TREND MICRO™

1.0 Trend Micro™ Endpoint Application Control

Administrator's Guide

Block Unwanted and Unknown Applications

Endpoint Security

Table of Contents

Chapter 4: Managing Endpoint Application Control Targets

Chapter 5: Enforcing Application Control on Users and Endpoints

Chapter 6: Monitoring the Endpoint Application Control Network

Chapter 7: Managing the Endpoint Application Control Server

Chapter 8: Getting Support

Index

Preface

Preface

Welcome to the Trend Micro™ Endpoint Application Control™ *chapter*. This document discusses getting started information, agent installation procedures, and Endpoint Application Control server and agent management.

Topics in this chapter:

Endpoint Application Control Documentation

Endpoint Application Control documentation includes the following:

TABLE 1. Endpoint Application Control Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing Endpoint Application Control.
Administrator's Guide	A PDF document that discusses getting started information, agent installation procedures, and Endpoint Application Control server and agent management.
Help	HTML files that provide "how to's", usage advice, and field-specific information. The Help is accessible from the Endpoint Application Control web console.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation.
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

Download the latest version of the PDF documents and readme at:

http://docs.trendmicro.com

Audience

Endpoint Application Control documentation is intended for administrators responsible for Endpoint Application Control management, including Endpoint Application Control installation and management. These administrators are expected to have advanced networking and server management knowledge.

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
 **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 Application Control documentation:

TABLE 3. Endpoint Application Control Terminology

TERMINOLOGY	DESCRIPTION
Endpoint Application Control agent	The Endpoint Application Control agent program
Endpoint	The computer where the Endpoint Application Control agent is installed
Agent user (or user)	The person managing the Endpoint Application Control agent on the endpoint
Server	The Endpoint Application Control server program
Server computer	The computer where the Endpoint Application Control server is installed
Administrator (or Endpoint Application Control administrator)	The person managing the Endpoint Application Control server
Console	The user interface for configuring and managing Endpoint Application Control server and agent settings The console for the Endpoint Application Control server program is called "web console", while the console for the Endpoint Application Control agent program is called "agent console".
Endpoint Application Control service	Services hosted through Microsoft Management Console (MMC). For example, `TMACServerService.exe`, the Trend Micro Endpoint Application Control Server Service.
Program	Includes the Endpoint Application Control agent and Plug-in Manager

TERMINOLOGY	DESCRIPTION

`Agent installation folder`	The folder on the endpoint that contains the Endpoint Application Control agent files. If administrators accept the default settings during installation, find the installation folder at any of the following locations:
	`C:\Program Files\Trend Micro\Acagent`
	`C:\Program Files (x86)\Trend Micro\Acagent`

`Server installation folder`	The folder on the endpoint that contains the Endpoint Application Control server files. If administrators accept the default settings during installation, find the installation folder at any of the following locations:
	`C:\Program Files\Trend Micro\Endpoint Application Control`
	`C:\Program Files (x86)\Trend Micro\Endpoint Application Control`
	For example, if a particular file is found under `\AcServer` on the server installation folder, the full path to the file is:
	`C:\Program Files\Trend Micro\Endpoint Application Control\AcServer\<file_name>`.

Dual-stack	An entity that has both IPv4 and IPv6 addresses. For example: • A dual-stack endpoint is a computer with both IPv4 and IPv6 addresses. • A dual-stack agent refers to a single agent installed on a dual-stack endpoint. • A dual-stack Update Agent distributes updates to agents. • A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses.
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

TERMINOLOGY	DESCRIPTION
Plug-in solutions	Native OfficeScan features and plug-in programs delivered through Plug-in Manager

Chapter 1

Getting Started with 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:

Accessing the Web Console

There are two ways to access the web console:

- Locally on the Endpoint Application Control server
- Remotely using any compatible browser

Accessing the Web Console Locally from the Endpoint Application Control Server

Procedure

1. Click **Start** > **Programs** > **Trend Micro Endpoint Application Control** > **Endpoint Application Control Server**.
2. Type the user name and password.
3. Click **Log On**.

Accessing the Web Console Remotely

Procedure

1. Type the following in the browser's address field to open the logon screen:

   `http(s)://{host name}:port/`

   Where `host name` is the Endpoint Application Control server's fully qualified domain name (FQDN), IP address, or server name.
2. Type the user name and password in the fields provided.
3. Click **Log On**.

Logon Account

During Endpoint Application Control server installation, Setup creates a root account as the default user account. When opening the web console for the first time, type "root" as the user name and the root account password. If you forget the password, contact the support provider for help in resetting the password.

Set up additional user accounts to allow other users to access the web console without using the root account. For more information, see *Understanding User Accounts on page 7-5*.

Using the Web Console

The web console is the central point for monitoring Endpoint Application Control throughout the corporate network. The console comes with a set of default settings and values that administrators can configure to comply with the corporate requirements and specifications.

