use the fast port for server communication.

Agent Communication Port

This screen identifies the port that Deep Discovery Endpoint Sensor agents use for incoming server communication.

Figure 2-7. Setting the Agent Communication Port

Accept the default port (8081), or specify a new one.
Internal Proxy for Server Connection to Agent

This screen defines the settings for server-to-agent communication through a proxy. These settings can be changed from the Deep Discovery Endpoint Sensor management console later.

![Setting the Proxy for Server-to-Agent Communication](image)

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

The following options are available:

- **Use the following proxy settings when the server connects to agents**: Check this box to enable the proxy connection.

- **Proxy type**: Deep Discovery 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 port of the proxy server.

• **Authentication**: If the proxy server requires a user name or password, specify the credentials here.

**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 Deep Discovery Endpoint Sensor server. After agents have been installed, the agent-to-server proxy settings cannot be changed from the Deep Discovery 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.
Figure 2-9. 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**: Deep Discovery 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

Deep Discovery 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 symbol character
- The password does not contain any of these unsupported symbols: |><" or space

Record the user name and password for future reference.

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

Before you begin

Confirm that all installation requirements have been met. For details, see Local Agent Installation Considerations on page 1-6.
Deep Discovery Endpoint Sensor Installation

Procedure

1. On the target endpoint, run cmd.exe as an administrator.

2. Go to the folder where EndpointSensor.exe is copied.

3. Issue the following command:

   C:\>EndpointSensor.exe

   EndpointSensor.exe installs the agent program in the background.

4. Log on to the Deep Discovery 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.

Remote Agent Installation

Before you begin

Confirm that all installation requirements have been met. For details, see *Remote Agent Installation Considerations* on page 1-7.

Procedure

1. On the Deep Discovery Endpoint Sensor server, go to `<Deep Discovery Endpoint Sensor server installation path>\CmdTool\Remote Helper\`, and then open the following files:

   - PCList.csv
   - TargetedPCs.csv
Tip

Back up these files to protect your configuration in case the original files are damaged or deleted.

2. For each target endpoint, insert a new line and add the following information:
   • Target endpoint's IP address or host name
   • User name and password for a user account with administrative rights on the target endpoint

Important

• Do not modify the first lines of PCList.csv and TargetedPCs.csv.
• Ensure the security of these files as they are in cleartext and contain sensitive information.

![Sample PCList.csv/TargetedPCs.csv Entry with “10.201.206.74” as a Target Endpoint](image)

3. Launch command prompt (cmd.exe) using an administrator account, and then issue the following command:

   ```cmd
   C:\...\CmdTool\Remote Helper>RemoteHelper.exe TargetedPCs.csv ..\..\Download\Agent\install.zip
   ```
The following output appears:

![Command Line Output](image)

**Figure 2-11. Installing the Deep Discovery Endpoint Sensor Agent on Endpoint “10.201.206.74”**

Check `Deploy.log` and `Targetpc.csv` to determine whether the installation is successful. Based on the sample results above, an agent with the IP address of “10.201.206.74” 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.
Deep Discovery Endpoint Sensor Server Uninstallation

Procedure

1. On the server which hosts Deep Discovery Endpoint Sensor, click Control Panel > Programs and Features. Locate and double-click “Deep Discovery 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. Go to the folder where EndpointSensor_Uninstall.exe is copied.

3. Issue the following command:

   EndpointSensor_Uninstall.exe

   The program uninstalls the agent program in the background.

The management console Endpoints screen should no longer list the host name and other information related to the uninstalled agent.
Remote Agent Uninstallation

Procedure

1. On the Deep Discovery Endpoint Sensor server, go to <Deep Discovery Endpoint Sensor server installation path>\CmdTool\Remote Helper\, and then open the following files:
   - PCList.csv
   - TargetedPCs.csv

   **Tip**
   
   Back up these files to protect your configuration in case the original files are damaged or deleted.

2. For each target endpoint, insert a new line and add the following information:
   - Target endpoint's IP address or host name
   - User name and password for a user account that has administrative rights on the target endpoint

   **Important**
   
   - Do not modify the first lines of PCList.csv and TargetedPCs.csv.
   - Ensure the security of these files as they are in clear text and contain sensitive information.

