



1.0 Trend Micro™ Endpoint Application Control

Installation Guide (Patch 1)

Block Unwanted and Unknown Applications



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-application-control.aspx>

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

© 2014 Trend Micro Incorporated. All Rights Reserved.

Document Part No.: APEM16419/140430

Release Date: June 2014

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>

Table of Contents

Chapter 1: Installing Endpoint Application Control

System Requirements	1-2
Installation Flow	1-2
Required Components	1-3
Welcome	1-4
License Agreement	1-5
Proxy Server	1-6
Registration and Activation	1-7
Web Server	1-8
Backend Server	1-12
Root Account	1-14
Installation Path	1-15
Installation Complete	1-16
Uninstalling the Endpoint Application Control Server Using the Uninstallation Program	1-17

Chapter 2: Getting Support

Contacting Technical Support	2-2
Speeding Up the Support Call	2-2

Index

Index	IN-1
-------------	------

Chapter 1

Installing Endpoint Application Control

Trend Micro Endpoint Application Control manages application usage on users and endpoints. The product consists of the Endpoint Application Control agent that resides at the endpoint and a server program that manages all agents. The agent reports its status and application usage to the server. The server, through the web-based management console, makes it easy to set application control policies and deploy updates to every agent.

Topics in this chapter:

- *System Requirements on page 1-2*
- *Installation Flow on page 1-2*
- *Uninstalling the Endpoint Application Control Server Using the Uninstallation Program on page 1-17*

System Requirements

Visit the following website for a complete list of system requirements:

<http://docs.trendmicro.com>

Installation Flow

Setup goes through the following screens to install Endpoint Application Control.

1. *Required Components on page 1-3*
2. *Welcome on page 1-4*
3. *License Agreement on page 1-5*
4. *Proxy Server on page 1-6*
5. *Registration and Activation on page 1-7*
6. *Web Server on page 1-8*
7. *Backend Server on page 1-12*
8. *Root Account on page 1-14*
9. *Installation Path on page 1-15*
10. *Installation Complete on page 1-16*

Required Components

Setup checks the system for required components. The following screen appears if Setup does not detect the components.

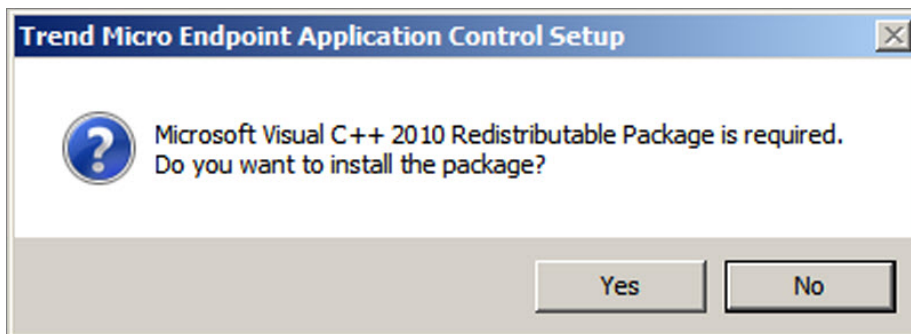


FIGURE 1-1. Installing the Visual C++ 2010 Redistributable Package

Procedure

- Click **Yes** to install the Microsoft Visual C++ 2010 Redistributable Package.
-