Access the main menu items to perform the following tasks:

TABLE 1-1. Using the Web Console

TASKS	MAIN MENU ITEM
Monitor the usage of policies, rules, and applications using customizable widgets.	Dashboard
Manage targets, rules, and policies.	Management
View logs and configure log maintenance settings.	Logs
Update components and configure scheduled updates.	Updates
Manage the Endpoint Application Control server settings.	Administration

Configuring Web Console Time-out Settings

When the console times out, Endpoint Application Control requires user authentication (logging on) to access the web console.

Procedure

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

   The **Server Settings** screen appears.

2. Under **Endpoint Application Control Server**, specify the time to keep the logon session.

3. Click **Save**.

Chapter 2

Updating Components

Keep product components and programs up-to-date to ensure product functionality and control of the latest applications.

Topics in this chapter:

Endpoint Application Control Components and Programs

Trend Micro recommends keeping the components up-to-date to effectively control application usage.

The following table describes the available components and programs:

TABLE 2-1. Endpoint Application Control Components

COMPONENT	DESCRIPTION
Endpoint Application Control Agent 32-bit/64-bit	Trend Micro Endpoint Application Control agent programs for 32-bit and 64-bit platforms
Widget pool	Endpoint Application Control widget framework components
Trend Micro Certified Safe Software Service Pattern	Contains the latest application list

Configuring Update Settings

Procedure

1. Go to **Updates**.

   The **Component Updates** screen appears.

2. Under **Update Settings**, select the update source.

   - **Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server
   - **Other update source**: Specify the URL of the update source

3. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

Tip

Click **Save** before proceeding to the next step to keep the changes.

4. If a proxy server is in use on the network, click **Edit** to configure the settings on the **Proxy Settings** screen.

   See *Configuring External Proxy Settings on page 7-3* for more details.

Configuring Scheduled Updates

Procedure

1. Go to **Updates**.

   The **Component Updates** screen appears.

2. Click the **Scheduled Update** column to enable the function.
3. Click the **Update Schedule** column to expand the schedule settings.
4. Specify the update frequency by minute, hour, day, or week.
5. Specify the time the schedule starts to take effect in **Start time**.
6. Click **Save**.

Updating Components Manually

When updates become available, an **Update now** link appears in the **Latest Version** column.

Procedure

1. Go to **Updates**.

   The **Component Updates** screen appears.

2. Click **Update now**.

Chapter 3

Installing Endpoint Application Control Agents

Choose an installation method that best suits the requirements of the environment to install the agents.

Topics in this chapter:

Installation Methods

The Endpoint Application Control agent can be installed on endpoints running Microsoft Windows platforms. View the following website for a complete list of system requirements:

http://docs.trendmicro.com

Endpoint Application Control supports the following methods for agent installation:

- *Installing Endpoint Application Control Agents Using OfficeScan on page 3-3*
- *Installing Agents Using MSI Packages on page 3-4*
- *Installing MSI Packages Using Logon Scripts on page 3-5*
- *Deploying an MSI Package Using Active Directory on page 3-5*
- *Deploying an MSI Package Using Microsoft SMS on page 3-7*

Installation Considerations

Before installing agents, consider the following:

TABLE 3-1. Agent Installation Considerations

CONSIDERATION	DESCRIPTION
IPv6 support	The Endpoint Application Control agent can be installed on dual-stack or pure IPv6 agents. However: • Some of the Windows operating systems to which the Endpoint Application Control agent can be installed do not support IPv6 addressing. • For some of the installation methods, there are special requirements to install the Endpoint Application Control agent successfully.

CONSIDERATION	DESCRIPTION
Endpoint Application Control agent IP addresses	For agents with both IPv4 and IPv6 addresses, you can choose which IP address will be used when the agent registers to the server.

Agent IP Addresses

Short Name servers installed in an environment that supports IPv6 addressing can manage the following Endpoint Application Control agents:

- Short Name servers installed on pure IPv6 host machines can manage pure IPv6 agents.
- Short Name servers installed on dual-stack host machines and have been assigned both IPv4 and IPv6 addresses can manage pure IPv6, dual-stack, and pure IPv4 agents.

After you install or upgrade agents, the agents register to the server using an IP address.

- Pure IPv6 agents register using their IPv6 address.
- Pure IPv4 agents register using their IPv4 address.
- Dual-stack agents register using either their IPv4 or IPv6 address. You can choose the IP address that these agents will use.

Installing Endpoint Application Control Agents Using OfficeScan

Perform this task in the OfficeScan Plug-in Manager. For more information on using the plug-in program, refer to the *Trend Micro Endpoint Application Control Plug-in Program Help* in the plug-in program console.

Use the OfficeScan agent tree to install Endpoint Application Control agents.

Before performing this task, configure the Endpoint Application Control server settings in the plug-in program console.

Procedure

1. Open the plug-in program console.
2. Click **Agent Management**.
3. In the OfficeScan agent tree, click the root domain icon () to include all agents or select specific domains or agents.
4. Click **Install Agent**.

