Trend Micro Endpoint Application Control v2.0 Patch 1

Best Practice Guide

About this document

Trend Micro Endpoint Application Control 2.0 is an application whitelisting solution that uses whitelists to control which applications are permitted to execute on an endpoint. It helps to stop the execution of malware, unlicensed software, and other unauthorized and unknown software on your corporate endpoints.

This guide is intended to help users to get the best productivity out of the product. It contains a collection of best practices which are based on knowledge gathered from previous enterprise deployments, lab validations, and lessons learned in the field.

Examples and considerations in this document provide guidance only and do not represent strict design requirements. The guidelines in this document do not apply to every environment but will help guide you through the decisions that you need to configure Endpoint Application Control for optimum performance.

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the latest version of the applicable user documentation.

This document is designed to be used in conjunction with the following guides, all of which provides more detail about Endpoint Application Control than are given here:

Trend Micro Endpoint Application Control 2.0 Installation and Admin Guides

http://docs.trendmicro.com/en-us/enterprise/endpoint-application-control.aspx

____

This Best Practice Guide Contains:

- Deployment considerations and recommendations
- Product sizing guide
- Recommended system and hardware requirements for Server and Agents
- Guide to policy deployment
- Sever tuning properties
- Backup and Disaster Recovery procedure
- Endpoint Application Control tools

AUTHOR: RAYMOND F. VILLAFANIA
RELEASED: APRIL 13, 2016

Terms and Abbreviations

The following are the Terms and Abbreviations used in this document:

Abbreviation	Terminology	Description
TMEAC	Trend Micro Endpoint Application Control	Trend Micro Endpoint Application Control 2.0 Patch 1
EAC	Endpoint Application Control	Trend Micro Endpoint Application Control 2.0 Patch 1
AC Server	Endpoint Application Control Server	Server Component
AC Agent	Endpoint Application Control Agent	Agent Component
WebUI	Management Console	Web Console
PLS	Plug-in Manager Service	OfficeScan Plug-in Service
TMCSSS	Trend Micro Certified Safe Software Service	Whitelist Pattern

Table of Contents

1 Product Information

It is important to remember that Application Control software is not a replacement of a regular Anti-Virus program which utilize file signature or Blacklist pattern to detected malicious files and applications. Rather, Endpoint Application Control adds additional layer of protection by allowing only approved applications or Whitelist to run on an endpoint.

The table below is a simple illustration about the difference between Blacklisting and Whitelisting approach when protecting endpoints from unknown or unwanted files and applications.

Whitelisting	Blacklisting
Default-deny	Default-allow
Operates using a list of approved software	Operates using a list of unapproved/malicious software
Applications not on the approved list of softwares are denied execution	Applications not on the unapproved list of softwares are allowed to execute

Table 1 *Whitelisting vs Blacklisting Approach*

1.1 About Trend Micro Endpoint Application Control

A number of new malwares such as those that are used in targeted attacks can evade traditional, signature-based Anti-Virus Solution that only use Blacklisting Approach to block malicious applications. Trend Micro™ Endpoint Application Control 2.0 Patch 1 uses Whitelisting Approach and allows you to enhance your defenses against malware and targeted attacks by preventing unwanted, unknown and malicious applications from executing on your corporate endpoints.

1.2 Product Features

Monitors and blocks Portable Executable (PE) files (i.e, CMD, COM, EXE, BIN, SCR, CPL/DLL), as well as "touch-screen" friendly applications for Windows Runtime (WinRT) devices, such as "Windows Apps" or UWP Apps – formerly known as Metro Style Apps.

Use Trend Micro Certified Safe Software Service (TMCSSS)

- Provides a comprehensive list of applications considered to be safe by Trend Micro, called Certified Safe Software by Endpoint Application Control.
- The list includes most popular operating system files and binaries as well as applications for desktops, servers, and mobile devices.

Uninstall of Competitor's Product

- Ensure conflicting 3rd-party Application Control software can be uninstalled while installing the AC agent component.

Compatible with Trend Micro or any 3rd party Anti-Malware Software:

- *Can run with Trend Micro OfficeScan or any other 3rd party AV Vendors including the latest versions of Symantec, Sophos, McAfee, Kaspersky, Microsoft.*

Integration with Trend Micro Products and Services

- Control Manager 6.0 SP3
- OfficeScan 10.5, 10.6, 11 and later
- Smart Protection Network
- Smart Protection Suite

Please visit our Online Help for complete list of product features:

Features and Benefits

New Features in v2.0

1.3 New in Trend Micro Endpoint Application Control 2.0 Patch 1

The table below is an overview of Endpoint Application Control’s added and enhanced features from its predecessor.

Feature	Description
Agent Self-Protection	Prevents Endpoint Application Control agents from being stopped or uninstalled by either an end-user or an external third-party application or process.
AIR Score Part of the Smart Protection Network™	Enables administrators to allow or block applications based on a comprehensive security score from Trend Micro.
Global Usage Part of the Smart Protection Network™	Specify applications based on global or regional usage patterns. Allow or block applications using a score generated by the Smart Protection Network team using a "prevalence index".
Enhanced Control Manager Integration	Manage Endpoint Application Control policies , logs and dashboard with Control Manager 6.0 SP3.
Dynamic Application Lists	Match Trend Micro Certified Safe Software and endpoint inventory applications dynamically.
Key Performance Indicators Dashboard Widget	Customize a score card on the Endpoint Application Control and Control Manager product dashboards regarding the performance of your application control environment.
Health Meter	Monitor the health of applications in your environment.
Process Blocking (Also known as kernel-level or driver-level blocking)	Block applications from executing by evaluating if files are allowed prior to execution.
Trusted Sources for Applications	Trust newly installed software automatically for all users on an endpoint.

Table 1.3 *TMEAC v2.0 Patch 1 new features.*

2 Sizing Guide and Product Optimization

This chapter discusses system requirements for both server and workstation as well as scaling recommendations to guide administrators when allocating software and hardware resource before deploying Endpoint Application Control to corporate networks.

2.1 Server Scaling Recommendations

Endpoint Application Control server requirements depend on the number of managed agents. For instance;

- Manage up to 20,000 agents using a single Endpoint Application Control Server.
- Manage more than 20,000 agents using more than one servers.

Agents per Server	Minimum RAM	Minimum Processor Count	Minimum Available Disk Space	Endpoint Log Collection Suggested Interval	Endpoint Policy Update Suggested Interval
1,000 or fewer	4 GB	2 CPUs	45 GB	15 minutes	2 minutes
1,001 to 5,000	4 GB	2 CPUs	185 GB	15 minutes	5 minutes
5,001 to 10,000	4 GB	4 CPUs	360 GB	2 hours	15 minutes
10,001 to 20,000	8 GB	4 CPUs	710 GB	2 hours	15 minutes

Table 2.1 *Server Scaling Recommendations*

2.2 Server Memory Use Allocation

Endpoint Application Control uses Java Virtual Machine (JVM) applications. Using JVMs adds some processor and memory overhead. In most cases, the JVMs self-manage their settings, memory, and performance overhead.

Memory Use Source	Description	RAM Used
HEAP	Memory directly used by an application	Server processes Max: 256MB
		Data store processes Min: 512 MB Max: 25% of available RAM
Thread Stacks	Memory used for process threads	256 KB per live thread Typically, 20 – 60 MB
Direct Memory	Memory for buffers or to share data with operating system APIs	Typically, 5 – 30 MB
Java and JIT-compiled code	Memory for application libraries	Typically, 60 – 120 MB
Native code	Memory for shared libraries	Highly variable because this memory use is shared across all processes, it depends on the specifics of those processes.
Other	Memory overhead per process	Typically, 100 – 150 MB

Table 2.2 *EAC Memory Allocation*

2.3 Server and Agent Requirements

The Endpoint Application Control 2.0 Patch 1can be installed on servers running (IIS) v7.0 or later. Otherwise, the setup will automatically install Apache Tomcat v8. The agent component on the other hand, can be installed on both earlier and later versions of Windows Operating Systems such as XP, Windows 7/8.x/10, Server 2003/2008/2012 as well as POS and Embedded OS. Here’s the full list of supported windows platforms:

Server Requirements

Agent Requirements

2.4 Recommended Browser for Web UI Management

For best performance, use Internet Explorer v11.0 when accessing EAC Web UI. Moreover, you can also access the Web UI with web-kits like Google Chrome or Opera particularly the newest releases to date.