Welcome

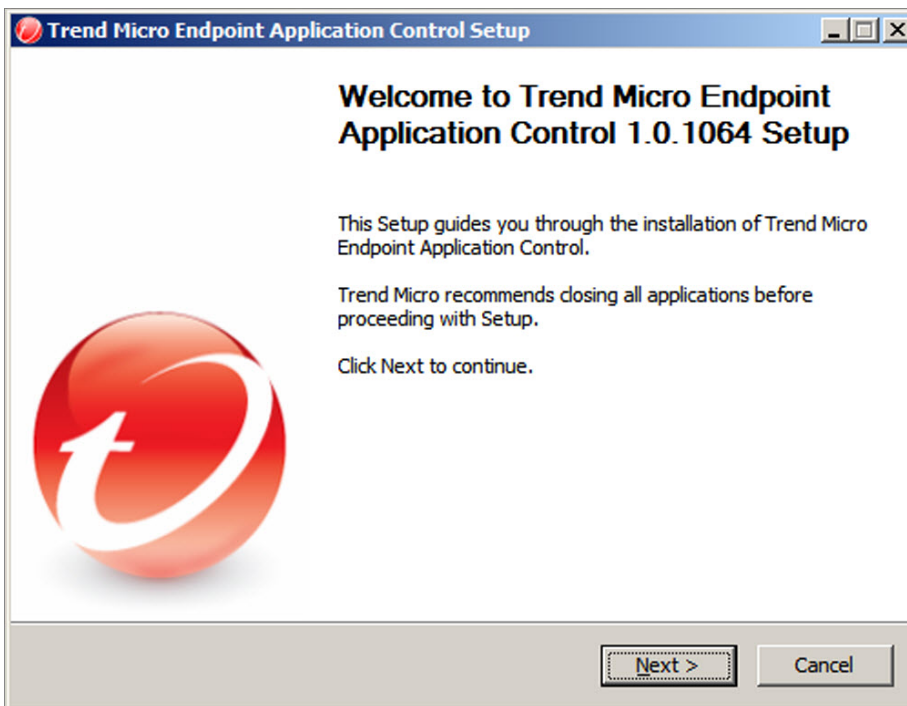


FIGURE 1-2. Welcome screen

Procedure

- Click **Next** to start installation.
-

License Agreement

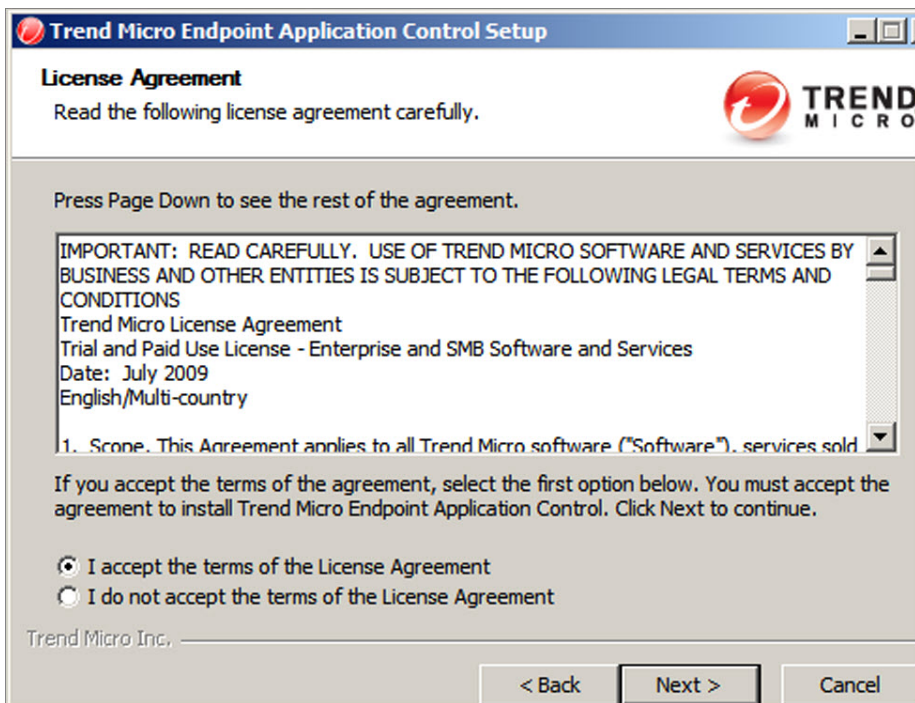


FIGURE 1-3. License Agreement screen

Read the license agreement carefully and accept the license agreement terms to proceed with installation. Installation cannot proceed without accepting the license agreement terms.