   A confirmation message appears. Allow some time for the command to propagate to all agents.
5. Go to the **Logs** screen to verify the installation status.

Downloading MSI Packages

Use the following methods to download the MSI package:

- Click the link on the logon screen of the Endpoint Application Control server web console
- Specify the link in a web browser:

  ```
  http://<server address>:<port>/acserver/downloads/agent-win32/latest/AcAgentSetup_x86.msi
  ```

  ```
  http://<server address>:<port>/acserver/downloads/agent-win64/latest/AcAgentSetup_x64.msi
  ```

Installing Agents Using MSI Packages

Procedure

1. Download the MSI package to the target endpoint.

2. On the **Command Prompt** screen, run `msiexec /i AcAgentSetup_x86.msi ServerHost=<server address>:<port>`.

Installing MSI Packages Using Logon Scripts

Procedure

1. Download the MSI package.
2. Copy the MSI package to a shared folder accessible to users.
3. Create a logon script that installs the agent when endpoints join domains.

   For example:

```
@ECHO OFF

if not exist "%programfiles%\Trend Micro\Endpoint
Application Control Agent\AcAgent.exe"msiexec /i \\<shared
folder address>\AcAgentSetup_x86.msi ServerHost=<server
address>:<port>
```

Deploying an MSI Package Using Active Directory

Take advantage of Active Directory features to deploy the MSI package simultaneously to multiple endpoints.

Procedure

1. Perform the following:
   - For Windows Server 2003 and lower versions:
     a. Open the Active Directory console.

b. Right-click the Organizational Unit (OU) where you want to deploy the MSI package and click **Properties**.

c. In the **Group Policy** tab, click **New**.

- For Windows Server 2008 and Windows Server 2008 R2:

  a. Open the Group Policy Management Console. Click **Start** > **Control Panel** > **Administrative Tools** > **Group Policy Management**.

  b. In the console tree, expand **Group Policy Objects** in the forest and domain containing the GPO that you want to edit.

  c. Right-click the GPO that you want to edit, and then click **Edit**. This opens the Group Policy Object Editor.

- For Windows Server 2012:

  a. Open the Group Policy Management Console. Click **Server Management** > **Tools** > **Group Policy Management**.

  b. In the console tree, expand **Group Policy Objects** in the forest and domain containing the GPO that you want to edit.

  c. Right-click the GPO that you want to edit, and then click **Edit**. This opens the Group Policy Object Editor.

2. Choose between Computer Configuration and User Configuration, and open **Software Settings** below it.

Tip

Trend Micro recommends using **Computer Configuration** instead of **User Configuration** to ensure successful MSI package installation regardless of which user logs on to the endpoint.

3. Below Software Settings, right-click **Software installation**, and then select **New** and **Package**.

4. Locate and select the MSI package.

5. Select a deployment method and then click **OK**.

- **Assigned**: The MSI package is automatically deployed the next time a user logs on to the endpoint (if you selected User Configuration) or when the endpoint restarts (if you selected Computer Configuration). This method does not require any user intervention.
- **Published**: To run the MSI package, inform users to go to Control Panel, open the Add/Remove Programs screen, and select the option to add/install programs on the network. When the Endpoint Application Control agent MSI package displays, users can proceed to install the Endpoint Application Control agent.

Deploying an MSI Package Using Microsoft SMS

Deploy the MSI package using Microsoft System Management Server (SMS) if you have Microsoft BackOffice SMS installed on the server.

The SMS server needs to obtain the MSI file from the Short Name server before it can deploy the package to target endpoints.

The instructions below assume that the SMS server and the Short Name server are on the same endpoint.

Known issues when installing with Microsoft SMS:

- "Unknown" appears in the Run Time column of the SMS console.
- If the installation was unsuccessful, the installation status may still show that the installation is complete on the SMS program monitor.

The following instructions apply if you use Microsoft SMS 2.0 and 2003.

Obtaining the Package Locally

Procedure

1. Open the SMS Administrator console.

2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New** > **Package From Definition**.

   The **Welcome** screen of the Create Package From Definition Wizard appears.
4. Click **Next**.

   The **Package Definition** screen appears.
5. Click **Browse**.

   The **Open** screen appears.
6. Browse and select the MSI package file, and then click **Open**.

   The MSI package name appears on the **Package Definition** screen. The package shows "Endpoint Application Control agent" and the program version.
7. Click **Next**.

   The **Source Files** screen appears.
8. Click **Always obtain files from a source directory**, and then click **Next**.

   The **Source Directory** screen appears, displaying the name of the package you want to create and the source directory.
9. Click **Local drive on site server**.
10. Click **Browse** and select the source directory containing the MSI file.
11. Click **Next**.

    The wizard creates the package. When it completes the process, the name of the package appears on the **SMS Administrator** console.

Distributing the Package to Target Endpoints

Procedure

1. On the **Tree** tab, click **Advertisements**.

2. On the **Action** menu, click **All Tasks** > **Distribute Software**.

   The **Welcome** screen of the **Distribute Software Wizard** appears.