2.5 Excluding Endpoint Application Control from AV Real-time Scan

When installing EAC Agent component on endpoints running an AV software such as the Trend Micro OfficeScan 11.0 Service Pack 1, be sure to add the following EAC applications in the Process Exclusion Management (Trusted Programs List) to configure the AV Program to skip scanning of trusted processes during Real-time scanning:

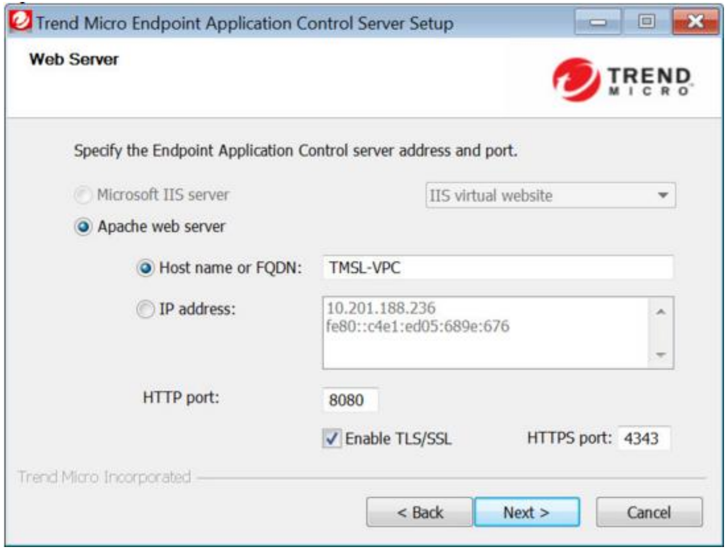
Both 64-bit/32-bit Systems
C:\Program Files\Trend Micro\Endpoint Application Control Agent\ac_bin\AcAgentScan.exe
C:\Program Files\Trend Micro\Endpoint Application Control Agent\ac_bin\AcAgentService.exe

See OfficeScan v11.0 Service Pack 1 Process Exclusion Management online help.

Adding these EAC processes in the Real-time Scan exclusion will improve the AV scanning performance and reduce the I/O resource used by the AC Agent when scanning the system to build Inventory Scan database. This improves the endpoint's system performance overall.

3 Installation and Deployment

Endpoint Application Control is composed of several components that need to communicate with each other. When deploying in a highly segmented network environment, knowledge about the various ports it uses will be useful for preventing unintended functionality disruptions. Make sure to note all ports that are required are open and, not reserved for other purposes. The ports are configurable during AC Server Installation in the Web Server Screen.



Trend Micro Endpoint Application Control Server Setup

Web Server

Specify the Endpoint Application Control server address and port.

○ Microsoft IIS server IIS virtual website

● Apache web server

● Host name or FQDN: TMSL-VPC

○ IP address: 10.201.188.236 fe80::c4e1:ed05:689e:676

HTTP port: 8080

☑ Enable TLS/SSL HTTPS port: 4343

Figure 3 *Web Server Screen*

Refer to Endpoint Application Control server online help to know the ***[Default Ports](#)*** *of the Trend Micro Endpoint Application Control.*

3.1 Main Components

- **Endpoint Application Control Server** – Provides the Endpoint Application Control (EAC) management console. The server manages Endpoint Application Control agents, agent inventories, event logs, policies, rules, and rule data. Standard http and https protocols are used for communication and to provide updates to managed AC agents.
- **Endpoint Application Control Agent** – A host reporting to a particular Endpoint Application Control Server. AC agent enforces policies retrieved from AC server. Policies contain rules which have three methods to control application usage: Allow, Block, and Lockdown.
- **OfficeScan Plug-in Addon (if OfficeScan is used)** – The AC Agent Installation Tool uses the OfficeScan domain tree to install AC agent component on the endpoints. This gives administrators an outlet to remotely deploy AC agent on endpoints.

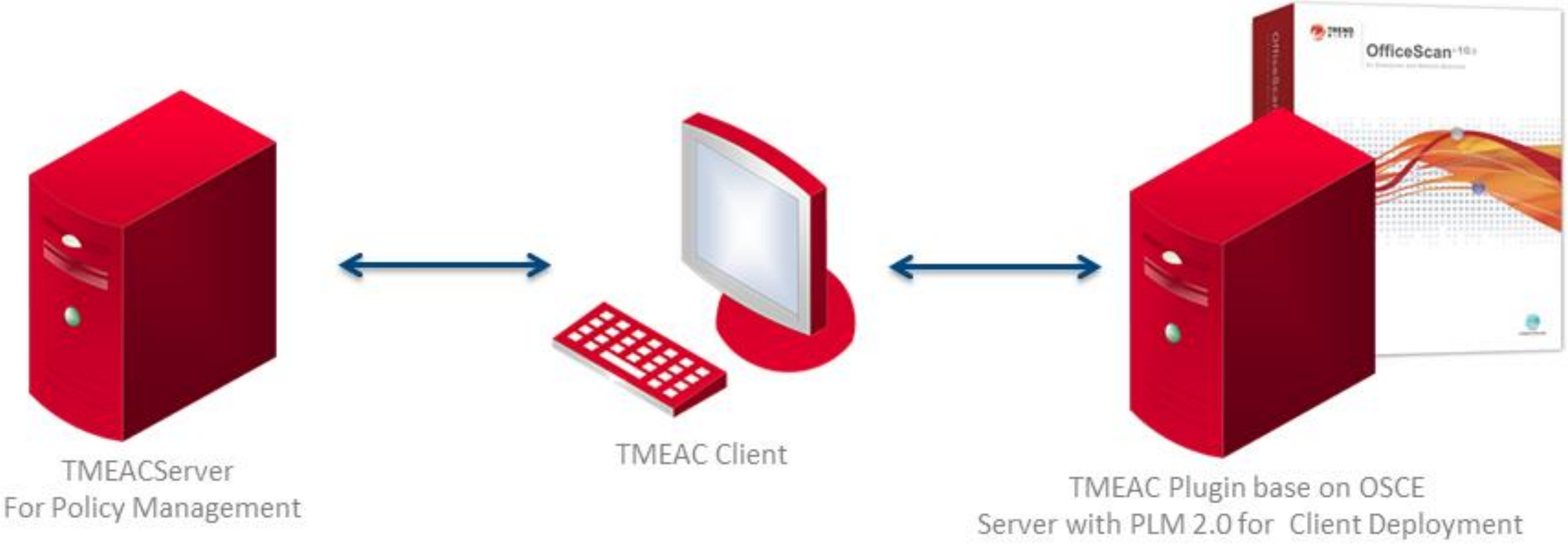

TMEACServer
For Policy Management
TMEAC Client
OfficeScan
TMEAC Plugin base on OSCE
Server with PLM 2.0 for Client Deployment

Figure 3.1 *Endpoint Application Control Components*

3.2 Deployment Planning

Project Plan

- Project Team should include executive management, IT Security and helpdesk administrators.
- In advance of roll-out, deploy the application control agent to capture the machine's application inventory, this will assist in creating acceptable usage policies based on device type.

Identifying In-House Applications

- In-house applications can be easily added to the database via the software inventory, defined by vendor certificate and application hash.
- Alternatively, administrators can use common tools such as Microsoft's SignTool to sign in-house or legacy applications that lack a file certificate.

Identifying System and Network Requirements

- Before your pilot, it is important to identify target systems you whish to protect.
  - For example, end-user devices, POS systems and servers
- Normally, the pilot starts with systems with minimal change and is then rolled out to more dynamic end-user devices.
- Each endpoint (or user) may have a unique policy based on the Operating System, device type and acceptable usage policies.

Tips and Tricks for a Pilot

- Always define a Default "Catch-all" machine-based policy for situations where applications are launched using alternate privileges for other users (system, root, etc.).
- Verify all policies run in "Log-only Mode" for an extended period of time to ensure you do not interrupt normal day-to-day operations
- Fully Test Applications and OS deployment, application deployment, and patching procedures during the POC.

3.3 Installation Guidelines

3.3.1 Endpoint Application Control Server

✓**Use Fully Qualified Domain Name (FQDN)**

Endpoint Application Control server installed on IPv4 endpoint cannot manage IPv6 endpoints. Specify fully qualified domain name to be able to manage both IPv4 and IPv6 endpoints.

✓**Selecting Apache Tomcat over Microsoft IIS for Web Server Management**

To avoid some common security compromises such as hackers taking control over web server, make sure to create a non-administrator account to run Apache Tomcat.