Proxy Server

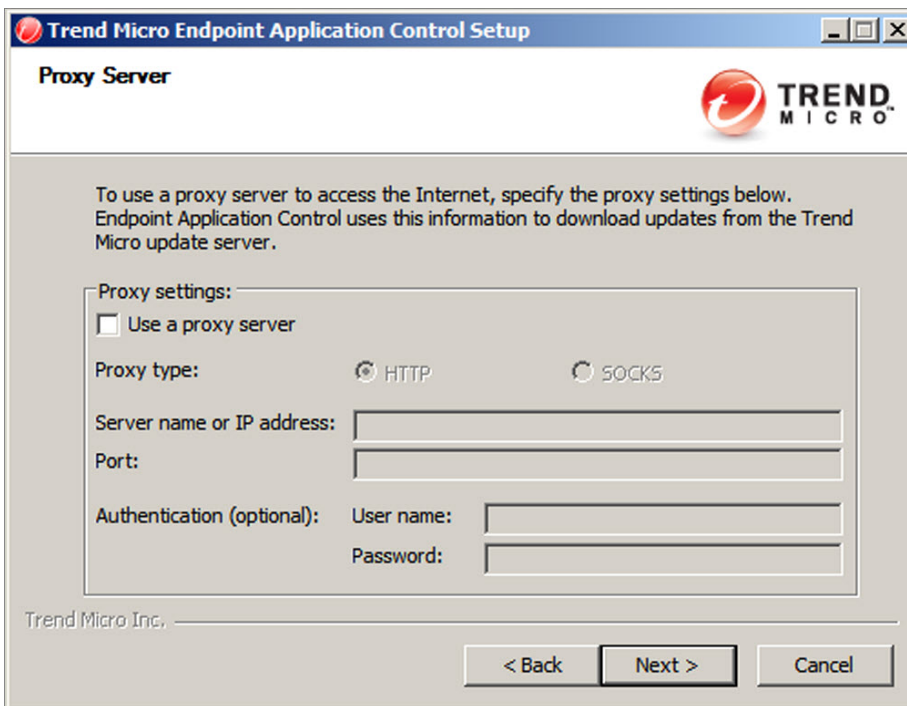


FIGURE 1-4. Proxy Server screen

The Endpoint Application Control server uses the HTTP protocol to connect to the Trend Micro ActiveUpdate server and registration server. If a proxy server handles Internet traffic on the network, Endpoint Application Control needs the proxy settings to ensure that the server can download updates from the ActiveUpdate server.

Administrators can skip specifying proxy settings during installation and do so after installation from the Endpoint Application Control web console.

IPv6 Support

When installing the Endpoint Application Control server on a pure IPv6 computer, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the ActiveUpdate server successfully.

Registration and Activation

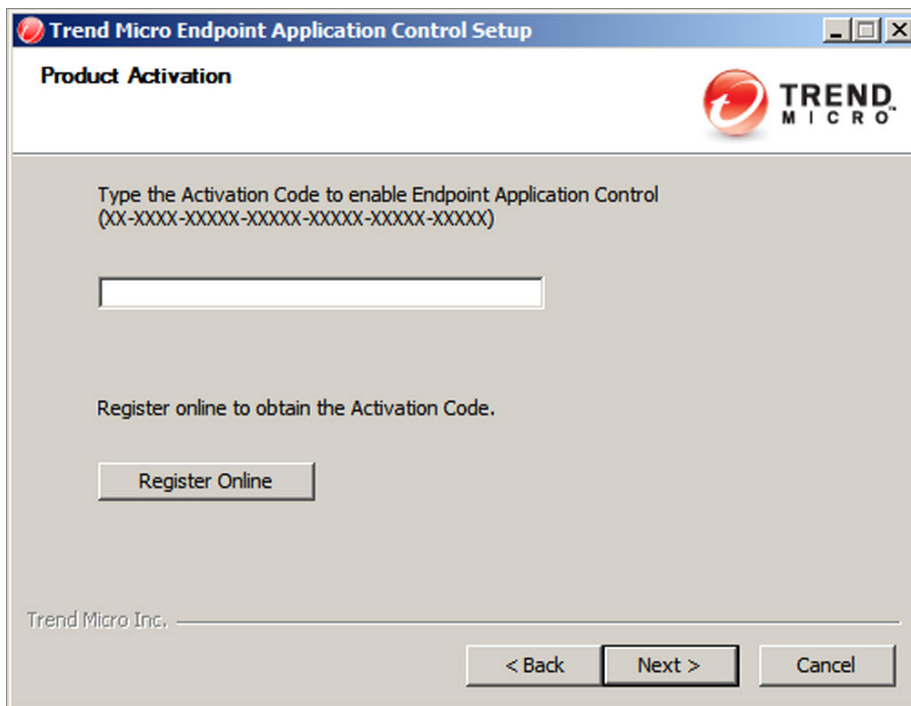


FIGURE 1-5. Product Activation screen

Register Endpoint Application Control using the Registration Key that came with the product and then obtain the Activation Codes. Skip this step if the Activation Codes are already available.