3. Click **Next**.

   The **Package** screen appears.

4. Click **Distribute an existing package**, and then click the name of the Setup package you created.

5. Click **Next**.

   The **Distribution Points** screen appears.

6. Select a distribution point to which you want to copy the package, and then click **Next**.

   The **Advertise a Program** screen appears.

7. Click **Yes** to advertise the Endpoint Application Control agent Setup package, and then click **Next**.

   The **Advertisement Target** screen appears.

8. Click **Browse** to select the target computers.

   The **Browse Collection** screen appears.

9. Click **All Windows NT Systems**.

10. Click **OK**.

    The **Advertisement Target** screen appears again.

11. Click **Next**.

    The **Advertisement Name** screen appears.

12. In the text boxes, type a name and your comments for the advertisement, and then click **Next**.

    The **Advertise to Subcollections** screen appears.

13. Choose whether to advertise the package to subcollections. Choose to advertise the program only to members of the specified collection or to members of subcollections.

14. Click **Next**.

    The **Advertisement Schedule** screen appears.

15. Specify when to advertise the Endpoint Application Control agent Setup package by typing or selecting the date and time.

Note

If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes. This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.

16. Click **Next**.

    The **Assign Program** screen appears.

17. Click **Yes, assign the program**, and then click **Next**.

    Microsoft SMS creates the advertisement and displays it on the SMS Administrator console.

18. When Microsoft SMS distributes the advertised program (that is, the Endpoint Application Control agent program) to target computers, a screen displays on each target endpoint. Instruct users to click **Yes** and follow the instructions provided by the wizard to install the Endpoint Application Control agent to their computers.

Chapter 4

Managing Endpoint Application Control Targets

This chapter describes Endpoint Application Control target management and configurations.

Topics in this chapter:

Understanding Target Management

In Endpoint Application Control, a target refers to an endpoint logged on with a specific user. Administrators can use the **Target Management** screen to perform the following tasks:

- Look up specific targets using the target tree or search function
- View policies assignment on targets
- Enable or disable application control on specific targets
- Export the target list

TABLE 4-1. Target Management Screen

ITEM	DESCRIPTION
Target tree	Endpoint Application Control or OfficeScan domain groups
Search function	Finds specific users or endpoints
Display all logon records	Displays all users that have logged on to a particular endpoint. For example, if two users have logged on to the same endpoint, the target list displays three records for this endpoint. If multiple users log into the same machine, each user generates one more instance. For example, if two users log into the same machine, three instances will appear on the console if you display all logon records. • WIN2008$ - system • administrator - login user 1 • administrator2 - login user 2

ITEM	DESCRIPTION
Enable/Disable Application Control	Select targets from the list and click one of the two buttons to enable or disable application control on the selected targets.
Export to CSV	Exports the target list
Endpoint	Endpoint name
User	• Displays when administrators select **Displays all logon records** • User name
Last Logon User	Displays the last user who has logged on to the endpoint
Operating System	Operating system type
Policy	Policy assigned to the target
Policy Status	• Compliant: The target has received the up-to-date policy • Non-compliant: Administrators have updated the policy settings, but the target has not yet received the changes.
Last Update	The most recent time and date when the target connected to the Endpoint Application Control server to receive policy updates
Application Control	Whether administrators have enabled or disabled application control on the target

Understanding the Endpoint Application Control Target Tree

Endpoint Application Control provides the following ways for administrators to manage users and endpoints in the Endpoint Application Control server web console:

- Domain: Constructed based on Endpoint Application Control agent users and endpoints
- OfficeScan target tree

  To import target information using the OfficeScan target tree, see *Installing Endpoint Application Control Agents on page 3-1* for more details.

Chapter 5

Enforcing Application Control on Users and Endpoints

This chapter describes how to use rules and policies to control application usage on users and endpoints.

Topics in this chapter:

Understanding Application Control

Endpoint Application Control uses policy management to enforce application control on users and endpoints. Administrators can define specific rules for application usage and assign policies to specific users and endpoints.

To enforce application control, administrators need to complete the following tasks:

- Define rules and specify applications to control
- Create and assign policies to users and endpoints

Understanding Rule Management

Endpoint Application Control provides the following types of rules to control application usage:

- **Allow**: Allows usage of specific applications
- **Block**: Blocks usage of specific applications
- **Lockdown**: Blocks any new installation except for specified applications. Users can still run applications already installed and allowed on endpoints.

After creating rules, adminsitrators can select the rules to include in different policies. There is no limit as how many times a rule can be reused, but if administrators make changes to a rule, the changes affect all policies using the rule.

Use the **Rule Management** to perform the following tasks:

- Create or edit rules
- Manage the rule list
- Check how rules have been used in policies in the **Policy Instances** column

Specifying Applications to Control

Endpoint Application Control provides the following methods for administrators to specify applications when creating rules:

Trend Micro Certified Safe Software Service

Trend Micro Certified Safe Software Service is a complete and comprehensive collection of good files covering most popular operating system files and binaries as well as applications, programs, and software for desktops, servers, and mobile devices. Trend Micro periodically provides updates to the safe software list. Administrators can check for updates from the **Component Updates** screen.