3. Launch command prompt (cmd.exe) using an administrator account, and then issue the following command:

   ```
   C:\...\Remote Helper>RemoteHelper.exe TargetedPCs.csv ..\..\Download\Agent\uninstall.zip
   ```

   The management console **Endpoints** screen no longer lists the host name and other information related to the uninstalled agent.
Chapter 3

OfficeScan Integration

The following content explains how to use the Deep Discovery Endpoint Sensor Deployment Tool OfficeScan plug-in to deploy Deep Discovery 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 Deep Discovery Endpoint Sensor Deployment Tool on page 3-5
- Deep Discovery Endpoint Sensor Agent Deployment Tasks on page 3-13
- Managing the Agent Tree on page 3-17
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:


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

After the Deep Discovery Endpoint Sensor Deployment Tool plug-in deploys the Deep Discovery Endpoint Sensor agent software, the Deep Discovery Endpoint Sensor agent synchronizes to the Deep Discovery Endpoint Sensor server specified in the plug-in. OfficeScan does not manage Deep Discovery Endpoint Sensor agents or perform investigations. The OfficeScan agent and the Deep Discovery 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 Deep Discovery Endpoint Sensor agents or hosts that only have an IPv6 address assigned.

Plug-in Manager delivers two types of solutions:

- **Native Product Features**
  
  Some native OfficeScan features are licensed separately and activated through Plug-in Manager. **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection** are examples of two features that fall under this category.

- **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 **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)**, and **Trend Micro Mobile Security**.

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:


For information on how to prepare the OfficeScan Deep Discovery Endpoint Sensor Deployment Tool before deploying agents, see the **Deep Discovery Endpoint Sensor Installation and Migration Guide**.
Agent Installation Considerations When Using OfficeScan

When using OfficeScan to install the Deep Discovery 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 10.5
  • OfficeScan version 10.5 Patch 1
  • 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

• The server must have one of the following browsers installed:
  • Microsoft Internet Explorer 9 or later
  • The latest version of Google Chrome
  • The latest version of Mozilla Firefox

• Plug-in Manager must be installed on the OfficeScan server.

• The OfficeScan server must not be installed in an Apache HTTP Server environment. Deep Discovery Endpoint Sensor does not support Apache HTTP Server environments.
Using the Deep Discovery Endpoint Sensor Deployment Tool

This section outlines how to configure OfficeScan in order to install or uninstall the Deep Discovery Endpoint Sensor Deployment Tool. Topics include:

- Deep Discovery Endpoint Sensor Deployment Tool Installation on page 3-5
- Plug-in Program Management on page 3-8
- Deep Discovery Endpoint Sensor Deployment Tool Uninstallation on page 3-9

Deep Discovery Endpoint Sensor Deployment Tool Installation

The Deep Discovery Endpoint Sensor Deployment Tool is installed as a plug-in program in OfficeScan.

OfficeScan plug-in programs appear 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 single sign-on function of Trend Micro Control Manager.
Preparing the Deep Discovery Endpoint Sensor Deployment Tool Installation Package

**Important**
Contact Support to receive the Deep Discovery Endpoint Sensor deployment tool before proceeding. This plug-in program is not available on the ActiveUpdate server.

**Procedure**

1. Save the Deep Discovery Endpoint Sensor deployment tool to any folder on the same machine as the OfficeScan server.

2. Create a deployment folder and extract the contents of the tool to this folder. The extracted files should be composed of a `server.ini` file and several *.zip files. Do not extract the *.zip files. Move the extracted files as follows:

   - Move `server.ini` to the root of the deployment folder.
   - Create the following subdirectory inside the deployment folder, and move the *.zip files there:

     `product\<language>`

**Note**

`<language>` refers to the language of OfficeScan installed (`enu` for English, `ja` for Japanese, `zh_tw` for traditional Chinese, etc). Check your OfficeScan installation to determine the correct language code to use.
For example, if the deployment tool is to be installed in an environment running the Japanese version of OfficeScan, use the following folder structure:

3. Share the deployment folder. Take note of the folder's Uniform Naming Convention (UNC) path.
4. Open the OfficeScan web console and go to Updates > Server > Update Source.
5. On the screen that appears, select Intranet location containing a copy of the current file, and type the UNC path of the folder containing the Deep Discovery Endpoint Sensor deployment tool. Specify the user name and password for the folder, if necessary.
6. Click Save.
7. Restart the OfficeScan Plug-in Manager service.
8. Open the OfficeScan web console and click Plug-in Manager in the main menu.
9. Verify that the Deep Discovery Endpoint Sensor plug-in appears in the list of available plug-in programs.
Installing Deep Discovery 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 **Download**.

   The size of the plug-in program package displays beside the **Download** button. Plug-in Manager stores the downloaded package to `<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 installation.

---

**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**.

---

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

**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 Deep Discovery 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**.

Deep Discovery Endpoint Sensor Deployment Tool Uninstallation

Uninstall a plug-in program in the following ways:

- Uninstall the plug-in program from the Plug-in Manager console.
- 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*.

Uninstalling Deep Discovery 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 Deep Discovery Endpoint Sensor Deployment Tool. Use the following list for potential solutions to issues you may encounter.