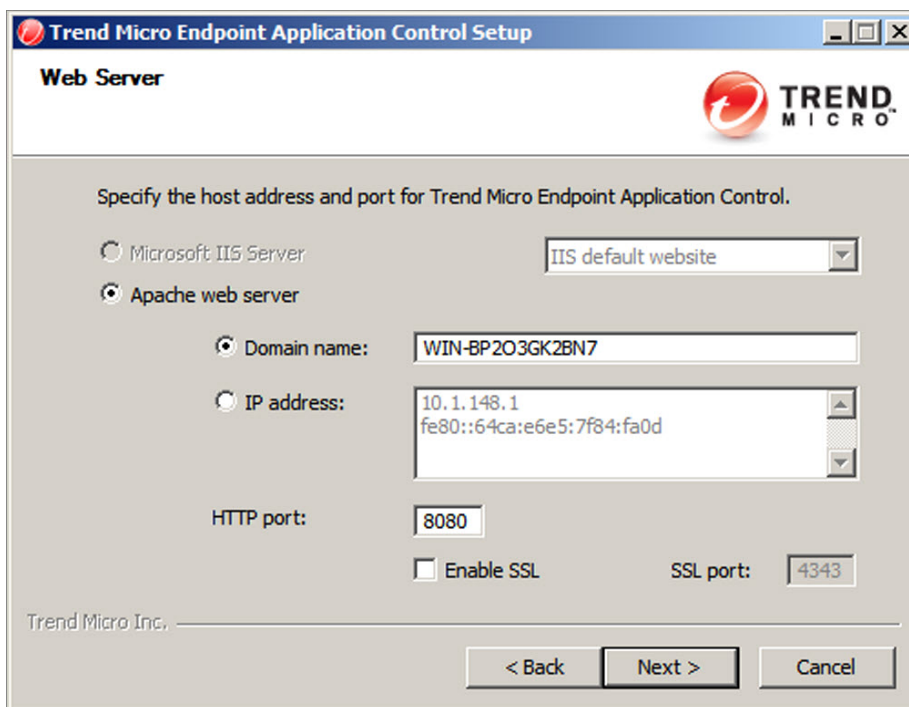
To obtain the Activation Codes, click **Register Online**. Setup opens the Trend Micro registration website. After completing the registration form, Trend Micro sends an email

with the Activation Codes. After receiving the codes, continue with the installation process.

When installing the Endpoint Application Control server on a pure IPv6 computer, set up a dual-stack proxy server that can convert between IP addresses. This allows the server to connect to the Trend Micro registration website successfully.

Specify the Activation Codes. The Activation Codes are case-sensitive.

Web Server



The screenshot shows the 'Web Server' configuration window of the Trend Micro Endpoint Application Control Setup. The window title is 'Trend Micro Endpoint Application Control Setup' and the sub-header is 'Web Server'. The Trend Micro logo is in the top right corner. The main instruction is 'Specify the host address and port for Trend Micro Endpoint Application Control.' There are two radio button options: 'Microsoft IIS Server' (unselected) and 'Apache web server' (selected). The 'IIS default website' is shown in a dropdown menu next to the IIS option. Under the 'Apache web server' option, there are three sub-options: 'Domain name:' with the value 'WIN-BP2O3GK2BN7', 'IP address:' with a list containing '10.1.148.1' and 'fe80::64ca:e6e5:7f84:fa0d', and 'HTTP port:' with the value '8080'. There is also an 'Enable SSL' checkbox (unchecked) and an 'SSL port:' field with the value '4343'. At the bottom left, it says 'Trend Micro Inc.' and at the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

FIGURE 1-6. Web Server screen

The Endpoint Application Control web server hosts the web console for administering Endpoint Application Control.