Path Expressions

Use this method to control applications by file path. Administrators can also use this method to control access to USB flash drives and network drives. Combine the expression with variables that are platform independent to effectively control applications.

Endpoint Application Control supports the following path expressions:

- **Global**: Typical file paths
- **Regular**: Perl Compatible Regular Expressions (PCRE)

Administrators can use the following variables in path expressions:

TABLE 5-1. Path Expression Variables

VARIABLE	DESCRIPTION
$ProgramFiles	Path that contains most applications installed on the endpoint • Windows: %ProgramFiles% and %ProgramFiles(x86)%
$SystemDrive	Hard drive or path that contains the root partition of the system • Windows: %SystemDrive%
$LocalDrives	Hard drives that physically connect to endpoints, including internal and external drives
$FixedDrives	Internal hard drives
$RemovableDrives	Removable drives, such as CD/DVD drives and USB flash drives
$RemoteDrives	Network drives

Certificate Attributes

Use this method to specify certificate attributes to match in subjects and issuers.

Administrators can specify the following:

- Common Name (CN)
- Organization (O)
- Organizational Unit (OU)
- Location (L)
- Country (C)
- State (S)

File Signatures (SHA-1)

Use one of the following methods to add file signature information:

- Obtain file signatures directly from executable files
- Use an existing SHA-1 list
- Specify file signatures manually

Creating a Rule

Procedure

1. Go to **Management** > **Rules**.

   The **Rule Management** screen appears.

2. Click **Create**.

   The **Create Rule** screen appears.

3. Select a rule type.

Option	Description
Allow	Allows usage of specific applications
Block	Blocks usage of specific applications
Lockdown	Blocks any new installation except for specified applications. Users can still use applications currently installed and allowed on endpoints.

   Endpoint Application Control automatically assigns a name to the rule in the **Name** field.

4. (Optional) To specify a rule name manually, click the **Name** field and start typing.

Tip

To restore the naming feature, press the `Esc` key. If the same naming rule already exists, the autonaming function will not create a duplicate name. You must manually type the name of the rule in this case.

5. Select an option from the **Method** list to specify applications to control. Administrators can use one method in each rule.

   See *Specifying Applications to Control on page 5-3* for more information on each method.

Option	Description
Trend Micro Certified Safe Software Service	Use the search field or browse through the list to selectapplications. You can use a wildcard character (*) to search, but the search results will always include terms that begin with what you entered. For example, a search for "Microsoft" will include "Microsoft Lync" in the results, but you should use "*Lync" if you specifically wanted to find Microsoft Lync.
Path expressions	Specify the path expression in the field and click **Add**. Repeat this procedure to add additional expressions to the list. • **Global**: Start the path with `glob:`. Use this option to define typical file paths. • **Regular**: Start the path with `regexp:`. Use this option to define Perl Compatible Regular Expressions (PCRE). **Tip** Before adding a path expression to the list, use the **Test path** field to verify the expression.
Certificate attributes	a. Specify the certificate attributes and click **Add**. Repeat this procedure to add additional attributes to the list. b. Select an validity option from the **Certificate validity** list and determine the validity of expired certificates.
File signatures (SHA-1)	Use one of the following options to add file signatures: • **Obtain from executable file**: Click **Browse** to select an excecutable file and click **Add**. Repeat this procedure to add additional file signatures to the list.

Option	Description
	• **Specify SHA-1 manually**: Type the file signature in the field and click **Add**. Repeat this procedure to add additional file signatures to the list. • **Upload SHA-1 list**: Click **Browse** to select a SHA-1 list and click **Add**.

6. To test the rule, select **Enable Assessment Mode**.

   Endpoint Application Control logs the events related to the rule without taking the specified action.

7. To prevent accidental modification to the rule, select **Lock rule modification**.

8. Click **Save**.

Editing a Rule

Note

Editing a rule can affect all policies currently using the rule.

Procedure

1. Go to **Management** > **Rules**.

   The **Rule Management** screen appears.

2. Click the rule to edit.

   The **Edit Rule** screen appears.

3. If the rule is locked, click **Unlock** and deselect **Lock rule modification**.

4. Make changes to the rule.

5. Click **Save**.

Understanding Policy Management

Policy management allows administrators to enforce application control and agent settings on users and endpoints. Administrators create a policy by selecting the targets and configuring a list of settings.

A policy consists of the following items:

- Policy name
- Targets: Administrators can assign a policy to a specific combination of users and endpoints
- Settings: Contain rules and agent settings

Use the **Policy Management** screen to perform the following tasks:

- *Creating a Policy on page 5-9*
- *Editing a Policy on page 5-13*
- *Copying Policy Settings on page 5-13*
- *Reordering the Policy List on page 5-14*

The policy list displays the information and status of policies created by all users. When a user logs on to an endpoint, the target goes through the policy list in descending order. Endpoint Application Control assigns the target to a policy with matching target criteria. One policy can apply to multiple filtering targets, but a given target can only be affected by one policy.