✓**Choose to enable TLS/SSL**

Endpoint Application Control can use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to help ensure secure communication between the web console and the server. However, enabling this feature requires you to import a server certificate authority (CA) to endpoints.

Enabling TLS/SSL is done during EAC Server installation. Please visit the Endpoint Application Control Online Help for steps to Enable TLS/SSL and How to Import the Trusted Root Certification Authorities to your Domain or via GPO.

3.3.2 Endpoint Application Control Agent

✓**DNS Resolution**

Ensure that each computer can resolve the fully qualified domain name of the AC Server for a successful deployment.

✓**Enable HTTPS Agent-Server Communication**

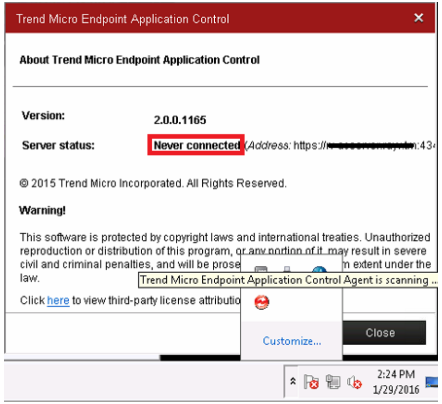
Although, the AC Agents can use either HTTP or HTTPS protocol to communicate to the AC Server, Trend Micro recommends using HTTPS to ensure that all types of data sent to the server is encrypted.

Using agent setup package, the following command line is used:

```
>AcAgentSetup_x86.exe ServerHost=<http_or_https>://<server_ip_or_fqdn>:<port>
```

✓Import EAC Server Public Key Cert to Endpoints when HTTPS Agent-Server communication is being used

When Agent-Server communication is using HTTPS protocol, the endpoint needs the server's Public Key Cert (TMAC_CA_Cert.pem) installed locally to authenticate to the server. If this is not done, the installed AC agent will show as disconnected.



About Trend Micro Endpoint Application Control

Version: 2.0.0.1165

Server status: **Never connected** (*Address:* https://[redacted]:43

© 2015 Trend Micro Incorporated. All Rights Reserved.

Warning!

This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prose m extent under the law.

Trend Micro Endpoint Application Control Agent is scanning ...

Click here to view third-party license attributio

Fig 3.3.2 *Agent Connection Status in AC Agent Console.*

For steps in how to import EAC Server's Public Key Cert (TMAC_CA_Cert.pem), refer to the Trend Micro Knowledgebase below:
http://esupport.trendmicro.com/solution/en-US/1102669.aspx

✓Disable Windows Hibernate and Sleep modes on Workstations and Laptops

The Endpoint Application Agent scans the endpoint system for existing applications to build it's Inventory Database. If the endpoint goes to Hibernate or Sleep mode, the scanning stops and building of Inventory Database could take more time to complete.

✓Exclude Endpoint Application Agent from OfficeScan or 3rd Party Ant-Virus software

Trend Micro recommends excluding the AC agent applications from being scanned by an Anti-Virus softwares' Real-time Scan because it can disrupt the operation and prolong the Inventory Scan period (see 2.5 Excluding Endpoint Application Control from AV Real-time Scan*)*.

✓**Take time to decide on the best deployment method.**

The EAC Agent can be deployed using various methods, including but not limited to:

- Manual deployment (Install locally)
- Group Policy (msiexec in silent mode)
- Enterprise Deployment Software (i.e. SCCM, BigFix)
- OfficeScan Plug-in
- Custom Scripts

Sample Scenarios:

*If **OfficeScan Plug-in** is used, it will be easier to perform a new Agent deployment or an upgrade as the update package can just be pushed via the same method – targeting all endpoints with existing OfficeScan agents.*

***Manual Deployment** or the **Enterprise Deployment** methods are best suited for a network with mixed environment such as peer-to-peer network or a workgroup that is not a member of the domain.*

Go to the Endpoint Application Control Agent Deployment online help page and find out the best deployment method available for your environment.

Deployment via Endpoint Application Control Web UI is not an available option. However, pushing software upgrades is possible through Web Console. If you plan on performing upgrades via Web Console, the overhead of pushing all of these upgrade packages via network should be taken into considerations.

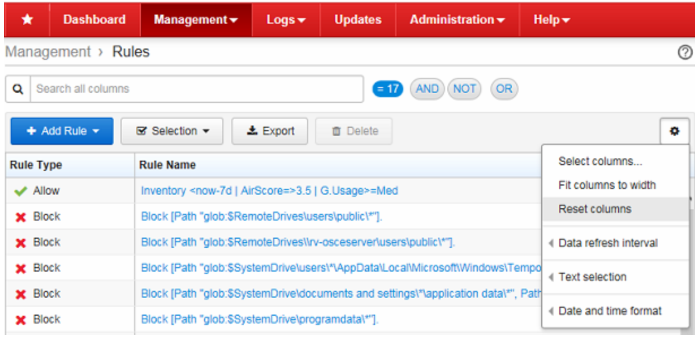
4 Rule and Policy Best Practices

A newly installed AC Agent has no policy to enforce until you assign one. That is why, creating rule and policy is a critical phase of application control deployment because it can cause programs to malfunction if an associated or a subsequent application was inadvertently added to a deny rule of the policy that the AC Agent is using. This chapter covers best practices about rules and policies to help administrators determine the acceptable usage policy based on the device type.

Refer to section *3.2 Deployment Planning* to learn more about application control pilot deployment recommendations.

4.1 Rule Basics

A Rule targets application(s) on an endpoint and can be applied to many different policies at a given time. This section discusses about rule types and settings as well as the different methods of finding target applications based on the available matching criteria.



Rule Type	Rule Name
✓ Allow	Inventory <now-7d | AirScore=>3.5 | G.Usage>=Med
✗ Block	Block [Path "glob:$RemoteDrives\users\public\*"].
✗ Block	Block [Path "glob:$RemoteDrives\\rv-osceserver\users\public\*"].
✗ Block	Block [Path "glob:$SystemDrive\users\*\AppData\Local\Microsoft\Windows\Tempo
✗ Block	Block [Path "glob:$SystemDrive\documents and settings*\application data*", Path
✗ Block	Block [Path "glob:$SystemDrive\programdata\*"].

Fig 4.1.1a *Rules Screen*

4.1.1 Managing Rules (Rule Screen)

Add, edit, import/export, and search rules in the Rules Screen page and perform all kinds of rules management tasks.

Search with Bolean Operators (And | Not | Or)

This is very useful when searching against a long list of Rules. The Bolean Operators adds more filtering functionality to eliminate unnecessary hits for a more 'on-target' results.

Column Selection

Remove or add columns according to the desired view. Each column can also be moved to left-most or right-most part of the screen by a "drag-and-drop" to enhance the viewing experience.

Add Rule

Add, import or duplicate rules using Add Rule feature. The **Duplicate** function allows for copying existing rules and have the same exact settings, or as an allow, block and a lockdown rule to save you time when creating rules with mostly similar target applications and configurations as the source.

Export

For disaster recovery management, regularly backup the rules with the Export feature in the event that rebuilding of the EAC Server is necessary or if you need to use the same rule(s) to another EAC Server.

Visit the Endpoint Application Control Online Help to know more about Rule Screen options.

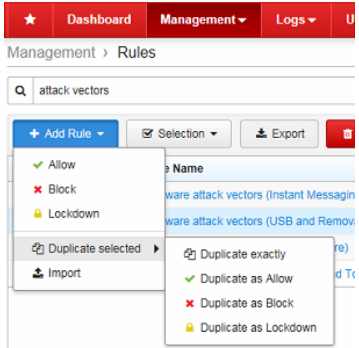


Fig 4.1.1b *Add Rule feature*

4.1.2 Rule Types

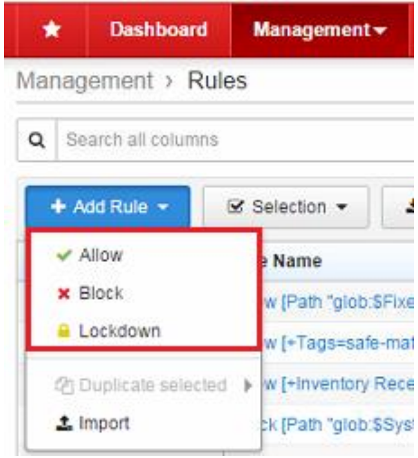


Fig 4.1.2 *Rule Types*

A Rule marks applications as either **Allow** or **Block**. A **Lockdown** rule, on the other hand, locks the endpoint to allow only existing applications to execute since the recent Inventory Scan.