Web Server

If the setup process detects both IIS and Apache web servers installed on the target endpoint, then administrators can choose either of the two web servers, if using IIS 7.0 or Apache 2.4.7 (or later versions).

If a version of the Apache web server older than 2.0.x has been installed, then Endpoint Application Control will upgrade it to version 2.4.7 without removing the existing Apache web server.

If IIS is not installed, then the administrator must install version 2.4.7 of the Apache web server (included in the setup package).

If neither IIS nor the Apache web server has been installed before, then administrators cannot choose IIS and Endpoint Application Control will install Apache web server 2.4.7 automatically.

If using an Apache web server:

- Apache web server 2.0.x is required. If Apache web server exists on the computer but the version is not 2.0.x, Endpoint Application Control installs and uses version 2.4.7. Endpoint Application Control does not remove the existing Apache web server.
- If enabling SSL, and Apache web server 2.0.x exists, the Apache web server must have SSL settings pre-configured.
- By default, the administrator account is the only account created on the Apache web server.



Tip

Trend Micro recommends creating another account from which to run the web server. Otherwise, the Endpoint Application Control server may become compromised if a malicious hacker takes control of the Apache server.

- Before installing the Apache web server, refer to the Apache website for the latest information on upgrades, patches, and security issues.

If using an IIS web server:

- One of the following versions of Microsoft Windows Server is required:
 - Microsoft Windows Server 2008 or Windows Server 2008 R2
 - Standard or Enterprise Edition
 - 32-bit or 64-bit
 - Windows Server 2012 or Windows Server 2012 R2
- The following version of Microsoft Internet Information Server (IIS) is required:
 - Microsoft Internet Information Server (IIS) version 7.0 or later with the following modules:
 - CGI
 - ISAPI
 - ISAPI Extensions

When installing on an IIS web server, administrators must manually select and install these three components: CGI, ISAPI filters, and ISAPI extensions.

Do not install the web server on a computer running IIS-locking applications because this could prevent successful installation. See the IIS documentation for more information.

HTTP Port

SSL Support

Enable Secure Sockets Layer (SSL) for secure communication between the web console and the server. SSL provides an extra layer of protection against hackers. Although Endpoint Application Control encrypts the passwords specified on the web console before sending them to the Endpoint Application Control server, hackers can still sniff the packet and, without decrypting the packet, "replay" it to gain access to the console. SSL tunneling prevents hackers from sniffing packets traversing the network.

The SSL version used depends on the version that the web server supports.

When selecting SSL, Setup automatically creates an SSL certificate, which is a requirement for SSL connections. The certificate contains server information, public key, and private key.

The SSL certificate should have a validity period between 1 and 20 years. The administrator can still use the certificate after it expires. However, a warning message appears every time SSL connection is invoked using the same certificate.

How communication through SSL works:

1. The administrator sends information from the web console to the web server through SSL connection.
2. The web server responds to the web console with the required certificate.
3. The browser performs key exchange using RSA encryption.
4. The web console sends data to the web server using RC4 encryption.

Although RSA encryption is more secure, it slows down the communication flow. Therefore, it is only used for key exchange, and RC4, a faster alternative, is used for data transfer.

Web Server Ports

The following table lists the default port numbers for the web server

TABLE 1-1. Port Numbers for the Endpoint Application Control Web Server

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
Apache web server with SSL enabled	8080 (configurable)	4343 (configurable)
Apache web server with SSL disabled	8080 (configurable)	N/A
IIS default website with SSL enabled	80 (not configurable)	443 (not configurable)
IIS default website with SSL disabled	80 (not configurable)	N/A

WEB SERVER AND SETTINGS	PORTS	
	HTTP	HTTPS (SSL)
IIS virtual website with SSL enabled	8080 (configurable)	4343 (configurable)
IIS virtual website with SSL disabled	8080 (configurable)	N/A

Backend Server

Trend Micro Endpoint Application Control Setup

Backend Server

Specify the host address and port for Trend Micro Endpoint Application Control. Agents use this information to communicate with the server.