The following table describes the items in the policy list:

TABLE 5-2. Policy List

MENU ITEM	DESCRIPTION
Priority	• Priority of the policies • Endpoint Application Control lists policies from the highest to the lowest priority • When administrators create a new policy, Endpoint Application Control saves the new policy as the lowest priority policy.
Policy	Name of the policy
Compliant Targets	Number of targets with up-do-date policy settings
Non-Compliant Targets	Number of targets with outdated policy settings. Click a number in the column to check target details.
Creator	User who created the policy
Targets without policies	Number of targets to which Endpoint Application Control has not assigned a policy
Total targets	Number of targets available for policy management

Creating a Policy

Procedure

1. Go to **Management** > **Policies**.

   The **Policy Management** screen appears.

2. Click **Create**.

   The **Create Policy** screen appears.

3. Type a name in the **Policy Name** field.

4. In the **Targets** section, click **Select**.

   The **Targets** screen appears.

5. Select and define the target criteria. Endpoint Application Control assigns the policy to a target that matches all of the selected criteria.

Option	Description
Host name	Define keywords based on the host name.
IP addresses	Define the IP address range.
Operating systems	Select operating systems.
Target tree	Select a group from the target tree.
Active Directory users/groups	Specify users or groups. To obtain Active Directory user and group information, see *Active Directory Integration on page 7-3* for more details.

6. Click **Save**.

   The **Targets** screen closes and returns to the **Create Policy** screen.

7. Under the settings section, click a feature to expand the tab and then configure the settings.

   See *Configuring Endpoint Application Control Target Settings on page 5-10* for more information on configuring each feature.

8. Click **Deploy**.

Configuring Endpoint Application Control Target Settings

Configure the following settings to create a policy:

- *Specifying Rules on page 5-11*
- *Configuring Log Settings on page 5-11*
- *Configuring Policy and Log Update Settings on page 5-12*
- *Configuring Server Connection Settings on page 5-12*

- *Configuring Privileges and Other Settings on page 5-13*

Specifying Rules

Endpoint Application Control processes the rule list in the following mannar:

- Rule priority: Allow > Block > Lockdown

  Endpoint Application Control combines and processes criteria from the same type of rules.

- Application method priority: Trend Micro Certified Safe Software Service/File signatures > Path expressions > Certificate attributes

  Endpoint Application Control uses the above priority when the rules in the same policy specify the same application using different methods.

Procedure

- Click **Add existing rules** to open the **Rule Management** screen and select the rules to include in the policy.
- Click **Create a rule** to create and add a new rule to the policy.

  Endpoint Application Control also adds the new rule to the **Rule Management** screen.

Configuring Log Settings

Procedure

1. Select an option from **Log** to log specific types of rules.

Option	Description
None	Does not log any rule included in the policy
Only block and lockdown rules	Only logs the block and lockdown rules

Option	Description
Specific rules	Logs specific rules. Use the list that appears to select the rules.
All executed applications	Logs all rules included in the policy. This option can generate large amounts of data.

2. Select **Exclude the following paths from log records** and specify the path. Separate each path with commas.
3. Specify the frequency to aggregate logs.

Configuring Policy and Log Update Settings

Procedure

- Select a time from **Update interval** for Endpoint Application Control to update policy and log settings.
- Specify the type of targets to perform a full policy update. Performing a full policy update may increase network traffic.

Configuring Server Connection Settings

Procedure

- Specify the Endpoint Application Control server for the targets to connect to.
  - **Default server**: The current server
  - **Specific server**: A different server

    This option is useful to redirect agents when the Endpoint Application Control server has moved to another location with a new server address.
- Select **Use secure and validated HTTPS for the connection** if necessary.

Configuring Privileges and Other Settings

Procedure

- To hide or show the agent icon in the system tray, turn on or off the option. You can also control how often the endpoint will be scanned to determine if any applications have been added or removed. First select either a daily or a weekly scan, and then decide what time the scan should begin.

Copying Policy Settings

Administrators can copy the settings from an existing policy, create a new policy with the same settings, and deploy the settings to different targets.

Procedure

1. Go to **Management** > **Policies**.

   The **Policy Management** screen appears.

2. Select a policy from the list.

3. Click **Copy Settings**.

   The **Copy and Create Policy** screen appears.

4. Type a name in the **Policy Name** field.

5. Assign targets to the policy.

6. Click **Deploy**.

Editing a Policy

Administrators can change the information of a policy including the policy name, targets, and settings.

Procedure

1. Go to **Management** > **Policies**.

   The **Policy Management** screen appears.

2. Click a policy name in the **Policy** column.

   The **Edit Policy** screen appears.