**TABLE 3-1. Deployment Tool Error Codes**

<table>
<thead>
<tr>
<th>ERROR CODE</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>-113</td>
<td>Deep Discovery Endpoint Sensor is unable to obtain required Windows environment information. Deep Discovery Endpoint Sensor cannot determine whether the environment uses x86 or x64 architecture. Contact your system administrator.</td>
</tr>
</tbody>
</table>
| -114       | Verification of the installation package or Deep Discovery Endpoint Sensor program was unsuccessful.  
• If you were installing Deep Discovery Endpoint Sensor, download the installation package again and retry installation.  
• If you were uninstalling Deep Discovery Endpoint Sensor, check if the program files have been successfully removed from the endpoint. If files have not been removed, contact technical support. |
<p>| -116       | The Deep Discovery Endpoint Sensor certificate or the certificate manager tool is either missing or corrupt. Download the installation package again and retry installation. |</p>
<table>
<thead>
<tr>
<th><strong>ERROR CODE</strong></th>
<th><strong>DETAILS</strong></th>
</tr>
</thead>
</table>
| -151           | Deep Discovery 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 Deep Discovery 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 Deep Discovery Endpoint Sensor agent is already installed on the endpoint. If you were attempting to update the Deep Discovery Endpoint Sensor agent version, uninstall the previous agent, and try again. |
| -153           | Deep Discovery 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. |
<p>| -154           | The Deep Discovery Endpoint Sensor service, ESClient, 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. |</p>
<table>
<thead>
<tr>
<th>ERROR CODE</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>-157</td>
<td>Deep Discovery 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.</td>
</tr>
<tr>
<td>-158</td>
<td>Deep Discovery Endpoint Sensor is unable to read the Windows registry. Check that the user account has sufficient permissions regarding registry and try again.</td>
</tr>
<tr>
<td>-167</td>
<td>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.</td>
</tr>
</tbody>
</table>
| -170       | Deep Discovery 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       | Deep Discovery 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. |
Deep Discovery Endpoint Sensor Agent Deployment Tasks

The following procedure explains how to install Deep Discovery Endpoint Sensor agents.

Procedure

1. Install and open the Deep Discovery Endpoint Sensor Deployment Tool plug-in.  
   For details, see Using the Deep Discovery Endpoint Sensor Deployment Tool on page 3-5.

2. Configure the Deep Discovery Endpoint Sensor server and download the agent installation package.  
   For details, see Configuring the Server and Downloading the Installation Package on page 3-14.

3. Install the Deep Discovery 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 3-18.

---

**ERROR CODE** | **DETAILS**
--- | ---
-199 | Deep Discovery 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.
For information about agent installation, see *Installing the Deep Discovery Endpoint Sensor Agent on page 3-15*.

Once installation is complete, each OfficeScan agent acts independently of each Deep Discovery Endpoint Sensor agent.

4. On the **Summary** screen, verify that all agents have been installed.

For information about the **Summary** screen, see *Monitoring Deep Discovery Endpoint Sensor Agents on page 3-16*.

5. Use the Deep Discovery Endpoint Sensor management console to manage agents and perform investigations.

---

**Configuring the Server and Downloading the Installation Package**

Before you can deploy the Deep Discovery Endpoint Sensor agents, you must specify the location where the Deep Discovery 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 Deep Discovery Endpoint Sensor Server URL and proxy server**.

---

**Procedure**

1. Go to **Administration > Server Setup**.

2. Specify the URL of the Deep Discovery Endpoint Sensor server.

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

3. If you intend to download the agent installation package over a proxy, specify your proxy settings.
Deep Discovery Endpoint Sensor can also use the same proxy server set in OfficeScan. To specify proxy settings for Deep Discovery Endpoint Sensor, use the Deep Discovery Endpoint Sensor Deployment Tool Set Server screen.

**Table 3-2. Proxy Setting Requirements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy settings toggle</td>
<td>Check the box to enable communication over a proxy.</td>
</tr>
<tr>
<td>Proxy protocol</td>
<td>Deep Discovery Endpoint Sensor supports proxy over HTTP or SOCKS5 protocols.</td>
</tr>
<tr>
<td>Server name or IP address</td>
<td>Specify the IP address or URL of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port of the proxy server.</td>
</tr>
<tr>
<td>User ID</td>
<td>If the proxy server requires authentication, specify the user name for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>If the proxy server requires authentication, specify the password for authentication.</td>
</tr>
</tbody>
</table>

4. Click **Set and Download**.

Deep Discovery Endpoint Sensor tests the connection to the server, sets the server for Deep Discovery 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 Deep Discovery Endpoint Sensor Agent**

**Note**

You can install the Deep Discovery 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*

If the selected agents or domains include endpoints with unsupported operating systems, the Deep Discovery Endpoint Sensor Deployment Tool notifies you of the supported operating systems. Installation on endpoints with supported operating systems will still proceed normally, but the Deep Discovery Endpoint Sensor agent is not installed on endpoints with unsupported operating systems. Deep Discovery Endpoint Sensor will generate a list of the endpoints that the Deep Discovery Endpoint Sensor agent was not installed on after installation.