Domain name:

IP address:

HTTP port:

Enable SSL
 SSL port:

Trend Micro Inc.

FIGURE 1-7. Backend Server screen

Specify if Endpoint Application Control agents identify the server computer by its host (domain) name or IP address.

Communication between the server computer and agents is dependent on the specified IP address. Changing the IP address results in agents not being able to communicate with the Endpoint Application Control server. The only way to restore communication is to redeploy all the agents. The same situation applies if the server computer is identified by a host name that changes.

In most networks, the server computer's IP address is more likely to change than its host name, thus it is usually preferable to identify the server computer by a host name. Trend Micro recommends not changing the IP address if Endpoint Application Control obtains an IP address from a DHCP server.

When using static IP addresses, identify the server by its IP address. In addition, if the server computer has multiple network interface cards (NICs), consider using one of the IP addresses instead of the host name to ensure successful agent-server communication.

IPv6 Support

If the server manages IPv4 and IPv6 agents, it must have both IPv4 and IPv6 addresses and administrators must identify the server by its host name. If administrators identify the server by its IPv4 address, IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 agents connect to a server identified by its IPv6 address.


If the server manages only IPv6 agents, the minimum requirement is an IPv6 address. Server identification can be by its host name or IPv6 address. When administrators identify the server by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

TABLE 1-2. Port Numbers for the Endpoint Application Control Web Server

BACKEND SERVER	PORTS
HTTP	8085 (configurable)
HTTPS (SSL) if enable SSL setting	8443 (configurable)

Root Account

Trend Micro Endpoint Application Control Setup

Root Account 


Specify the root account information. Use letters, numbers, dashes, and underscores.

User name:

Full name:

Password:

Confirm password:

Trend Micro Inc. 

< Back **Next >** Cancel

FIGURE 1-8. Root Account screen

Specify the description, password, and then confirm the password.

Installation Path

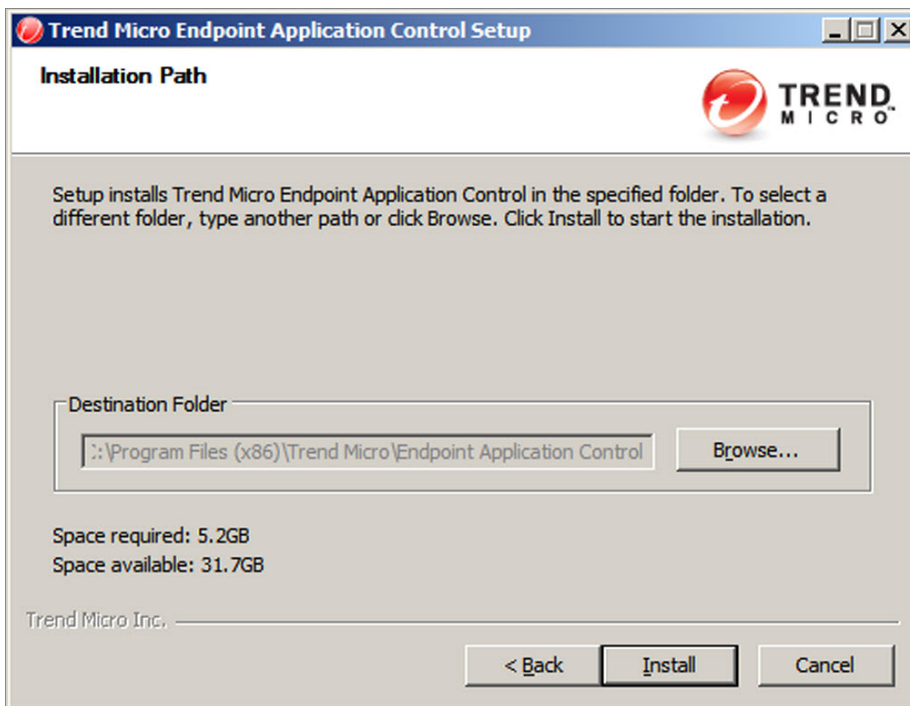


FIGURE 1-9. Installation Path screen

Accept the default installation path or specify a new one.