3. Modify the policy.

   Note

   Editing the target criteria can affect target allocation. Endpoint Application Control may re-assign some targets to other policies, or add additional targets to the current policy.

4. Click **Deploy**.

Reordering the Policy List

Use the **Reorder** button to change the order of the policies. Rearranging the policy list can affect target allocation. Endpoint Application Control may re-assign some targets to different policies.

Procedure

1. Go to **Management** > **Policies**.

   The **Policy Management** screen appears.

2. Click **Reorder**.

   The **Reorder Policies** screen appears.

3. Rearrange the order of the **Priority** column.

4. Click **Save**.

Chapter 6

Monitoring the Endpoint Application Control Network

This chapter describes how to use the dashboard and work with logs.

Topics in this chapter:

Using the Dashboard

The Endpoint Application Control dashboard provides at-a-glance information for the Endpoint Application Control network. The dashboard contains the following components:

- **Tabs:** Allow administrators to create a screen that contains one or more widgets
- **Widgets:** Provide specific information about various events

Understanding Tabs

The Endpoint Application Control dashboard uses tabs to provide flexibility for administrators. Tabs provide a container for widgets allowing administrators to create their own customized dashboard. The dashboard supports up to 30 tabs per user account.

Administrators can move widgets on tabs by dragging widgets to various locations on the tab. The layout for a tab determines where widgets can be placed.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Adding a Tab

Procedure

1. Go to **Dashboard**.
2. Click the add icon next to the tab on the far right.

   The **New Tab** screen appears.
3. Specify the following:
   - **Title**: Name of the tab

- **Layout**: The number of widgets that administrators can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, administrators need to remove a widget from the tab or create a new tab for the widget.
- **Auto-fit**: Enable auto-fit if the selected layout contains several boxes and each box contains only one widget. Auto-fit adjusts a widget to fit the height of a box.

4. Click **Save**.

   The empty tab appears on the dashboard.

5. Click **Add Widget** to populate the tab with widgets.

Editing a Tab

Procedure

1. Go to **Dashboard**.
2. Select a tab and click **Tab Settings**.

   The **Tab Settings** screen appears.

3. Change the tab name, layout, or auto-fit settings.
4. Click **Save**.

Understanding Widgets

Widgets are the core components for the dashboard. Tabs provide the layout and widgets provide the actual data for the dashboard.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Update the Endpoint Application Control widget pool (under **Widget pool** on the **Component Updates** screen) periodically to get new or updated widgets.

Using Widgets

Each widget provides information about the Endpoint Application Control, policy and rule events, and user and endpoint events. Widgets can display information in one of the following ways:

- Bar chart
- Pie chart
- Line chart
- Table

Click the help icon on a widget to view detailed information on using the widget.

Widget List

The following table describes the widgets available for the dashboard:

TABLE 6-1. Widget List

WIDGET	DESCRIPTION
Target Management	Connection status of Endpoint Application Control agents
System Summary	Essential system information
Top Block and Lockdown Applications	Applications that have triggered the most block and lockdown rules
Top Block and Lockdown Rules	Block and lockdown rules that have triggered the most instances
Top Triggered Policies	Policies in which the block and lockdown rules have triggered the most instances

WIDGET	DESCRIPTION
Top Block and Lockdown Users	Users that have triggered the most block and lockdown rules
Top Block and Lockdown Endpoints	Endpoints that have triggered the most block and lockdown rules
Top Applied Policies	Policies that have been assigned to the most targets
Top Unmanaged Applications	Applications that are not managed by any rules
Top Used Applications	Applications that have been run the most

Adding a Widget

Procedure

1. Go to any tab on the dashboard.
2. Click **Add Widget**.

   The **Add Widget** screen appears.
3. Select one or more widgets to add to a tab.
4. Click **Add**.

Editing a Widget

Procedure

1. Go to **Dashboard**.
2. Find a widget with an edit icon.
3. Click the **Edit** icon on the widget.
4. Change the widget name and any other settings available on the widget.

Note

Click the Help icon on the widget for more information on the available settings.

5. Click **Save**.

   The widget reloads applying the new settings.

Working with Logs

Endpoint Application Control records events related to the server, agents, and policies. Use these logs to verify server performance and monitor incidents of inappropriate application usage.

Endpoint Application Control logs the following events:

- Policy violations
- Administrator activities
- Endpoint events
- Server events

Querying Logs

Procedure

1. Go to **Logs** > **Log Query**.

   The **Log Query** screen appears.

2. Select a log type from the list.

   The screen refreshes to load data for the specified log type.

3. Specify the dates in **From** and **To** to filter data.

Deleting Logs

To keep the size of logs from occupying too much space on the hard disk, configure log deletion schedules from the web console.

Procedure

1. Go to **Logs** > **Log Maintenance**.

   The **Log Maintenance** screen appears.

2. Specify the following for all logs:

   - **Maximum Log Size**: When logs reach this size, Endpoint Application Control delete these logs automatically.
   - **Maximum Log Age**: When logs reach this age, Endpoint Application Control delete these logs automatically.