IMPORTANT: *It is highly advisable to enable the **Log-only Mode** with the Lockdown rule and make an initial assessment to know which critical-mission applications of endpoint systems will be affected and be able to proactively address issues by adding exceptions or creating additional Allow rules to add to the Lockdown Policy.*

There are a couple of rule options and settings that can be configured upon rule creation. Section 4.1.3 provides overview of all the rule settings in the **Edit Rule Screen** page to give you a quick grasp and understanding of what functions are available depending on the type of the rule to manage or create.

Visit the Endpoint Application Control Online Help to learn more about Rule Types.

4.1.3 Add/Edit Rule Screen

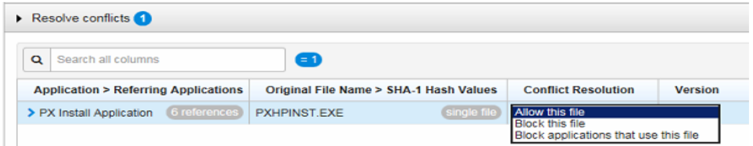
Understand how each Rule settings work to achieve the primary objective of the rule being created when specifying target applications. Below table is an overview of the configurable settings in the Edit Rule Screen:

		Rule Type			Bolean Operators (And | Not | Or)
		Allow	**Block**	**Lockdown**	
Rule Settings	**Name**	Y	Y	Y	-
	Log-only mode	Y	Y	Y	-
	[Match method]				
	Known applications dynamic search	Y	Y	Y	Y
	Certified Safe Software list	Y	Y	Y	N
	File Path	Y	Y	Y	Y ("Or" only)
	Certificates	Y	Y	Y	Y
	SHA-1 hash values	Y	Y	Y	N
	Show Matches / Hide Matches	Y	Y	Y	N
	[Rule Options]				
	Specify metadata: (Optional)	Y	Y	Y	-
	Prevent Editing	Y	Y	Y	-
	Trusted Source (None, Medium, High)	Y	N	N	-
	Resolve conflicts *(Appears only in "Known applications dynamic search" and "Certified Safe Software list" Match Criteria.)*	N	Y	N	-

Table 4.1.3 *Edit Rule Screen settings and options.*

Visit the Endpoint Application Control Online Help to know more about Add/Edit Rule Screen properties and settings.

The **Trusted Source** under Rule Options is only applicable in the Allow rule. By default, subsequent applications and DLLs of a permitted application will not be exempted from a deny rule such as the Lockdown. For example, you define windows update "wuauclt.exe" in an Allow rule of a Lockdown policy, when windows update "updates" certain binaries and DLLs, EAC will block these DLLs by the applicable Block rule if no trust-level is selected. Trust Levels are None, Medium and High and each level is described briefly in EAC Online Help - Trusted Source.

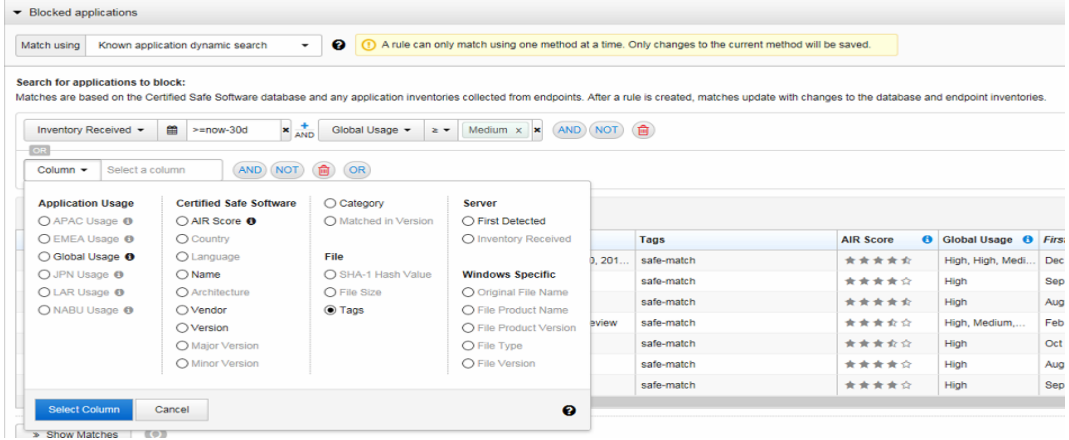


Application > Referring Applications	Original File Name > SHA-1 Hash Values	Conflict Resolution	Version
PX Install Application 6 references	PXHPINST.EXE single file	Allow this file Block this file Block applications that use this file	

Fig. 4.1.3a *Conflict Resolution.*

The **Resolve conflicts** on the other hand, is only available in Block rule when selecting applications with **Known applications dynamic search** or **Certified Safe Software list** match criteria. It is used to ensure that associated files shared with other apps not in the Block list is handled properly as well by allowing or blocking the file, or blocking the application that uses the file.

When creating a rule based on **Known applications dynamic search**, **File Paths** and **Certificates** match criteria , the **Bolean Operators (And | Not | Or)** can be used to dynamically search applications and save time and effort by eliminating inappropriate hits. Using these operators can greatly reduce or expand the amount of the records returned by focusing searches for a more ‘on-target’ results. When used against **Known applications dynamic search**, you can add several different filter categories such as “Application Usage”, “Certified Safe Software”, “File”, “Server”, and “Windows Specifics“ to enhance the result.



A rule can only match using one method at a time. Only changes to the current method will be saved.

Search for applications to block:
Matches are based on the Certified Safe Software database and any application inventories collected from endpoints. After a rule is created, matches update with changes to the database and endpoint inventories.

Tags	AIR Score	Global Usage
safe-match	★★★★☆	High, High, Medi...
safe-match	★★★★☆	High
safe-match	★★★★☆	High
safe-match	★★★☆☆	High, Medium,...
safe-match	★★★☆☆	High
safe-match	★★★★☆	High
safe-match	★★★★☆	High

Fig. 4.1.3b *Filtering applications by combining different search categories (Column) with Bolean Operators.*

Some parts of he Endpoint Application Control web console utilize **Dynamic Search** (Auto-complete) feature in search fields. It helps to dynamically search strings of data matching any of the columns available on that screen as you type something in. In the **Edit Rule Screen** this feature is enabled when searching for target applications based on **Known applications dynamic search**, **File Paths** and **Certificates** match methods.

> *Visit the Endpoint Application Control Online Help to learn more about Dynamic Search feature.*

4.1.4 Rules Guidelines

Here are few of the best practices and guidelines when creating a rule:

✓**Rule Priority**

The Allow and Block applications takes precedence over a Lockdown rule. Likewise, an Allow rule would take precedence over a Block rule. Refer to the process flow below.

✓**Enabling Log-only Mode**

Evaluate Block and Lockdown rules first by enabling the "Log-only mode" option before fully enforcing in a Policy.

✓**One Match Method per Rule Type**

A Rule can only use one Match Method at a time (e.i., Known applications dynamic search, Certified Safe Software list, File paths, Certificates and SHA-1 hash values). Switching from one match method to another is allowed but it will remove previously selected applications.

✓**One Rule Per Application or Application Group**

Create one (1) Rule per allowed or blocked application or group of application in the same category such thus Firefox Browser is for Web Browser category - so you can easily reuse it to other Policies that might require that rule.

✓**Trusted Source - Allow Rule Option**

Always add your patch management and software deployment applications such as Windows Updates, Windows Software Update Services (WSUS), BigFix and System Center Configuration Manager (SCCM) to an Allow Rule with Trusted Source enabled in a Lockdown Policy or policies with Block rules.

