

# Control Manager (TMCM) 7.0 Best Practice Guide



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.

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

Copyright© 2018 Trend Micro Incorporated. All rights reserved.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact your Technical Account Manager.

## Contents

<b>Preface</b> .....	<b>6</b>
<b>1. Product Description</b> .....	<b>7</b>
<b>2. Site Planning</b> .....	<b>7</b>
2.1. Single Site .....	8
2.2. Multiple Sites .....	8
Considerations .....	9
<b>3. Policy Management</b> .....	<b>10</b>
3.1. Planning Policy Management per Product .....	10
3.1.1. Get an overview of the settings available .....	10
3.1.2. Which policies will take effect first (Specified, Filtered) .....	13
3.1.3. Planning policy for specific machines (Specified Policy) .....	13
3.1.4. Planning policy for most machines (Filtered Policy) .....	19
3.2. Central Management and Policy inheritance .....	24
3.3. Effects of removing Policies .....	33
3.4. Coverage of User who creates the policy .....	33
3.5. User-based Device Control .....	39
<b>4. Log Query</b> .....	<b>45</b>
4.1. Log Query summary .....	45
4.2. How to query logs .....	45
4.2.1. Basic Filters - Data View .....	46
4.2.2. Basic Filters - Product Scope .....	47
4.2.3. Basic Filters - Time Range .....	48
4.2.4. Advanced Filters .....	48
4.2.5. Query Results .....	49
4.2.6. Save and Share the Query Results .....	50
4.3. Role-Based Access Control Log Queries .....	51
4.4. Drill-down Query Views .....	52
4.5. How to Aggregate Logs .....	53
4.6. How to Delete Logs .....	54
4.7. Log Query Specifications .....	55

- 4.8. Log Query Data Views .....55
- 5. Report ..... 58**
  - 5.1. Static template and Custom template .....58
    - 5.1.1. New Reports added in Static Template .....62
    - 5.1.2. New Reports added in Static Template .....63
  - 5.2. Static template and Custom template .....64
- 6. Connected Threat Defense (CTD) ..... 67**
  - 6.1. Architecture .....68
  - 6.2. Architecture .....69
    - 6.2.1. Type of Suspicious Objects.....69
    - 6.2.2. Suspicious Object Sync Interval.....70
    - 6.2.3. Suspicious Object Sync Now .....72
  - 6.3. Hub and Node TCM .....74
    - 6.3.1. Hub and Node.....74
    - 6.3.2. How to register Hub and Node TCM .....75
  - 6.4. Suspicious Object Tools .....77
  - 6.5. IOC Management .....78
    - 6.5.1. Adding IOCs.....79
    - 6.5.2. Removing IOCs.....79
    - 6.5.3. Impact Assessment.....80
    - 6.5.4. At-risk Endpoints .....81
    - 6.5.5. OfficeScan Endpoint Isolation.....82
  - 6.6. CTD Integrated Products .....84
- 7. Major Functions and Tips ..... 85**
  - 7.1. Early Discovery.....86
  - 7.2. Minimize Threat Influence .....95
  - 7.3. Deliver latest pattern and engine .....96
  - 7.4. Minimize false alarm detection.....97
  - 7.5. Modify Settings after incident review .....97
- 8. Migration from Cascading Mode..... 98**
  - 8.1. Collect Configurations .....98
    - 8.1.1. User Accounts and Roles .....98
    - 8.1.2. Product List .....98

- 8.1.3. Policy .....99
- 8.1.4. DLP Templates and Identifiers .....99
- 8.1.5. Report .....99
- 8.1.6. Notifications .....99
- 8.1.7. Update .....100
- 8.1.8. Suspicious Objects .....100
- 8.1.9. Other Settings .....100
- 8.2. Review/Re-design of management model .....101
  - 8.2.1. Account and Access Control .....101
  - 8.2.2. Product Grouping .....102
  - 8.2.3. Policy .....103
  - 8.2.4. Notifications .....103
  - 8.2.5. Reports .....103
  - 8.2.6. Scheduled Update/Deploy Plan .....104
  - 8.2.7. Register Products .....104
- 8.3. Migration and Configuration .....104
  - 8.3.1. Evaluate when to do the migration .....104
  - 8.3.2. Install TCM .....104
  - 8.3.3. Apply some of the basic configuration .....104
  - 8.3.4. Moving managed products .....105
  - 8.3.5. Post Migration .....105
  - 8.3.6. Administrator logon .....105
- Appendix A: TCM functions with managed products ..... 106**



# Preface

Welcome to Trend Micro Control Manager 7.0 Best Practices Guide. This document is designed to help resellers and customers develop a set of best practices when deploying and managing the Trend Micro Control Manager (TCCM).

This document is also designed to be used in conjunction with the following guides, both of which provide more details about TCCM than are given here:

- Trend Micro Control Manager 7.0 Installation Guide
- Trend Micro Control Manager 7.0 Administrator's Guide

# 1. Product Description

Trend Micro Control Manager (TMCM) is a security management solution that gives an administrator the ability to control the enterprise products or appliances from a central location -- regardless of the program or the appliance's physical location or platform. It allows the formulation of effective deployment and response plans.

## 2. Site Planning

In this document, you will learn about deployment methods for Control Manager, including their advantages and disadvantages. Specific examples are presented based on the deployment methods.

*Tip For large and very large enterprises, contact the Trend Micro solution architects for guidance.*

This document uses the term site. A site is an independent region within an organization that has its own IT department. It is separate from other regions—physically across different segments of the network, or administratively handled by another team. In most situations, a site would be country- or continent-based.

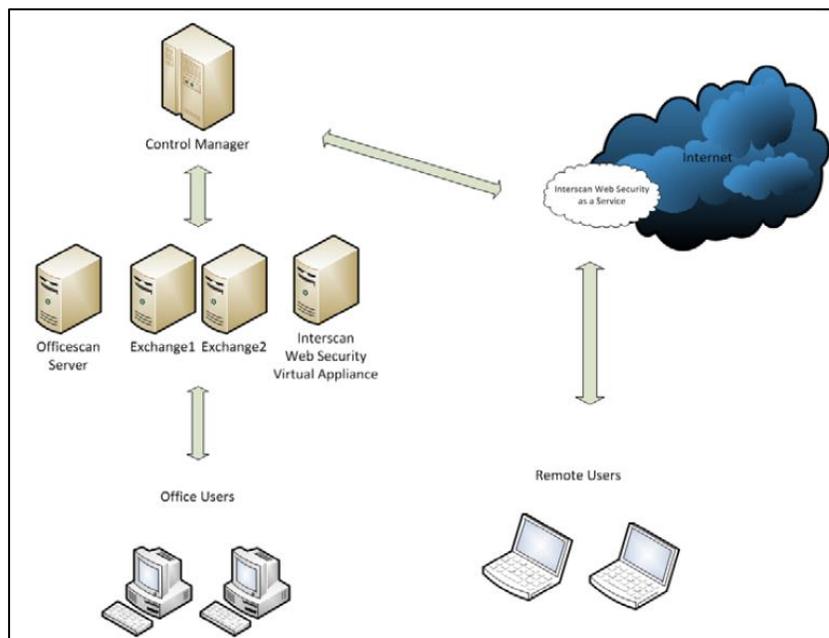
Planning the placement of Control Manager, in conjunction with a target site(s), is a key step.

In most deployments, a single Control Manager server is sufficient for most regions. Having a single Control Manager server in one site is the primary application of central management. A Control Manager server is required for organizations with multiple Trend Micro products installed. With one site, the communication between Control Manager and its managed products is open. Although a site is generally contained within a single datacenter, a datacenter may have multiple sites. For example, separate IT departments may have managing servers for their respective sites within the same datacenter.

DIFFERENT DATACENTERS - Ports must be opened to ensure connectivity between the Control Manager server and registered managed products located in different datacenters. For details, refer to <http://esupport.trendmicro.com/solution/en-US/1038211.aspx>.

## 2.1. Single Site

The following is an example of a single-site deployment:



The company runs the following solutions for single and small enterprise:

- Small enterprise
  - A single OfficeScan deployment, which protects 5,000 endpoints
  - Servers running ScanMail for Exchange, which protect the Exchange servers
  - A subscription to InterScan Web Security as a Service

## 2.2. Multiple Sites

Multiple IT departments and sites are typical features of a large network environment used by multinational corporations. Although there are multiple sites, it is still possible to manage multiple Trend Micro products using a single Control Manager server.

The biggest advantage of having a single Control Manager server serving multiple sites is having only one management console. This simplifies administration by creating policies, templates, user roles, and other settings through a single Control Manager server. Consequently, there is only one update source. This approach limits the number of endpoints that connect to the Internet to download updates and reduces network traffic.

## Considerations

Consider the following when deploying a single TCM server on multiple sites:

- The hardware features of the servers hosting TCM and Microsoft™ SQL Server™ must be powerful enough.
- The firewall ports must be open to ensure connectivity between the TCM server and agents on managed products. For details, see <http://esupport.trendmicro.com/solution/en-US/1038211.aspx>.
- TCM must be positioned where sufficient bandwidth between servers and agents is available. This is important if Control Manager will serve as the source for component updates.
- The TCM server has Internet connectivity.

This allows TCM to download updates and use the License Extension feature. Hosting TCM on a server without Internet connection prevents the use of such features.

- Medium enterprise
  - A single or multiple OfficeScan servers deployment, which protects 20,000 endpoints
  - Servers running ScanMail for Exchange, which protect the Exchange servers
  - Deploy multiple InterScan Web Security Virtual Appliances
  - Apply the Connected Threat Defense solution
- Large enterprise
  - Multiple OfficeScan servers deployment, which protect 100,000 endpoints
  - Servers running ScanMail for Exchange, which protect the Exchange servers
  - Deploy multiple InterScan Web Security Virtual Appliances
  - Apply the Connected Threat Defense solution
  - Integrate the Control Manager with third-party SIEM system

# 3. Policy Management

This chapter deals with Best Practices for Policy Management. Policy Management is a powerful functionality in Control Manager which allows administrators to enforce settings on specific products and specific targets. However, it is an option which can be easily misunderstood. The chapter deals with planning, testing, implementing, and administering policy Management.

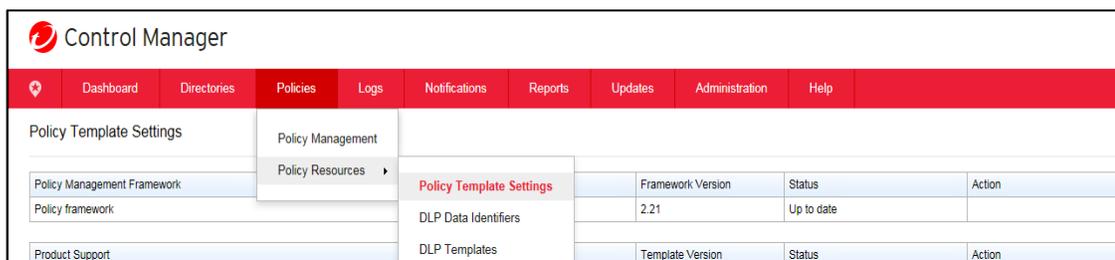
## 3.1. Planning Policy Management per Product

### 3.1.1. Get an overview of the settings available

#### Which products support policy Management

The first important step in planning the Policy Management is to see the settings which can actually be implemented in Policy Management. Not all settings can actually be implemented in policy Management. It is important for administrators to be able to find which settings are available.

To see the actual list of products which support policy management, an administrator can easily find it in the Control Manager console. Just go to **Policy** -> **Policy Resources** -> **Policy Template Settings**.



The “Product Support” table lists the products which support Policy Management. Pointing the mouse to the “i” button shows the product versions which support Policy management.

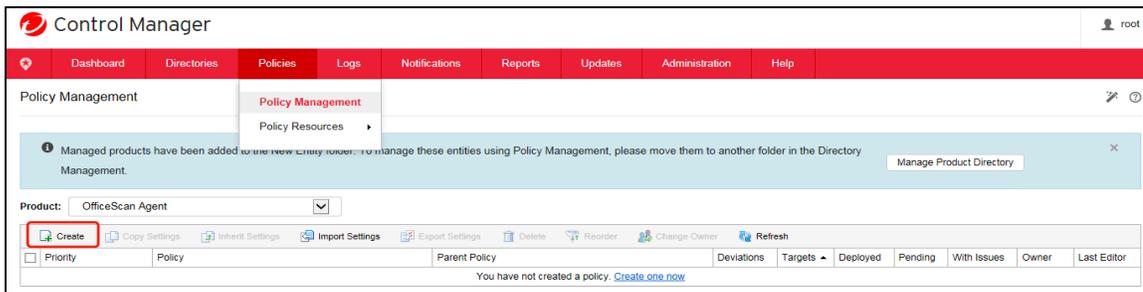
Policy Template Settings			
Policy Management Framework		Framework Version	Status
Policy framework:		2.21	Up to date
Product Support		Template Version	Status
Deep Discovery Inspector		1.19 (i)	Up to date
Endpoint Encryption		1.22 (i)	Up to date
InterScan Messaging Security Virtual Appliance		1.0 (i)	Up to date
InterScan Web Security Suite		1.2 (i)	Up to date
InterScan Web Security Virtual Appliance		1.2 (i)	Up to date
OfficeScan Agent		2.24 (i)	Up to date
OfficeScan Data Loss Prevention		2.1 (i)	Up to date
ScanMail for Microsoft Exchange		1.4 (i)	Up to date
Endpoint Application Control		1.0	Up to date
Trend Micro Endpoint Sensor		1.0	Up to date
Mobile Security for Enterprise		1.19	Up to date
Trend Micro Security (for Mac)		2.0 (i)	Up to date

The screenshot is based on the Control Manager 7.0 without additional widget updates (as of Jun 21, 2018). It is possible that a new set of widgets is released in the future. Once this occurs, it is possible that the list of products which support Policy Management will be increased.

### Which settings are available

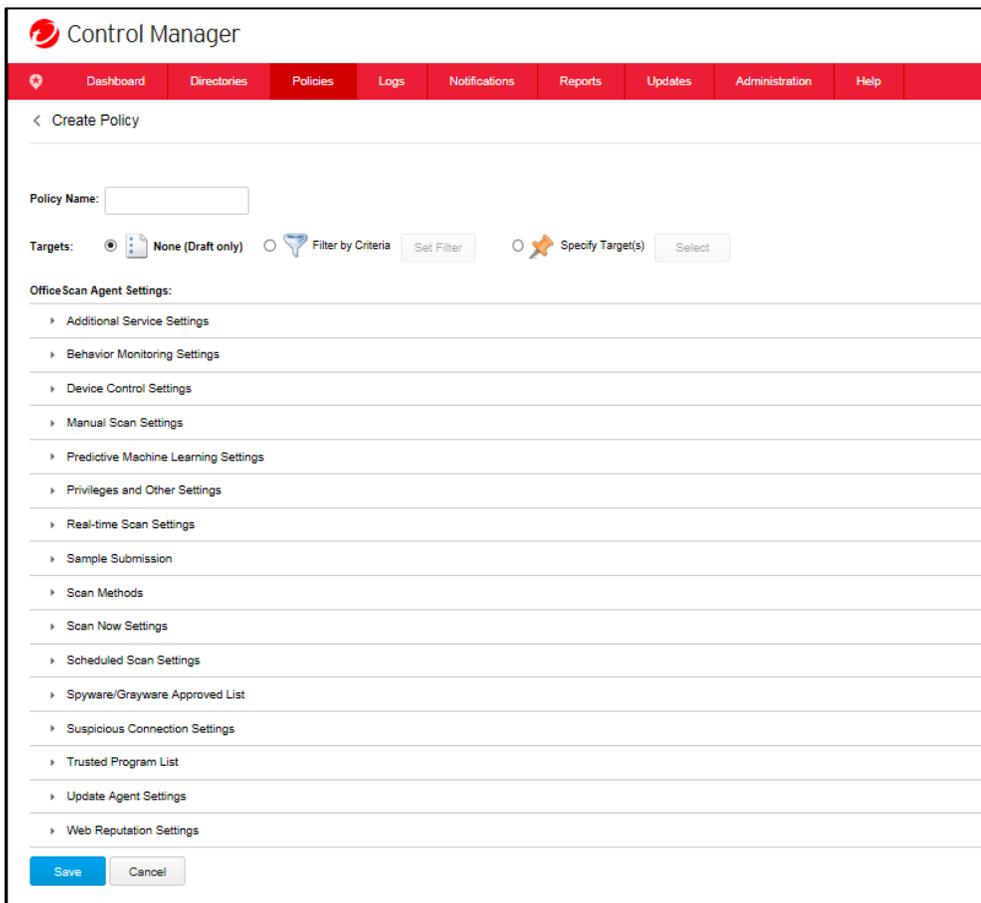
The next step is to check which settings are available for each product. This can be easily done by going to **Policies** -> **Policy management**.

Once there, a draft template can be created to see what settings are available. Draft policies are policies which are not deployed to any product. Simply set the product and click the **Create** button.



The screenshot shows the Control Manager interface. At the top, there is a navigation bar with tabs for Dashboard, Directories, Policies, Logs, Notifications, Reports, Updates, Administration, and Help. The 'Policies' tab is selected. Below the navigation bar, there is a 'Policy Management' section. A dropdown menu is open, showing 'Policy Management' and 'Policy Resources'. A message box is displayed, stating: 'Managed products have been added to the new Policy framework. To manage these entities using Policy Management, please move them to another folder in the Directory Management.' Below the message box, there is a 'Product:' dropdown menu set to 'OfficeScan Agent'. A 'Create' button is highlighted with a red box. Other buttons include 'Copy Settings', 'Inherit Settings', 'Import Settings', 'Export Settings', 'Delete', 'Reorder', 'Change Owner', and 'Refresh'. At the bottom, there is a 'Parent Policy' dropdown set to 'Parent Policy' and a status bar with buttons for 'Deviations', 'Targets', 'Deployed', 'Pending', 'With Issues', 'Owner', and 'Last Editor'. A message at the bottom says: 'You have not created a policy. [Create one now](#)'.

Below is a sample of how the OfficeScan Agent Policies look like.



Each option can be expanded to see what settings are available. Please note that this is different for each product and also, once new versions are available. There is no standard guideline, which makes it important for administrators to get an overview.

### 3.1.2. Which policies will take effect first (Specified, Filtered)

One important thing to note is that only one policy will take effect. This is very important in the planning. Administrators can make the mistake of thinking that two policies can be set on an endpoint or entity and that they will be merged. As such, it is very important to plan the policies.

The order of application is as follows:

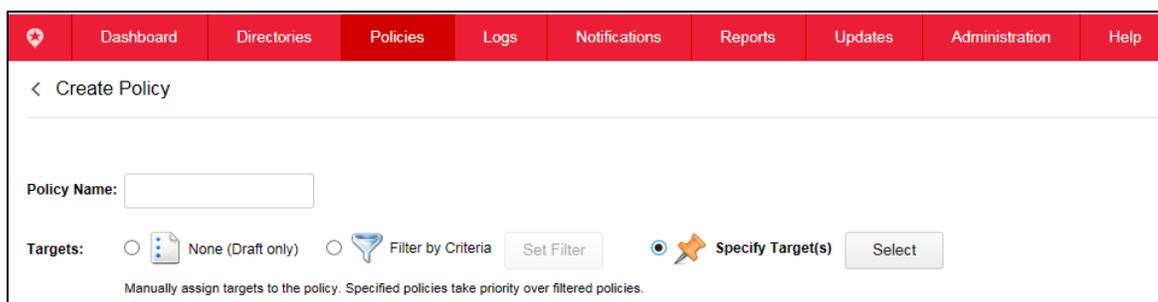
1. A Specified Policy takes precedence over a Filtered Policy.
2. A Specified Policy does not have a Priority number and only shows “Locked”.  
When an entity is assigned a Specified Policy, it is locked to that machine.

The next sub chapters will deal with examples on how to plan policies.

### 3.1.3. Planning policy for specific machines (Specified Policy)

In some situations, customers would want to set a policy only for a specific set of computers. These computers would deviate from the Filtered policy which would normally take effect. Specified Policies are then ideal for these situations.

Specified Policies are policies where the “Targets” are specified. This indicates that the machines are already present in the environment.



Dashboard Directories **Policies** Logs Notifications Reports Updates Administration Help

< Create Policy

Policy Name:

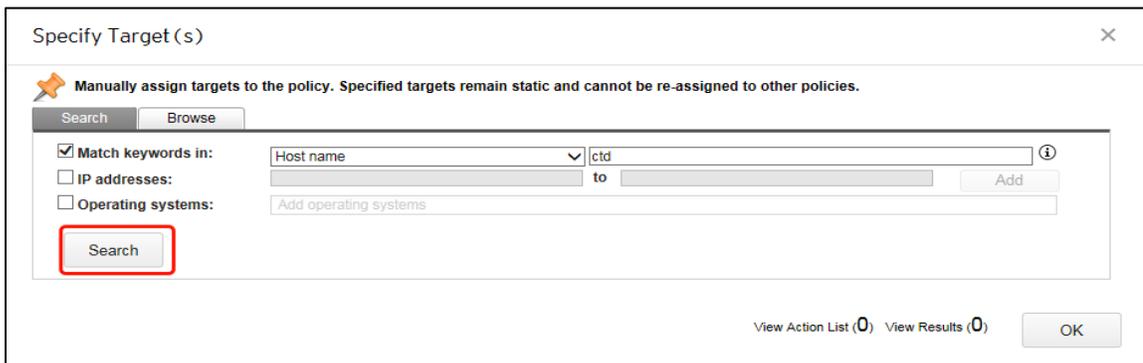
Targets:  None (Draft only)  Filter by Criteria   Specify Target(s)

Manually assign targets to the policy. Specified policies take priority over filtered policies.

Unlike the Filtered Policy, a Specified policy targets allows users to search for the endpoints or Entities where the policy is to be applied. As indicated, the entity must already be in the Control Manager server to be able to use a Specified Policy on it. By finding the entity or endpoint, administrators can add the Entity to the targets. The policy will not take effect on the endpoint until it is added to the list.

In the Search tab, when running a search using the first criteria, the Search button must be clicked first to find the match.

An example of which is running a search for “Host name” TCMC.



Specify Target (s)

Manually assign targets to the policy. Specified targets remain static and cannot be re-assigned to other policies.

Search | Browse

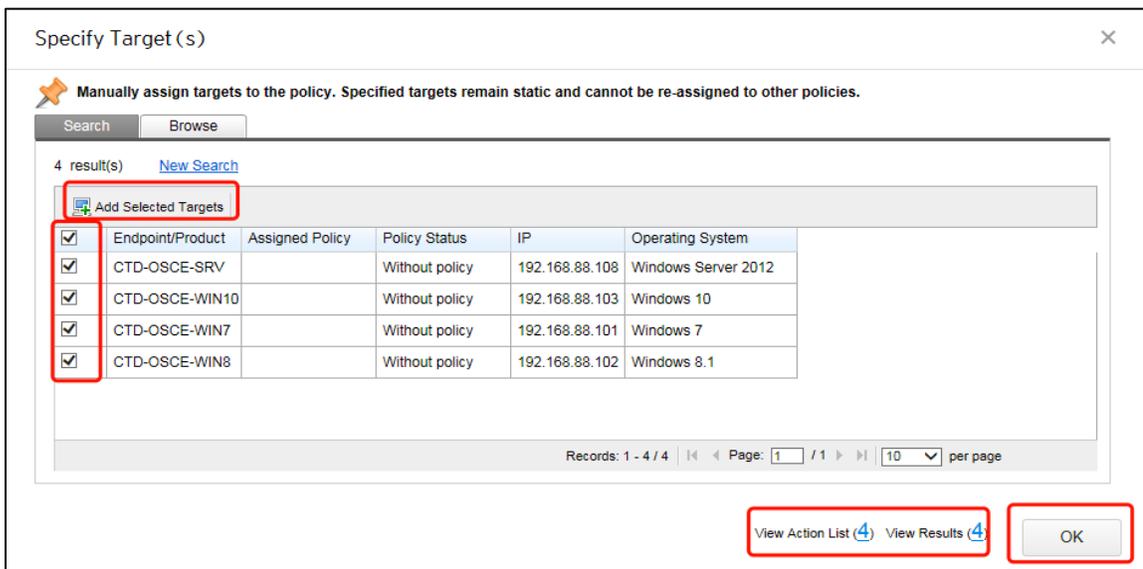
Match keywords in: Host name | ctd

IP addresses: | to | Add

Operating systems: Add operating systems

**Search**

View Action List (0) | View Results (0) | OK



Specify Target (s)

Manually assign targets to the policy. Specified targets remain static and cannot be re-assigned to other policies.

Search | Browse

4 result(s) [New Search](#)

**Add Selected Targets**

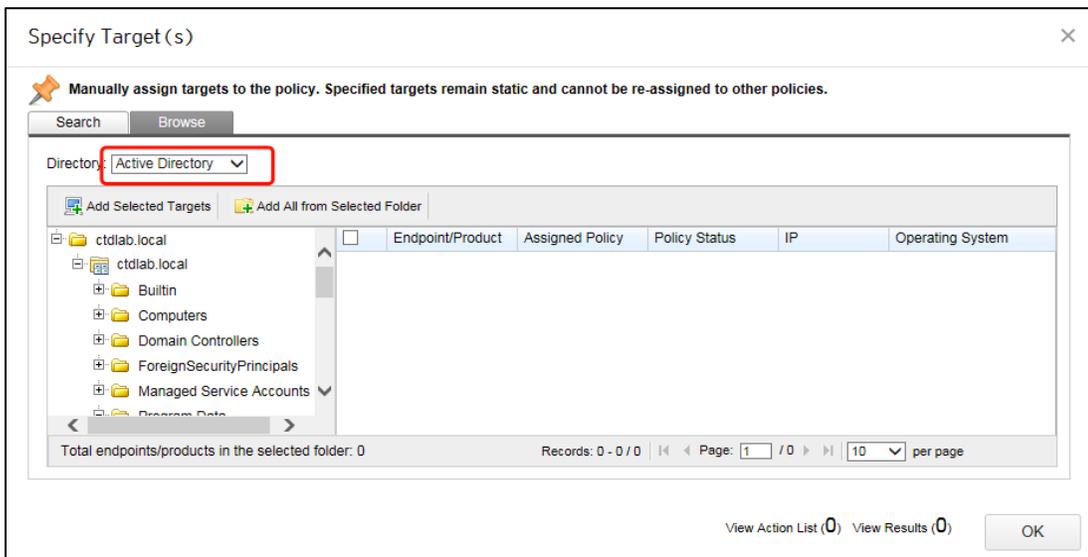
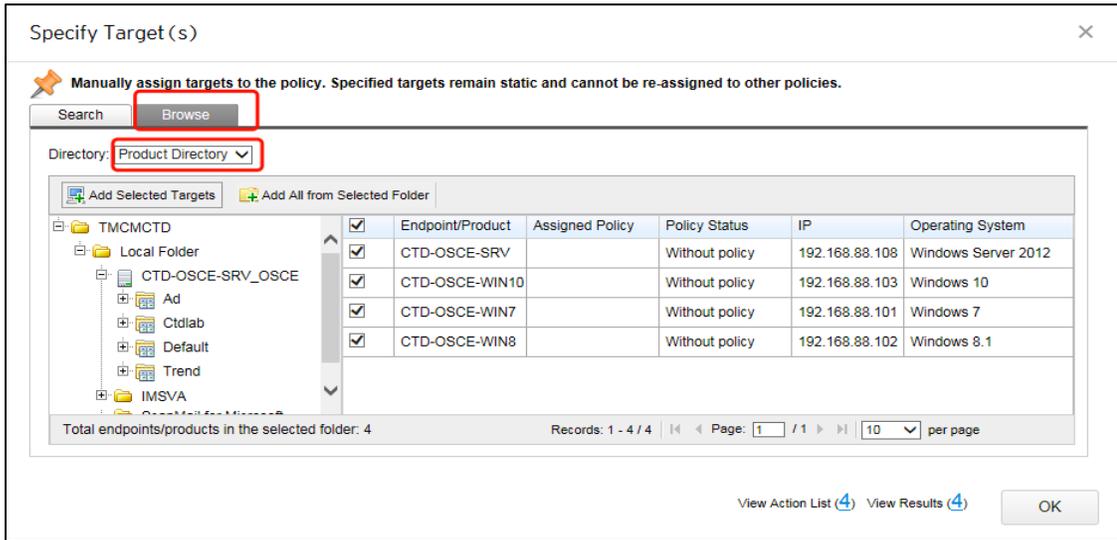
<input checked="" type="checkbox"/>	Endpoint/Product	Assigned Policy	Policy Status	IP	Operating System
<input checked="" type="checkbox"/>	CTD-OSCE-SRV		Without policy	192.168.88.108	Windows Server 2012
<input checked="" type="checkbox"/>	CTD-OSCE-WIN10		Without policy	192.168.88.103	Windows 10
<input checked="" type="checkbox"/>	CTD-OSCE-WIN7		Without policy	192.168.88.101	Windows 7
<input checked="" type="checkbox"/>	CTD-OSCE-WIN8		Without policy	192.168.88.102	Windows 8.1

Records: 1 - 4 / 4 | Page: 1 / 1 | 10 per page

**View Action List (4) | View Results (4) | OK**

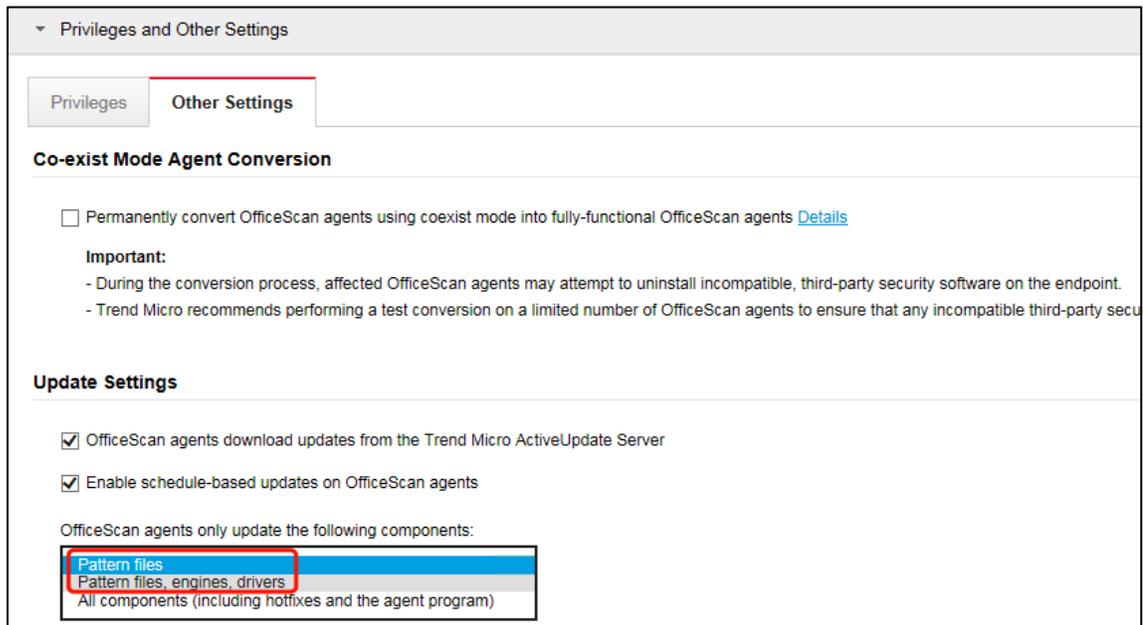
Only by selecting the entity and clicking Add Selected Targets will the policy take effect on the endpoint.