3. Specify the diagnostic log level for diagnostic logs.

4. Click **Save**.

Chapter 7

Managing the Endpoint Application Control Server

This chapter describes Endpoint Application Control server management and configurations.

Topics in this chapter:

Configuring Proxy Server Settings

Configure the internal and external proxy settings for agent connection and component updates.

Internal Proxy Server System Requirements

- Support for HTTP 1.1
- Squid 3.2 or higher
- Basic authentication support with:
  - System proxy (without a username and password)
  - Defined Proxy (with or without a username and password
  - Proxy mode support: HTTP, SOCKS, SOCKS4, SOCKS4a, SOCKS5

Configuring Internal Proxy Settings

Endpoint Application Control agents use internal proxy settings to connect to the Endpoint Application Control server to update components, obtain policy settings, and send logs.

Procedure

1. Go to **Administration** > **Proxy Settings**.

   The **Proxy Settings** screen appears.

2. Under the **Internal** section, select **Use the following settings for agent communication**.

3. Select one of the following:

   - **Proxy settings configured on endpoints**: Endpoint Application Control agents use the proxy settings configured in Internet Explorer

- **Specific proxy settings**: Endpoint Application Control agents use specific proxy settings. Specify the proxy server information.

4. Click **Save**.

Configuring External Proxy Settings

Endpoint Application Control uses the external proxy to download updates from the Trend Micro ActiveUpdate server and manage the product license.

Procedure

1. Go to **Administration** > **Proxy Settings**.

   The **Proxy Settings** screen appears.

2. Under the **External** section, select **Use the following settings for pattern, engine, and license updates**.

3. Select one of the following:

   - **Proxy settings configured on endpoints**: The Endpoint Application Control server uses the proxy settings configured in Internet Explorer
   - **Specific proxy settings**: The Endpoint Application Control server uses specific proxy settings. Specify the proxy server information.

4. Click **Save**.

Active Directory Integration

Integrate Endpoint Application Control with the Microsoft Active Directory structure to assign user-based policies to control application usage.

Procedure

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

The **Server Settings** screen appears.

2. Under **Active Directory Server**, specify the user name and password to access the Active Directory server.

3. Click **Save**.

   Endpoint Application Control starts to discover and connect to the Active Directory server automatically.

Note

When connection has been lost in a network environment containing multiple Active Directory servers, Endpoint Application Control tries to discover a different Active Directory server automatically.

Configuring Active Directory Server Manually

If Endpoint Application Control cannot discover the Active Directory server automatically, administrators can choose to configure one manually.

Procedure

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

   The **Server Settings** screen appears.

2. Under **Active Directory Server**, type the user name and password to access the Active Directory server.

3. Select **Manual settings**.

4. In the area that expands, specify the server information.

5. Click **Save**.

Understanding User Accounts

Set up user accounts and assign a particular role to each user. The user role determines the web console menu items a user can view or configure.

During Endpoint Application Control server installation, Setup automatically creates a built-in account called "root". Users who log on using the root account can access all menu items. You cannot delete the root account but you can modify account details, such as the password and full name or the account description. If you forget the root account password, contact your support provider for help in resetting the password.

Understanding User Roles

A user role determines the web console menu items accessible to a user. Endpoint Application Control provides the following user roles:

- **Administrator**: Views and configures all menu items
- **Guest**: Views and configures the dashboard and user account information

Creating a User Account

Procedure

1. Go to **Administration** > **User Accounts**.

   The **User Accounts** screen appears.

2. Click **Create**.

   The **Create Account** screen appears.

3. Select a role for the account.

4. Type the user name, full name, and password and then confirm the password.

5. Click **Save**.

   Endpoint Application Control adds the account to the **User Accounts** list.

6. Click the icon under **Status** to enable the account.

Editing a User Account

Procedure

1. Go to **Administration** > **User Accounts**.

   The **User Accounts** screen appears.

2. Click a user account.

   The **Edit Account** screen appears.

3. Modify the account information

4. Click **Save**.

Enabling or Disabling a User Account

Procedure

1. Go to **Administration** > **User Accounts**.

   The **User Accounts** screen appears.

2. Click the icon under **Status**.

   Note

   The root account cannot be disabled.

Viewing License Information

The **License Information** screen displays product information for Endpoint Application Control.

Use the **License Information** screen to do the following:

- Specify a different Activation Code
- Check the license status

The following table describes the license information:

TABLE 7-1. License Information

ITEM	DESCRIPTION
Expiration date	Date when the Activation Code expires
Version	• **Full**: Allows full use of the product for the maintenance period (typically 1 year) • **Trial**: Allows full use of the product for the evaluation period (typically 3 months)
Status	Activated or expired
Activation Code	Activation Code for the product

Chapter 8

Getting Support

This chapter describes how to contact support.

Topics in this chapter:

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 client version
- Serial number or activation code
- Detailed description of install environment

- Exact text of any error message received.

Index

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: APEM16315/140224