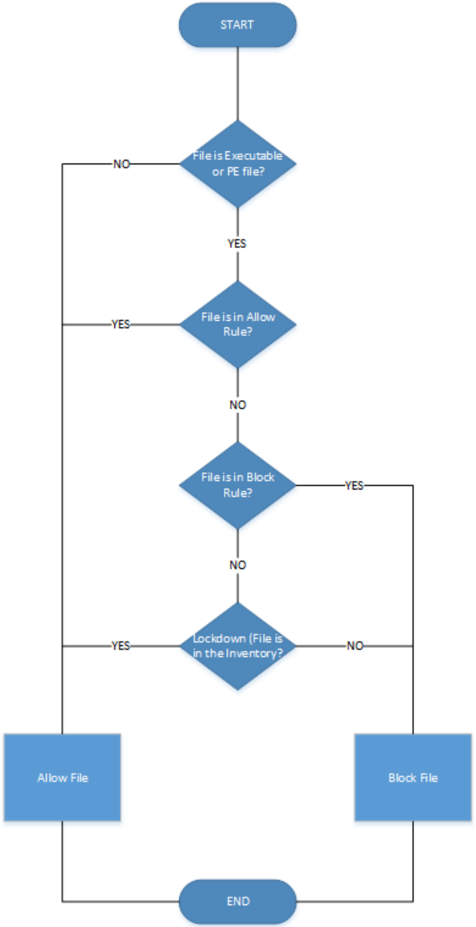
✓**Only assign Lockdown Rule to Computer-based Policy**

Features such as “Trusted Source” and “User-level blocking” only works in User-based Policies. Thus, only assign Lockdown rule to a Computer-based Policy to be able to use these features:

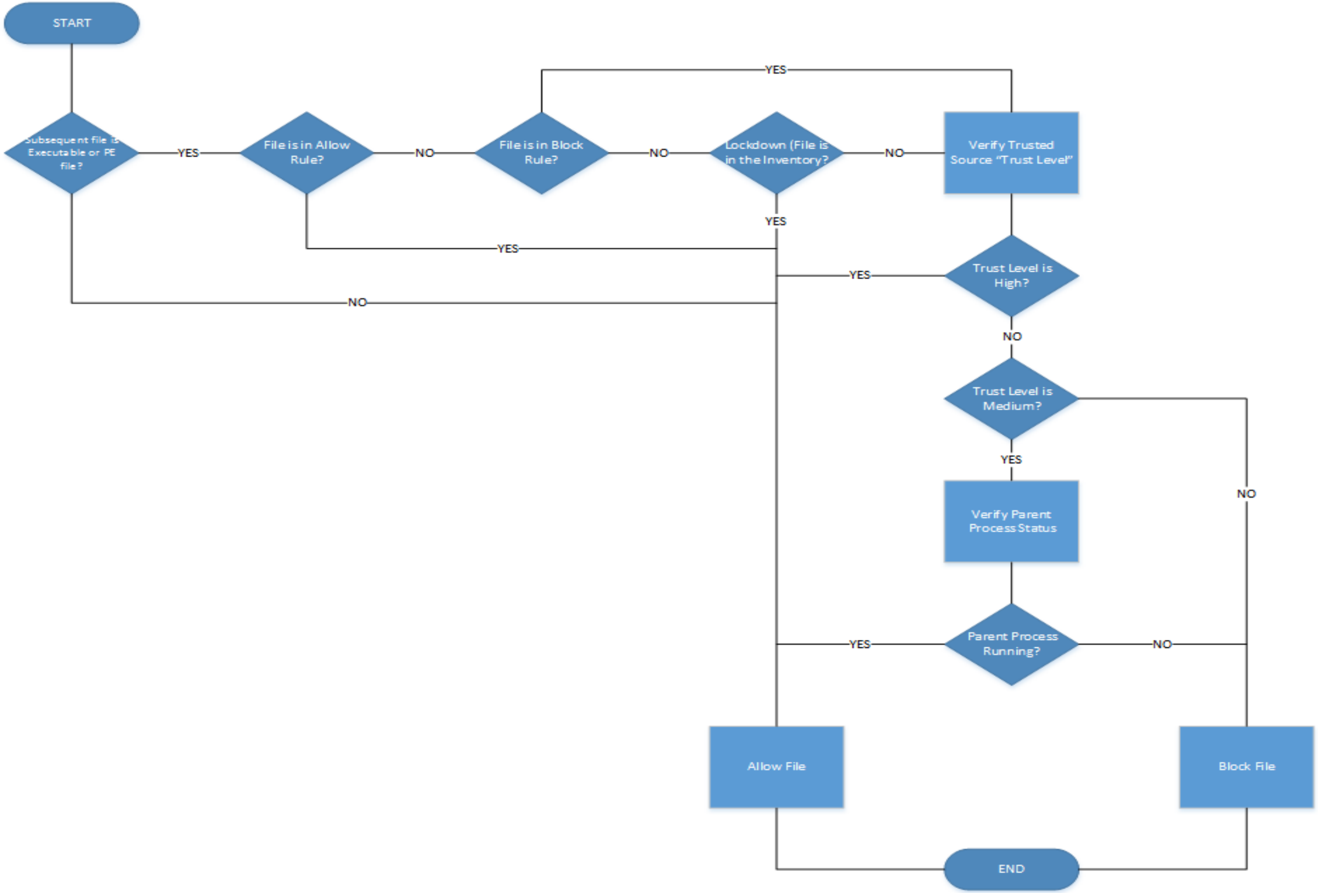
> *See 4.1.6 Application Scanning Flow with Trusted Source Enabled to understand how the feature works.*
>
> *See 4.2.2 Add/Edit Policy Screen for information about how to switch between “User-level” and “Kernel-level” blocking with the “Use the more compatible, less feature-rich, user-level blocking method.” configuration checkbox.*

Defining User and Computer based policies will be discussed in section 4.2.3 Policy Guidelines of this document.

4.1.5 Application Scanning Flow



4.1.6 Application Scanning Flow with Trusted Source Enabled



START

Subsequent file is Executable or PE file?

YES

File is in Allow Rule?

NO

File is in Block Rule?

NO

Lockdown (File is in the Inventory?

NO

Verify Trusted Source "Trust Level"

YES

YES

YES

NO

Trust Level is High?

YES

NO

Trust Level is Medium?

YES

NO

Verify Parent Process Status

Parent Process Running?

YES

NO

Allow File

Block File

END

4.2 Policy Basics

Policy is where to assign the Rules and specify the target users and endpoints. The following can be used to match users and endpoints to a policy.

-Endpoint Name
-Windows Operating System
-Agent Version
-Domain
-User or Group
-IP Address
-OfficeScan Domain

An endpoint can only have one policy at a time. It weighs all relevant policies and applies the policy with the most number of matching classification. In the event that there are two or more Policies with the same number of matched classifications, the endpoint will select the policy with the highest Priority Level (i.e., 1 ~ n | Highest ~ Lowest).

4.2.1 Managing Policies (Policy Screen)

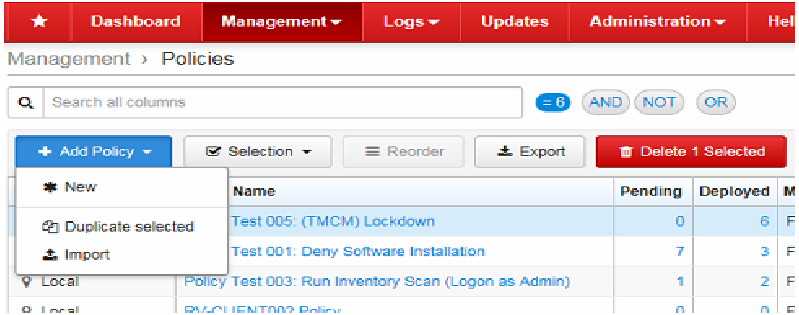
Here are some of the functions that come handy when working with policies:

Search with Bolean Operators (And | Not | Or)

This is very useful when searching against a long list of policies. The Bolean Operators adds more filtering ability to eliminate unnecessary hits for a more ‘on-target’ results.

Import, Export and Duplicate

Backup and restore policies whether for disaster recovery purposes or when Replicating policies from one AC server to another. Moreover, using the **Duplicate** feature can save you time when creating Policies with mostly similar configurations as the source.



	Name	Pending	Deployed
	Test 005: (TMCM) Lockdown	0	6
	Test 001: Deny Software Installation	7	3
Local	Policy Test 003: Run Inventory Scan (Logon as Admin)	1	2

Fig. 4.2.1 *Policy Management screen.*

Reorder

Set the priority level of each policy according to the desired usage and to match endpoints based on most current system properties and classifications.

Column Selection

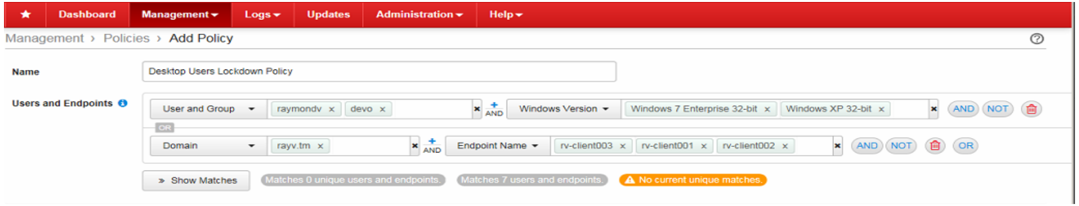
Remove or add columns according to the desired view and save them to display the same set of columns every time you go to the Policy Screen. Each columns can also be moved to left-most or right-most part of the screen by a “drag-and-drop” to enhance the viewing experience.