However, the main difference is the section for Product Directory and Active Directory. It is in a separate tab called "Browse". Using the browse tab, it is possible to specify directly the machines to apply, either from the Active Directory (if Active Directory integration is activated), or by browsing the tree. The "View Results" and "View Action List" shows which endpoints or entities will have the policy.



## Example 1: Enabling hotfix update for OfficeScan clients by using Specified Policies

The Trendy-A company has already created two Filtered Policies, one for users in the United States, and one for users in Germany. Every new computer that they add immediately receives the policy that disables deployment of OfficeScan hotfixes and program upgrades. This allows them to prevent a large amount of network bandwidth.



Privileges and Other Settings

Privileges Other Settings

**Co-exist Mode Agent Conversion**

Permanently convert OfficeScan agents using coexist mode into fully-functional OfficeScan agents [Details](#)

**Important:**

- During the conversion process, affected OfficeScan agents may attempt to uninstall incompatible, third-party security software on the endpoint.
- Trend Micro recommends performing a test conversion on a limited number of OfficeScan agents to ensure that any incompatible third-party security software is properly handled.

**Update Settings**

OfficeScan agents download updates from the Trend Micro ActiveUpdate Server

Enable schedule-based updates on OfficeScan agents

OfficeScan agents only update the following components:

- Pattern files
- Pattern files, engines, drivers
- All components (including hotfixes and the agent program)

After applying a hotfix on the OfficeScan server, the administrators will need to enable the option “OfficeScan agents can update components but not upgrade the agent program or deploy hotfixes”. However, they do not want to enable it for all OfficeScan clients, only for 100 clients at a time until all clients have completely upgraded.

To do this using Specified Policies:

1. Create a copy of the policy you want to modify and set the Target first to **None (Draft only)**. This allows administrators to plan properly the policy, but make sure that it does not apply first.
2. It is now possible to update the setting.

Privileges and Other Settings

Privileges Other Settings

### Co-exist Mode Agent Conversion

Permanently convert OfficeScan agents using coexist mode into fully-functional OfficeScan agents [Details](#)

**Important:**

- During the conversion process, affected OfficeScan agents may attempt to uninstall incompatible, third-party security software on the endpoint.
- Trend Micro recommends performing a test conversion on a limited number of OfficeScan agents to ensure that any incompatible third-party security software is removed.

### Update Settings

OfficeScan agents download updates from the Trend Micro ActiveUpdate Server

Enable schedule-based updates on OfficeScan agents

OfficeScan agents only update the following components:

All components (including hotfixes and the agent program) ▼

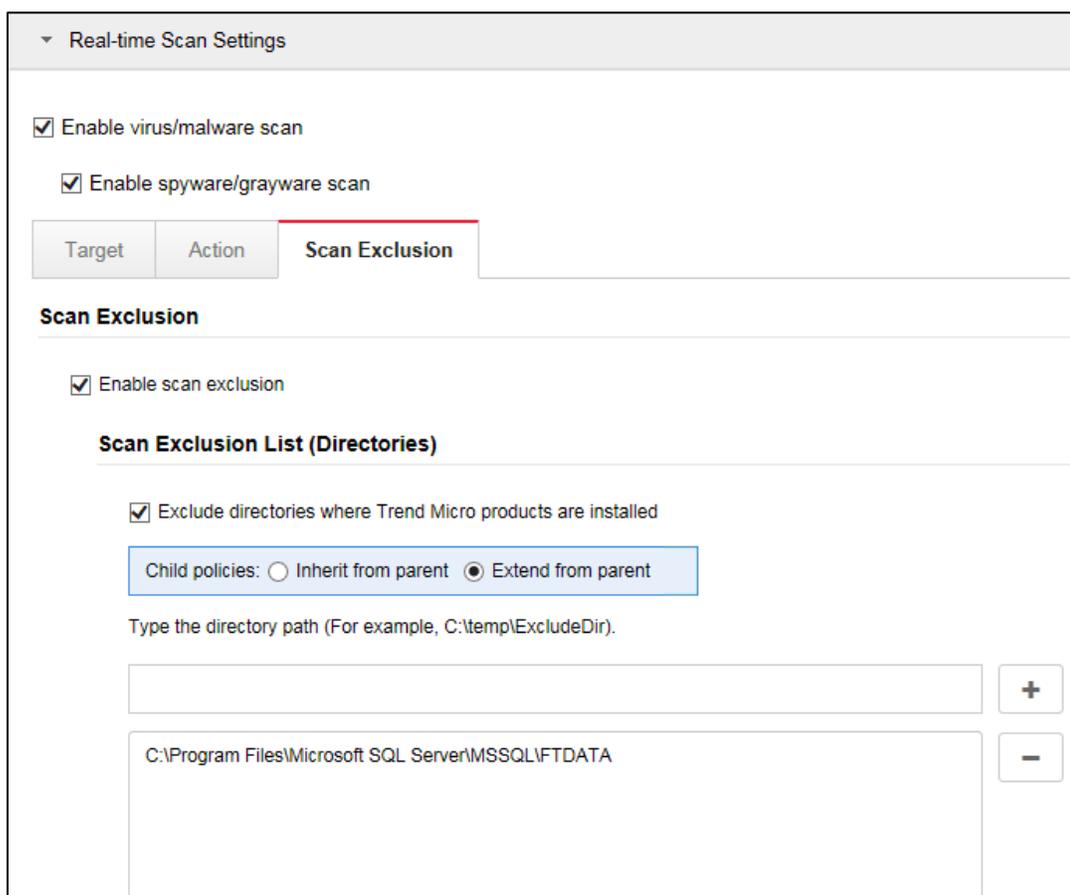
3. After making the changes, it is now possible to set the Target to “Specify Targets” and manually assign the OfficeScan clients chosen to be upgraded.
4. Please take note of the following:
  - If the previous policy was a Specified Policy, then the clients will be removed from the previous Specified Policy list. Please take note: Only one Policy per endpoint.
  - The Filtered Policy takes a lower precedence and will be in the bottom of the list.
5. Once the OfficeScan clients have finished applying the hotfixes or Service Packs, customer can now check if the OfficeScan client should be added again to the older specified Policies. This will allow the OfficeScan clients to restore old policies.
  - a. Assign the OfficeScan clients to “Specified Policies” if they are meant to be under previous “Specified Policies.”
  - b. The OfficeScan clients will be sorted into previous Filtered Policies automatically, once the “Specified Policy” is removed.
6. Once all OfficeScan clients are upgraded, it is now possible to delete the policy.

## Example 2: Specify different Exclusion Directories

The Trendy-B company has created a Filtered Policy for all Windows 2012 Servers in the Datacenter. However, they have noticed that they have started encountering performance issues on Microsoft SQL Servers. After searching through Trend Micro's knowledgebase, they had found an article that indicates specific folders to exclude from scanning to improve the performance of SQL Servers: <http://esupport.trendmicro.com/solution/en-US/1059770.aspx>

In this case, Specified Policies are also a good option to use. The steps are similar to the first example.

1. Create a copy of the policy you want to modify and set the Target first to **None (Draft only)**. This allow administrators to plan properly the policy, but make sure that it does not apply first.
2. In the Scan Exclusion, the SQL Server paths for exclusion can be added.

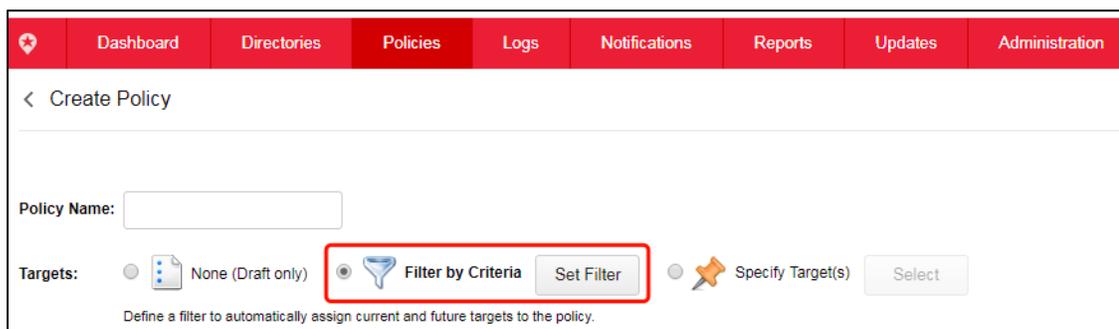


The screenshot shows the 'Real-time Scan Settings' window. Under 'Scan Exclusion', the 'Enable scan exclusion' checkbox is checked. The 'Scan Exclusion List (Directories)' section has the checkbox 'Exclude directories where Trend Micro products are installed' checked. Below this, the 'Child policies' are set to 'Extend from parent'. A text input field is labeled 'Type the directory path (For example, C:\temp\ExcludeDir)'. A list of excluded directories is shown, with 'C:\Program Files\Microsoft SQL Server\MSSQL\FTDATA' selected. '+' and '-' buttons are visible next to the input field and the list item, respectively.

3. After making the changes, the Target to "Specify Targets" can be set and manually assign the SQL Servers. The Search Criteria can be used to find the targets.

### 3.1.4. Planning policy for most machines (Filtered Policy)

In some situations, customers want to automatically assign a set of policies to entities based on a set of criteria. These would be the so-called Filtered Policy. These are set by choosing “Filter by Criteria” and setting the Filter.



By choosing this option, the policy will be automatically applied to any new entity that is registered to the Control Manager when:

- No other Filtered Policy with higher order matches
- No other Specified Policy matches
- The criteria matches

Please note that Filtered Policy takes lower precedence than Specified Policies.

Filtered Policies are ideal for the following scenarios:

1. A large number of computers have similar settings. These are normally baseline policies, or policies which must be enforced on all machines within the company unless exceptions are made. In this case, the Specified Policies become the exceptions, and the Filtered Policies are the rule if there are no exceptions.
2. Filtered Policies can also be applied to future machines. Even though, for example, an OfficeScan client is not yet installed, but once installed, and the criteria matches, the policy is automatically deployed.

The administrator’s guide explains what each of the settings available. We highly recommend to make sure to test first Filtered Policies before applying them.

#### Understanding the Filters for Filtered Policy

When setting the targets, the “Set Filter” option can be clicked and allows administrators to specify the targets of the Filtered Policy.

### Filter by Criteria

Define a filter to automatically assign current and future targets to the policy.

Match all of the selected criteria:

- Match keywords in: Host name  ⓘ
- IP addresses:  to  Add
- Operating systems: Add operating systems
- Directories: Product Directory

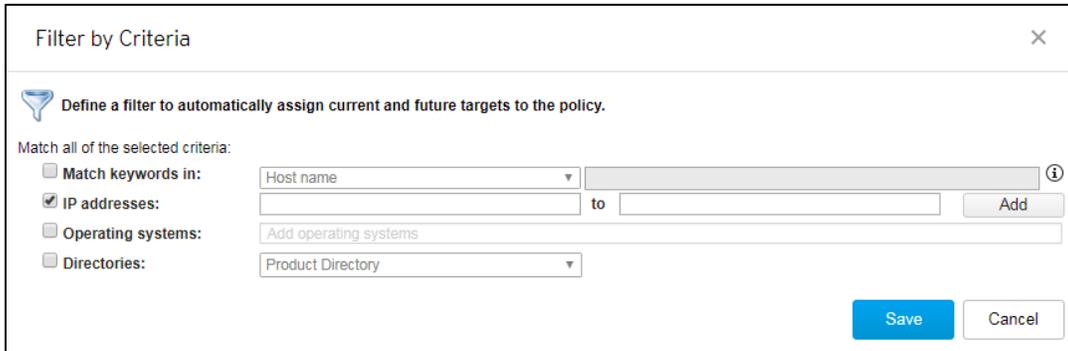
Save Cancel

Important to note are as follows:

1. When specifying this option, all criteria must match.
2. When a naming convention is available, it is also possible to use the Match keywords in: for Hostname.
3. Tree Paths are also available for OfficeScan clients in multi-domain environments.
4. For customers who have specific IP address ranges for their environments, it is also an option to take note when creating a policy.
5. Policies can be based on the Product Directory. This allows administrators to define policies for an entire folder within the Control Manager tree.
6. We also support AD filter which allows users to select targets in the OUs of synchronized forests.
7. The “Tree path” criteria has been renamed as “OfficeScan domain hierarchy”, and was moved to [Directories] from [Match keywords in].

### Example 1: Using IP addresses as criteria

**Scenario:** The Trendy-A company has all employees divided into IP address blocks for users using their production environment for each country:



172.16.0.1 to 172.16.1.254 - All users are from the United States

172.16.2.1 to 172.16.3.254 - All users are from the Germany

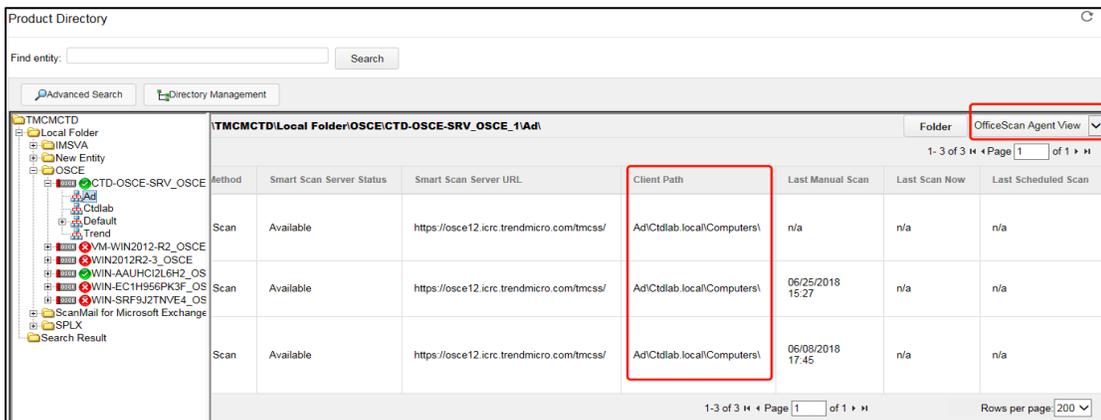
**Solution:** In this case, the administrators can use the IP addresses criteria to set the criteria to make sure that the Filtered policy applies to the IP address range.

### Example 2: Using OfficeScan Multi-layer domain

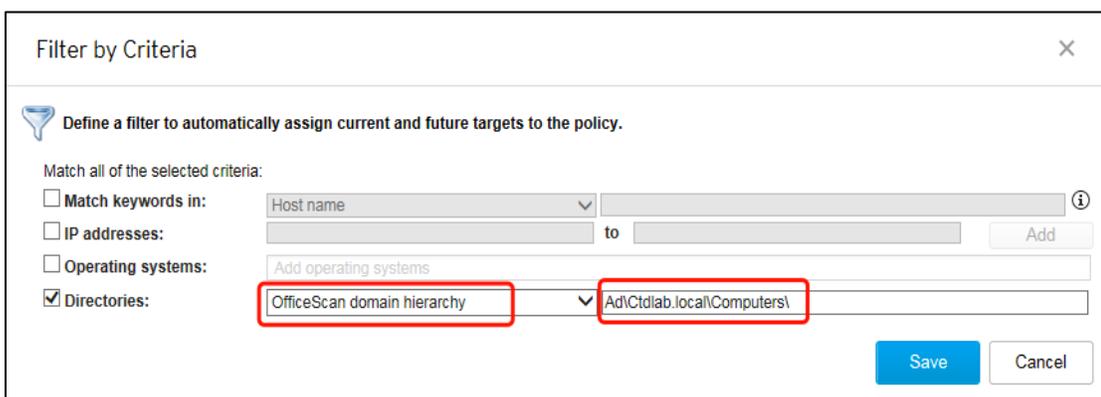
**Scenario:** The Trendy-B company wants uses OfficeScan Client Grouping to reorder the OfficeScan clients into the multiple layer Domains. The company decided that Control Manager must automatically create a configuration for all sub domains and also change them using the policy.

**Solution:** Control Manager is only able to display the first layer domain. This is a current limitation of Control Manager. To be able to configure multiple layer domains to be applied the sub-layer, multiple criteria must be specified and all the criteria must match:

Once “OfficeScan domain hierarchy” has been specified in Directories, the Client Path of the OfficeScan client can be seen in the OfficeScan client view from the Control Manager console.



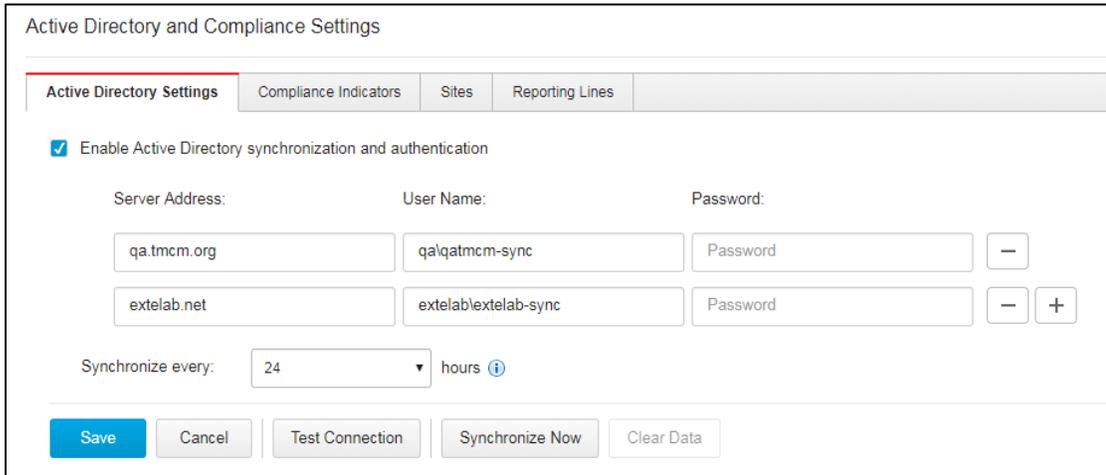
As you can see, the format is actually: layer1\layer2\layer3. As such, it is possible to set the criteria to be “layer1\layer2\layer3” or specify only “layer2\layer3”. Note that wildcards are not supported.



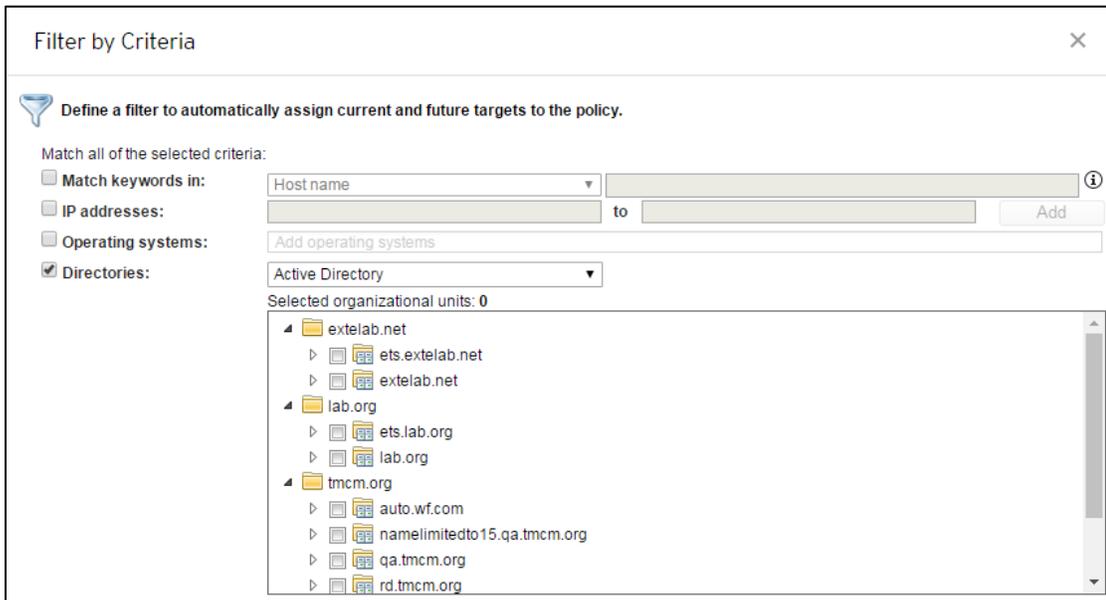
New OfficeScan clients added to this domain will automatically take the policy.

### Example 3: Using targets in the OUs of synchronized forests

Synchronization with multiple AD Forests is supported, which means that specific OUs from different AD can be selected.



The screenshot shows the 'Active Directory and Compliance Settings' window. It has tabs for 'Active Directory Settings', 'Compliance Indicators', 'Sites', and 'Reporting Lines'. The 'Active Directory Settings' tab is active. A checkbox 'Enable Active Directory synchronization and authentication' is checked. Below this are three rows of input fields for 'Server Address', 'User Name', and 'Password'. The first row has 'qa.tmcn.org', 'qa\qatmcm-sync', and 'Password'. The second row has 'extelab.net', 'extelab\extelab-sync', and 'Password'. A 'Synchronize every:' dropdown is set to '24' hours. At the bottom are buttons for 'Save', 'Cancel', 'Test Connection', 'Synchronize Now', and 'Clear Data'.



The screenshot shows the 'Filter by Criteria' dialog box. It has a close button (X) in the top right. Below the title bar is a funnel icon and the text 'Define a filter to automatically assign current and future targets to the policy.' There are four sections: 'Match all of the selected criteria:' with a sub-section 'Match keywords in:' containing a dropdown for 'Host name' and an input field; 'IP addresses:' with an input field and an 'Add' button; 'Operating systems:' with an input field and an 'Add operating systems' button; and 'Directories:' which is checked and contains a dropdown for 'Active Directory'. Below this is a list of 'Selected organizational units: 0' with a tree view showing folders for 'extelab.net', 'lab.org', and 'tmcn.org' with their respective sub-organizational units.

This is also supported in Specify Policy.

### Other important notes

As indicated in the samples, the Specified Policies are designed more for creating exemptions to Filtered policies. However, this is only a basic sample, but is a more recommended practice.

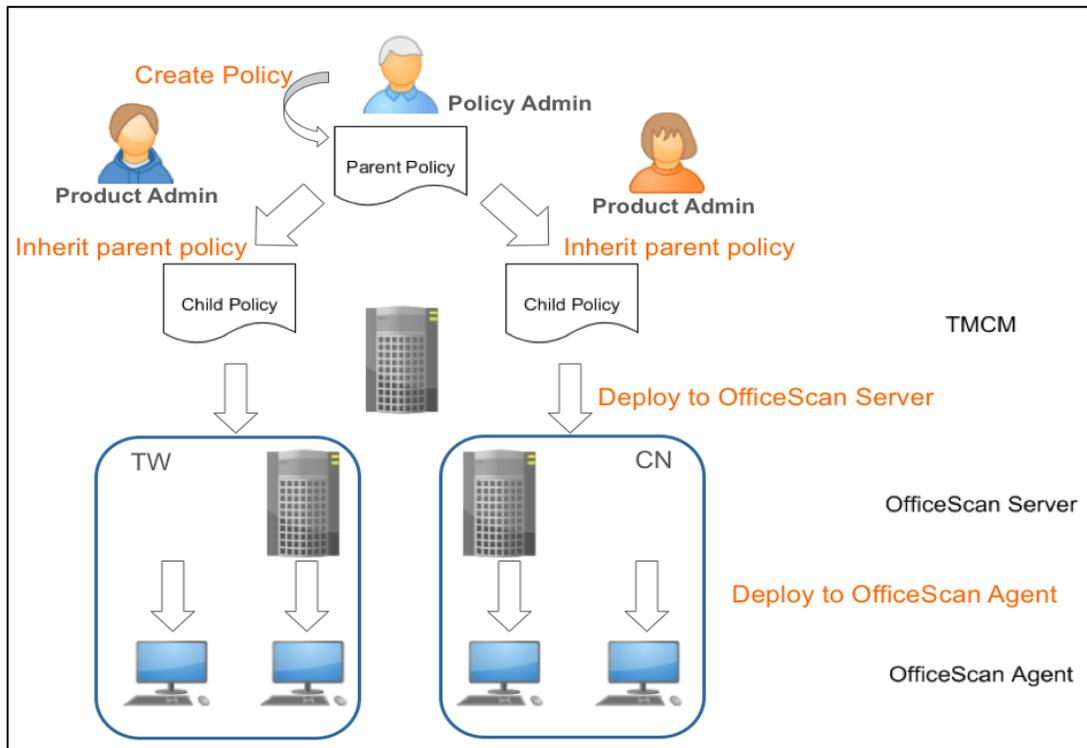
Another thing to note is that any specific policies we create are copies of the Filtered policies. This allows administrators to copy the original settings from old policies, and make minor deviations.

## 3.2. Central Management and Policy inheritance

By default, all permissions are set to be centrally-managed by Control Manager, which means that the settings of the Policy will take precedence over the Product console.

Our customer can benefit from the Policy inheritance feature.

This flow chart shows how policy inheritance works:



Note: The Policy Inheritance is applicable to OfficeScan only.

Once the policy admin creates a draft policy, the other policy owner can create the child policy by inheriting the parent policy. They can deploy the child policy to the specific OfficeScan server and agents.

Policy Management

Product: OfficeScan Agent b

<input checked="" type="checkbox"/>	Priority	Policy	Parent Policy	Deviations	Targets
<input checked="" type="checkbox"/>	1 <span style="border: 1px solid red; padding: 2px;">a</span>	<a href="#">Test_Sample</a>	N/A	N/A	Filtered

Endpoints/Products without policies: 10  
Total endpoints/products: 24

Policy Management

Product: OfficeScan Agent

<input type="checkbox"/>	Priority	Policy	Parent Policy	Deviations	Targets
<input type="checkbox"/>	Locked	<a href="#">scheduledscan_sample</a>	Parent Policy <a href="#">Test_Sample</a>	Deviations 1	Specified
<input type="checkbox"/>	1	<a href="#">Test_Sample</a>	N/A	N/A	Filtered

Endpoints/Products without policies: 10  
Total endpoints/products: 24

Deviation

Settings	Parent Policy: Test_Sample	Child Policy: scheduledscan_sample
Scheduled Scan Settings > Schedule	Weekly, every Monday. Start time: 12:00	Daily. Start time: 12:00

If the policy admin wants to change any of the settings for all OfficeScan agents, he can just edit the parent policy. The changes will affect all its child policies and be deployed to all the target agents.

There are three inheritance types:

- Customizable

Child policies:  Inherit from parent  Are customizable

- Extend from parent

Child policies:  Inherit from parent  Extend from parent

- Extend from parent + Neutralize List

**Scan Exclusion List (Files)**

Child policies:  Inherit from parent  Extend from parent

Type the file name or the file name with full path (For example, ExcludeDoc.hlp; C:\temp\excldir\ExcludeDoc.hlp).

**Child Policy Restrictions**

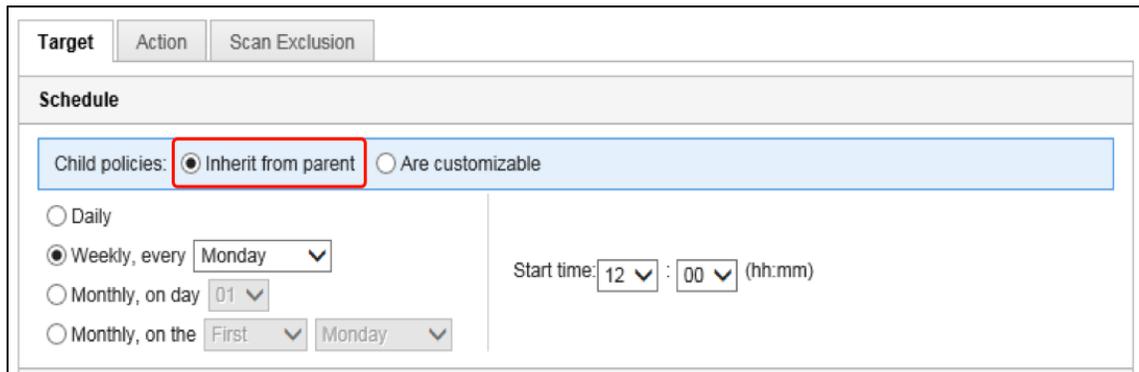
Child policies cannot exclude files in the following list

Type the file name or the file name with full path (For example, ExcludeDoc.hlp; C:\temp\excldir\ExcludeDoc.hlp).

Below are things to note per policy type:

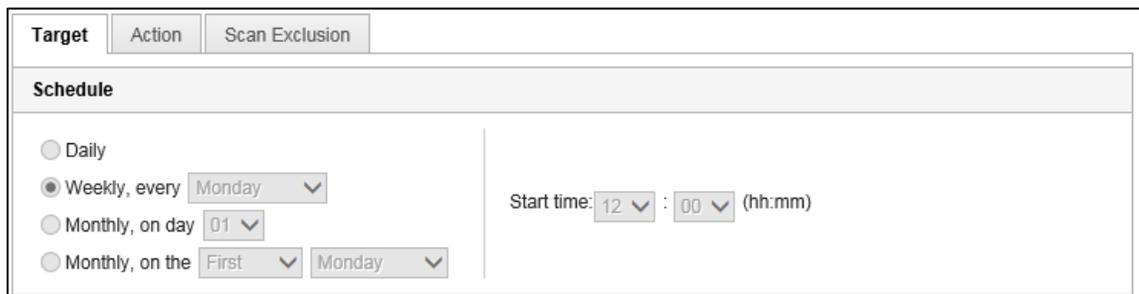
- For Customizable type:  
Policy admin can set child policies to inherit the setting from parent or customize by itself.  
If the permission is inheriting from the parent, the setting in child policy is disabled and the user cannot change the value of the settings.

– Parent Policy



The screenshot shows the 'Schedule' configuration for a Parent Policy. At the top, there are three tabs: 'Target', 'Action', and 'Scan Exclusion'. Below the tabs, the 'Schedule' section is highlighted. It contains two radio buttons: 'Inherit from parent' (which is selected and highlighted with a red box) and 'Are customizable'. Below these are four scheduling options: 'Daily', 'Weekly, every Monday' (selected), 'Monthly, on day 01', and 'Monthly, on the First Monday'. To the right of these options is a 'Start time' field set to '12 : 00 (hh:mm)'. The 'Monthly, on day 01' and 'Monthly, on the First Monday' options are greyed out.

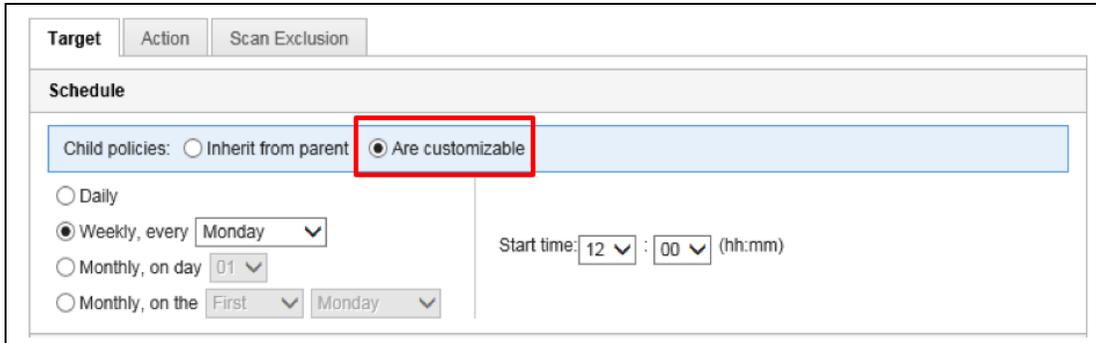
– Child Policy (options are grey, which means you cannot edit them)



The screenshot shows the 'Schedule' configuration for a Child Policy. It has the same tabs and layout as the Parent Policy. However, the 'Inherit from parent' radio button is not selected. The 'Are customizable' radio button is selected. The scheduling options are: 'Daily', 'Weekly, every Monday' (selected), 'Monthly, on day 01', and 'Monthly, on the First Monday'. The 'Start time' field is set to '12 : 00 (hh:mm)'. In this view, all scheduling options are greyed out, indicating they are not editable.