4. Click Install.

Deep Discovery Endpoint Sensor begins deploying the agent to the selected endpoints.

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

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

Monitoring Deep Discovery Endpoint Sensor Agents

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

The Agent Installation Status widget displays the number of endpoints with the Deep Discovery Endpoint Sensor agent installed.
Managing the Agent Tree

This section outlines how to install, manage, and uninstall Deep Discovery Endpoint Sensor agents.

Topics include:

- The OfficeScan Agent Tree on page 3-17
- Agent Tree Specific Tasks on page 3-18

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.

![OfficeScan agent tree](image)

**Figure 3-1. OfficeScan agent tree**
Agent Tree Specific Tasks

The agent tree appears 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 providing more search criteria.

  For details, see *Performing an Advanced Search on page 3-19.*

• **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 3-20.*

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

  For details, see *Installing the Deep Discovery Endpoint Sensor Agent on page 3-15.*

• **Uninstall**: Uninstall Deep Discovery Endpoint Sensor agents from the selected endpoints.

  For details, see *Uninstalling the Deep Discovery Endpoint Sensor Agent on page 3-20.*

Administrators can also manually search the agent tree to locate endpoints or domains.
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>
<thead>
<tr>
<th>TABLE 3-3. Search Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CRITERIA</strong></td>
</tr>
<tr>
<td>IPv4 range</td>
</tr>
<tr>
<td>Host name</td>
</tr>
<tr>
<td>Platform</td>
</tr>
<tr>
<td>Connection status</td>
</tr>
<tr>
<td>Installation status</td>
</tr>
<tr>
<td>Domain name</td>
</tr>
<tr>
<td>Build version</td>
</tr>
</tbody>
</table>

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 Deep Discovery 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.
Tip
Allow some time for the uninstallation process to complete. Click the Refresh button periodically to view the updated status.
Chapter 4

Technical Support

This chapter describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

• *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

2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The Technical Support product page appears.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Submit a Support Case from the left navigation and add any relevant details, or submit a support case here:


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

Threat Encyclopedia

Most malware today consists of “blended threats” - two or more technologies combined 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, fax, or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Inc., 10101 North De Anza Blvd., Cupertino, CA 95014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Toll free: +1 (800) 228-5651 (sales)</td>
</tr>
<tr>
<td></td>
<td>Voice: +1 (408) 257-1500 (main)</td>
</tr>
<tr>
<td>Fax</td>
<td>+1 (408) 257-2003</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:


- 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 hardware connected to the endpoint
• Amount of memory and free hard disk space
• Operating system and service pack version
• Endpoint agent version
• 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:


File Reputation Services

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


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.

TrendLabs

TrendLabs™ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.
TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

Index

A
about
  OfficeScan, 3-2
agent
  install, 3-15
  listening port, 2-18
  local installation, 2-22
  monitoring, 3-16
  remote installation, 2-23
  uninstall, 3-20
agent tree, 3-17, 3-18
  about, 3-17
  specific tasks, 3-18
  synchronize, 3-20
admin password, 2-22

O
OfficeScan
  synchronize, 3-20
  update source, 3-6

P
password, 2-22
Plug-in Manager, 3-2
plug-in program
  installation, 3-5
  uninstall, 3-9
port
  agent communication, 2-18
  server communication, 2-17
proxy
  agent connection to server, 2-20
  server connection to agent, 2-19

R
requirements
  agent, 1-6
  server, 1-2–1-4

S
server
  communication, 2-17
  database, 2-11
  identification, 2-15
  installation, 2-2
  listening port, 2-17
  requirements, 1-2–1-4
  uninstallation, 2-26
  server identification, 2-15

C
connection
  agent connection to server, 2-20
  server connection to agent, 2-19

D
database server, 2-11

I
installation
  agent, 3-15
    local, 2-22
    remote, 2-23
  plug-in program, 3-5
  prepare package, 3-6
  server, 2-2
  status, 3-16
installation package, 3-6

M
management console, 2-14
SQL
   Express, 2-12
   screen, 2-14
   Server, 2-13

U
   uninstallation
      agent, 3-20
      local agent, 2-26
      plug-in program, 3-9
      remote agent, 2-27