4.2.2 Add/Edit Policy Screen

Specifying users and endpoints, and assign rules in Add Policy screen.

Policy Name

The name of the policy must reflect the kinds of rules you assign to it and the target devices or endpoints. For example, if you intend to add a Lockdown rule to the policy and the target endpoints are servers, we can use names such as “Lockdown Policy for Servers” or “Windows Server Lockdown Policy”.


★
Dashboard
Management ▾
Logs ▾
Updates
Administration ▾
Help ▾
Management › Policies › Add Policy
Users and Endpoints
OR
AND
NOT
OR
» Show Matches
Matches 0 unique users and endpoints.
Matches 7 users and endpoints.
No current unique matches.

Name Desktop Users Lockdown Policy

Users and Endpoints
User and Group: raymondv, devo AND Windows Version: Windows 7 Enterprise 32-bit, Windows XP 32-bit
OR
Domain: rayv.tm AND Endpoint Name: rv-client003, rv-client001, rv-client002

Fig 4.2.2 *‘Add Policy’ screen – Policy Name, User and Endpoints settings.*

Users and Endpoints

A Policy can be “User-based” or “Computer-Based”, or a combination of both (see 4.2.3 Policy Guidelines). Use the **Bolean (AND | NOT | OR)** operators to fine-tune the matched endpoints that will be affected by the policy (see section 4.2 Policy Basics for list of available target classifications).

Show Matches

Another useful feature while tweaking the **Users and Endpoints** target classifications is the Show Matches. It displays the endpoints that matches the current set of classifications in real-time. It also changes the display as you make adjustments. With this feature, you ‘ll know which unique matches (or, users and endpoints with no policy applied) will apply the policy even before deploying it.

Rules Section

You can assign an existing rule or add a new Allow, Block and Lockdown rule to a policy. When you combine all Rule Types (Allow, Block and Lockdown) into one policy, the Allow rule takes precedence over the Block and Lockdown rules. The Block rules, on the other hand, have higher priority than the Lockdown. There’s no known limit to the number of rules you can add to a policy.

Here are additional options you can enable and disable in the Policy screen Rules Section:

- [Default Status: Enabled] Always allow all applications in the Windows directory (overrides Block and Lockdown rules)
- [Default Status: Disabled] Automatically apply Lockdown rules to endpoints while they are disconnected.
- [Default Status: Disabled] Use the more compatible, less feature-rich, user-level blocking method.

4.2.3 Policy Guidelines

Here are few of the best practices and guidelines when managing and deploying policies:

Creating User-based and Computer-based Policies.

User-based Policy

- User-based policy must have the highest priority level than a Computer-based policy.
- Policy target used is or includes "User and Group" with matching Standard Users such as Domain Users and Groups or locally created user on the endpoint.

Computer-based Policy

- Policy target “User and Group” is System, IUSR, DefaultAppPool, or any users that DO NOT belong to Active Directory and locally created users on the endpoint.
- Policy with targets that does not include “User and Group” match criteria.

Using Bolean Operators

- If "AND" is used to match endpoints with more than 1 criteria, then ALL of the criteria must be matched for the endpoints to apply the policy.
- If "OR" is used to match endpoints with more than 1 criteria, then ANY of the criteria must be matched for the endpoints to apply the policy.
- If "NOT" is used to match endpoints with more than 1 criteria, then ONLY the first criteria before the "NOT" operator must be matched for the endpoints to apply the policy.

Arranging Priority Level

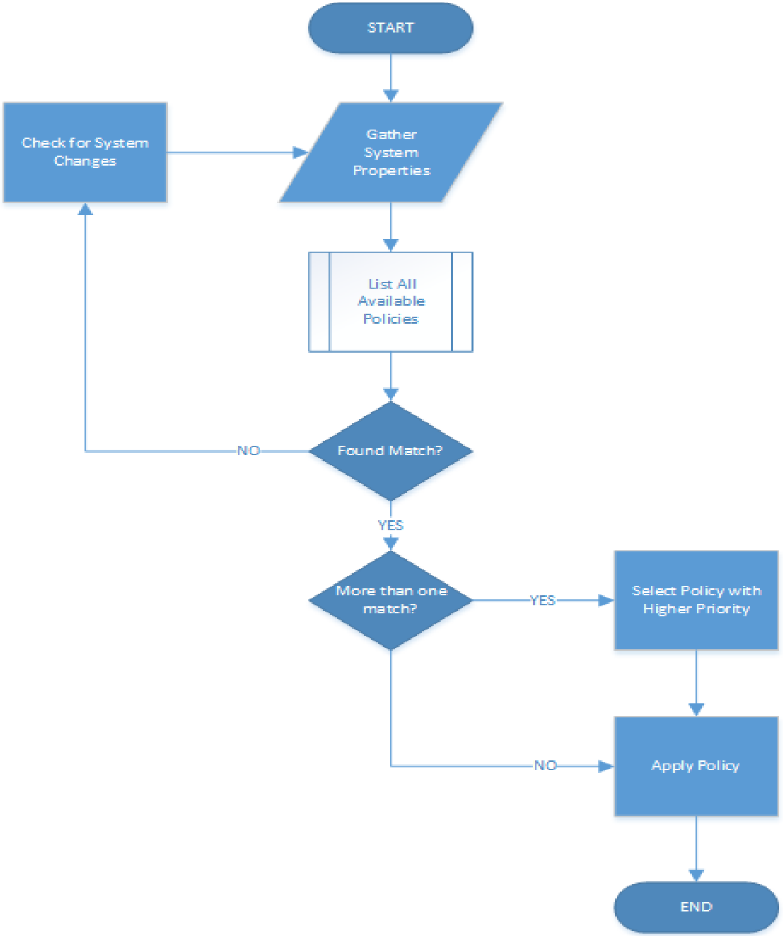
Policies with the most number of matched targets must be assigned the Lowest Priority Level. Likewise, Policies with least number of matched targets must be assigned the Highest Priority Level. For example, using “Windows Operating System” as target endpoints will match more endpoints than the “Endpoint Name” match criteria. If “Windows Operating System” has the highest Priority Level than the “Endpoint Name”, there will be no more endpoints that will match to the policy that use “Endpoint Name” because all Windows computers have already applied the policy that used “Windows Operating System” match criteria. This scenario is thoroughly illustrated in the following Trend Knowledgebase:

> *Creating rules and deploying policy in Endpoint Application Control (EAC)*
> http://esupport.trendmicro.com/solution/en-US/1102440.aspx

Lockdown Policy

A policy with Lockdown Rule is called a Lockdown Policy and Trend Micro recommends to assign this rule only to Computer-based Policies. (see 4.1.4 Rules Guidelines). The target agent(s) performs Inventory Scan when applying or switching to this policy. However, in TMEAC v2.5, there will be an option to disable and enable the Inventory Scan within the Policy Edit Screen to give administrators more control to this type of event.

4.2.4 Policy Deployment Flow



START

Gather System Properties

Check for System Changes

List All Available Policies

Found Match?

NO

YES

More than one match?

YES

NO

Select Policy with Higher Priority

Apply Policy

END

4.3 Creating Rules and Deploying Policies

In sections 4.1 Rule Basics and 4.2 Policy Basics, we learned that the Rule is for target applications and Policy is for specifying users and endpoint, and to where the Rules are placed. In this section, we will learn about how to effectively prevent execution and installation of unknown and unwanted applications (including malwares) on an endpoint with Trend Micro Endpoint Application Control.

4.3.1 Understanding the Threat

Here's an example of Ransomware "CRYPWALL" infection chain. It starts with a SPAM e-mail containing JS and HTML files in a ZIP attachment. Unsuspecting user opens the attachment and clicks the files which then trigger the JS_DLOADER to download the CRYPWALL executables such as SCR and EXE. When these files are run, they would start injecting malicious codes into registries and spawn legitimate processes such as svchost.exe and run32dll.exe to disguise and perform its malicious activities (PAYLOAD).