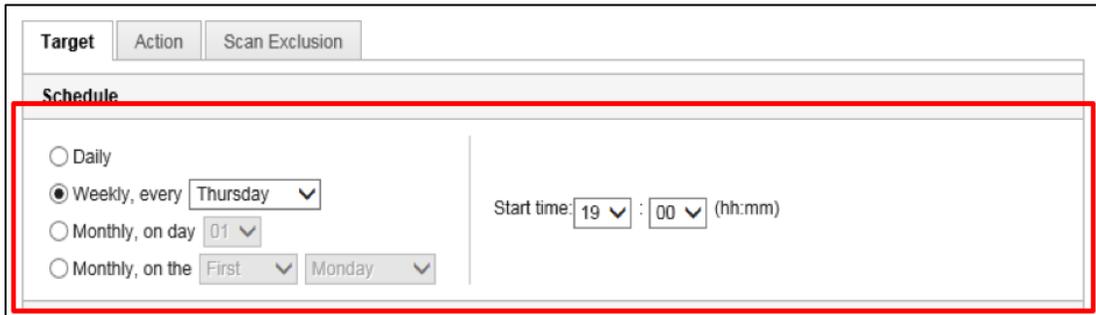
If the settings have been set to “Are customizable”, the value of settings can be changed in child policy.

– Parent Policy



The screenshot shows the 'Schedule' section of a policy configuration interface. At the top, there are three tabs: 'Target', 'Action', and 'Scan Exclusion'. Below the tabs, the 'Schedule' section is highlighted. It contains a 'Child policies' section with two radio buttons: 'Inherit from parent' and 'Are customizable'. The 'Are customizable' option is selected and highlighted with a red box. Below this, there are four scheduling options: 'Daily', 'Weekly, every Monday', 'Monthly, on day 01', and 'Monthly, on the First Monday'. The 'Weekly, every Monday' option is selected. To the right, there is a 'Start time' field set to '12 : 00 (hh:mm)'.

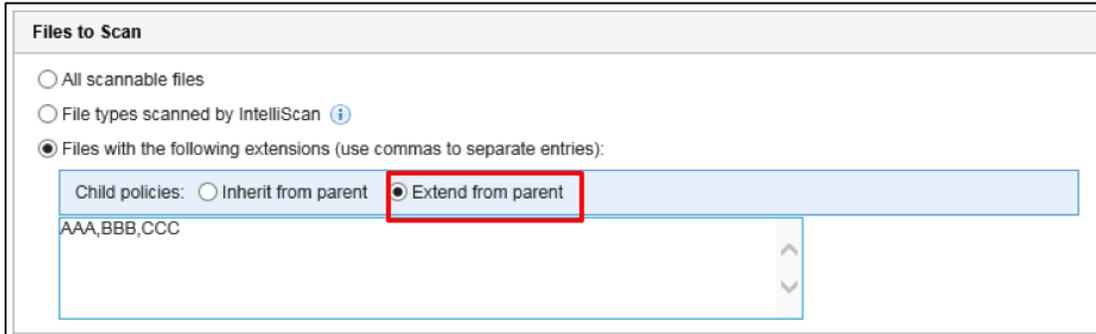
– Child Policy



The screenshot shows the 'Schedule' section of a child policy configuration interface. It features the same 'Target', 'Action', and 'Scan Exclusion' tabs as the parent policy. The 'Schedule' section is highlighted with a red box. It contains the same 'Child policies' section with 'Inherit from parent' and 'Are customizable' radio buttons. Below this, there are four scheduling options: 'Daily', 'Weekly, every Thursday', 'Monthly, on day 01', and 'Monthly, on the First Monday'. The 'Weekly, every Thursday' option is selected. To the right, there is a 'Start time' field set to '19 : 00 (hh:mm)'.

- For “Extend from policy” type:  
If you choose “Extend from parent”, you can extend the configuration to the child policy

– Parent policy



**Files to Scan**

All scannable files

File types scanned by IntelliScan ⓘ

Files with the following extensions (use commas to separate entries):

Child policies:  Inherit from parent  Extend from parent

AAA,BBB,CCC

– Child policy



**Files to Scan**

All scannable files

File types scanned by IntelliScan ⓘ

Files with the following extensions (use commas to separate entries):

AAA,BBB,CCC

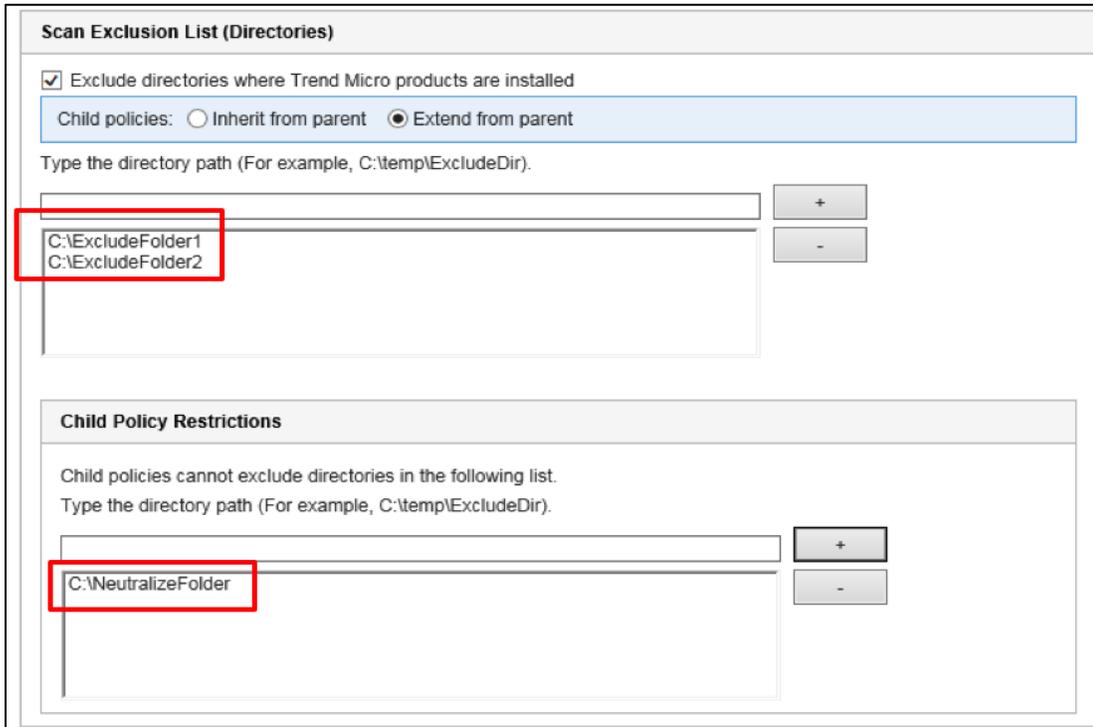
In addition to the above:

DDD,EEE

- For Extend from parent + Neutralize List type:  
“Extend from parent with neutralize list” settings can restrict the extend the settings of child policy.

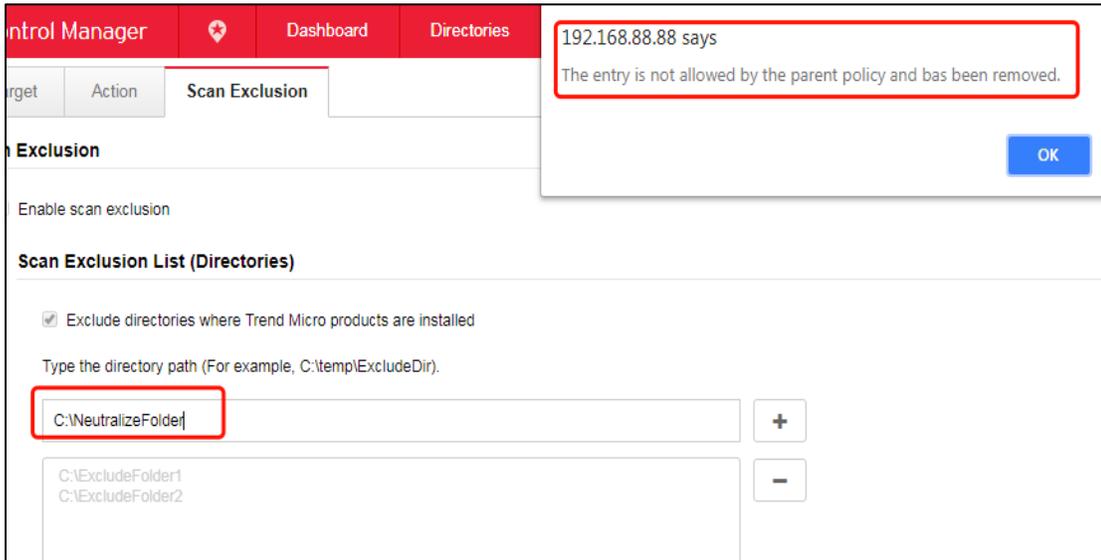
For example, the policy admin has added “C:\NeutralizeFolder” to the Child Policy Restrictions. This will make it so that the “C:\NeutralizeFolder” directory cannot be added by the Child Policy to the Scan Exclusion List.

– Parent policy



The screenshot displays two configuration windows from the Trend Micro Control Manager interface. The top window, titled "Scan Exclusion List (Directories)", has a checked option "Exclude directories where Trend Micro products are installed". Below this, the "Child policies" section shows "Extend from parent" selected. A text input field is followed by a list of directories: "C:\ExcludeFolder1" and "C:\ExcludeFolder2", with a red box highlighting these entries. The bottom window, titled "Child Policy Restrictions", contains the text "Child policies cannot exclude directories in the following list." and a list of restricted directories: "C:\NeutralizeFolder", also highlighted with a red box.

– Child policy



The screenshot shows the Trend Micro Control Manager interface. At the top, there are navigation tabs: "Control Manager", "Dashboard", and "Directories". The "Directories" tab is active. Below the navigation, there are tabs for "Target", "Action", and "Scan Exclusion". The "Scan Exclusion" tab is selected. A warning message box is overlaid on the interface, stating: "192.168.88.88 says The entry is not allowed by the parent policy and has been removed." with an "OK" button. Below the warning, the "Scan Exclusion" section is visible. It includes a checkbox labeled "Exclude directories where Trend Micro products are installed" which is checked. Below this, there is a text input field for "Type the directory path (For example, C:\temp\ExcludeDir)". The input field contains "C:\NeutralizeFolder|". To the right of the input field is a "+" button. Below the input field, there is a list of excluded directories: "C:\ExcludeFolder1" and "C:\ExcludeFolder2". To the right of this list is a "-" button.

Below are the configuration sections of OfficeScan Agent policies that supports inheritance:



### 3.3. Effects of removing Policies

When a policy is removed, Control Manager will no longer impose the settings to the product. However, the product does not rollback any settings. This is very important in the planning. If a setting was made on the product, and there is a need to roll back the setting, the rollback maybe done using the following:

1. If there is no more policy affecting the endpoint, a customer can log in using the Local console to revert to the original settings.
2. The customer can create another Filtered or Specified policy that will change the setting to the intended setting.

This is one of the reasons why it is recommended to have a Filtered Policy that enforces the default configuration settings of the products. The filtered policy essentially becomes the default setting.

### 3.4. Coverage of User who creates the policy

When a policy is created, administrators are able to specify:

1. The targets of the Policy.
2. The settings to be applied.
3. Change certain policy owner from a user to another user (or AD group).
4. Owner who last modify the policy will also be displayed

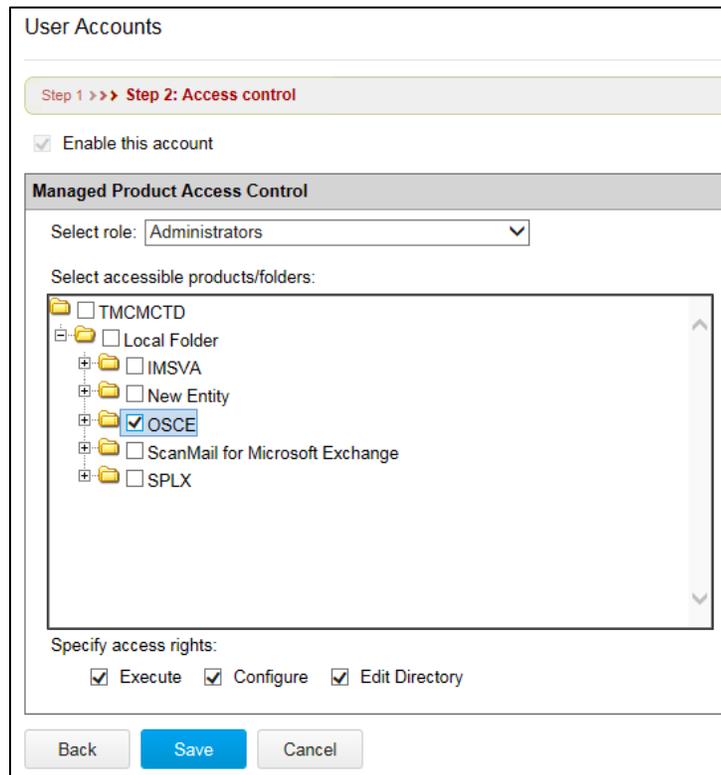
It is worth noting that the Policy can only cover endpoints where the Control Manager user has access. As such, it becomes important also to plan who will create the Policy.

It is also possible that multiple administrators actually have the same policy settings, but different targets because they have only access to specific endpoints and Entities.

### Scenario 1: Security Coverage based on Control Manager Folders

In the User Accounts section, it is possible to view the coverage of each user. This is accessible by choosing the Administration tab, and going to **Administration -> Account Management > User Accounts**. By clicking the User itself, we can see the Access Control.

In the example shown below, the user “CTDLAB\TMCMDM” only has access to the entity under the “OSCE” folder. The user will not be able to apply any policy to entities or endpoints under the other folders.



User Accounts

Step 1 >>> Step 2: Access control

Enable this account

Managed Product Access Control

Select role: Administrators

Select accessible products/folders:

- TCMCTD
- Local Folder
  - IMSVA
  - New Entity
  - OSCE
  - ScanMail for Microsoft Exchange
  - SPLX

Specify access rights:

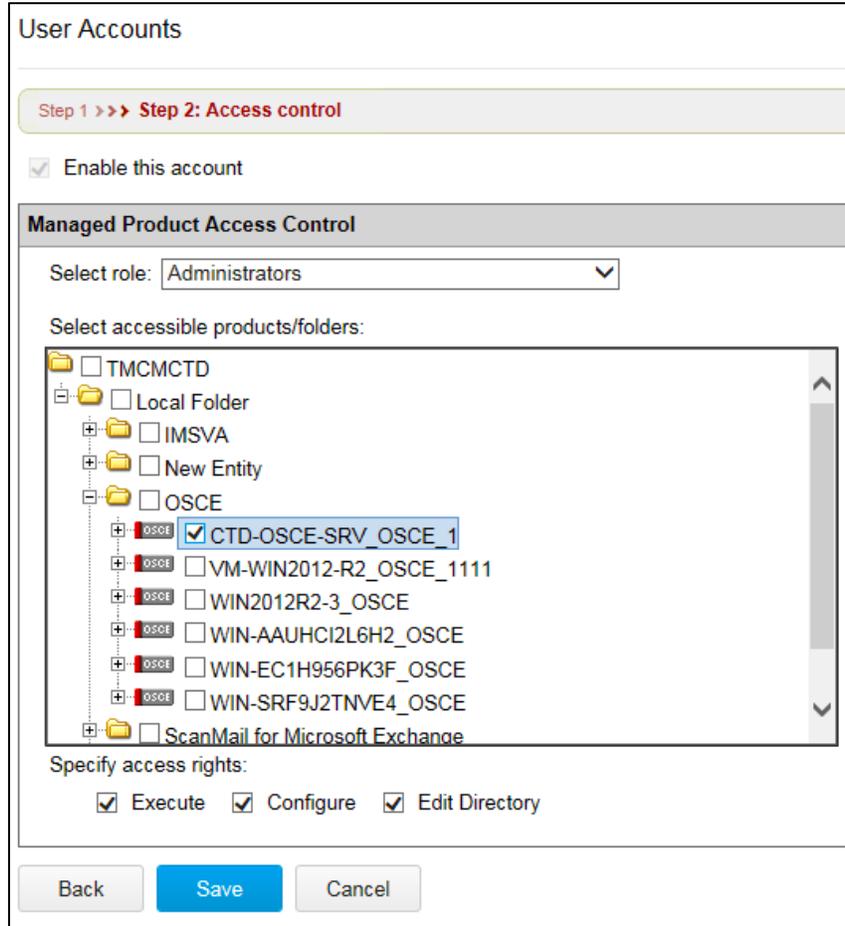
Execute  Configure  Edit Directory

Back Save Cancel

## Scenario 2: Security Coverage based on Products

Instead of Folders, policy admin can specify that the user has access to the Entities only.

In the example below, it can be seen that the account has access to the CTD-OSCE-SRV\_OSCE\_1. Because of this, the account is only able to apply policies to the CTD-OSCE-SRV\_OSCE\_1.



User Accounts

Step 1 >>> Step 2: Access control

Enable this account

**Managed Product Access Control**

Select role: Administrators

Select accessible products/folders:

- TCMCTD
- Local Folder
  - IMSVA
  - New Entity
  - OSCE
    - CTD-OSCE-SRV\_OSCE\_1
    - VM-WIN2012-R2\_OSCE\_1111
    - WIN2012R2-3\_OSCE
    - WIN-AAUHCI2L6H2\_OSCE
    - WIN-EC1H956PK3F\_OSCE
    - WIN-SRF9J2TNVE4\_OSCE
  - ScanMail for Microsoft Exchange

Specify access rights:

Execute  Configure  Edit Directory

Back Save Cancel

### Scenario 3: Security Coverage based on OfficeScan Subdomains

Administrators may also create policies that are based on OfficeScan domains.

In the example below, the account has access to two domains - Ad and Ctdlab. In this kind of setup, the account is restricted from applying policies to other domains.

**User Accounts**

---

Step 1 >>> **Step 2: Access control**

Enable this account

---

**Managed Product Access Control**

Select role: Administrators

Select accessible products/folders:

- TCMCTD
- Local Folder
- IMSVA
- New Entity
- OSCE
  - CTD-OSCE-SRV\_OSCE\_1
  - Ad
  - Ctdlab
  - Default
  - Trend
- VM-WIN2012-R2\_OSCE\_1111
- WIN2012R2-3\_OSCE

Specify access rights:

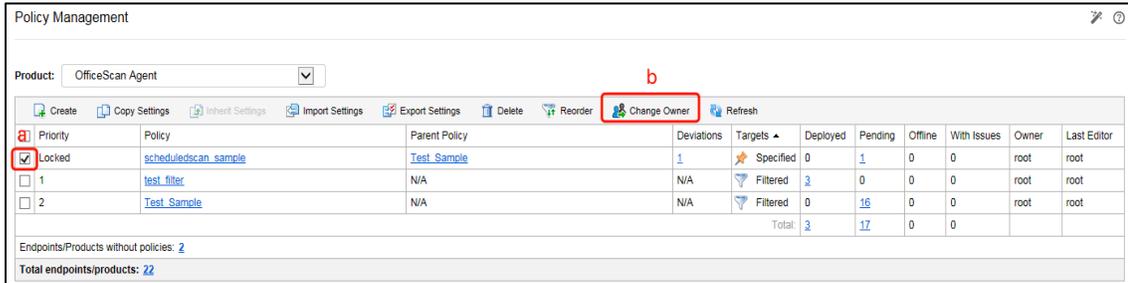
Execute  Configure  Edit Directory

Back Save Cancel

### Scenario 4: Change the policy owner to another User Account or AD Group

If there is an AD group that has multiple administrators who are able to edit this policy, we can change the policy owner to that specific AD group.

As an example, users may click the “Change Owner” to change the owner of policy “scheduledscan\_sample” from “root” to “CTDLABITMCMADM”.



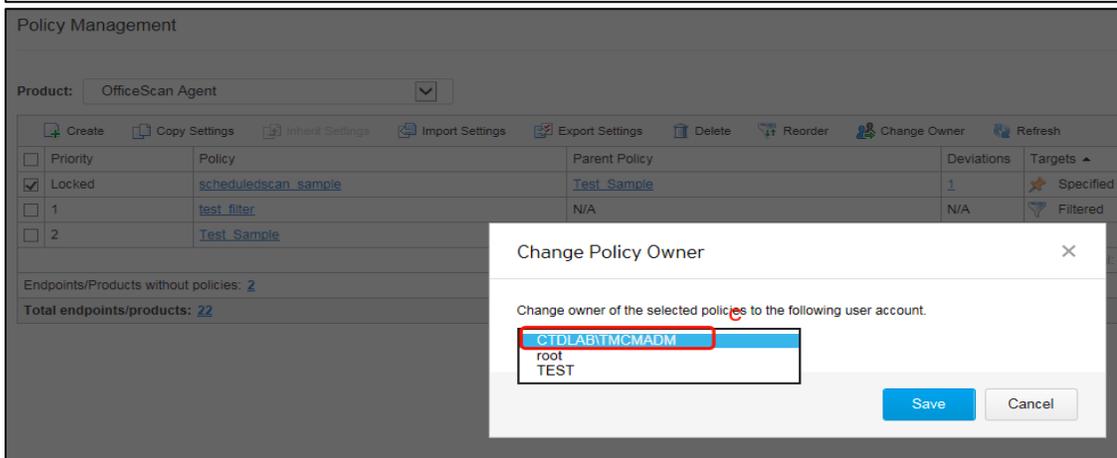
Policy Management

Product: OfficeScan Agent

Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With Issues	Owner	Last Editor	
<input checked="" type="checkbox"/>	Locked	<a href="#">scheduledscan_sample</a>	<a href="#">Test_Sample</a>	1	Specified	0	1	0	0	root	root
<input type="checkbox"/>	1	<a href="#">test_filter</a>	N/A	N/A	Filtered	3	0	0	0	root	root
<input type="checkbox"/>	2	<a href="#">Test_Sample</a>	N/A	N/A	Filtered	0	16	0	0	root	root
					Total:	3	17	0	0		

Endpoints/Products without policies: [2](#)

Total endpoints/products: [22](#)



Policy Management

Product: OfficeScan Agent

Priority	Policy	Parent Policy	Deviations	Targets
<input checked="" type="checkbox"/>	Locked	<a href="#">scheduledscan_sample</a>	<a href="#">Test_Sample</a>	1
<input type="checkbox"/>	1	<a href="#">test_filter</a>	N/A	N/A
<input type="checkbox"/>	2	<a href="#">Test_Sample</a>	N/A	Filtered

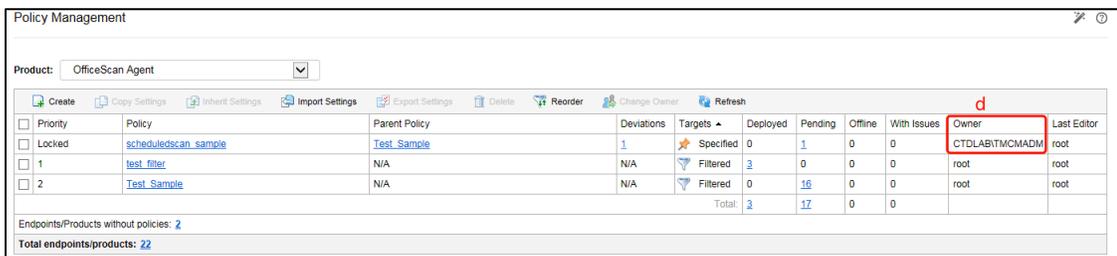
Endpoints/Products without policies: [2](#)

Total endpoints/products: [22](#)

**Change Policy Owner**

Change owner of the selected policies to the following user account.

- 
- 
-



Policy Management

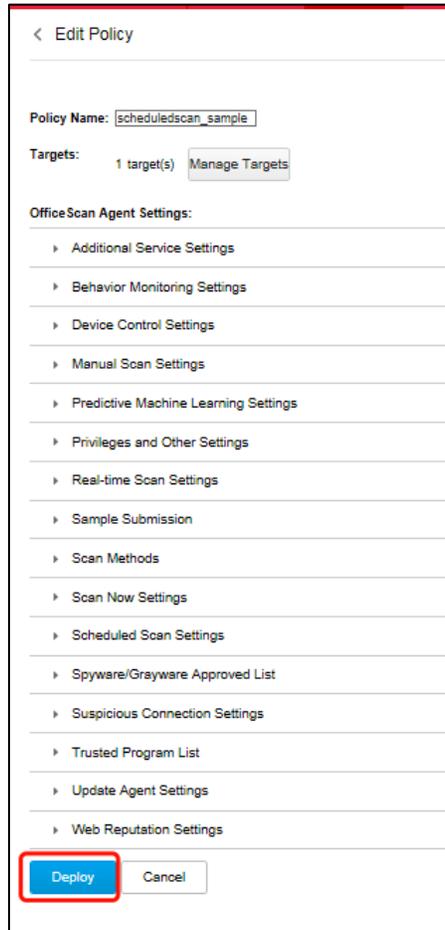
Product: OfficeScan Agent

Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With Issues	Owner	Last Editor
<input type="checkbox"/>	Locked	<a href="#">scheduledscan_sample</a>	<a href="#">Test_Sample</a>	1	Specified	0	1	0	CTDLABITMCMADM	root
<input type="checkbox"/>	1	<a href="#">test_filter</a>	N/A	N/A	Filtered	3	0	0	root	root
<input type="checkbox"/>	2	<a href="#">Test_Sample</a>	N/A	N/A	Filtered	0	16	0	root	root
					Total:	3	17	0	0	

Endpoints/Products without policies: [2](#)

Total endpoints/products: [22](#)

Here is an admin whose account is “CTDLAB\admin1” belongs to this AD group. When they login to the TMCM web console with this account “CTDLAB\admin1”, he is able to edit this policy “scheduledscan\_sample”.



Once he modifies and deploys a policy, his account name will be recorded in the the Last Editor column.

Policy Management

Product: OfficeScan Agent

Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With Issues	Owner	Last Editor
Locked	<a href="#">scheduledscan_sample</a>	<a href="#">Test_Sample</a>	0	Specified	0	1	0	0	CTDLAB\MCMADM	CTDLAB\admin1
1	<a href="#">test_filter</a>	N/A	N/A	Filtered	3	0	0	0	root	root
2	<a href="#">Test_Sample</a>	N/A	N/A	Filtered	0	16	0	0	root	root
					Total:	3	17	0	0	

Endpoints/Products without policies: 2  
Total endpoints/products: 22

Note that it is also affected by on the access scope of the specific user account.

The user can't perform "Change Owner" operation if:

- The user belongs to a role which does not have the permission to [Create, copy and import policies].

Specify access rights:

- Full control, except:
  - Create, copy and import policies ⓘ
  - Monitor, review, and investigate DLP incidents triggered by all users
- Read only

- The user belongs to a role which has [Read only] access.

### 3.5. User-based Device Control

Machine-based device control is a traditional feature. The major purpose is to restrict device access permission on endpoint (e.g. USB drive, network drive, floppy and CD-ROM).

Now we can deploy the device control policy from Control Manager to OfficeScan based on the user accounts.

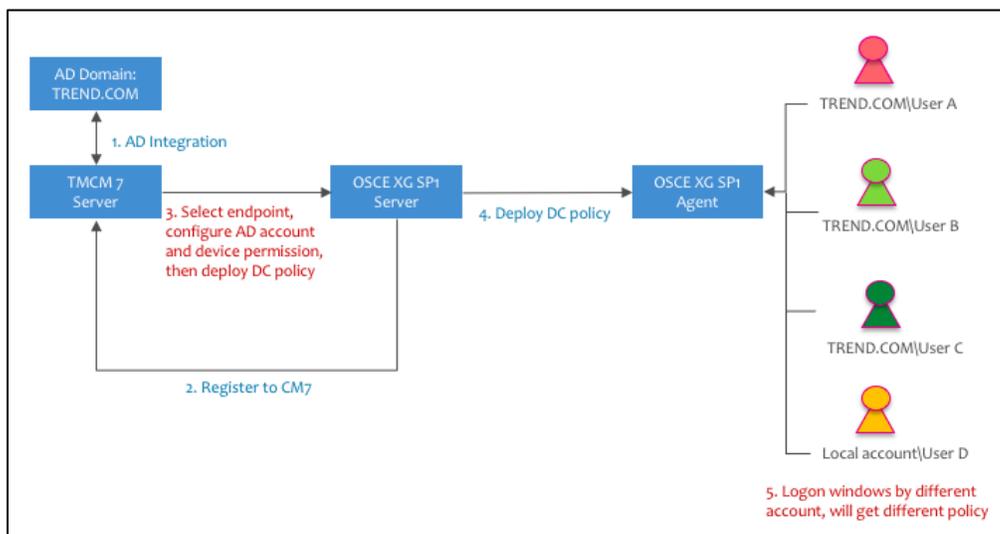
**Scenario: The customer wants to apply different policies by individual AD account on the endpoint**

First, the customer need to integrate Control Manager server with AD.

Second, the OfficeScan server need to be registered to Control Manager server.

Third, we can select the endpoint and configure the AD account, device permission from Control Manager web console and deploy the policy to the OfficeScan agent.

Finally, the users will get different device permissions base on which account they logon to the Windows OS with.



Policy deployment:

- a. Select the target AD user

The admin can specify AD groups or AD accounts in user-selector:

- Show the first 5 matching tokens in searching result list.
- The maximum token count is 30.

Policy Name:

Targets:  None (Draft only)  Filter by Criteria   Specify Target(s)

Manually assign targets to the policy. Specified policies take priority over filtered policies.