Installation Complete

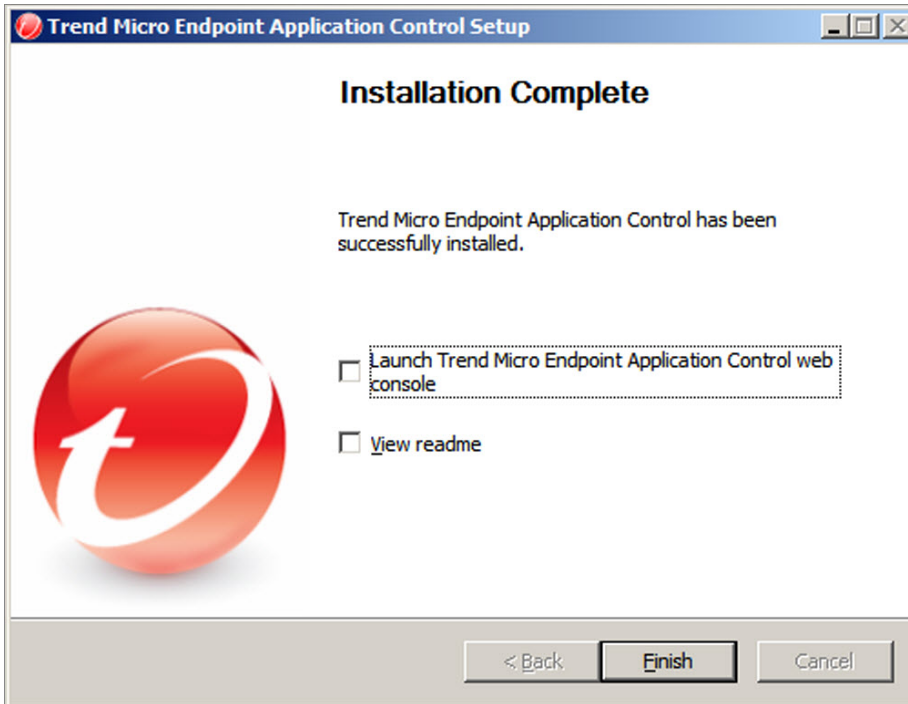


FIGURE 1-10. Installation Complete screen

When the installation is complete, view the readme file for basic information about the product and known issues.

Administrators can launch the web console to start configuring Endpoint Application Control settings.

Uninstalling the Endpoint Application Control Server Using the Uninstallation Program

Procedure

1. Run the uninstallation program. There are two ways to access the uninstallation program.
 - Method A
 - a. On the Endpoint Application Control server computer, click **Start > Programs > Trend Micro Endpoint Application Control > Uninstall Endpoint Application Control**. A confirmation screen appears.
 - b. Click **Yes**. The server uninstallation program prompts you for the administrator password.
 - c. Type the administrator password and click **OK**. The server uninstallation program starts removing the server files. A confirmation message appears.
 - d. Click **OK** to close the uninstallation program.
 - Method B
 - a. Double-click the Endpoint Application Control server program on the **Windows Add/Remove Programs** screen.
 - b. Click **Control Panel > Add or Remove Programs**. Locate and double-click **Trend Micro Endpoint Application Control**. Follow the on-screen instructions until you are prompted for the administrator password.
 - c. Type the administrator password and click **OK**. The server uninstallation program starts removing the server files. A confirmation message appears.
 - d. Click **OK** to close the uninstallation program.
-

Chapter 2

Getting Support

This describes how to contact support.

Topics in this :

- *Contacting Technical Support on page 2-2*
- *Speeding Up the Support Call on page 2-2*

Contacting Technical Support

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

Address: Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014

Phone: Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

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 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.

Index

A

activation, 1-7
Activation Code, 1-7
Apache web server, 1-9

E

Endpoint Application Control server
 identification, 1-12

I

IIS web server, 1-9
installation path
 server, 1-15

R

readme file, 1-16
registration, 1-7
RSA encryption, 1-11

S

SSL port, 1-10
SSL tunneling, 1-10
support
 contact technical support, 2-2
 resolve issues faster, 2-2

T

technical support, 2-2

U

uninstallation
 using the uninstallation program, 1-17

W

Web console, 1-16
Web server, 1-9



TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM16419/140430