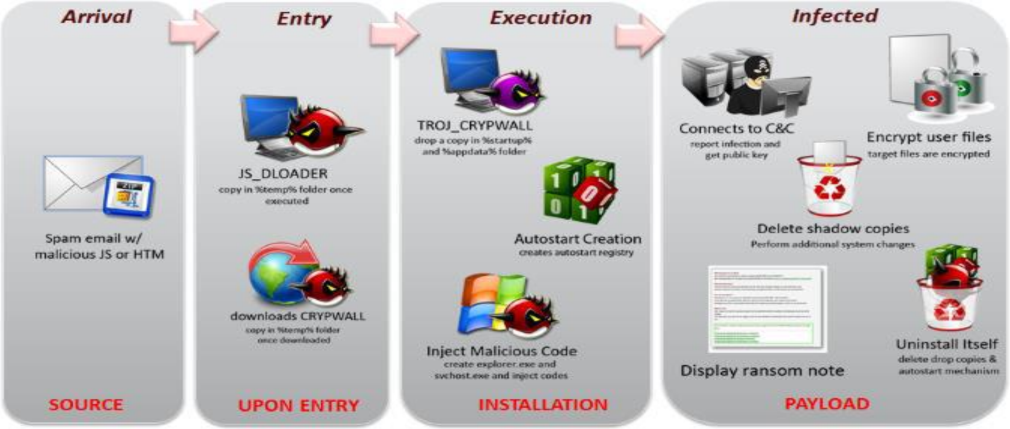

Arrival
Spam email w/ malicious JS or HTM
SOURCE
Entry
JS_DLOADER
copy in %temp% folder once executed
downloads CRYPWALL
copy in %temp% folder once downloaded
UPON ENTRY
Execution
TROJ_CRYPWALL
drop a copy in %startup% and %appdata% folder
Autostart Creation
creates autostart registry
Inject Malicious Code
create explorer.exe and svchost.exe and inject codes
INSTALLATION
Infected
Connects to C&C
report infection and get public key
Encrypt user files
target files are encrypted
Delete shadow copies
Perform additional system changes
Display ransom note
Uninstall Itself
delete drop copies & autostart mechanism
PAYLOAD

Fig 4.3.1 *Troj_CRYPWALL infection chain.*

Looking at the Infection Chain described in **Fig 4.3.1**, Endpoint Application Control can protect the system at the Installation (Execution) Phase by preventing the execution of TROJ_CRYPWALL that injects malicious codes into the system registry – preventing the rest of the malware work such as encrypting documents and sending them back to the Command and Control (C&C) servers owned by the attacker.

In the following sections, we will discuss how to create rules and policies in Endpoint Application Control to protect the endpoint systems from malwares and prevent unwanted or unknown applications from running.

Visit the Trend Micro Threat Encyclopedia to learn about the latest threats.

4.3.2 Preventing Malware Execution

Malwares or file infectors has to be executed or installed in order to do damage to endpoints. After being downloaded, it scans common folder variables such as %TEMP%, %USERPROFIE%, Startup folders and especially network shares and removable storage to propagate or execute its payloads. By denying execution of any unknown and unwanted applications to these folders, we can ensure that endpoint systems are only allowed to run regular programs and executables that are either approved by the company or "certified safe" by Trend Micro Census Server. Here's an example rule-set we can use as a reference:

Rule Type	Target Applications or Folder Location	Application Match Method
Allow	Inventory Scan and Applications based on TMCSS Pattern	Known applications dynamic Search
Allow	Applications based on TMCSS Pattern and File hash	Certified Safe Software list | SHA-1 Hash
Block	\Users\<*user name*>\AppData\Local\Temp \Users\<*user name*>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup \<*file server*>\users\Public\Downloads	File Paths

Table 4.3.2 *Rule-set to prevent Malware Execution in variable folders while allowing approved and safe applications to run in the same directories.*

Use real "username" and "server name" or the wildcard "" in <user name> and <file server> to specify actual targets.*

The "Allow" rules is as important as the "Block" rule in the example rule-set above to make sure that legitimate applications and existing programs of the endpoint can still utilize the folder locations we specified in the blocking rule and avoid unexpected system behavior that could affect end-users' daily tasks.

Check out the list of folder variables from Microsoft that malwares often use to propagate and execute on the endpoints .

Windows Common folder variables

https://www.microsoft.com/security/portal/mmpc/shared/variables.aspx

4.3.3 Stopping "Drive-by" Exploit

Also known as "Drive-by" Download. This happens when visiting a website, viewing an email message or when clicking a fraudulent pop-up window that downloads and executes the infected file to the local machine. The following folders are common download and execute locations of this attack:

For Email and Website

%AppData%\Local\Microsoft\Windows\Temporary Internet Files\Content.OUTLOOK
%AppData%\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

Pop-up Window

%AppData%\Local\Temp

Chat and Instant Messaging

%UserProfile%\Documents\My Received Files

For this, we can use the following Block rule to protect the users and prevent "Drive-by" download from happening:

Rule Type	Target Applications or Folder Location	Application Match Method
Block	\Users\<*user name*>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.OUTLOOK \Users\<*user name*>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 \Users\<*user name*>\AppData\Local\Temp \Documents\My Received Files	File Paths

Table 4.3.3 *Block rule to stop "Drive-by" Exploits.*

Use real "username" or the wildcard "" in <user name> to specify actual targets.*

Again, not all applications that use these folders are uncategorized. Thus, it is important to associate "Allow" rules such as those that were found in **Table 4.3.2** with this Block rule to ensure uninterrupted end-user experience when running their regular applications.

4.3.4 Application Usage Policy

For a less-conservative application control policy, we can create a Rule-set based on specific application or group of applications without applying a “Default Deny” rule to an entre directory or folder path. For example, to prevent installation of new Web Clients but at the same time, allowing only Google Chrome to be installed on the endpoints, you can define rules in the following manner:

Rule Type	Target Applications or Folder Location	Application Match Method
Allow	Google Chrome	Certified Safe Software list | Known application dynamic search
Block	Browsers	Certified Safe Software list

Table 4.3.4 *Allow Google Chrome installation while blocking the rest of the web browsers.*

This method of allowing applications while blocking the rest in the same category (e.g. Web Browsers) is recommended if you want certain group of end-users such as Power Users and Domain Users who are granted with limited admin rights, to be able to control some applications on their own while making sure that practical use of company resources are enforced.

4.3.5 Lockdown Policy

In a nutshell, a Lockdown Policy creates SHA1 hashes of all present applications in an endpoint so that it will allow only these applications to run on the system.

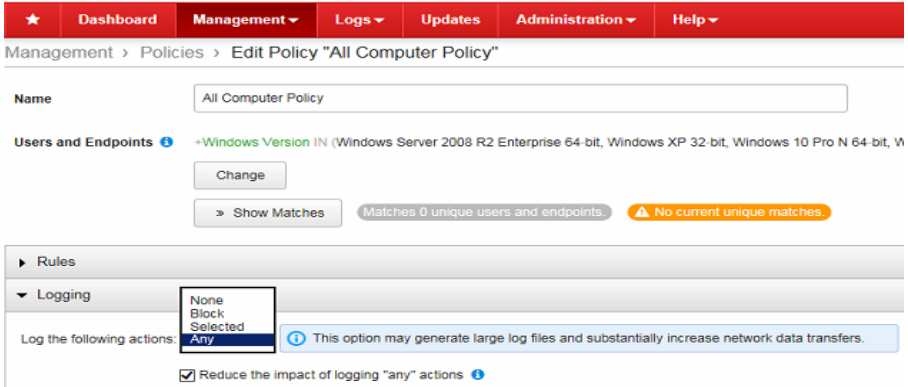
IMPORTANT: *Features such as “Trusted Source” and disabling of “Driver Support (Kernel-level Blocking)” will NOT work if the Lockdown Rule is assigned to a User-Based Policy (see 4.1.4 Rules Guidelines)*

Enable the “Log-only mode” before deploying this policy and be sure to select only a group of endpoint systems to evaluate the result prior to fully implementing the rule to a larger group of endpoints. Use the EAC Log Query Screen to identify which applications are affected by this rule and create consequent “Allow” rules that will be used alongside the Lockdown rule. We can also leverage the “Trusted Source” feature as described in 4.1.3 Add/Edit Rule Screen so that subsequent processes of the permitted applications in the “Allow” rule will not be denied from running in the Lockdown policy.

Visit our Online Help and learn more about TMEAC Monitoring features.