**OfficeScan Agent Settings:**

- ▶ Additional Service Settings
- ▶ Behavior Monitoring Settings
- ▼ **Device Control Settings**

Additional Services required

External Agents **Internal Agents**

Enable Device Control

Apply all settings to external agents

**Rules**

Priority	User Accounts	Device Permissions
1	All users (default)	Allowed:14, Blocked:0, Restricted access:0

Device Control Rule

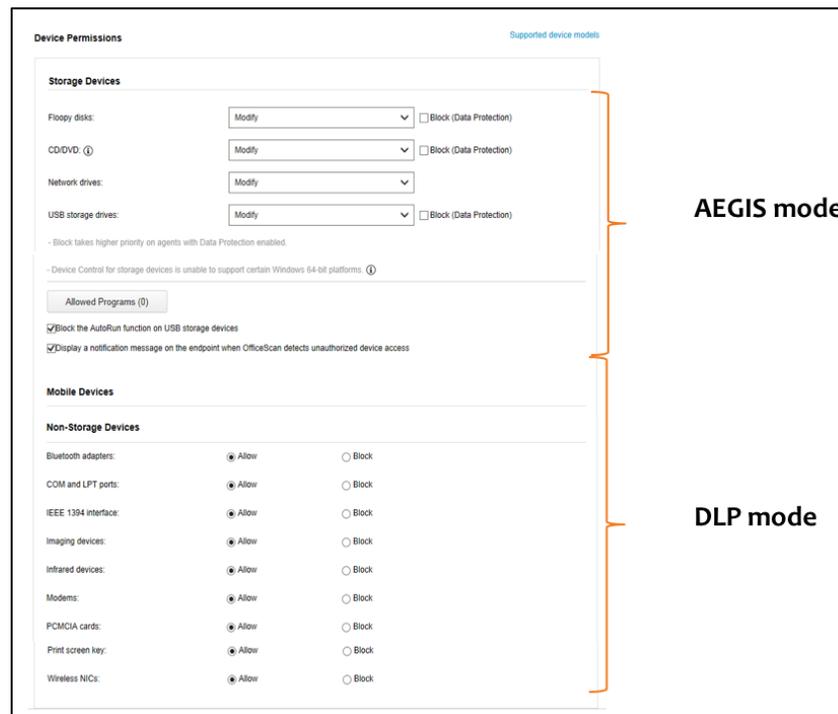
**User Accounts**

- admin1  
CTDLAB
- Admin2  
CTDLAB
- Administrators  
ctdlab.local
- DnsAdmins  
ctdlab.local
- Domain Admins  
ctdlab.local

CD/DVD: ⓘ Full access  Block (Data Protection)

b. Configure the Device Control permission

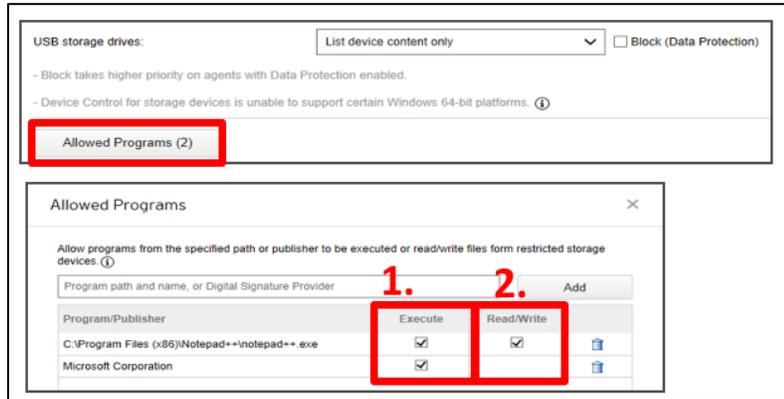
The admin can configure AEGIS and DLP Device Control permission in the same UI.



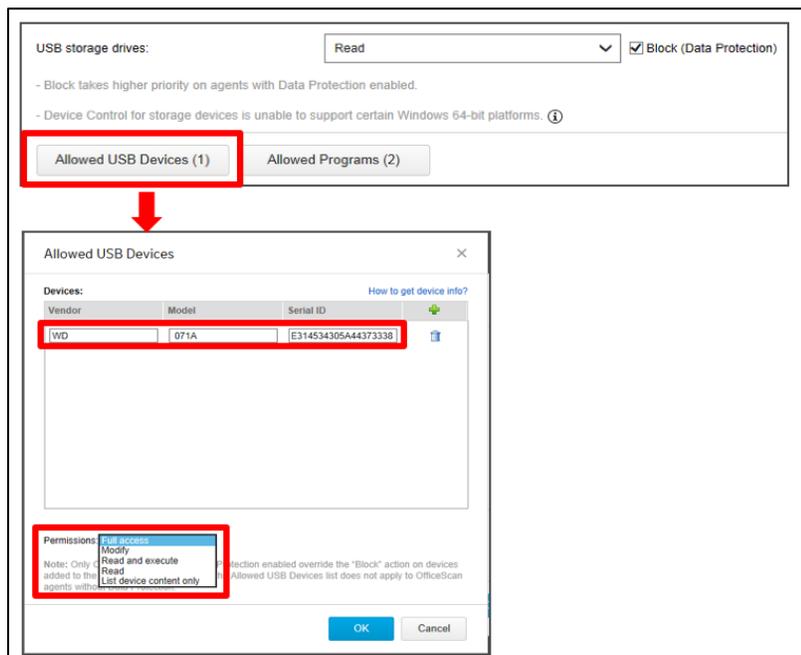
c. Configure the Device Control exception list

The admin can configure two types of exception lists:

- Allowed Programs  
If a device is set to be have strict permission, the exception list could be used to grant **full access** to the device.
- Allowed USB Devices.  
If admin set Block permission on all USB storage devices, the exception list could be used to grant any permission to specific vendor of USB devices.
- Allowed Programs  
For example, if the admin set the USB drive permission in READ only, but users want to execute a Microsoft tool on their USB drive. You can add Microsoft digital signature into the exception list, and tick Execute option. Users will have full access to execute the file on USB drive.  
Another example: if the admin set the USB drive permission in READ only, but users want to modify a python script on their USB drive. You can add the program path of notepad++ into the exception list, and tick READ/Write option. After that users can use notepad++ to modify the python script on their USB drive.



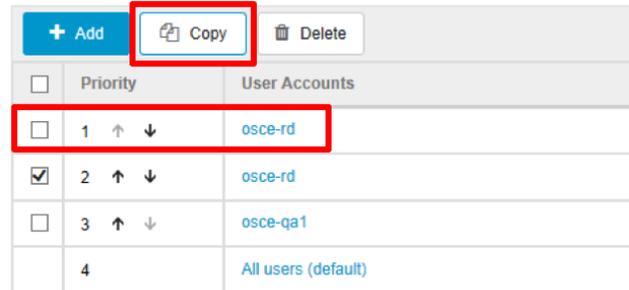
- Allowed USB Devices.  
If the admin set USB storage permission in Block, but they want to allow some specified USB drive to READ, you can add the Vendor, model and Serial ID into USB device list. The specified USB drive will be allowed to access.



d. Manage the Device Control policies

- Copy

The admin can copy any existing customized policy rules. However the default machine-based rule “All users” cannot be duplicated.



<input type="checkbox"/>	Priority		User Accounts
<input type="checkbox"/>	1	↑ ↓	osce-rd
<input checked="" type="checkbox"/>	2	↑ ↓	osce-rd
<input type="checkbox"/>	3	↑ ↓	osce-qa1
	4		All users (default)

- Delete

The admin can select any existing customized policy to delete. It will show a message box to confirm the action.

The default machine-based rule “All users” cannot be deleted.



<input checked="" type="checkbox"/>	Priority		User Accounts
<input checked="" type="checkbox"/>	1	↑ ↓	osce-qa1
<input checked="" type="checkbox"/>	2	↑ ↓	osce-qa1
<input checked="" type="checkbox"/>	3	↑ ↓	osce-qa1
<input checked="" type="checkbox"/>	4	↑ ↓	osce-qa1

**Delete Rules**

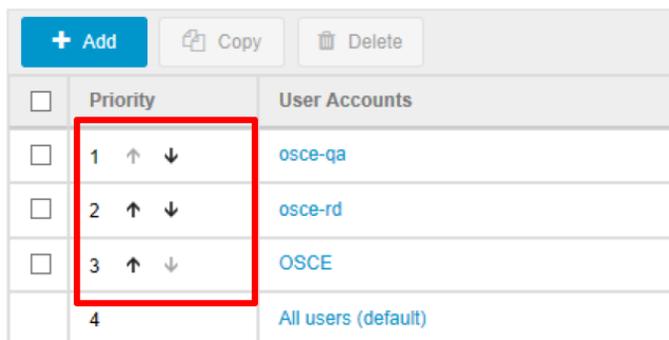
Do you want to permanently delete the selected Device Control rules?

Delete Cancel

- Adjust priority

The admin can adjust priority for customized policy rules. But we can NOT adjust the priority for machine-based rule “All users”.

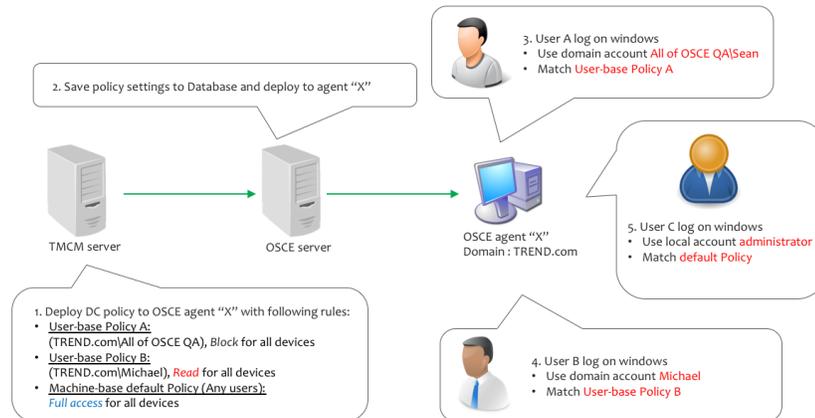
The higher priority of the policy rule will override the lower policy if the same users are in the different policy rules.



<input type="checkbox"/>	Priority		User Accounts
<input type="checkbox"/>	1	↑ ↓	osce-qa
<input type="checkbox"/>	2	↑ ↓	osce-rd
<input type="checkbox"/>	3	↑ ↓	OSCE
	4		All users (default)

e. Policy matching:

Here is an example workflow for policy matching.



f. Check the violation log

The domain user info will be recorded in the violation log on Control Manager’s web console.

- **Logs > Log Query > System Event > Device Control violations**
- The user with Device Control violations will be shown on the console

Log Query

Generated	Received	Product Entity...	Product	Target Process	File Name	Device Type	Permission	User
07/14/2017 05:12:30	07/14/2017 05:13:03	CA-2012R2DCX64	OfficeScan	C:\Windows\System...	E:\autorun.inf	USB storage device	List device content...	CA2008AD\osce-qa1
07/14/2017 04:49:16	07/14/2017 04:49:57	CA-2012R2DCX64	OfficeScan	C:\Windows\explor...	A:\extract.exe	Floppy disks	Modify	CA2008AD\osce-qa1

# 4. Log Query

This chapter explains how Log Query can help with your daily operations.

## 4.1. Log Query summary

Control Manager allows you to query the Control Manager database for Control Manager generated logs and log data from registered managed products.

Control Manager also allows you to:

- Use advanced filters to narrow log query search results.
- Configure log aggregation settings to reduce network traffic when sending log data from managed products to the Control Manager server.
- Manually delete log entries by type or configure automatic log deletion.

## 4.2. How to query logs

Log Query allows users to generate precise and customized queries. This is done using a user-friendly interface which does not require an extensive knowledge of SQL or the related database schema.

In TCM 7.0, the User Interface (UI) has been enhanced to allow the query be performed on a single page. The **New Ad Hoc Query** and **Save Ad Hoc Queries** options in previous versions have been consolidated into single page accessed via **Logs > Log Query** in TCM 7.0.

The new design in TCM 7.0 for Log Query distinguishes itself from Reports to reduce the similar functions between different features. Thus users should query summary data results in Reports, and query raw logs in **Log Query**.

Log Query



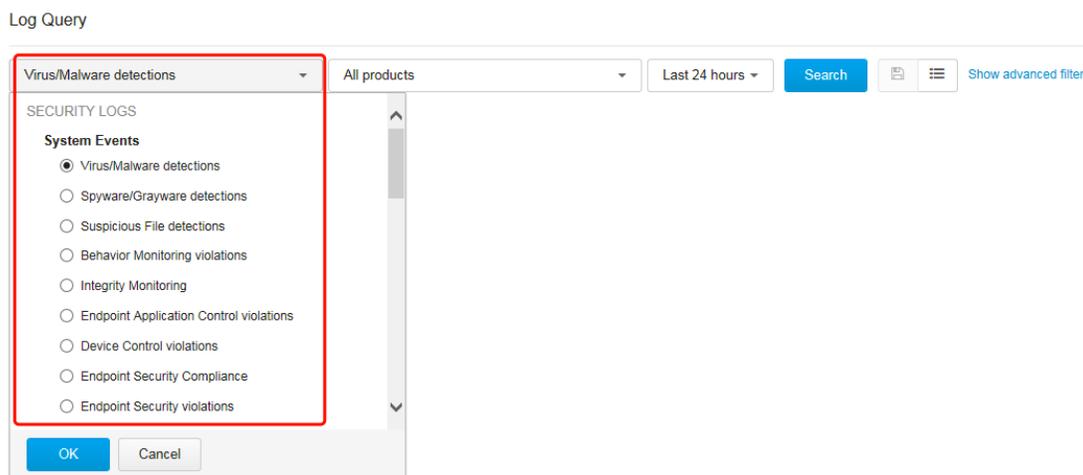
Virus/Malware detections   All products   Last 24 hours   Search   Show advanced filters

Date View   Product Scope   Time Range

As shown above, the **Data View**, **Product Scope** and **Time Range** fields have been simplified to ease the output.

## 4.2.1. Basic Filters - Data View

The wording of the data views has been refined to make the names in the data view sections more straightforward.



For example, **Detailed Virus/Malware Information** becomes **Virus/Malware detections**, and **Detailed Endpoint Security Compliance Information** has been changed to **Endpoint Security Compliance**.

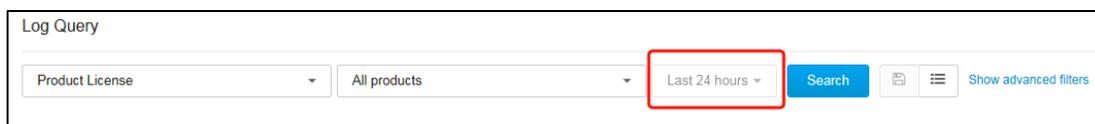
- The following are new Data Views that have been added:
- Detailed Predictive Machine Learning Information
- Virtual Analyzer Detections (sandbox detection)
- Detailed Virtual Analyzer Suspicious Object Impact Information

Correlation between the Data View and the Product Scope/Time Range fields is automatically applied when the Data View is changed.

For example, the product scope will be disabled if you select Command Tracking in Data View, because command tracking belongs to TMCM only.



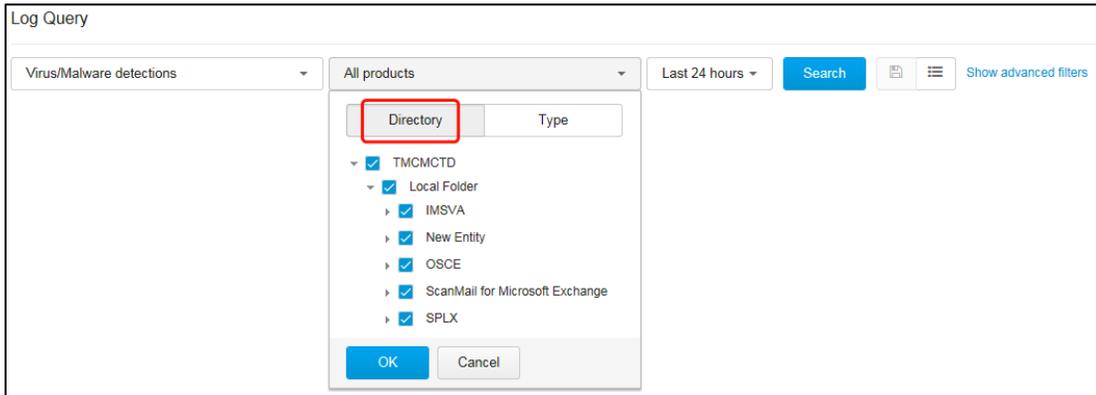
If you select Product License as the Data View, the Time Range will be disabled because it is not required criteria.



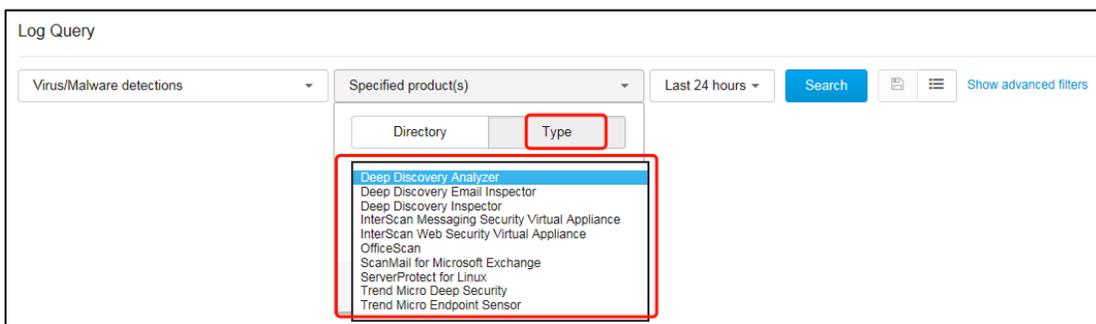
## 4.2.2. Basic Filters - Product Scope

If the Product Scope field is available, you can either use product Directory or product Type to define the selection of product scope.

The product Directory allows you to locate and select managed products from the Product Directory structure.

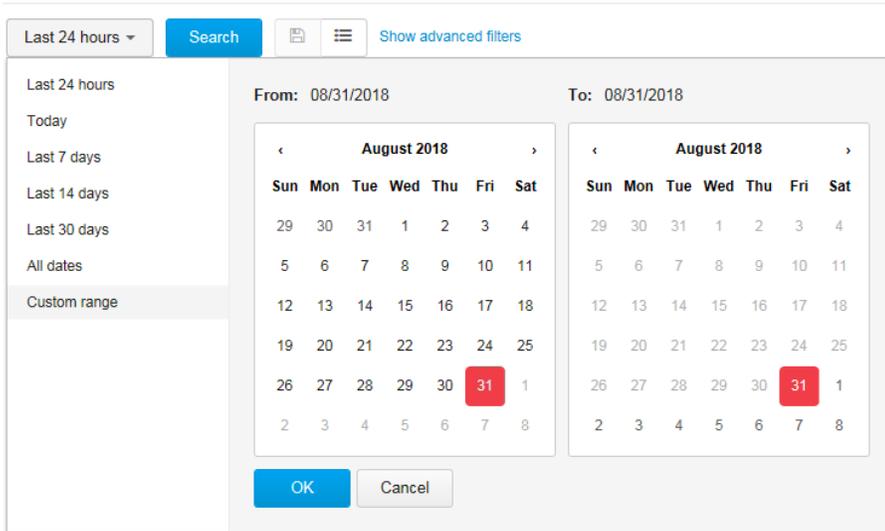


The product **Type** dropdown list only shows the products registered to TCM.



### 4.2.3. Basic Filters - Time Range

You can select default time range, such as Last 24 hours, All dates, or use date picker to customize the range you want in time filter.



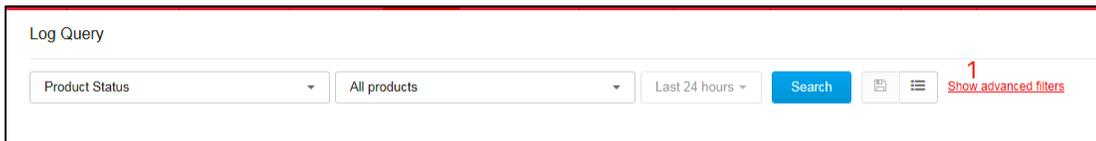
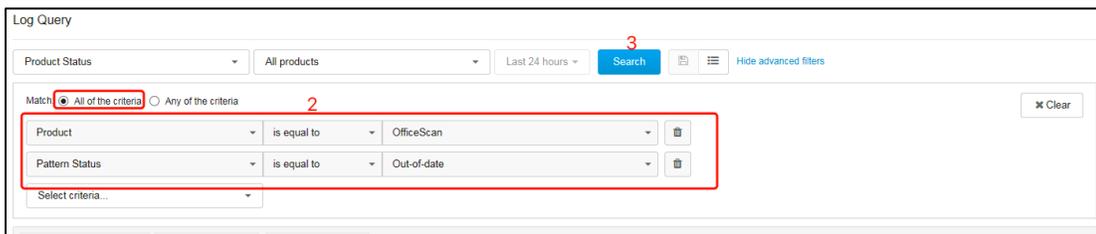
### 4.2.4. Advanced Filters

By clicking the blue **Show advanced filters** link, you can add up to 20 advanced filters per query in this panel, to narrow down query results.

The advanced filters correspond to the Customized Criteria used in the older versions' Ad hoc Query.

Same as with Ad hoc queries, you can select that these filters are applied by matching **"All of the criteria"** or **"Any of the criteria"**.

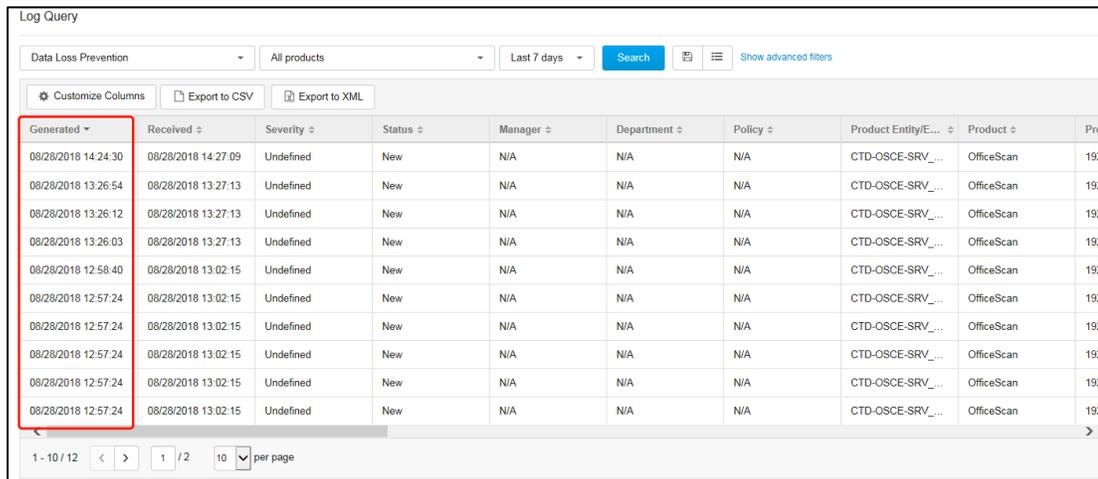
For example, you want to filter out how many OfficeScan Agents' pattern are out of date.

## 4.2.5. Query Results

After configuring the advanced filters and clicking **Search**, the query result is shown as a table, with the results shown in the order of log generation time (Generated column) as the default sorting column, instead of the log received time (**Received**) as used in the older versions of TCM.

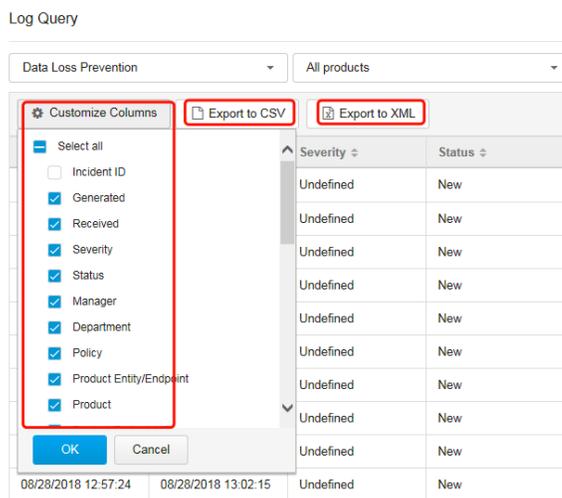
The reason for this is that the user may want to pay more attention to the log generated time that stands for the detection time on the product side instead of the log received time, which is when the TCM server received the logs from the product side.



Generated	Received	Severity	Status	Manager	Department	Policy	Product Entity/E...	Product	Pro
08/28/2018 14:24:30	08/28/2018 14:27:09	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 13:26:54	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 13:26:12	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 13:26:03	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:58:40	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A	CTD-OSCE-SRV...	OfficeScan	192

Moreover, the user can change the columns displayed via the **Customize columns** button, or export data in CSV/XML format.

If you add new columns, the new added column will become the first column in the current search results.



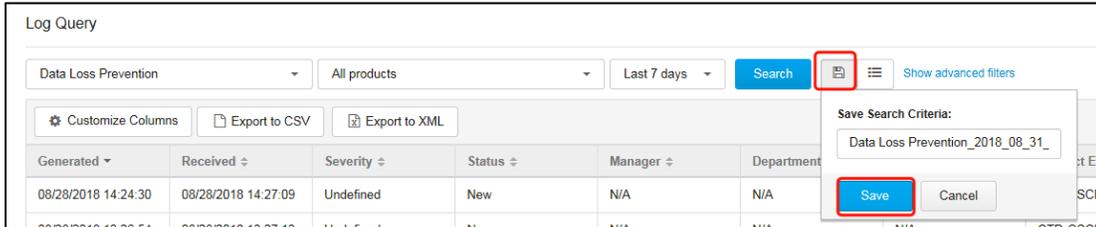
Severity	Status
Undefined	New
08/28/2018 12:57:24	08/28/2018 13:02:15

By default, the maximum number of entries which can be displayed in a query result is 10000, but this can be modified by editing the following key in the `..\Program Files\Trend Micro\Control Manager\SystemConfiguration.xml` file:

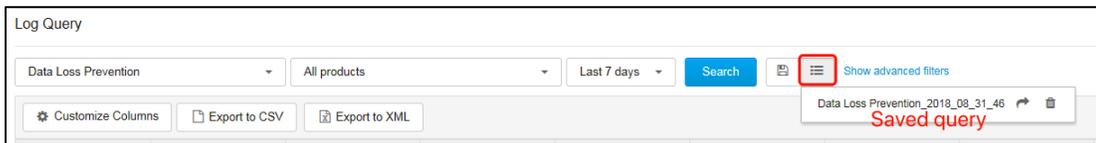
`P Name="m_iAdhocQueryUIMaxResultSize" Value="`

## 4.2.6. Save and Share the Query Results

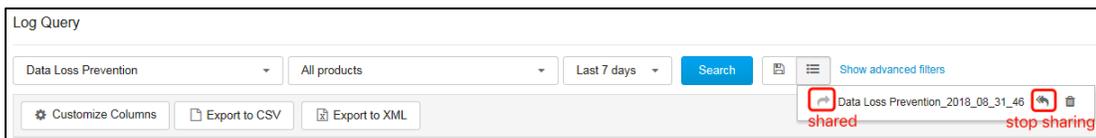
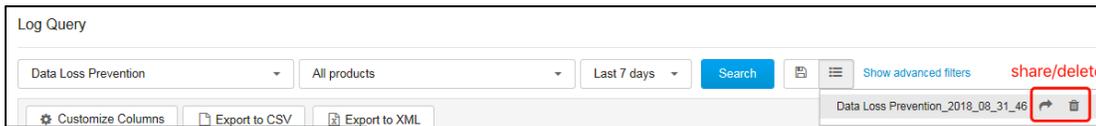
After performing a Query/Search, the Save Query button (floppy disk icon) becomes clickable. Users can click **Save** to save query.



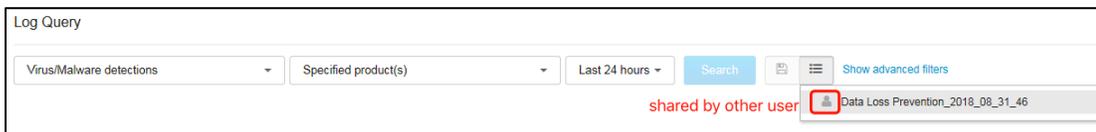
When at least one query has been saved, user can click the Saved queries button to view a list of saved queries.



The user can share the saved queries to others. Read-only users can also save and share queries.



After sharing, other users can see and access your shared query. A grey portrait icon means this query was saved and shared by other users. Hovering the mouse pointer over the grey portrait reveals the sharer's username.



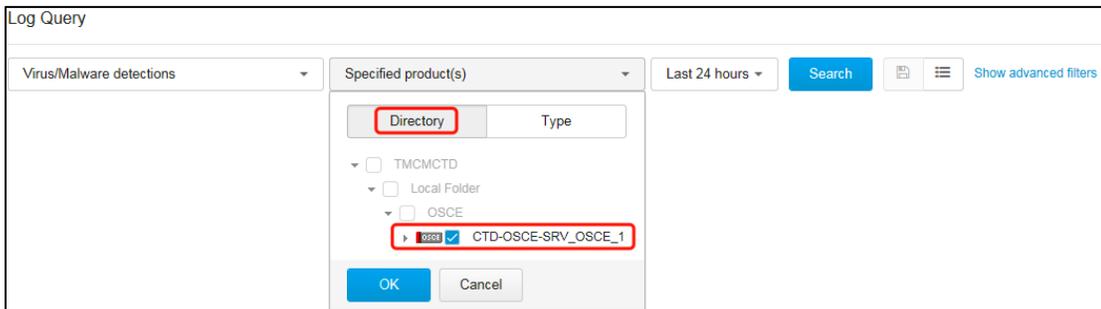
## 4.3. Role-Based Access Control Log Queries

In Log Query, the following parts are controlled by Role-Based Access Control (RBAC):

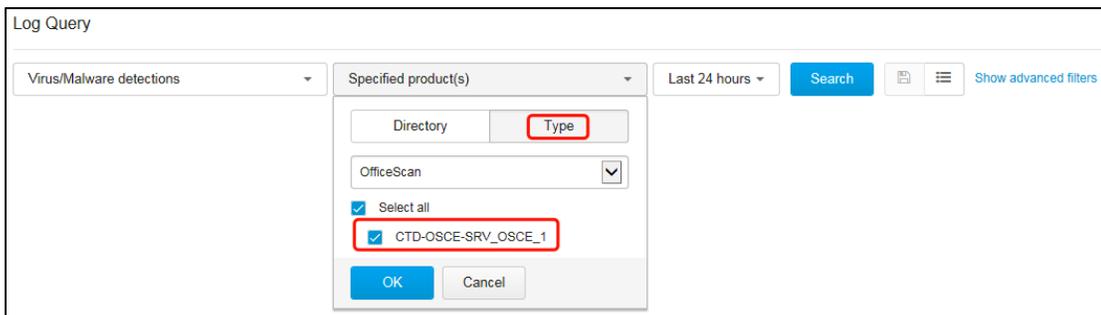
- Product Scope Filter
- Query Results
- Shared Queries

When a user gets into log query page, the product filter, including product directory and product type, will be generated based on the user's product scope.

For example, if the user can only manage one OSCE server, their options in both product directory and product type will be limited to the OSCE server that they manage.



The screenshot shows the 'Log Query' interface. The 'Specified product(s)' dropdown is open, showing a tree view. The 'Directory' tab is selected and highlighted with a red box. Under the 'OSCE' category, the item 'CTD-OSCE-SRV\_OSCE\_1' is selected with a checkmark and highlighted with a red box. Other options like 'TMCCTD' and 'Local Folder' are visible but not selected. The 'Type' tab is also visible but not selected.



The screenshot shows the 'Log Query' interface. The 'Specified product(s)' dropdown is open, showing a list of product types. The 'Type' tab is selected and highlighted with a red box. The 'OfficeScan' product type is selected in the dropdown. Below the dropdown, the 'Select all' checkbox is checked. The item 'CTD-OSCE-SRV\_OSCE\_1' is selected with a checkmark and highlighted with a red box. The 'Directory' tab is also visible but not selected.