4.3.6 Default “Catch-all” Policy

We can monitor the behavior and activities of all applications on endpoints with a “Catch-all” Policy. This is done by creating a Computer-based Policy without assigning any rules (not even Lockdown rule), and configured to Log “Any” actions to all applications on endpoints. When no Rule is assigned to a policy, the rule “Identify” is automatically applied. Use this policy as a baseline with the lowest priority that matches only Windows OS or System Accounts, during the Deployment Planning phase to help determine the acceptable usage policy based on the device type.



Management › Policies › Edit Policy "All Computer Policy"

Name All Computer Policy

Users and Endpoints +Windows Version IN (Windows Server 2008 R2 Enterprise 64-bit, Windows XP 32-bit, Windows 10 Pro N 64-bit, W

Matches 0 unique users and endpoints.

⚠ No current unique matches.

Log the following actions: None / Block / Selected / Any

This option may generate large log files and substantially increase network data transfers.

☑ Reduce the impact of logging "any" actions

Fig 4.3.6 *Default “Catch-all” Policy monitors application activities without assigning any Rules.*

4.3.7 Roll-Your-Own Policy

Use the “Hash List Importer Tool” and create a rule with the “SHA-1 hash values” match method for company approved or owned applications and assign it to a policy that applies to mission-critical endpoints which do not always change or upgrade their applications such as the Fileservers, Database Servers and POS systems. The “Certificates” match method can also be used when creating these kinds of rules.

5 Administration and Configuration

This chapter covers the following product management best practices and recommendations:

- Server and Agent Management
- Web Console Management

5.1 Server and Agent Management

5.1.1 Component Update

Web Management Console > Updates

Aside from the endpoint Inventory Scan database, the Endpoint Application Control Server keeps and maintains other server and client side components which are regularly updated whenever a new version is available in Trend Micro Active Update cloud. Here's the list of AC Components and the recommended update schedules.

Certified Safe Software (Update Frequency: Daily)

This is the whitelist pattern which Trend Micro updates in a daily basis.

TMEAC Agent Setup x86/x64 | Server UI & Dashboard Widgets (Update Frequency: Weekly)

Product build and new version releases occurs in a quarterly (for product patches) and yearly (for Service Pack and Product Version) basis.

5.1.2 Active Directory Integration

Web Management Console > Administration > Server Settings

Enable the Active Directory Server Integration to accurately specify Active Directory Users as targets when creating User-based Policies (see 4.2.3 Policy Guidelines). To secure communication between Endpoint Application Control and Active Directory servers, select the “Digest-MD5” authentication method over the “Plain Text”.

Manually configure Active Directory Server settings in Endpoint Application Control
http://esupport.trendmicro.com/solution/en-US/1105988.aspx

5.1.3 Trend Micro OfficeScan Integration as a Plug-In Service

See Managing Plug-In Programs and Installing Agents Using the OfficeScan Plug-In online help.

Endpoint Application Control 2.0 Patch 1 can be managed as a Plug-in Service in OfficeScan 10.5 or later to enable deployment of AC Agents to endpoints with OfficeScan installed. To ensure accurate AC Agent deployment status, review the following guidelines:

- Regularly do a "Synchronize with OfficeScan" to get updated state of each endpoints in the list.
- When you deployed AC Agent from PLS, never use other methods when upgrading or uninstalling the agent component.
- Only use PLS to deploy AC Agent to OfficeScan managed endpoints.

5.1.4 Trend Micro Control Manager Integration as a Managed Server

See Registering with Control Manager online help.

As the name implies, Trend Micro Control Manager is a product that centralizes management of Managed Entities. As such, deployed Policies from Control Manager takes precedence over the policies deployed from the AC Server(s). Thus, it is recommended to use ONLY the Trend Micro Control Manager for Application Control Policy Management. However, if you only intend to use Control Manager for centralized logging and viewing of Application Control Statistics through the Dashboard and Widgets, manage your policies only from the EAC WebUI (see 4.2.1 Managing Policies).

5.1.5 Agent-Server SSL Communication

Before deploying AC Agent component to endpoints, make sure to import the TMEAC Self-Signed Cetificate (TMAC_CA_Cert.pem) on target endpoints to encrypt communication when transferring information between the Agent and Server. Follow the steps in the below Trend Micro Knowledgebase article:

Agent does not appear on the web console of Endpoint Application Control (EAC)
http://esupport.trendmicro.com/solution/en-US/1102669.aspx

See "TLS Considerations" in Endpoint Application Control 2.0 Patch 1 Online Help for more information about enhancing password and communication security in Endpoint Application Control.

5.2 Web Console Management

5.2.1 Dashboard and Widgets

We recommend that at least the following widgets are included and placed on the area best seen on the dashboard page:

a. Health Meter – Displays the health-level of Endpoint Application Control environment based on selected "Unhealthy" indicators such us number of Applications started but not in Certified Safe Sofware list, Applications not in recent inventory database, and so on. See Health Meter Widget section of the product's online help.

b. Key Performance Indicator – Displays average number of endpoint and application events (occurrences of blocked applications and disconnected agents) over time period. See Key Performance Indicators section in the product's online help.

c. Server Summary – Displays overall EAC Server system performance and status.

d. User and Endpoint Summary – Displays AC Agents' overall status such as average or number of up-to-date vs out-of-date agents, Top 3 Applied Policies and so on.

Review all existing tabs and re-group them, or reconfigure each widgets as you see fit to allow administrators to easily switch between tabs. This allows for easier management for large scale environments.

5.2.2 User Accounts

The EAC Web UI supports multiple user logins to allow other users to login to the Web Console and perform administrative tasks. This feature is helpful when viewing what recent changes were made by other users who have been given access to the EAC WebUI.

5.2.3 Logs Query

Web Management Console > Logs > Query

We can view almost all kinds of EAC Events using logs query. Not only it can help administrators see all blocked and allowed applications by rules and policies from each endpoints, it can also generate series of events of the EAC Server itself like Pattern Updates, Server Connectivity, changes to Rules, Policies and Server Settings and who's EAC User Account Administrator made those changes. Administrators can also save current searches or export to CSV for record purposes.

Administrators can manage the amount of information that the AC Server will keep in the *Logs > Maintenance* screen and change the preconfigured Purge size and frequency as seen fit. Refer to 2.1 Server Scaling Recommendations to know the minimum available disk space that the server must have to store logs depending on the number of managed endpoints.

6 Product Tools

6.1 Hashlist-Importer

The tool can be downloaded from the Endpoint Application Control Server install directory:

for x86-bit OS

C:\Program Files\Trend Micro\Endpoint Application Control\hashlist-importer.zip

for x64-bit OS

C:\Program Files (x86)\Trend Micro\Endpoint Application Control\hashlist-importer.zip

Pre-Requisite:

You have to install "Microsoft Visual C++ 2010 Redistributable Package (x86)" before running the tool on the endpoint.

https://www.microsoft.com/en-US/download/details.aspx?id=5555

Tool Usage

Copy and extract the "hashlist-importer.zip" to a local folder of the target endpoint and run the following command argument:

```
>HashListImporter.bat List "SourcePath=%windir%"
```

When this command succeeds, it writes the hashes of all executables below **C:\Windows** into a “sha1-list.txt” file. The list can be used to create or edit a Rule with “SHA-1 hash values” match criteria.

Running "HashListImporter.bat" with NO arguments displays all available Commands and Options. This tool can also be used to create and import hash list to the Endpoint Application Control Server as a new rule or to update and existing rule. Refer to the Trend Micro Knowledgebase below:

*Creating SHA1 hash lists from a set of *.exe, *.com, *.scr, and *.bin files in Endpoint Application Control (EAC)*

http://esupport.trendmicro.com/solution/en-US/1102651.aspx

7 Backup and Disaster Recovery

7.1 Full Backup

A complete backup of Application Control Server can be performed at cold state, meaning all services related to Application Control Server must be stopped. The full backup can be easily achieved by copying the complete folder “$INSTALL_DIR/AcServer-Data”.

This full backup contains all settings, policies, rules, logs, statistical client data and also all volatile cached information.

> *Main reason why this backup requires the services to be shutdown is databases and tree stores. Their copy inside a backup set would not be restorable when the services were running at the time of the backup.*

Restoring a Full Backup

Pre-requisites:

- Complete content of "**$INSTALL_DIR/AcServer-Data**" was backupped in **cold-state**.
- A working (e.g. fresh installed) instance of ACSERVER can be found at "**$INSTALL_DIR**“

Steps to Restore:

1. Shutdown the service.
2. Replace current content of "**$INSTALL_DIR/AcServer-Data**" with the backup.
3. Start the service.