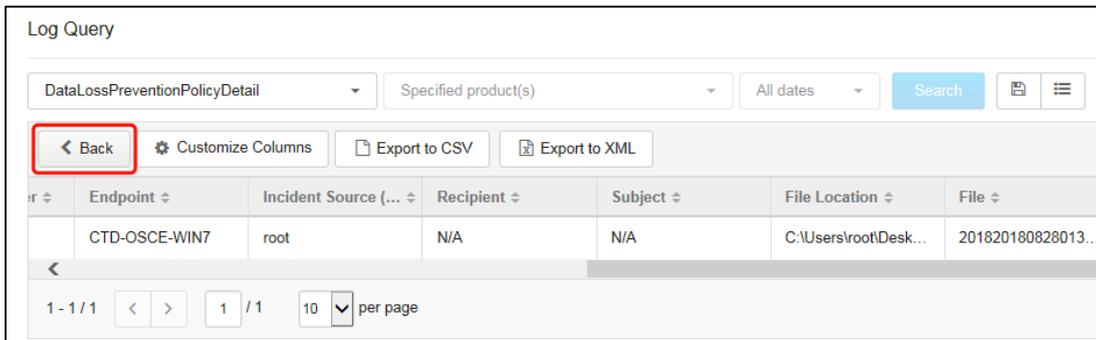
## 4.4. Drill-down Query Views

In Log Query, users normally need to provide different conditions before each query. With drill-down or jump query, it is possible to execute a query within another query without the need of providing the conditions.

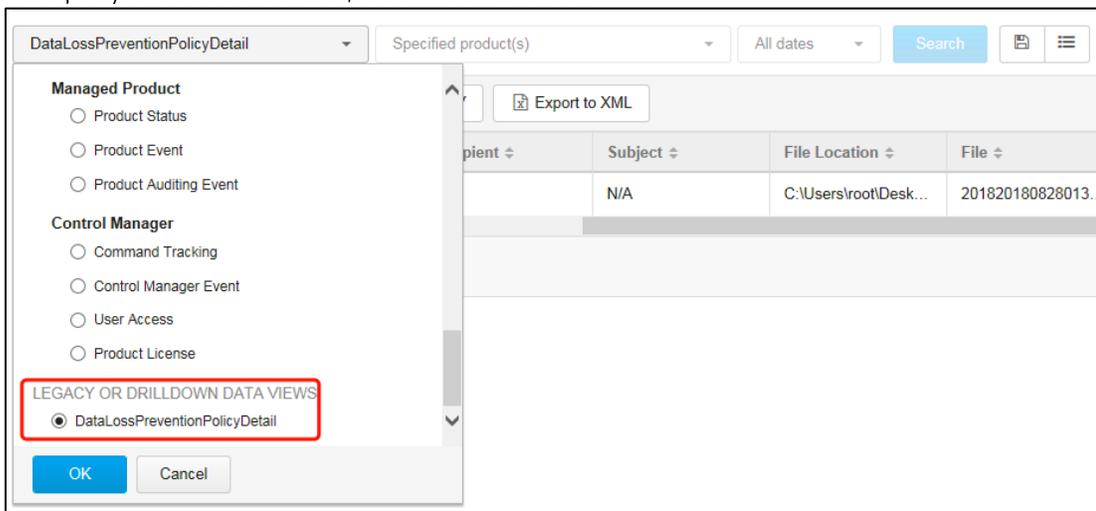
In TCM 7.0, we can drill down to Log Query from the following:

- Default data views in Log Query
- Widgets
- Inventory view
- Policies

If you drill-down from the query result of Default Data View in Log Query itself, you will find a Back button which provides users to go back to previous query result.



When customers migrate to TCM 7.0 and have some saved queries with summary or legacy data views, you will see the data view under the under "LEGACY OR DRILLDOWN DATA VIEWS". This query cannot be modified, but could be shared.

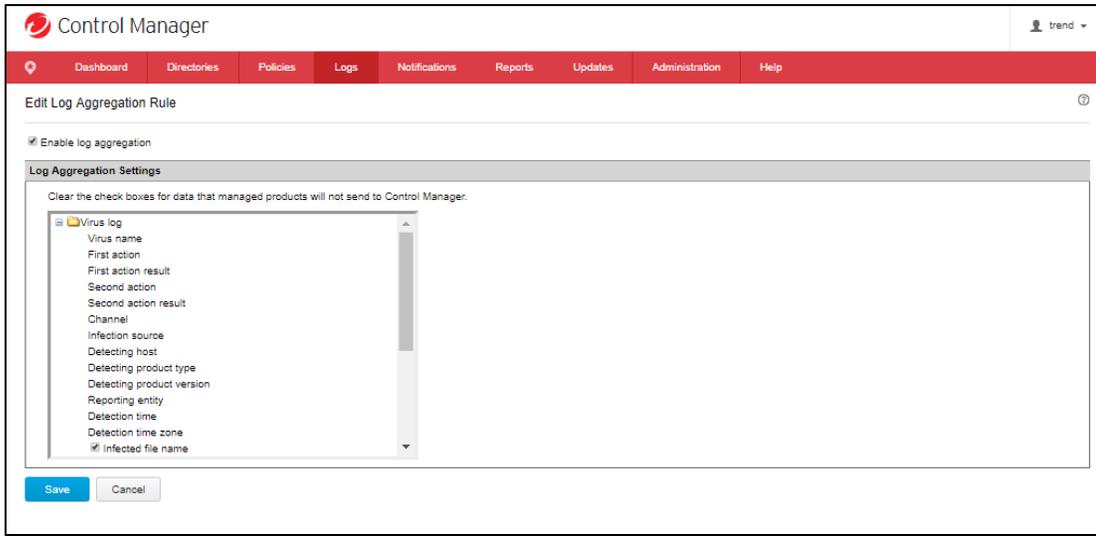


## 4.5. How to Aggregate Logs

Log aggregation allows you to conserve network bandwidth by sending only selected data from managed products to the Control Manager server.

By default the feature is disabled.

You can enable it in **Log Query > Log Aggregation Settings**.



## 4.6. How to Delete Logs

Log Maintenance can help you delete log entries by type manually or configure automatic log deletion.

- How to delete the logs manually:  
The user can click Delete All, in the corresponding row, to delete all logs for the selected type.

Log Maintenance

<input checked="" type="checkbox"/>	Log Name	Log Entries	Maximum Log Entries	Purge Offset	Maximum Log Age	
<input checked="" type="checkbox"/>	Virus/Spyware/Grayware log	35	1000000 logs	1000 logs	90 days old	Delete All
<input checked="" type="checkbox"/>	Product event log	0	1000000 logs	1000 logs	90 days old	Delete All
<input checked="" type="checkbox"/>	Security log	0	1000000 logs	1000 logs	90 days old	Delete All
<input checked="" type="checkbox"/>	Web security log	32	1000000 logs	1000 logs	90 days old	Delete All
<input checked="" type="checkbox"/>	Network virus log	0	1000000 logs	1000 logs	90 days old	Delete All
<input checked="" type="checkbox"/>	Endpoint log	0	1000000 logs	1000 logs	90 days old	Delete All

- How to delete the logs automatically  
Select the check box for the log type.

In the Maximum Log Entries column, specify the maximum number of logs that Control Manager retains.

In the Purge Offset column, specify the number of logs that Control Manager deletes when the number of logs reaches the number specified in the Maximum Log Entries column.

In the Maximum Log Age column, specify the age of logs that Control Manager deletes automatically.

Log Maintenance

<input type="checkbox"/>	Log Name	Log Entries	Maximum Log Entries	Purge Offset	Maximum Log Age	
<input checked="" type="checkbox"/>	Virus/Spyware/Grayware log	35	50000 logs	5000 logs	30 days old	Delete All
<input type="checkbox"/>	Product event log	0	1000000 logs	1000 logs	90 days old	Delete All
<input type="checkbox"/>	Security log	0	1000000 logs	1000 logs	90 days old	Delete All
<input type="checkbox"/>	Web security log	32	1000000 logs	1000 logs	90 days old	Delete All
<input type="checkbox"/>	Network virus log	0	1000000 logs	1000 logs	90 days old	Delete All

By default, TCM retains a maximum of 1,000,000 log entries, the purge offset value is 1,000 log entries, and the maximum log age is 90 days.

## 4.7. Log Query Specifications

- All summary data views have been removed from Log Query. Only saved summary data views can be queried after migration to TCM 7.0.
- Users can generate custom reports to create summary data views.
- By design, users with the DLP Incident Reviewer and DLP Compliance Officer roles cannot click Search in the Log Query page.

## 4.8. Log Query Data Views

TCM log types correspond to specific data views used in reports. You can use the following data views to create custom report templates for your log query results.

Log Type	Data View	Description
<b>System Events:</b>		
<b>Virus/Malware</b>	Detailed Virus/Malware Information	Provides specific information about the virus/malware detections on your network, such as the managed product that detected the viruses/malware, the name of the virus/malware, and the infected endpoint
<b>Spyware/Grayware</b>	Detailed Spyware/Grayware Information	Provides specific information about the spyware/grayware detections on your network, such as the managed product that detected the spyware/grayware, the name of the spyware/grayware, and the name of the infected endpoint
<b>Suspicious File</b>	Detailed Suspicious File Information	Provides specific information about suspicious files detected on your network
<b>Behavior Monitoring</b>	Detailed Behavior Monitoring Information	Provides specific information about Behavior Monitoring events on your network
<b>Integrity Monitoring</b>	Integrity Monitoring Information	Used to monitor specific areas on a computer for changes, such as installed software, running services, processes, files, directories, listening ports, registry keys, and registry values
<b>Endpoint Application Control violations</b>	Detailed Endpoint Application Control Violation Information	Provides specific information about endpoint application violations on your network, such as the violated policy and rule name
<b>Device Control violations</b>	Device Access Control Information	Provides specific information about Device Access Control events on your network
<b>Endpoint Security Compliance</b>	Detailed Endpoint Security Compliance Information	Provides specific information about endpoint security compliance on your network

<b>Endpoint Security violations</b>	Detailed Endpoint Security Violation Information	Provides specific information about endpoint security violations on your network
<b>Detailed Predictive Machine Learning Information</b>	Detailed Predictive Machine Learning Information	Provides specific information about advanced unknown threats detected by Predictive Machine Learning
<b>Virtual Analyzer Detections</b>	Detailed Virtual Analyzer Detection Information	Provides specific information about advanced unknown threats detected by Virtual Analyzer
<b>Network Events:</b>		
<b>Spam Connection</b>	Spam Connection Information	Provides specific information about the source of spam on your network
<b>Content Violation</b>	Detailed Content Violation Information	Provides specific information about content violations on your network
<b>Email Messages with Advanced Threats</b>	Email Messages with Advanced Threats	Provides specific information about email messages with suspicious and malicious behavior patterns
<b>Web Reputation</b>	Detailed Web Reputation Information	Provides security threat information about policy or rule violations detected by Web Reputation Services
<b>Web Violation</b>	Detailed Web Violation Information	Provides specific information about web violations on your network
<b>Firewall Violation</b>	Detailed Firewall Violation Information	Provides specific information about firewall violations on your network
<b>Network Content Inspection</b>	Network Content Inspection Information	Provides specific information about network content violations on your network
<b>Intrusion Prevention</b>	Detailed Intrusion Prevention Information	Provides specific information to help you achieve timely protection against known and zero-day attacks, defend against web application vulnerabilities, and identify malicious software accessing the network
<b>C&amp;C Callback</b>	Detailed C&C Callback Information	Provides specific information about C&C callback events detected on your network
<b>Suspicious Threat</b>	Detailed Suspicious Threat Information	Provides specific information about suspicious threats on your network, such as the managed product that detected the suspicious threat, specific information about the source and destination, and the total number of suspicious threats on the network
<b>Application Activity</b>	Detailed Application Activity	Displays specific information about application activities that violate network security policies
<b>Mitigation</b>	Detailed Mitigation Information	Provides specific information about tasks carried out by mitigation servers to resolve threats on your network

<b>Correlation</b>	Detailed Correlation Information	Provides specific information about detailed threat analyses and remediation recommendations
<b>Data Protection Events:</b>		
<b>Data Loss Prevention</b>	DLP Incident Information	Displays specific information about incidents detected by Data Loss Prevention
<b>Data Discovery</b>	Data Discovery Data Loss Prevention Detection Information	Displays specific information about incidents detected by Data Discovery
<b>Managed Product:</b>		
<b>Product Status</b>	Product Status Information	Displays specific information about managed products registered to the Control Manager server
<b>Product Event</b>	Product Event Information	Displays specific information about managed product events
<b>Product Auditing Event</b>	Product Auditing Event Log	Displays auditing information related to managed products
<b>Control Manager:</b>		
<b>Command Tracking</b>	Command Tracking Information	Displays specific information about commands issued to managed products
<b>Control Manager Event</b>	Control Manager Event Information	Displays specific information about Control Manager server events
<b>User Access</b>	User Access Information	Displays Control Manager user access and the activities users perform while logged on to Control Manager
<b>Product License</b>	Detailed Product License Information	Displays information about the Activation Code and information on managed products that use the Activation Code

# 5. Report

Report generation is one of the most important features of TCM. This is based on the design of the product being a centralized management platform for Trend Micro business products.

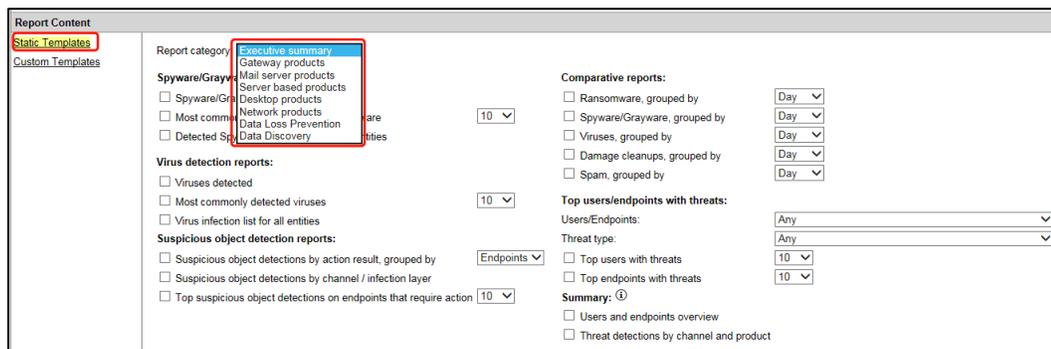
## 5.1. Static template and Custom template

There are three sets of pre-defined report templates available by default in this release of TCM 7.0. These are:

- Custom Templates (Formerly TCM 5.0 Templates)
- Static Templates (Formerly TCM 3.0 Templates)
- TCM 2.5 Templates(hidden by default)

The main difference between the two template sets (Custom\Static Templates) are that the Static templates used to utilize Crystal Reports while Custom templates utilized MS SQL reports. As of CM 7.0, Static Reports no longer use Crystal reports, and are implemented using MS SQL reports as well.

Static Templates:



**Report Content**

**Static Templates**

**Custom Templates**

**Report category:** Executive summary  
 Gateway products  
 Mail server products  
 Server based products  
 Desktop products  
 Network products  
 Data Loss Prevention  
 Data Discovery

**Spyware/Grayware:**  
 Spyware/Grayware  
 Most common  
 Detected Spyware

**Virus detection reports:**  
 Viruses detected  
 Most commonly detected viruses  
 Virus infection list for all entities

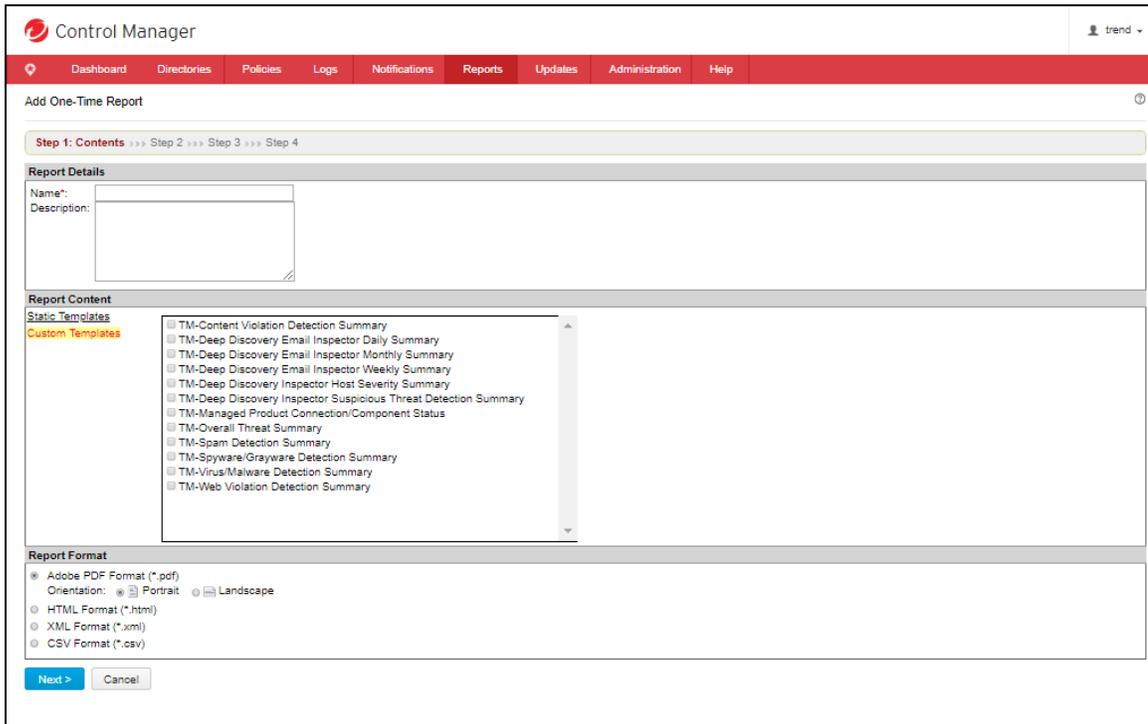
**Suspicious object detection reports:**  
 Suspicious object detections by action result, grouped by  
 Suspicious object detections by channel / infection layer  
 Top suspicious object detections on endpoints that require action

**Comparative reports:**  
 Ransomware, grouped by  
 Spyware/Grayware, grouped by  
 Viruses, grouped by  
 Damage cleanups, grouped by  
 Spam, grouped by

**Top users/endpoints with threats:**  
 Users/Endpoints: Any  
 Threat type: Any  
 Top users with threats  
 Top endpoints with threats

**Summary:**  
 Users and endpoints overview  
 Threat detections by channel and product

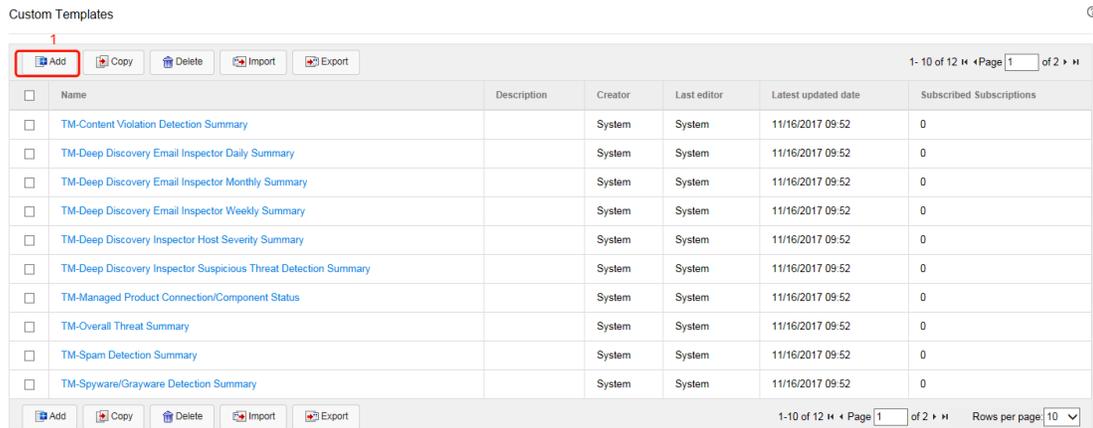
Custom Templates:



You can edit or add your own customer template via web console > Reports > Custom Templates.

For example, the users can create a template of the managed product's pattern and engine status.

1. Click **Add** to create a new custom template.

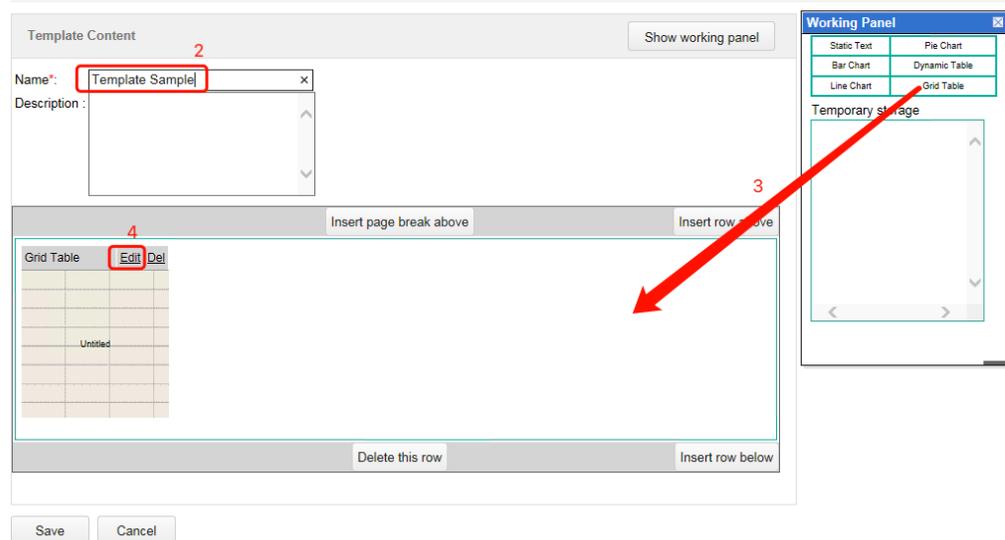


2. Type in a name for the template and drag the needed content unit from the working panel. Six types of content unit are available:

Category	Description
Static Text	Generated by the template creator and can be used to provide a summary of the information that the report provides
Bar Chart	Display report data using a bar chart
Line Chart	Display report data using a line chart
Pie Chart	Display report data using a pie chart
Dynamic Table	Display report data in a format similar to a pivot table or a spreadsheet
Grid Table	Display report data in a format similar to the Log query result

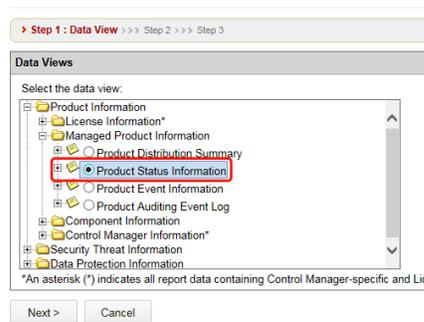
For example, you choose the “Grid Table”.

Add Report Template



3. After clicking the **Edit** for the Grid Table, you need to choose the specific date view.

Edit Grid Table



## 4. Set the custom criterial if needed.

## Query Criteria

Step 1 >>> **Step 2: Set Query Criteria** >>> Step 3

**Result Display Settings**

Selected View: Product Status Information [Change column display](#)

**Criteria Settings**

Required criteria

Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (\*) can be selected to filter data only once.

Product Role is equal to Client

< Back   Next >   Cancel

## 5. Type in the name of this Grid Table, choose the needed fields, and then click Save.

## Edit Grid Table

Step 1 >>> Step 2 >>> **Step 3 : Specify Design**

Name:

Select fields to display on the report:

Available Fields

Selected Fields

- Product Entry/Endpoint
- Product Host/Endpoint
- Product/Endpoint IP
- Product/Endpoint MAC
- Managing Control Manager Entity
- Managing Server Entity
- Domain
- Connection Status
- Pattern Status
- Engine Status
- Product
- Product Version
- Product Build
- Product Role
- Operating System

Move Up   Move Down

Sorting: Select a field   Descending

Display quantity: 25

< Back   Save   Cancel

## 6. The newly added template will now be seen under the Custom Templates.

Custom Templates

Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
<input checked="" type="checkbox"/> Template Sample		root	root	09/05/2018 13:45	0
<input type="checkbox"/> TM-Content Violation Detection Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Deep Discovery Email Inspector Daily Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Deep Discovery Email Inspector Monthly Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Deep Discovery Email Inspector Weekly Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Deep Discovery Inspector Host Severity Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Deep Discovery Inspector Suspicious Threat Detection Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Managed Product Connection/Component Status		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Overall Threat Summary		System	System	11/16/2017 09:52	0
<input type="checkbox"/> TM-Spam Detection Summary		System	System	11/16/2017 09:52	0

1-10 of 13   Page 1 of 2   Rows per page 10

## Control Manager 2.5 Templates

With the release of TCM 5.0 report sets, TCM 5.0 and higher version users are not encouraged to use Control Manager 2.5 templates anymore.

By default, Control Manager 2.5 templates are not displayed in the product UI.

To display the list of Control Manager 2.5 templates on the console, a parameter inside ...\\Control Manager\\WebUI\\WebApp\\web.config needs to be modified:

```
<appSettings>
<add key="EnableCM25Report" value="false" />
<add key="CharSpanToAddWbr" value="20" />
<add key="CrystallImageCleaner-AutoStart" value="true" />
<add key="CrystallImageCleaner-Sleep" value="60000" />
<add key="CrystallImageCleaner-Age" value="120000" />
</appSettings>
```

After changing the value of the EnableCM25Report key to "true", Control Manager 2.5 templates will be displayed as illustrated.

### 5.1.1. New Reports added in Static Template

Executive Summary:

- Comparative reports:
  - Ransomware
- Top users/endpoints with threats:
  - Top users with threats
  - Top endpoints with threats
- Suspicious object detection reports:
  - Suspicious object detections by action result by endpoints/users
  - Suspicious object detections by channel / infection layer
  - Top suspicious object detections on endpoints that require action
- Summary:
  - Users and endpoints overview
  - Threat detections by channel and product

Desktop products:

- ✓ Predictive Machine Learning detection reports:
  - Unknown threats
  - Most commonly detected unknown threats
- Comparative reports:
  - Infection channel
  - Predictive Machine Learning detections

## 5.1.2. New Reports added in Static Template

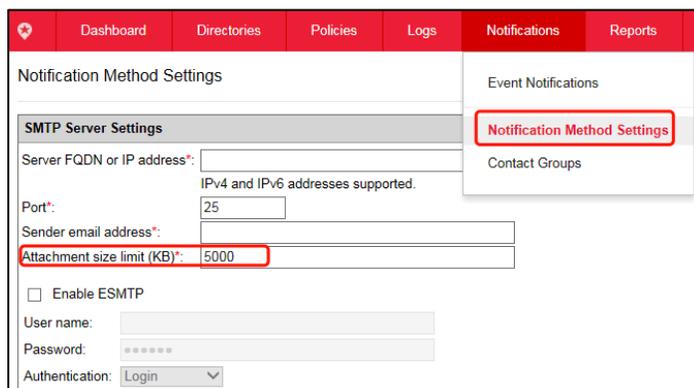
- ✓ Custom Template:
  - Adobe PDF format (\*.pdf)
  - HTML format (\*.html)
  - XML format (\*.xml)
  - CSV format (\*.csv)
  
- ✓ Static Template:
  - Adobe PDF format (\*.pdf)
  - Microsoft Word format (\*.docx)
  - Microsoft Excel format (\*.xlsx)
  
- ✓ After migration to TMCM7.0, the format in next scheduled report will be converted.
  - Rich text (\*.rtf) -> Microsoft Word format (\*.docx)
  - Other -> Adobe PDF format (\*.pdf)

## 5.2. Static template and Custom template

You are able to generate your own reports and send out them by emails.

The SMTP settings for sending report notification emails is now located under **Notification > Notification Method Settings**.

A setting for attachment file size limit has been added, and is set to 5000 KB by default. If notification reports exceed the size limit, then the report is sent as a download link in the email instead of as an attachment. Clicking the link redirects to the TCMC console. After log-on, the report will be downloaded. This was added due to issues when TCMC reports would not be sent when the attachment size exceeds the SMTP server attachment size limitations.



Notification Method Settings

Event Notifications

Notification Method Settings

Contact Groups

**SMTP Server Settings**

Server FQDN or IP address\*:

IPv4 and IPv6 addresses supported.

Port\*:

Sender email address\*:

Attachment size limit (KB)\*:

Enable ESMTP

User name:

Password:

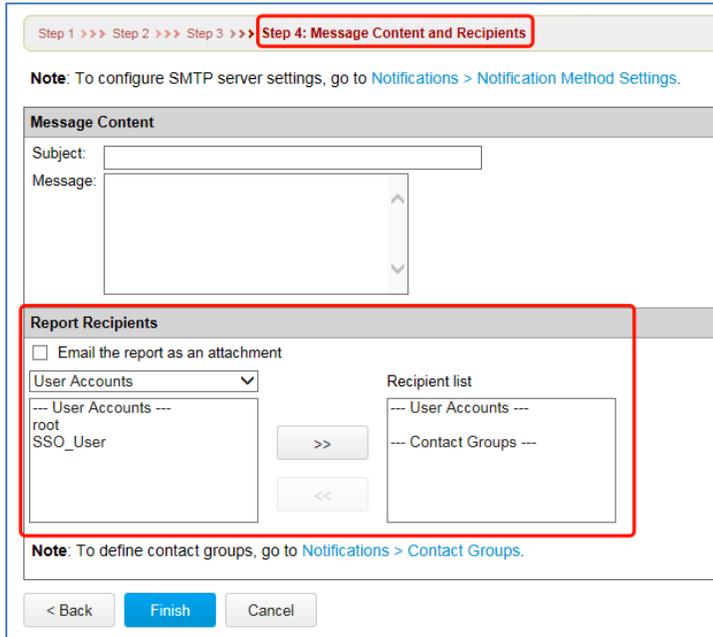
Authentication:



This setting can be altered to conform to the limits set on the domain's SMTP server.

## 5.3. Access Control List

The fourth step during the creation of a new report requires a subscription to define the recipient list of the report.

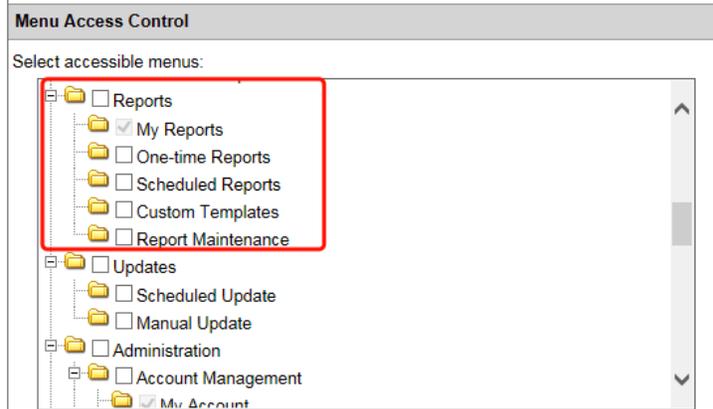


This configuration, together with the role's menu access control, dictates the operations that a specific user can perform to report related items.

	Template	Subscription			Instance		Maintenance
	Create Edit Delete	Create	Edit Delete	Read	Delete Forward	Read	Update
Role can access Report menu	✓	✓	✓	✓	✓	✓	✓
Recipient list only	✗	✗	✗	✗	✗	✓	✗

Details of the report access control are listed below:

- A user assigned with a role that can access the highlighted report menus in the following figure can perform all operations related to report template, subscription, instance and maintenance. The behavior listed for “Role can access Report menus” is only limited by what specific menu a user can or cannot access.



- Report template operations and report maintenance can only be performed by a user who can access the corresponding report menu.
- Creating, editing and deleting report subscriptions can only be performed by a user who can access the One-time Reports and Scheduled Reports menu.
- A report instance can only be forwarded by a user assigned with a role that is authorized to create, edit and delete report subscriptions.
- A user account that does not have report menu access but is in the recipient list for a specific report instance gains a read-only permission to that report instance.

## 5.4. My Reports

The items listed under My Reports are limited to reports generated using Static and Custom templates and are dependent on the logged-in account. Two conditions determine whether a report instance (one-time, scheduled or quick) are included in a user's My Reports view:

- The logged-in account is the creator of the subscription which generated the report instance
- The logged-in account belongs to the recipient list of the subscription which generated the report instance

The specific reports that are listed under My Reports are determined by the authorization module discussed in the Account Management and Access Control.

# 6. Connected Threat Defense (CTD)

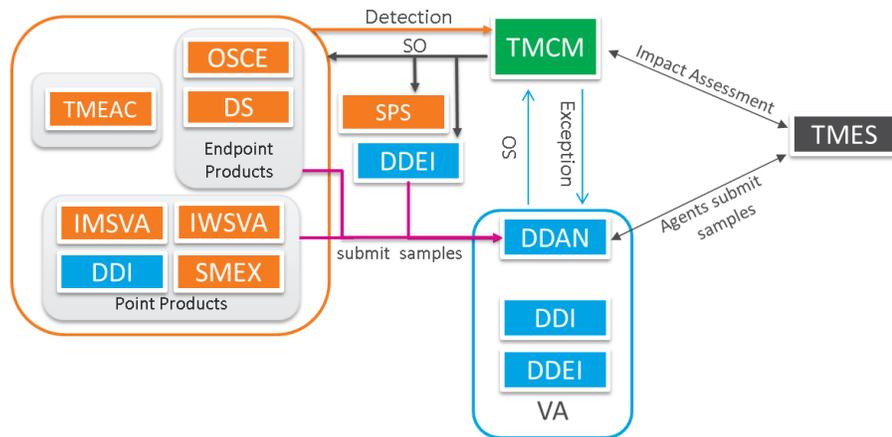
To help customers locate and mitigate these threats, Trend Micro introduced Connected Threat Defense (CTD), which provides a comprehensive and more complete solution to this problem.

As a solution, CTD uses the following components:

- Deep Discovery Inspector (DDI) and Deep Discovery Analyzer (DDAn) monitor and generate Suspicious Objects (SO).
- Trend Micro Endpoint Sensor (TMES) leverages SOs or Indicators of Compromise (IOCs) to conduct impact assessment on all clients or a specific one.
- OfficeScan and Smart Protection Server mitigate confirmed threats
- TCMCM functions as the controlling component in implementing the CTD functions

## 6.1. Architecture

TMCM functions as the control center of the CTD solution framework.



This diagram shows an overview of the CTD Products:

- Products in the Virtual Analyzer (VA) group (DDAN, DDI and DDEI) send SOs to TMCM, also get Exception lists from TMCM.
- Trend Micro Endpoint Sensor (TMES) agents submit samples to the Deep Discovery Analyzer (DDAN), and received requests for IOC or SO Impact Assessment from TMCM.
- The Endpoint Products, Point Products, and TMEAC get SOs from TMCM and send back detection information to TMCM.
- Point and Endpoint Products submit samples for analysis to DDAN.
- Smart Protection Server (SPS) gets SOs from TMCM
- Deep Discovery Email Inspector (DDEI) gets SOs from TMCM and also submits samples to DDAN for analysis.

## 6.2. Architecture

### 6.2.1. Type of Suspicious Objects

- VASO: Virtual Analyzer Suspicious Object
  - File SHA-1
  - IP Address
  - URL
  - Domain
- UDSO : User Defined Suspicious Object
  - File (filterCRC)
  - File SHA-1
  - IP Address
  - URL
  - Domain
- Exception List(s)  
 The following table explains SO type, available actions and product which support to configure action from Control Manager.

Type of SO	Available action	Exception handling	Note
File SHA-1	Log Block Quarantine	✓ Only VASO can be added into exception list.	✓ When Block action is taken by Office Scan, real-time scan deny file access and manual, scheduled scan or scan now does not take any action. ✓ When quarantine action is taken by Office Scan, file is encrypted.
IP address	Log Block	✓ Only VASO can be added into exception list.	
URL	Log Block	✓ Only VASO could be added into exception list. ✓ Wild card is supported	

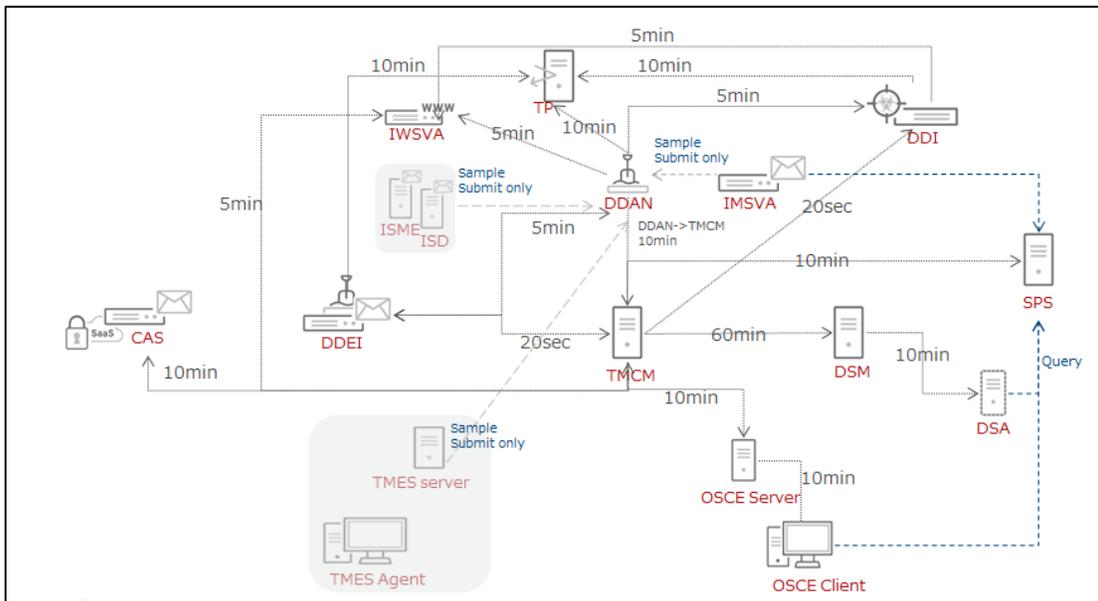
Domain	Log	✓ Only VASO can be added into exception list.	
	Block	✓ Wild card is supported	
File (UDSO)	Log	✓ UDSO has the highest priority	
	Block	✓ CM will still display the detection log on the UDSO page even if it matches to the wildcard exception list	
	Quarantine		

### 6.2.2. Suspicious Object Sync Interval

DDAN, DDEI and DDI can be the VASO source, and TCMCM can deliver them to OSCE, DSM, TP, IWSVA, SPS and CAS.

- ✓ DDAN sends the SO to TCMCM every 10 min
- ✓ DDI sends the SO to TCMCM every 5 min

Please refer following picture to confirm sync interval for each product.

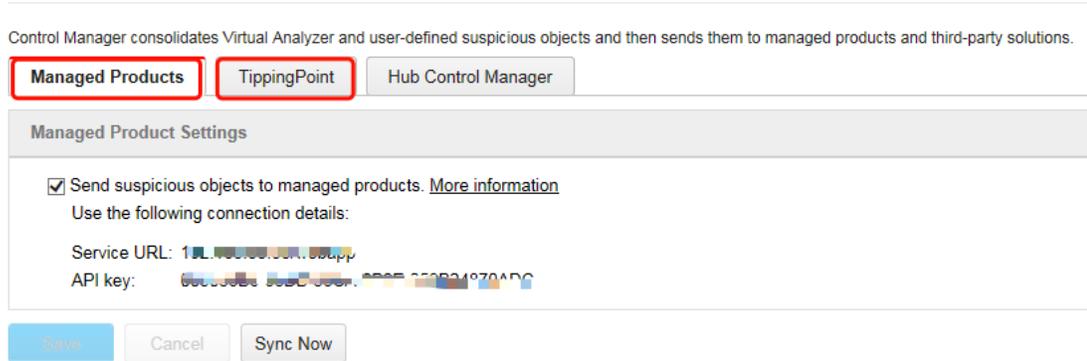




### 6.2.3. Suspicious Object Sync Now

In TMCM 6.0, there were two sections under the Distribution Settings console: Trend Micro Managed Product Settings and the HP TippingPoint Settings. In TMCM 7.0, these sections are separated into separate tabs: Managed Products and TippingPoint.

#### Distribution Settings



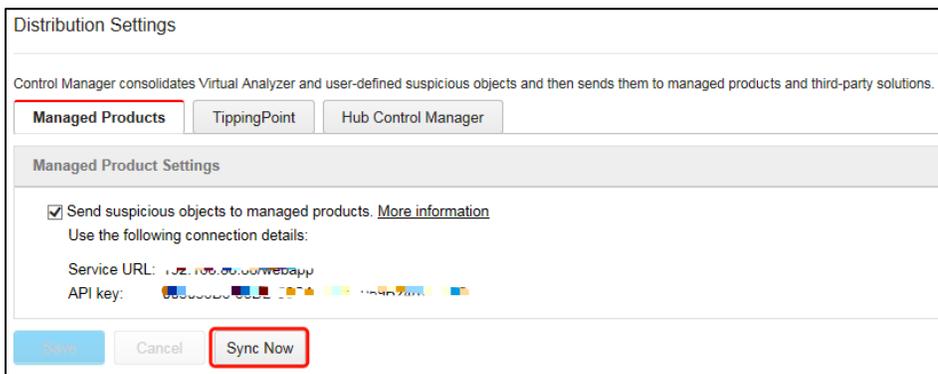
Normally, we can automatically deploy two kinds of API keys: the **DDAN API key** and the **TMCM API key**.

If you don't have DD products registered as Virtual Analyzers, in order to deploy the CM API key, we need to disable the DDAN checking in SystemConfiguration.xml by setting **m\_EnableDDANCheck** to 0 and restarting the LogProcessor process.

- 0 -> Turn off DD products checking. Deploy API key despite no DD product registered
- 1 -> Turn on DD products checking. Deploy API key if there are DD products registered. If none, then do not deploy the API key.

Here we will focus on the Managed Products Sync Now.

You can manually trigger synchronization of the managed products by clicking the Sync Now button in the **Administration > Suspicious Objects > Distribution Settings > Managed Products** tab.





After you click Sync Now, it will do the following steps:

1. Synchronize SO with Vas. You can find the result via Command Tracking

Command Details			
<b>Sync Now - Synchronize Virtual Analyzer suspicious object lists</b>			
Issued: 07/14/2017 10:08:37		Successful: 1	
Last updated: 07/14/2017 10:08:37		Unsuccessful: 1	
User: root		In Progress: 0	
Parameters: N/A			
Last Reported	Server/Entity	Status	Description
07/14/2017 10:08:37	d65-1309-1	Successful	Sync Now - d65-1309-1 successfully synchronized suspicious objects lists
07/14/2017 10:08:37	DDD1	Not available	Sync Now - localhost version unsupported, Upgrade localhost to newest version or wait for scheduled synchronization to begin
<input type="button" value="Back"/>			

2. Consolidate the SO in TCM
3. Notify products to sync SO
4. Products attempt to synchronize SO with TCM. If the product does not sync SO within 3 minutes, then this is considered a failed action. You can find the result via Command Tracking

Sync Now - Send suspicious object lists to managed products			
Issued: 10/31/2017 09:45:53		Successful: 0	
Last updated: 10/31/2017 09:45:53		Unsuccessful: 2	
User: admin		In Progress: 0	
Parameters: N/A			
Last Reported	Server/Entity	Status	Description
10/31/2017 09:45:53	IMSVAD1	Time out	Sync Now - IMSVAD1 unreachable, Unable to synchronize suspicious object lists
10/31/2017 09:45:53	DDD1	Not available	Sync Now - localhost version unsupported, Upgrade localhost to newest version or wait for scheduled synchronization to begin

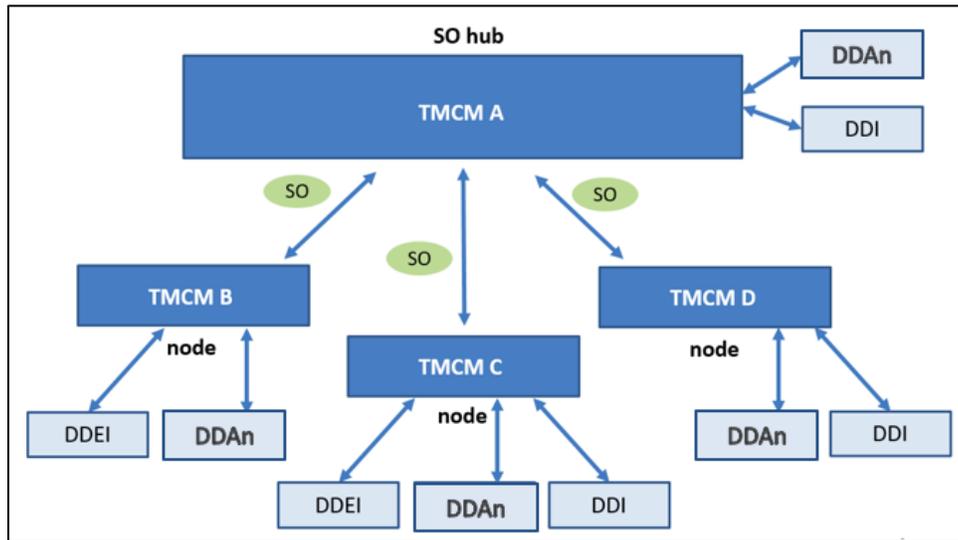
## 6.3. Hub and Node TCMC

### 6.3.1. Hub and Node

One of TCMC servers can be set as the hub server, to share Suspicious Object among other TCMC servers.

The SO can be synced between Hub and Nodes.

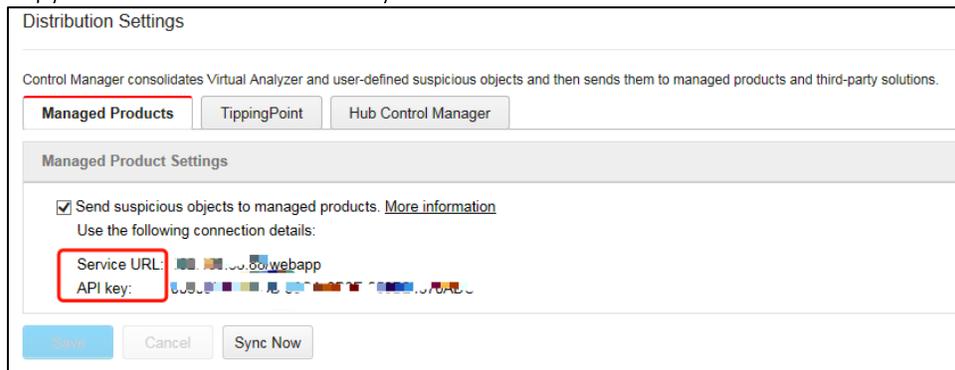
All the TCMC servers will have the same VASOs and UDSOs.



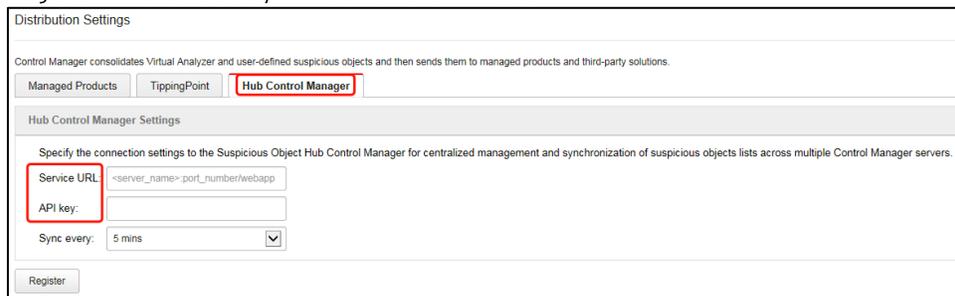
### 6.3.2. How to register Hub and Node TCM

Control Manager which should be the Node needs to register to the Hub TCM.

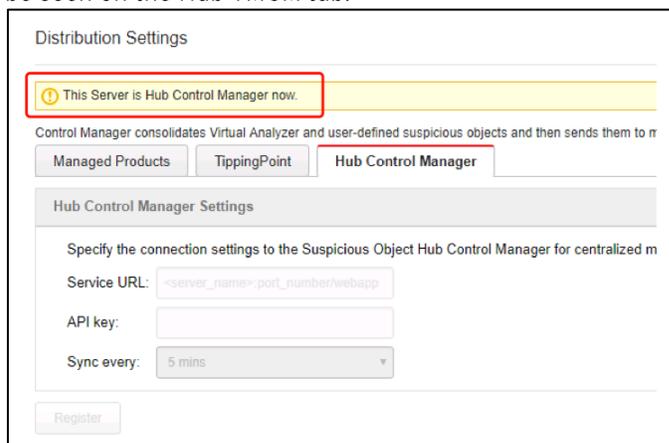
1. Go to **Administration** -> **Suspicious Objects** -> **Distribution Settings**.
2. Copy the Service URL and API key of the Hub TCM.



3. Go to **Administration** -> **Suspicious Objects** -> **Distribution Settings**.
4. Go to the **Hub TCM** tab on the **Node TCM**.
5. Enter the Service URL and API key that was copied from Hub TCM and click Register. The default sync interval is 5 minutes.



After becoming a Hub, the "This Server is Hub Control Manager now" message will be seen on the Hub TCM tab.



The following operations are allowed for Hub Node mode.

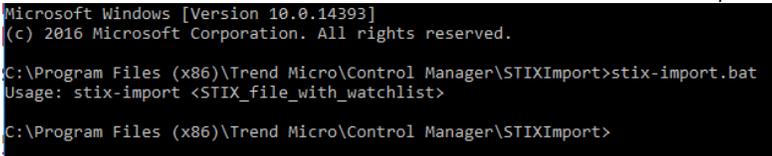
Seq.	Case	Hub to Node	Node to Hub
1	Add UDSO	O	⊗
2	Delete UDSO	O	⊗
3	Add Exception	X*	X
4	Delete Exception	X*	X
5	Add VASO	O	O
6	VASO add to Exception	▲	X
7	VASO never expire	O	⊗
8	VASO never expire and expire Now	O	⊗
9	VASO expire Now	O	⊗
10	VASO Configure Scan Action	O	⊗

- ⊗ Node can't perform this operation
- X Action possible on Node, but not synchronized with Hub
- ▲ Node CM will only remove VASO, but not add to exception
- O Action Synchronized
- X\* Hub to Node exception Sync can be enabled via configuration.

There are two ways to enable exception synchronization from Hub to Node.

- Migrate from TCM 6.0 and register as hub and node. Exception sync is enabled after migration
- Enable manually
  1. Edit <CM\_ROOT>\SystemConfiguration.xml on Hub CM.
  2. Set m\_iTmcmSoDist\_ForceSyncWhitelist to 1.
  3. Restart LogProcessor process.

## 6.4. Suspicious Object Tools

- **ImportSOFromCSV**  
Users can import properly formatted \*.csv files of suspicious object data (UDSO\Exception lists) into Control Manager. Please refer to the OLH for details:  
<http://docs.trendmicro.com/en-us/enterprise/control-manager-70/tools-and-additional/suspicious-object-li12/using-suspicious-obj1.aspx>
- **STIX-Import**  
Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. It can be a good SO resource, and as a tool, was created to allow importing STIX data. We support STIX v1.2.  
  
This tool is located at <CM\_ROOT>/ImportSOFromCSV.exe.  
  
The command syntax is “stix-import.bat <STIX\_file\_with\_watchlist>”.  
  
The tool retrieves the SO information from the STIX file and imports it into UDSO.  


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Trend Micro\Control Manager\STIXImport>stix-import.bat
Usage: stix-import <STIX_file_with_watchlist>

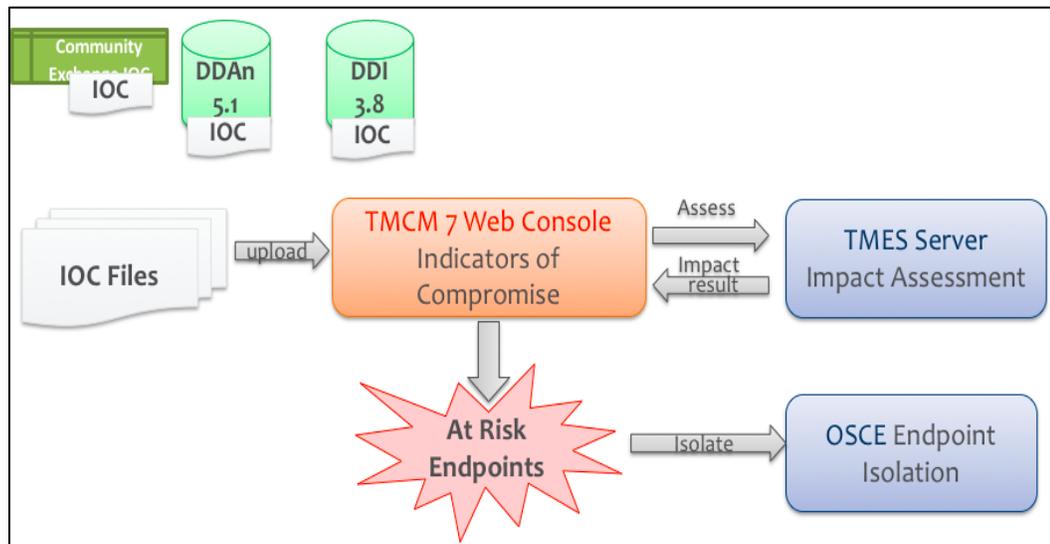
C:\Program Files (x86)\Trend Micro\Control Manager\STIXImport>
```
- **SuspiciousObjectExporter**  
This tool is used in the following cases:
  - Export SO without accessing the UI
  - Export SO into a different format other than CSV
  - Please refer to the OLH for details:  
<http://docs.trendmicro.com/en-us/enterprise/control-manager-70/tools-and-additional/suspicious-object-li12/using-suspicious-obj.aspx>
- **SOMigrationTool**  
This tool exports SOs from CM and import those SOs into a third-party software or other device (i.e. CheckPoint Firewall).  
Please refer to the OLH for details:  
<http://docs.trendmicro.com/en-us/enterprise/control-manager-70/tools-and-additional/suspicious-object-mi/using-the-suspicious.aspx>

## 6.5. IOC Management

Indicators-of-Compromise (IOC) Sources:

- DDAn 5.1
- DDI 3.8
- OpenIOC Samples

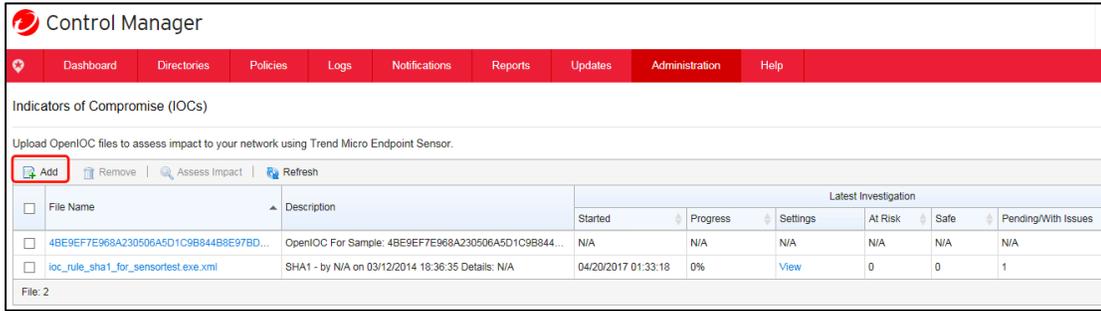
It is recommended to use community IOC as an input for TCM. Though TCM supports DDI/DDAn IOC, those DDI/DDAn IOC are automatically converted to SO and sent to TCM. To avoid redundancy, it is not recommended to use DDI/DDAn IOCs. Once IOC is uploaded to TCM, the administrator use TMES to perform impact assessment which determines the endpoints compromised using the criteria found inside the IOC. The mitigation is performed once the endpoint is validated as compromised and isolated from the network.



### 6.5.1. Adding IOCs

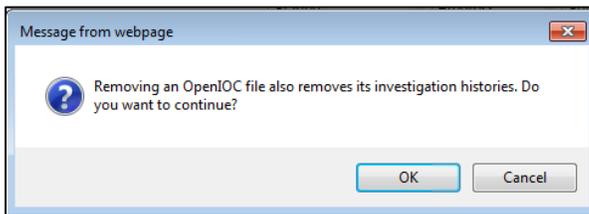
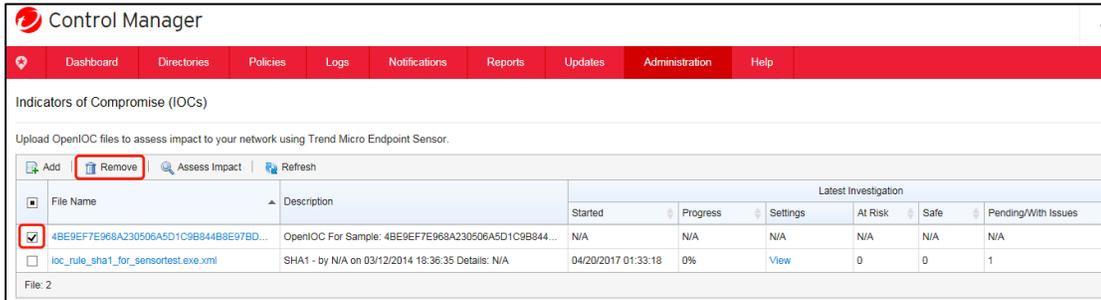
The Add button allows customers to add IOC files from either Deep Discovery Inspector or from OpenIOC samples.

1. Open the TMCM console.
2. Go to **Administration > Indicators of Compromise**.



### 6.5.2. Removing IOCs

The Remove button removes IOC files and reports previously added.



### 6.5.3. Impact Assessment

The Impact Assessment at this stage uses the same mechanism as the Impact Assessment in Suspicious Object Management. Instead of assessing only one object, an entire IOC file is investigated on the endpoints.

Control Manager initiates a command to Trend Micro Endpoint Sensor (TMES) to assess the endpoints which are at risk.

Indicators of Compromise (IOCs)

Upload OpenIOC files to assess impact to your network using Trend Micro Endpoint Sensor.

File Name	Description	Latest Investigation					
		Started	Progress	Settings	At Risk	Safe	Pending/With Issues
<input type="checkbox"/> 4BE9EF7E968A230506A5D1C9B844B8E97BD...	OpenIOC For Sample: 4BE9EF7E968A230506A5D1C9B844...	N/A	N/A	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/> ioc_rule_sha1_for_sensorstest.exe.xml	SHA1 - by N/A on 03/12/2014 18:36:35 Details: N/A	09/18/2018 10:52:58	0%	<a href="#">View</a>	0	0	0

File: 2

Impact assessment has started. Assessment time varies but will not exceed two hours in most cases.

Indicators of Compromise (IOCs)

Upload OpenIOC files to assess impact to your network using Trend Micro Endpoint Sensor.

File Name	Description	Latest Investigation					
		Started	Progress	Settings	At Risk	Safe	Pending/With Issues
<input type="checkbox"/> 4BE9EF7E968A230506A5D1C9B844B8E97BD...	OpenIOC For Sample: 4BE9EF7E968A230506A5D1C9B844...	N/A	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/> ioc_rule_sha1_for_sensorstest.exe.xml	SHA1 - by N/A on 03/12/2014 18:36:35 Details: N/A	09/18/2018 10:52:58	0%	<a href="#">View</a>	0	0	0

File: 2

## 6.5.4. At-risk Endpoints

When endpoints are determined to be at risk, they are displayed with a link in the console:

Impact assessment has started.

Indicators of Compromise (IOCs)

Upload OpenIOC files to assess impact to your network using Deep Discovery Endpoint Sensor. Click [here](#) to view indicators supported in an investigation.

Add Remove Assess Impact Refresh

File Name	Description	Lastest Investigation						
		Started	Status	Settings	At Risk	Safe	Pending	
<a href="#">5CF536F5BEC5247165DC0BCD644C7719BF554DB.ioc</a>	OpenIOC For Sample: 5CF536F5BEC5247165DC0BCD...	03/24/2015 1...	Ongoing	<a href="#">View</a>	0	5	4	
<a href="#">EZE_IOC.ioc</a>	EZE - by User_TMCM_Admin on 01/14/2015 07:25:13 Det...	03/24/2015 1...	Ongoing	<a href="#">View</a>	2	3	4	
<a href="#">GetOpenioc.xml</a>	OpenIOC For Sample: 0C529E8A484EC41F2BDD18724...	03/24/2015 0...	Completed	<a href="#">View</a>	1	1	0	

File: 3

Once clicked, the details of the at-risk endpoint will be shown:

Indicator of Compromise - At Risk Endpoints

Export all results Isolate Specify allowed traffic Restore

First Observed	Host Name	IP Address	Criticality	Matching Object(s)
03/17/2015 15:21:50	tw	10.1.173.164.192.168.197.1.192.16 8.187.1fe80:70a1c666:c4c9:1e45:f e80:8980:5207:2bb1f2b3fe80:a1e 4:1aac:e3c141b8	High	file: msnss.exe file: msnss.exe file: lsass.exe file: SmartTest.exe file: lsass.exe process: SmartTest.exe process: SmartTest.exe file: SmartTest.exe file: lsass.exe file: msnss.exe file: msnss.exe file: lsass.exe file: SmartTest.exe file: lsass.exe file: msnss.exe file: msnss.exe file: lsass.exe process: SmartTest.exe
<input checked="" type="checkbox"/> 03/16/2015 15:52:04	tw	10.1.172.27fd96:7568:9882:6:5722: 9189:621c:9c12fe80:28ab:5cb0:75	Critical	process: SmartTest.exe process: SmartTest.exe

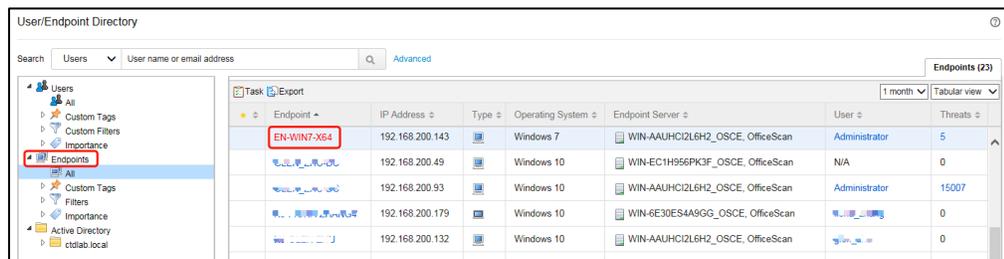
## 6.5.5. OfficeScan Endpoint Isolation

The network isolation, also known as Network Quarantine, it addresses the user scenario where an endpoint requires isolation from the network due to potential threat impact. If endpoint isolation is not performed, enterprise, network or sensitive information can be stolen from this specific endpoint. Implementing this action gives the TCM Administrator a method of mitigation to prevent further damage.

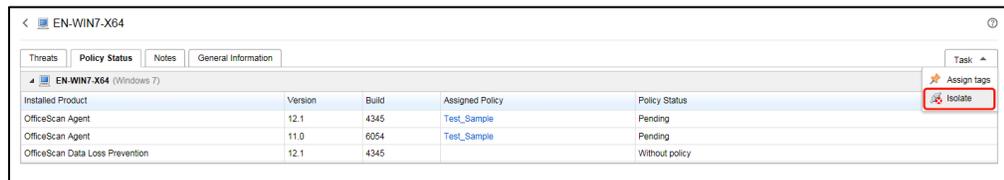
The OfficeScan firewall is used to isolate endpoints at risk. Please also ensure the Single-Sign On for the OSCE server is enabled.

### Deploying Endpoint Isolation Task

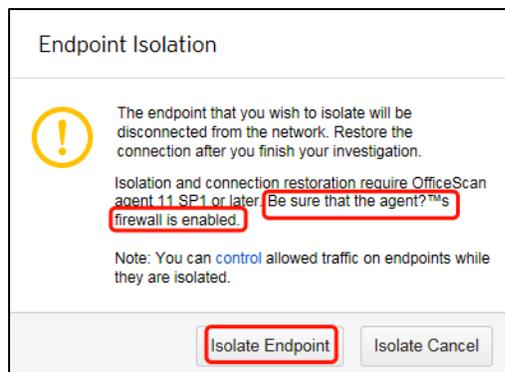
1. Find and select the infected endpoint (e.g. EN-WIN70-X64).



2. Click the Task drop-down list, and click the Isolate option.



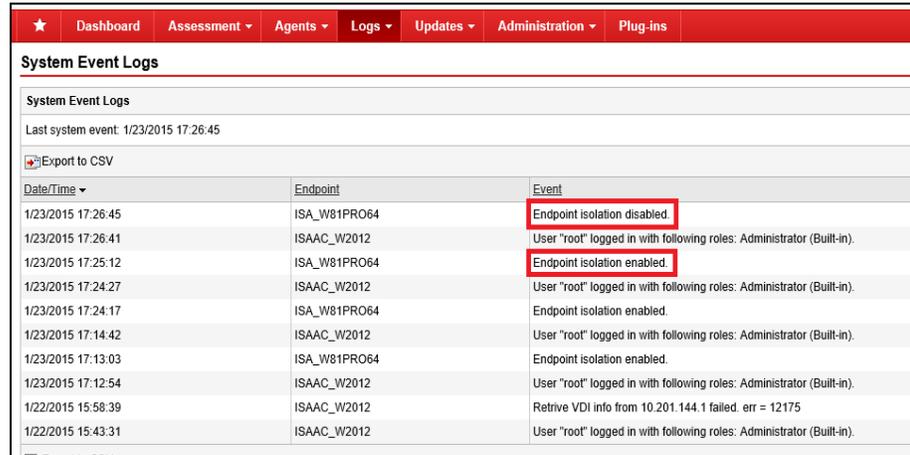
3. Click Isolate Endpoint.



## Verifying Endpoint Isolation

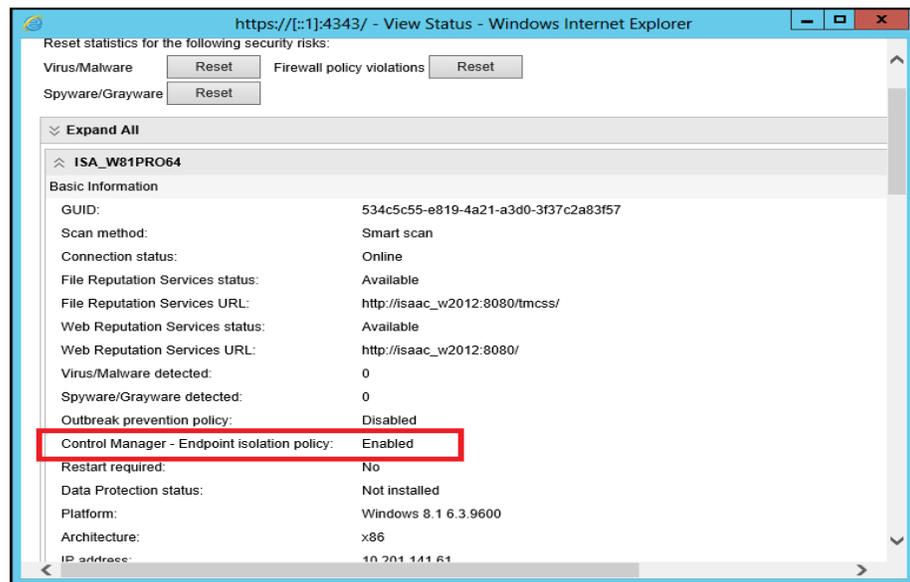
Once the OfficeScan agent has implemented endpoint isolation, the following pieces of tracking information are generated:

### 7. OfficeScan Server System Event Logs



Date/Time	Endpoint	Event
1/23/2015 17:26:45	ISA_W81PRO64	Endpoint isolation disabled.
1/23/2015 17:26:41	ISAAC_W2012	User "root" logged in with following roles: Administrator (Built-in).
1/23/2015 17:25:12	ISA_W81PRO64	Endpoint isolation enabled.
1/23/2015 17:24:27	ISAAC_W2012	User "root" logged in with following roles: Administrator (Built-in).
1/23/2015 17:24:17	ISA_W81PRO64	Endpoint isolation enabled.
1/23/2015 17:14:42	ISAAC_W2012	User "root" logged in with following roles: Administrator (Built-in).
1/23/2015 17:13:03	ISA_W81PRO64	Endpoint isolation enabled.
1/23/2015 17:12:54	ISAAC_W2012	User "root" logged in with following roles: Administrator (Built-in).
1/22/2015 15:58:39	ISAAC_W2012	Retrive VDI info from 10.201.144.1 failed. err = 12175
1/22/2015 15:43:31	ISAAC_W2012	User "root" logged in with following roles: Administrator (Built-in).

### 8. OfficeScan Server console displaying Client status



Reset statistics for the following security risks:

Virus/Malware  Firewall policy violations

Spyware/Grayware

Expand All

ISA\_W81PRO64

Basic Information

GUID: 534c5c55-e819-4a21-a3d0-3f37c2a83f57

Scan method: Smart scan

Connection status: Online

File Reputation Services status: Available

File Reputation Services URL: http://isaac\_w2012:8080/tmcss/

Web Reputation Services status: Available

Web Reputation Services URL: http://isaac\_w2012:8080/

Virus/Malware detected: 0

Spyware/Grayware detected: 0

Outbreak prevention policy: Disabled

**Control Manager - Endpoint isolation policy: Enabled**

Restart required: No

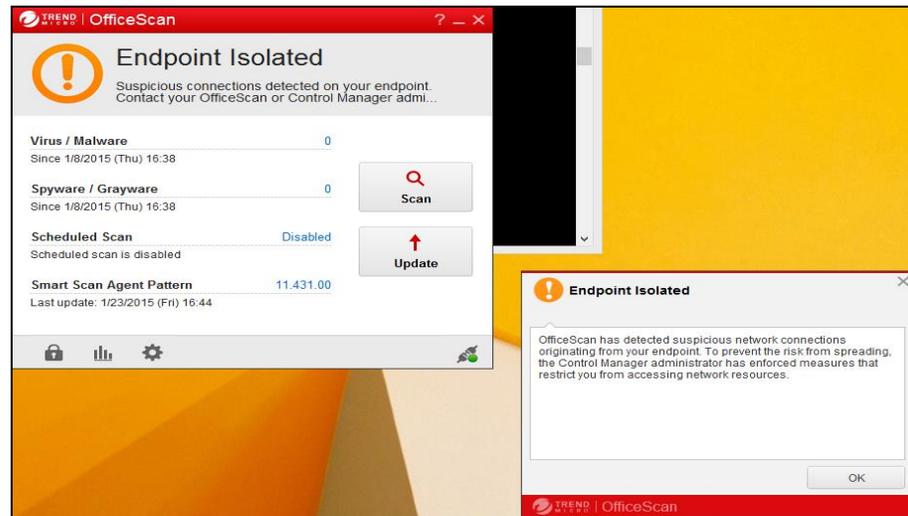
Data Protection status: Not installed

Platform: Windows 8.1 6.3.9600

Architecture: x86

IP address: 10.201.144.61

## 9. Pop-up Notification



## 6.6. CTD Integrated Products

Access this KB article to see the list of the detailed CTD product support capabilities in TCM 7.0: <http://esupport.trendmicro.com/solution/en-US/1118544.aspx>

## 7. Major Functions and Tips

Below are the major functions of Control Manager:

- ✓ Dashboard can show current threat status
- ✓ Collect and query managed product logs
- ✓ Execute malware scan for managed product
- ✓ Single Sign On for the managed product
- ✓ Provide product license status and update it
- ✓ Deliver policy like function settings and exception rules
- ✓ Deliver latest pattern and engine
- ✓ Generate report with managed product information
- ✓ Receive or share suspicious object (SO) between Control Manager and managed product to minimize threat impact
- ✓ Share exception list to minimize false alarm impact
- ✓ Notify alert or information by email (SMTP), SNMP, Syslog, Windows event log and Trigger Application Settings.

Refer to Appendix to know which function(s) each product could be supported.

## 7.1. Early Discovery

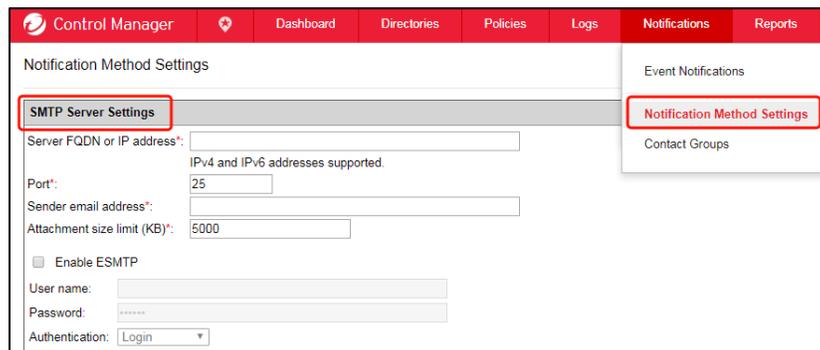
To realize the possible incident earlier, email notification, syslog or SNMP could be enabled by Control Manager.

### Event Notifications

- ✓ Email notification

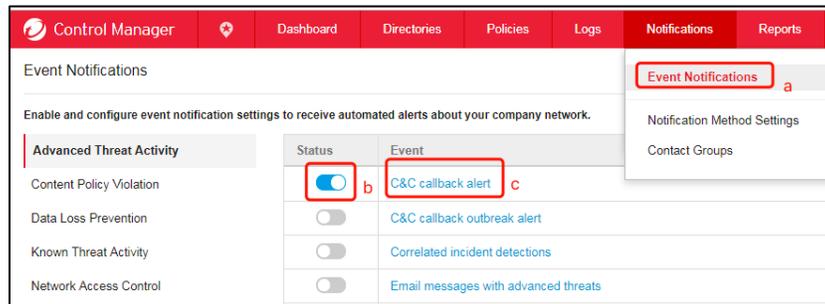
To identify possible issues earlier, email notification could be configured.

- Configure the SMTP Server Settings.



The screenshot shows the 'SMTP Server Settings' configuration page in the Control Manager interface. The page includes fields for 'Server FQDN or IP address\*', 'Port' (set to 25), 'Sender email address\*', and 'Attachment size limit (KB)' (set to 5000). There is an 'Enable ESMTP' checkbox and fields for 'User name' and 'Password'. The 'Authentication' dropdown is set to 'Login'. A sidebar menu on the right shows 'Event Notifications', 'Notification Method Settings', and 'Contact Groups'. The 'SMTP Server Settings' section is highlighted with a red box.

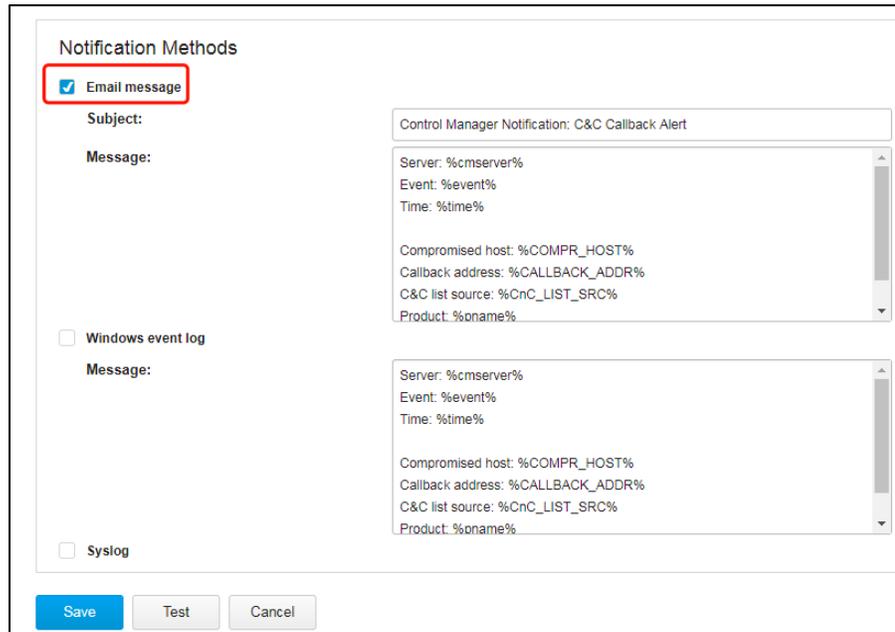
- Enable the specific event type, and click on the event name.



The screenshot shows the 'Event Notifications' configuration page in the Control Manager interface. The page includes a table with columns for 'Status' and 'Event'. The 'Advanced Threat Activity' section is selected. The 'C&C callback alert' event is highlighted with a red box, and its status is enabled (indicated by a blue toggle switch). A sidebar menu on the right shows 'Event Notifications', 'Notification Method Settings', and 'Contact Groups'. The 'Event Notifications' section is highlighted with a red box and labeled 'a', the toggle switch is labeled 'b', and the event name 'C&C callback alert' is labeled 'c'.

Status	Event
<input checked="" type="checkbox"/>	C&C callback alert
<input type="checkbox"/>	C&C callback outbreak alert
<input type="checkbox"/>	Correlated incident detections
<input type="checkbox"/>	Email messages with advanced threats

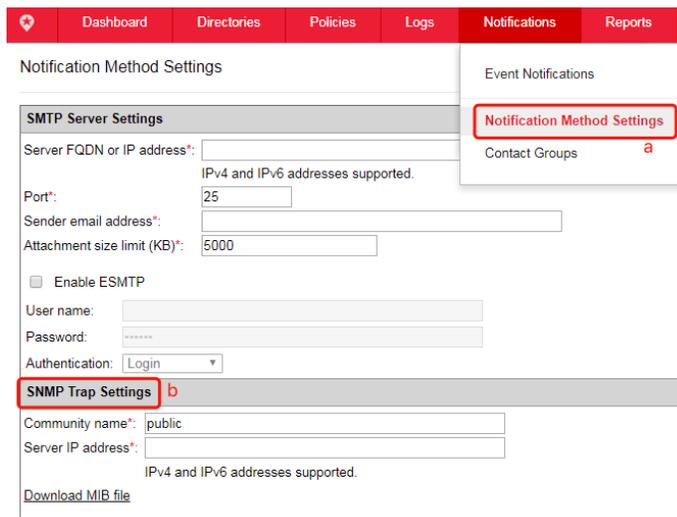
- c. Enable **Email message**. Modify the Subject and Message is needed.



- d. Click **Save**.

✓ **SNMP**

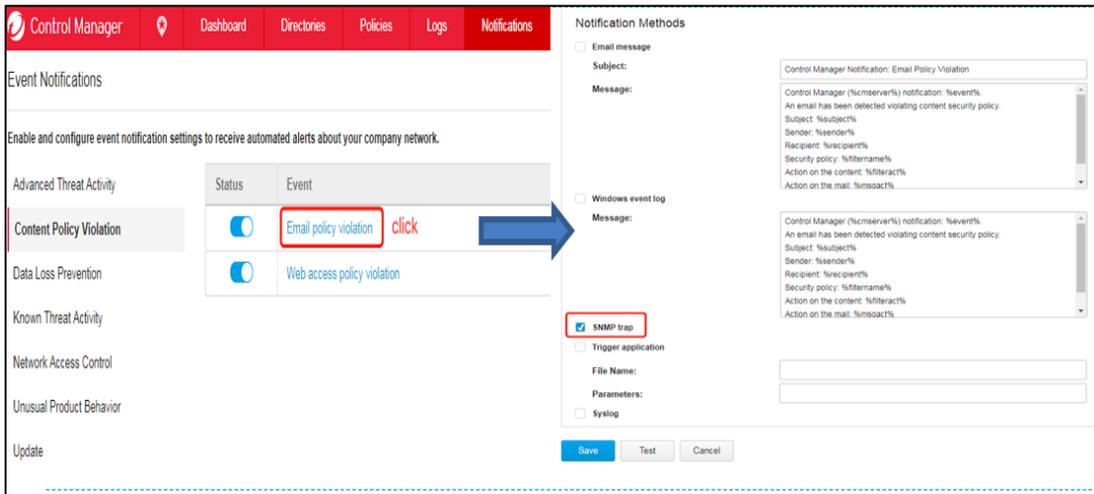
SNMP Trap sends a notification using Simple Network Management Protocol. TCMCM stores notifications in Management Information Bases (MIBs) and MIB browsers are used to view the SNMP notification.



In the SNMP Trap Settings section, specify the following:

- a. **Community name:** Type the SNMP community name.
- b. **Server IP address:** Type the IPv4 or IPv6 address of the SNMP server.

Check if the SNMP trap is supported.



The screenshot shows the 'Event Notifications' section in the Control Manager interface. On the left, a table lists various event types with their status and a 'click' link. A blue arrow points from the 'Email policy violation' link to the 'SNMP trap' checkbox in the 'Notification Methods' panel on the right.

Event Notifications	Status	Event
Advanced Threat Activity	<input type="checkbox"/>	
Content Policy Violation	<input checked="" type="checkbox"/>	Email policy violation <a href="#">click</a>
Data Loss Prevention	<input checked="" type="checkbox"/>	Web access policy violation
Known Threat Activity	<input type="checkbox"/>	
Network Access Control	<input type="checkbox"/>	
Unusual Product Behavior	<input type="checkbox"/>	
Update		

**Notification Methods**

Email message

Subject: Control Manager Notification: Email Policy Violation

Message: Control Manager (%cmserver%) notification: %event%. An email has been detected violating content security policy. Subject: %subject% Sender: %sender% Recipient: %recipient% Security policy: %filtername% Action on the content: %filteract% Action on the mail: %smsoact%

Windows event log

Message: Control Manager (%cmserver%) notification: %event%. An email has been detected violating content security policy. Subject: %subject% Sender: %sender% Recipient: %recipient% Security policy: %filtername% Action on the content: %filteract% Action on the mail: %smsoact%

**SNMP trap**

Trigger application

File Name:

Parameters:

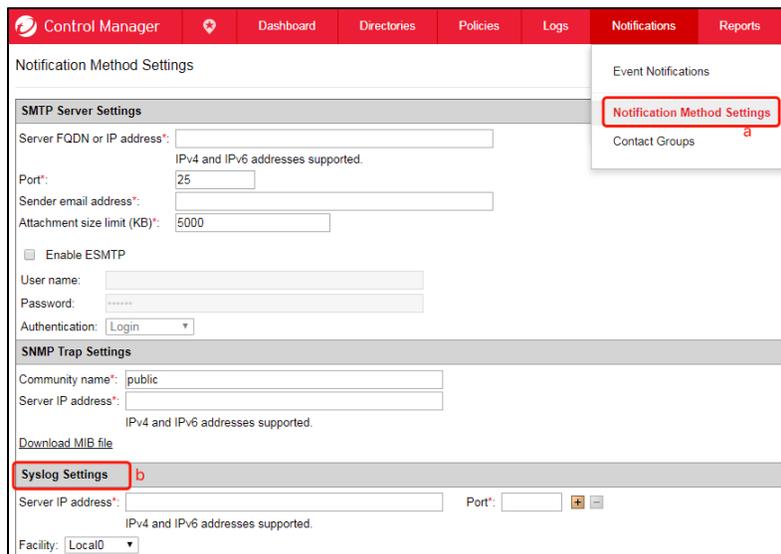
Syslog

Save Test Cancel

## ✓ Syslog

The following are the characteristics of the syslog message:

- Easier regular expression parsing
- Enhanced readability
- Uses the name value pair \_\_name = “\_\_value\_\_”
- Follows RFC 3164 for syslog format
- Applies ISO 8601 time format
- Maintains the same event ID with the SNMP message for better consistency



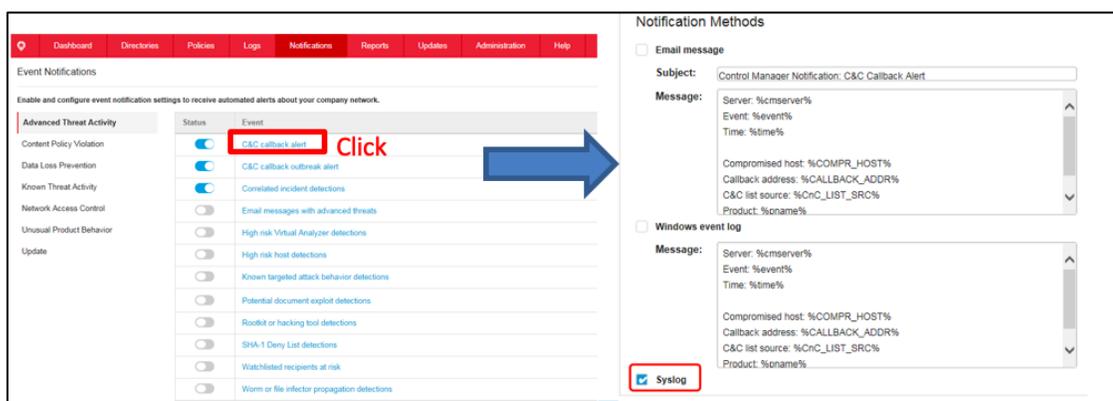
The screenshot shows the 'Notification Method Settings' page in the Control Manager interface. The 'Syslog Settings' section is highlighted with a red box. The settings include:

- SMTP Server Settings:** Server FQDN or IP address, Port (25), Sender email address, Attachment size limit (KB) (5000), Enable ESMTTP checkbox, User name, Password, Authentication (Login).
- SNMP Trap Settings:** Community name (public), Server IP address, Download MIB file link.
- Syslog Settings:** Server IP address, Port, Facility (Local0).

In the **Syslog Settings** section, specify the following:

- Server IP address: Type the IPv4 or IPv6 address of the syslog server.
- Port: The port number of the syslog server.
- Facility: Select the facility code.
- Add multiple syslog servers using the add icon if you have.

Check if Syslog is supported.



This table shows which event is supported by syslog.

Group	Events	Support Syslog
Advanced Threat Activity	C&C Callback alert	Y
	C&C Callback outbreak alert	N
	Correlated Incident Detections	N
	Email Messages with Advanced Threats	N
	High Risk Virtual Analyzer Detections	N
	High Risk Host Detections	N
	Known Targeted Attack Behavior	N
	Potential Document Exploit Detections	N
	Rootkit or Hacking Tool Detections	N
	SHA-1 Deny List Detections	N
	Worm or File Infector Propagation Detections	N
	Content Policy Violation	Email Policy Violation
Web Access Security Violation		Y
Data Loss Prevention	Incident Details Updated	N
	Scheduled Incident Summary	N
	Significant Incident Increase	N
	Significant Incident Increase by Channel	N
	Significant Incident Increase by Sender	N
	Significant Incident Increase by User	N
	Significant Template Match Increase	N

Known Threat Activity	Network Virus Alert	Y
	Special Spyware/Grayware Alert	Y
	Special Virus Alert	Y
	Spyware/Grayware Found - Action Successful	Y
	Spyware/Grayware Found - Further Action Required	Y
	Virus Found - First Action Successful	Y
	Virus Found - First Action Unsuccessful and Second Action Unavailable	Y
	Virus Found - First and Second Actions Unsuccessful	Y
	Virus Found - Second Action Successful	Y
	Virus Outbreak Alert	Y
Network Access Control	Network VirusWall Policy Violations	N
	Potential Vulnerability Attacks	Y
Unusual Product Behavior	Managed Product Unreachable	N
	Product Service Started	Y
	Product Service Stopped	Y
	Real-time Scan Disabled	Y
	Real-time Scan Enabled	Y
Updates	Antispam Rule Update Successful	Y
	Antispam Rule Update Unsuccessful	Y
	Pattern File/Cleanup Template Update Successful	Y
	Pattern File/Cleanup Template Update Unsuccessful	Y
	Scan Engine Update Successful	Y
	Scan Engine Update Unsuccessful	Y

## LogForwarder Tool

LogForwarder Tool can send several log types from the Control Manager database to a syslog server, in either ArcSight Common Event Format (CEF) or Control Manager (CM) format.

The following are the types of logs that the Log Forwarder Tool supports:

Log Types	CEF Log Format Support	TMCM Log Format Support
Behavior Monitoring	Yes	Yes
C&C Callback	Yes	No
Data Loss Prevention	Yes	Yes
Device Access Control	Yes	Yes
Engine Update Status	Yes	Yes
Suspicious File	Yes	No
Network Content Inspection	Yes	No
Virus/Malware	Yes	No
Pattern Update Status	Yes	Yes
Content Security	Yes	No
Spyware/Grayware	Yes	No
Web Security	Yes	No
Predictive Learning Machine	Yes	No
Endpoint Application Control*	Yes	No
Sandbox Detection Logs*	Yes	No

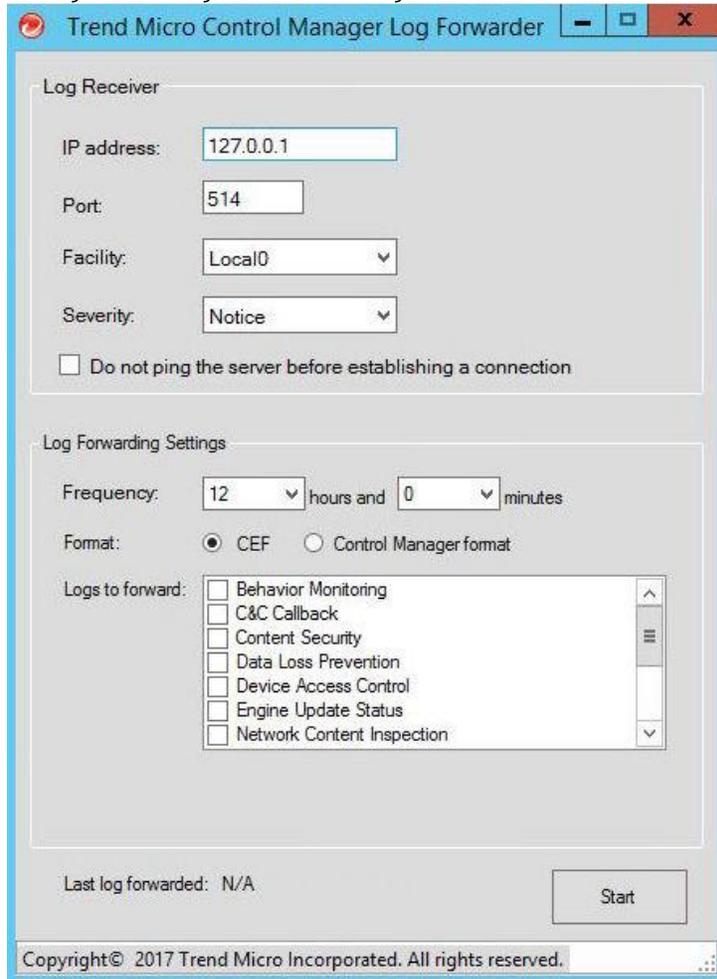
\* Means it is available after TMCM 7.0 Patch 1.

## Attention

- ✓ TMCM 7.0 discontinues support for the DataExport Tool. Administrators should use the new LogForwarder Tool (LogForwarder.exe).
- ✓ The LogForwarder Tool only supports UDP protocol.

## Configuring LogForwarder Settings

- Go to the TCMC installation directory. By default, the installation directory is C:\Program Files (x86)\Trend Micro\Control Manager.
- Execute the LogForwarder.exe file using administrator rights (Run as administrator) to open the LogForwarder console.
- Configure the Log Receiver settings.



The screenshot shows the 'Trend Micro Control Manager Log Forwarder' configuration window. It is divided into two main sections: 'Log Receiver' and 'Log Forwarding Settings'.  
**Log Receiver Section:**  
- IP address: 127.0.0.1  
- Port: 514  
- Facility: Local0 (dropdown)  
- Severity: Notice (dropdown)  
- A checkbox labeled 'Do not ping the server before establishing a connection' is currently unchecked.  
**Log Forwarding Settings Section:**  
- Frequency: 12 hours and 0 minutes (dropdowns)  
- Format: CEF (radio button selected), Control Manager format (radio button unselected)  
- Logs to forward: A list of log categories with checkboxes, all of which are currently unchecked:

- Behavior Monitoring
- C&C Callback
- Content Security
- Data Loss Prevention
- Device Access Control
- Engine Update Status
- Network Content Inspection

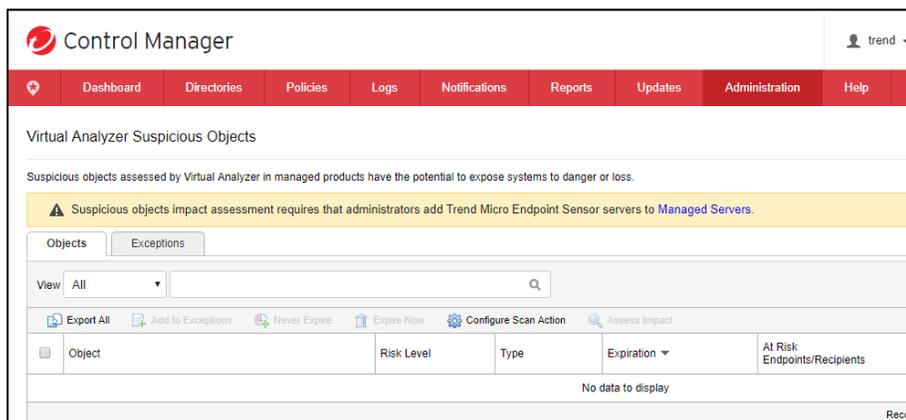
At the bottom of the window, there is a 'Last log forwarded: N/A' label, a 'Start' button, and a copyright notice: 'Copyright© 2017 Trend Micro Incorporated. All rights reserved.'

- IP address: Syslog server IP address
- Port: Syslog server port number
- Facility: Facility code of the syslog message  
This setting only applies to Control Manager format logs.
- Severity: Severity level of the syslog message  
This setting only applies to Control Manager format logs.

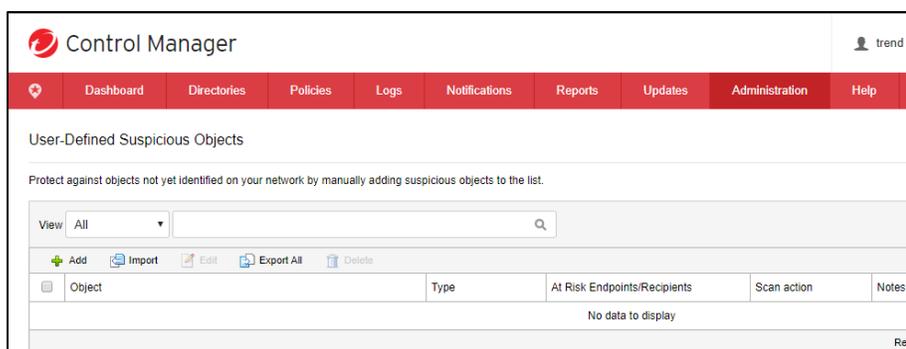
- (Optional) Do not ping the server before establishing a connection:  
Select to send the syslog message without having to ping the destination server first
- d. Configure the **Log Forwarding Settings**.
  - Frequency: The frequency in which the tool sends logs
  - Format: Select whether to use CEF or Control Manager log format
  - Logs to forward: Select the log types to forward to Control Manager
- e. Click **Start**.  
Note: Users will need to manually stop the LogForwarder Tool from its console, because it will continue to run in the background even after a successful restart of the TCM services.

## 7.2. Minimize Threat Influence

By delivering VASO and UDSO to managed products, they will be protected from possible threats.



The screenshot shows the 'Virtual Analyzer Suspicious Objects' page in the Control Manager web console. The page has a red navigation bar with tabs for Dashboard, Directories, Policies, Logs, Notifications, Reports, Updates, Administration, and Help. Below the navigation bar, the page title is 'Virtual Analyzer Suspicious Objects'. A message states: 'Suspicious objects assessed by Virtual Analyzer in managed products have the potential to expose systems to danger or loss.' A yellow warning banner indicates: 'Suspicious objects impact assessment requires that administrators add Trend Micro Endpoint Sensor servers to Managed Servers.' Below this, there are tabs for 'Objects' and 'Exceptions'. A search bar and a 'View' dropdown are present. Action buttons include 'Export All', 'Add to Exceptions', 'Never Expire', 'Expire Now', 'Configure Scan Action', and 'Assess Impact'. A table with columns 'Object', 'Risk Level', 'Type', 'Expiration', and 'At Risk Endpoints/Recipients' is shown, with the message 'No data to display'.



The screenshot shows the 'User-Defined Suspicious Objects' page in the Control Manager web console. The page has the same red navigation bar. Below the navigation bar, the page title is 'User-Defined Suspicious Objects'. A message states: 'Protect against objects not yet identified on your network by manually adding suspicious objects to the list.' Below this, there are tabs for 'Objects' and 'Exceptions'. A search bar and a 'View' dropdown are present. Action buttons include 'Add', 'Import', 'Edit', 'Export All', and 'Delete'. A table with columns 'Object', 'Type', 'At Risk Endpoints/Recipients', 'Scan action', and 'Notes' is shown, with the message 'No data to display'.

Note:

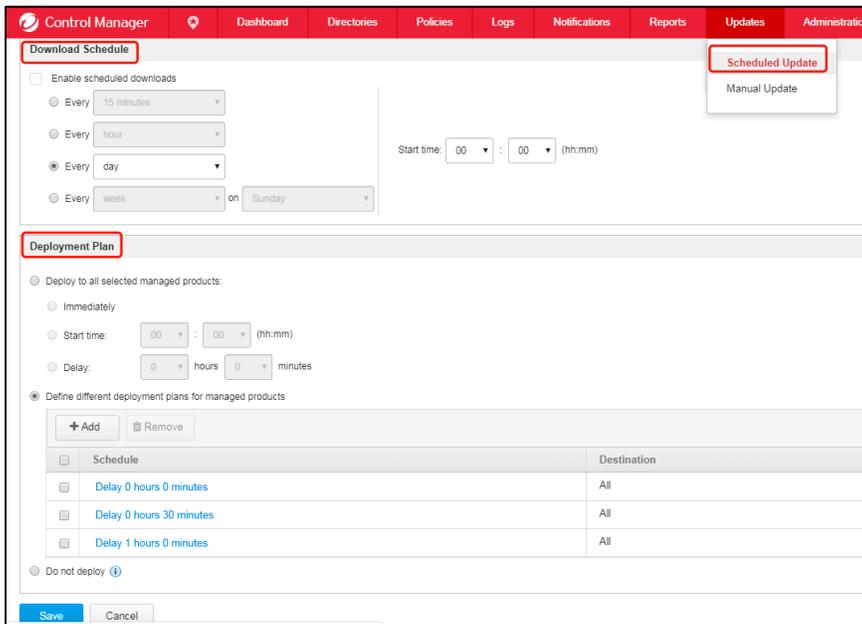
- Expired SO will be deleted every hour.
- From TMCM web console, expiration period can be configure to:
  - Expire now
  - Never expire

## 7.3. Deliver latest pattern and engine

Deliver latest pattern and engine to detect threats by managed products.

Scheduled Update the Manual Update are available.

For Scheduled Update, administrators can set the Download Schedule and Deployment Plan accordingly based on the network bandwidth and site scale.



**Download Schedule**

Enable scheduled downloads

Every 15 minutes  
 Every hour  
 Every day  
 Every week on Sunday

Start time: 00 : 00 (hh:mm)

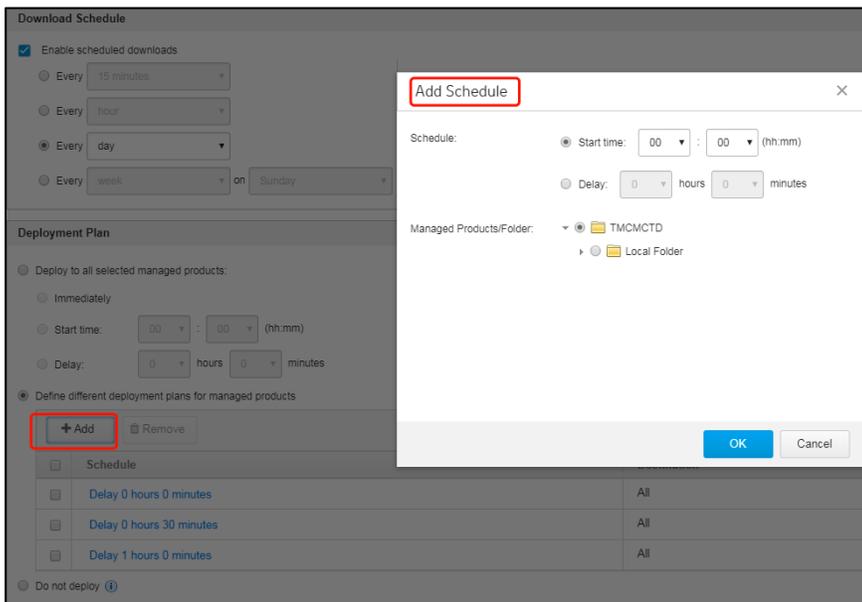
**Deployment Plan**

Deploy to all selected managed products:  
 Immediately  
 Start time: 00 : 00 (hh:mm)  
 Delay: 0 hours 0 minutes  
 Define different deployment plans for managed products

Schedule	Destination
Delay 0 hours 0 minutes	All
Delay 0 hours 30 minutes	All
Delay 1 hours 0 minutes	All

Do not deploy

Save Cancel



**Download Schedule**

Enable scheduled downloads

Every 15 minutes  
 Every hour  
 Every day  
 Every week on Sunday

**Deployment Plan**

Deploy to all selected managed products:  
 Immediately  
 Start time: 00 : 00 (hh:mm)  
 Delay: 0 hours 0 minutes  
 Define different deployment plans for managed products

**Add Schedule**

Schedule:

Start time: 00 : 00 (hh:mm)  
 Delay: 0 hours 0 minutes

Managed Products/Folder:

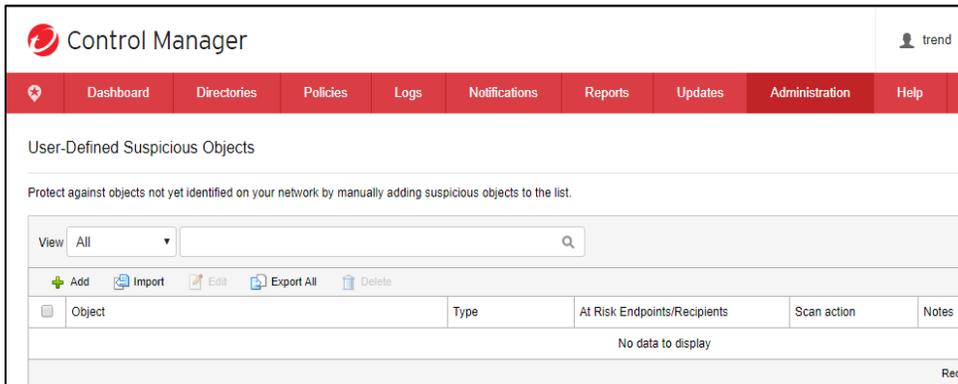
- TMC/MCTD
  - Local Folder

OK Cancel

For Manual Update, administrators should consider the reasonable and suitable the Deployment Plan.

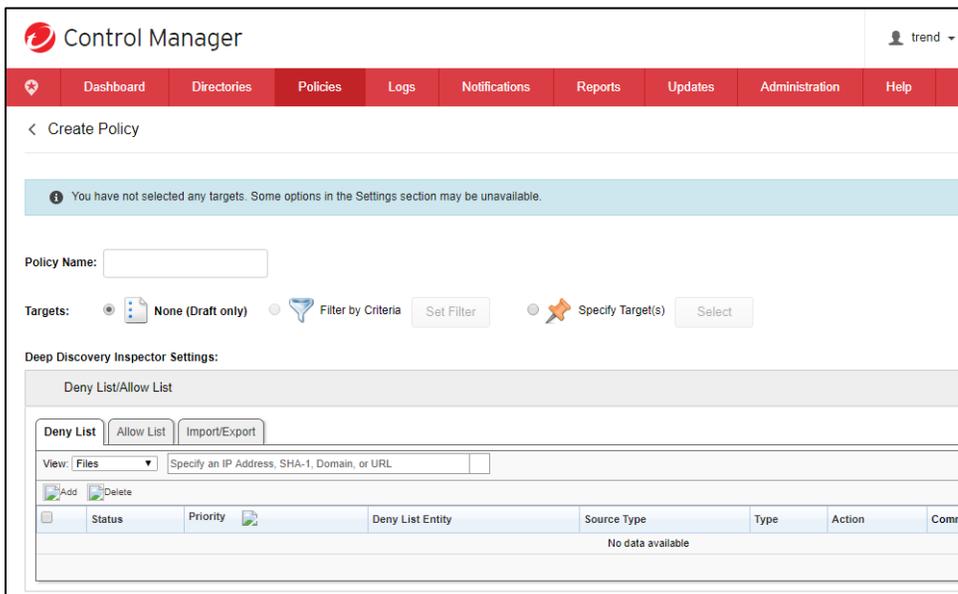
## 7.4. Minimize false alarm detection

Deploying the exception list to managed products will minimize the false alarm detection impact. Because Control Manager can sync exception list to DDAN, DDEI and DDI only, you need to configure exception list for other product with managed product console.



## 7.5. Modify Settings after incident review

Once incident happens and is reviewed for future protection, you may want to change settings for managed products. Then, you can deliver updated policy settings from Control Manger. Please refer Section 3 in detail.



# 8. Migration from Cascading Mode

To simplify centralized management and reduce latency, TCM 7.0 is moving away from cascading management, in which a single Control Manager parent server controls multiple Control Manager child servers.

New deployments should plan for a single Control Manager architecture. New features and functions will not be available for cascaded deployments in the future.

Based on the production experience of TCM customers, cascading management does not alleviate capacity limitations. Instead, cascading management only moves the problem from the child servers to the parent server through increased network complexity and latency.

Full-fledged role-based access control on a single TCM server also allows administrators to assign clear roles and responsibilities for teams in highly distributed organizations, for easier collaboration and coordination.

The new structure offers a single pane of glass on a single TCM server.

We believe this is the right direction for our customers and greatly improves centralized management.

## 8.1. Collect Configurations

Various configurations from all child TCM and the parent TCM server can be collected. Refer to the information below:

### 8.1.1. User Accounts and Roles

1. Go to **Administration > Account Management > User Accounts** and take note of the user role and access control for each account.
2. Go to **Administration > Account Management > User Roles** and take note of the Menu Access Control for customized roles.

### 8.1.2. Product List

1. Go to **Directories > Products** and take note of all the product servers.
2. Go to **Administration > Managed Servers** and take note of all the product servers (URL sand assigned names).

### 8.1.3. Policy

1. Go to **Policies > Policy Management**, and export all policies in the policy list.
2. Go to **Policies > Policy Management** > click on the number right after **"Total endpoints/products:"**, and then export the entire list to a CSV format.

Policy Management 🔍 ⌵

Product: OfficeScan Agent

Create Copy Settings Inherit Settings Import Settings Export Settings Delete Revoke Change Owner Refresh

Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	With Issues	Owner	Last Editor
1	Test_Sample	N/A	N/A	Filtered	0	25	0	root	root
Total:					0	25	0		

Endpoints/Products without policies: 0

Total endpoints/products: 25

Take note of the policy names, exported policy file names, and filter criteria in a table. If the policy is a specify policy, the targets should be listed in the endpoint policy list.

### 8.1.4. DLP Templates and Identifiers

1. a. Go to **Policies > Policy Resources > DLP Data Identifiers/DLP Templates**, find out the customized DLP templates and identifiers, and then export them.

### 8.1.5. Report

1. Go to **Reports > Custom Templates**, select and export all custom templates.
2. Go to **Reports > Scheduled Reports**, then take note of the necessary schedule report settings (e.g. Report Name, Report content, Format, Targets, Frequency and description for purpose).

### 8.1.6. Notifications

1. Go to **Notifications**, and take note of the following:
  - all settings from Notification Method Settings
  - all customized contact groups
  - all enabled notifications and its settings
2. Check the settings of LogForwarder tool:
  - the IP address\Port of the syslog server
  - the frequency that TCM send the logs to syslog server
  - the logs need to be forwarded to syslog server

## 8.1.7. Update

1. Go to **Updates > Scheduled Update**, then take note of the:
  - Download Schedule
  - Deployment Plan

## 8.1.8. Suspicious Objects

1. Go to **Administration > Suspicious Objects > Virtual Analyzer Objects**, export the Exception list.
2. Go to **Administration > Suspicious Objects > User Defined Objects**, export the User Defined Objects.
3. Note the TippingPoint information if it is set in **Administration > Suspicious Objects > Distribution Settings**.

## 8.1.9. Other Settings

1. Go to **Administration > Settings**, then take note of the settings that are required.

## 8.2. Review/Re-design of management model

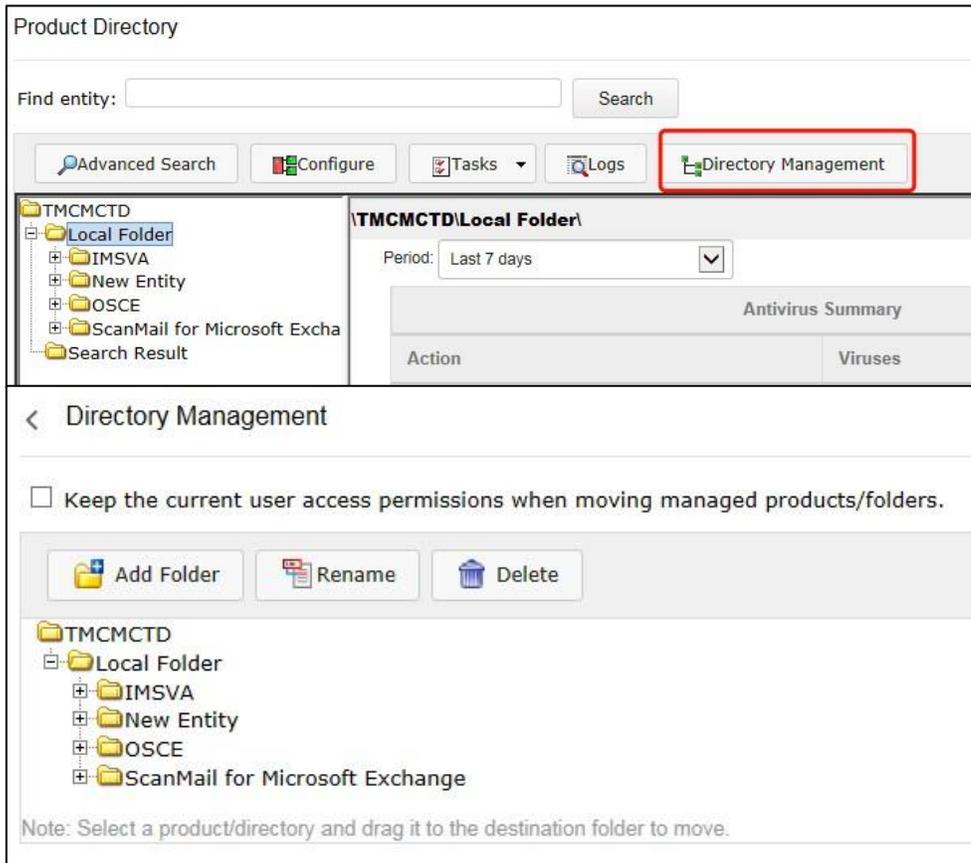
Since all child/parent TCM users will be merged into one TCM. Please refer to the questions below to re-design the management model.

### 8.2.1. Account and Access Control

- Review all accounts and access control scope from all Child/Parent TCM to remove non-used accounts and leave only necessary accounts and privilege.
- The TCM root account is a super user. By default, this account should login by purpose, not for daily administration. Users should login using their own account.
- Account management should depend on a central account manager (e.g.sync Active Directory to manage accounts).
- Group accounts into an AD group and import the AD group as TCM user account. You can grant the access control for the AD group.
- All AD accounts belong to the last imported AD group will have the AD group access control and its privilege.
- Accounts who are in *DLP\_Compliance\_Officer\DLP\_Incident\_Reviewer* roles only have DLP Incident Widget privilege.
- The access control for an account decides the data from which products that the account can View, Execute or Deploy policy.

## 8.2.2. Product Grouping

- Review all products from Child/Parent TCMC.
- Design a grouping model for all products (e.g. by geography or by function).
- Use Product Directory Management to sort the products.



**Product Directory**

Find entity:  Search

Advanced Search | Configure | Tasks | Logs | **Directory Management**

**TMCCTD**

- Local Folder
  - IMSV A
  - New Entity
  - OSCE
  - ScanMail for Microsoft Excha
  - Search Result

**\TMCCTD\Local Folder\**

Period: Last 7 days

Antivirus Summary	
Action	Viruses

**Directory Management**

Keep the current user access permissions when moving managed products/folders.

Add Folder | Rename | Delete

**TMCCTD**

- Local Folder
  - IMSV A
  - New Entity
  - OSCE
  - ScanMail for Microsoft Exchange

Note: Select a product/directory and drag it to the destination folder to move.

### 8.2.3. Policy

- Products in the “New Entity” folder, will NOT be assigned to any policy.
- For OfficeScan Agent policies:
  - Consolidate all the policies from Child/Parent TCM and define some parent policies as draft.
  - Login with AD group account to create an inherit policy from parent policy and assign targets.
  - The assignable targets are depended on AD group account access control scope.
  - The policy owner will be the AD group. All accounts that belong to this AD group can edit the policy.
  - Be careful of the Filtered policies. They only filter the targets who belong to the policy creator’s access control scope.
  - For some important and critical endpoints, please use the Specify Target policy
  - Change the policy name to represent the function of that policy.
- For other policies:
  - Consolidate all the policies from Child/Parent TCM.
  - Login with AD group account to create policies and assign the targets.
- For DLP related policies:
  - The DLP Template and Identifiers should be merged from all Child/Parent TCM, and then configure the DLP policies.
- Before deploying one policy, please expand the settings and double check them.

### 8.2.4. Notifications

- Consolidate all the notification settings and may consider to use Syslog or Logforwarder tool as the notification method
  - Refine users in the Contact Group
- Note: Currently, TCM only supports one SNMP receiver. However, multiple Syslog servers and Email addresses are supported.

### 8.2.5. Reports

- Users who have the “Report menu access” rights can manage reports
- Administrators can create reports that their own requirement and divide them by the name of the reports

## 8.2.6. Scheduled Update/Deploy Plan

- Finalize a suitable download frequency for all regions
- The Deployment Plan should group all the server into some different zones. For example, the servers in the Testing Zone should get the component first to evaluate the update.

## 8.2.7. Register Products

Some products (MCP) are registered from the product-side to TCM, but some products (WSI\SCO) are added on TCM side.

So, the network connections between TCM and managed products should be configured to allow two-way communication for TCM ports and product ports.

# 8.3. Migration and Configuration

## 8.3.1. Evaluate when to do the migration

- Older data or reports will not be available after the migration to the new TCM Server.
- If a monthly or weekly report is required, it needs to be generated before doing a migration.

## 8.3.2. Install TCM

- Perform a fresh installation of TCM 7.0 on a new machine.

## 8.3.3. Apply some of the basic configuration

- Sync Active Directory
- Create the product tree structure

Note: Create a backup of all child/parent TCM Databases and upgrade the managed products to the version that are supported by TCM 7.0

### 8.3.4. Moving managed products

- Move products from child TMCM first, and then parent TMCM
- Unregister the MCP products from TMCM on managed product's web console.
- Register the MCP products to TMCM from managed product's web console.
- Delete all the products on the TMCM Administration > Managed Servers > Server Registration page manually.
- Add all the products you removed in above step back to the new TMCM console manually.

Note: Trend Micro recommends that customer add Deep Discovery Analyzer (DDAN) first.

### 8.3.5. Post Migration

1. Logon with "root" account.
2. Move the products to their designated folders (refer to Chapter 9.2.2 for recommended Product Groupings).
3. Import AD users/groups from AD and apply the access control scopes
4. (If an AD user belongs to two AD groups, he will be sorted into the latest import AD group).
5. Configure the notifications.
6. Import the report templates.
7. Import the SO exception lists and User-Defined SO.
8. Import IOC.
9. Create the parent policies.
10. Configure the update schedule and deployment plan.

### 8.3.6. Administrator logon

- The administrator start to logon to check their own access control scopes.
- Create their own child policies.
- Create their own reports.

# Appendix A: TMCM functions with managed products

This section provide which functions control manager support for the managed product.

Function	Description	OfficeScan	Office Scan Plug-in	
		11, XG, XG SPI	DLP option	Vulnerability detection
Dashboard	Dashboard can show connection status with managed product	Supported	N/A	N/A
Directory > Product	<b>Directory &gt; Product</b> can show product information	Supported	N/A	N/A
Directory > Endpoint	When Endpoint name is selected, product information is shown in policy status or threat status.	Supported	N/A	N/A
Scan Now	TMCM can send scan now command to product	Supported	N/A	N/A
Log Query	TMCM can query collected product logs.	Supported	Supported	N/A
Single Sign On	TMCM allow single sign on to product management console.	Supported	Supported	N/A
License Management Expired date	TMCM show expired date for product	Supported	N/A	N/A
License Management Renew AC	TMCM can renew AC for product	Supported	N/A	N/A
License Management Register new AC	TMCM can register new AC for product	Supported	N/A	N/A

Update > Component delivery	TMCM can deliver components to product	Supported	N/A	N/A
Update > AU source	TMCM can be set as the Active Update source for product	Supported	N/A	N/A
Policy Management	TMCM can deliver policy to product	Supported	Supported	N/A
Report	TMCM can include product log information in TMCM report	Supported	Supported	N/A
Suspicious Object collection	TMCM can receive Suspicious object information from product	N/A	N/A	N/A
Suspicious Object sharing	TMCM can share Suspicious object information to product	Supported	N/A	N/A

Function	Office Scan Plug-in	Trend Micro Security for Mac	Trend Micro Virtual Patch for Endpoint	Smart Protection Server	Worry Free Business Security
	Trend Micro VDI option	2.0 3.0	2.0	3.0 3.1	9.5 10
Dashboard	N/A	Supported	Supported	Supported	Supported
Directory > Product	N/A	N/A	N/A	N/A	N/A
Directory > Endpoint	N/A	Supported	Supported	N/A	Supported
Scan Now	N/A	N/A	N/A	N/A	N/A
Log Query	N/A	Supported	Supported	N/A	Supported
Single Sign On	N/A	Supported	Supported	N/A	Supported

License Management Expired date	N/A	Supported	Supported	N/A	Supported
License Management Renew AC	N/A	N/A	N/A	N/A	N/A
License Management Register new AC	N/A	N/A	Supported	N/A	N/A
Update > Component delivery	N/A	N/A	N/A	N/A	N/A
Update > AU Source	N/A	Supported	Supported	Supported	N/A
Policy Management	N/A	Supported	N/A	N/A	N/A
Report	N/A	Supported	Supported	N/A	Supported
Suspicious Object collection	N/A	N/A	N/A	N/A	N/A
Suspicious Object sharing	N/A	N/A	N/A	Supported	N/A

Function	Trend Micro Endpoint Sensor	Trend Micro Portable Security	Trend Micro Safe Lock	Trend Micro Deep Security	Trend Micro Secure Cloud
	1.6	2.0	1.0 1.1 2.0	9.6 10.0	-
Dashboard	Supported	N/A	N/A	Supported	N/A
Directory > Product	N/A	N/A	N/A	N/A	N/A
Directory > Endpoint	Supported	N/A	N/A	N/A	N/A
Scan Now	N/A	N/A	N/A	N/A	N/A
Log Query	Supported	N/A	N/A	Supported	N/A
Single Sign On	Supported	N/A	N/A	N/A	N/A
License Management Expired date	N/A	N/A	N/A	N/A	N/A
License Management Renew AC	N/A	N/A	N/A	N/A	N/A
License Management Register new AC	N/A	N/A	N/A	N/A	N/A
Update > Component delivery	N/A	N/A	N/A	N/A	N/A
Update > AU Source	Supported	N/A	N/A	N/A	N/A
Policy Management	Supported	N/A	N/A	N/A	N/A
Report	N/A	N/A	N/A	N/A	N/A

Suspicious Object collection	N/A	N/A	N/A	N/A	N/A
Suspicious Object sharing	N/A	N/A	N/A	Supported	N/A

Function	Server Protect for Windows/ NetWare	Server Protect for Linux	Deep Discovery Email Inspector	Trend Micro Deep Discovery Inspector	Deep Discovery Analyzer
	5.8	3.0	3.0	5.0	6.0
Dashboard	Supported	Supported	Supported	Supported	Supported
Directory > Product	Supported	Supported	Supported	Supported	N/A
Directory > Endpoint	N/A	N/A	N/A	N/A	N/A
Scan Now	N/A	N/A	N/A	N/A	N/A
Log Query	Supported	Supported	Supported	Supported	Supported
Single Sign On	N/A	Supported	Supported	Supported	Supported
License Management Expired date	Supported	Supported	Supported	N/A	N/A
License Management Renew AC	N/A	Supported	N/A	N/A	N/A
License Management Register new AC	N/A	Supported	N/A	N/A	N/A
Update > Component delivery	Supported	Supported	Supported	Supported	N/A
Update > AU Source	Supported	Supported	Supported	Supported	Supported

Policy Management	N/A	N/A	N/A	Supported	N/A
Report	Supported	Supported	Supported	Supported	N/A
Suspicious Object collection	N/A	N/A	Supported	Supported	Supported
Suspicious Object sharing	N/A	N/A	N/A	N/A	N/A

Function	Deep Discovery Director	InterScan Messaging Security Virtual Appliance	Trend Micro Hosted Email Security	InterScan Web Security Virtual Appliance	InterScan Web Security Suite Linux
	3.0	9.0 9.1		6.5	6.5
Dashboard	N/A	Supported	Supported	Supported	Supported
Directory > Product	N/A	Supported	N/A	Supported	Supported
Directory > Endpoint	N/A	Supported	N/A	Supported	Supported
Scan Now	N/A	Supported	N/A	Supported	Supported
Log Query	N/A	Supported	Supported	Supported	Supported
Single Sign On	N/A	N/A	Supported	Supported	Supported
License Management Expired date	N/A	Supported	Supported	Supported	Supported
License Management Renew AC	N/A	N/A	N/A	Supported	Supported
License Management	N/A	N/A	N/A	Supported	Supported

Register new AC					
Update > Component delivery	N/A	Supported	N/A	Supported	Supported
Update > AU source	N/A	Supported	N/A	Supported	Supported
Policy Management	N/A	Supported	N/A	Supported	Supported
Report	N/A	Supported	Supported	Supported	Supported
Suspicious Object collection	Supported	N/A	N/A	N/A	N/A
Suspicious Object sharing	N/A	N/A	N/A	Supported	N/A

Function	Trend Micro Cloud App Security	InterScan for Microsoft Exchange	InterScan for IBM Domino	Portal Protect	Server Protect for EMC
	6.0	12.5	5.6	2.5	5.8
Dashboard	Supported	Supported	Supported	Supported	Supported
Directory > Product	N/A	Supported	Supported	Supported	Supported
Directory > Endpoint	N/A	Supported	Supported	Supported	N/A
Scan Now	N/A	N/A	N/A	N/A	N/A
Log Query	Supported	Supported	Supported	Supported	Supported
Single Sign On	Supported	Supported	N/A	Supported	Supported
License Management	Supported	Supported	Supported	Supported	Supported

Expired date					
License Management Renew AC	N/A	Supported	Supported	Supported	N/A
License Management Register new AC	N/A	Supported	Supported	Supported	N/A
Update > Component delivery	N/A	Supported	Supported	Supported	Supported
Update > AU Source	N/A	Supported	Supported	Supported	Supported
Policy Management	N/A	Supported	N/A	N/A	N/A
Report	Supported	Supported	Supported	Supported	Supported
Suspicious Object collection	N/A	N/A	N/A	N/A	N/A
Suspicious Object sharing	Supported	N/A	N/A	N/A	N/A

Function	Server Protect for NetApp	ServerProtect for Storage	Trend Micro Mobile Security	Network VirusWall Enforcer
	5.8	6.0	9.6 9.7	3.5
Dashboard	Supported	Supported	Supported	Supported
Directory > Product	Supported	Supported	N/A	Supported
Directory > Endpoint	N/A	N/A	Supported	N/A
Scan Now	N/A	N/A	N/A	N/A
Log Query	Supported	Supported	Supported	Supported
Single Sign On	Supported	Supported	N/A	Supported
License Management Expired date	Supported	Supported	Supported	Supported
License Management Renew AC	N/A	N/A	Supported	Supported
License Management Register new AC	N/A	N/A	Supported	Supported
Update > Component delivery	Supported	Supported	Supported	Supported
Update > AU Source	Supported	Supported	Supported	Supported
Policy Management	N/A	N/A	Supported	N/A
Report	Supported	Supported	Supported	Supported
Suspicious Object collection	N/A	N/A	N/A	N/A
Suspicious Object sharing	N/A	N/A	N/A	N/A