Control Manager (TMCM) 7.0 Best Practice Guide

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

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 (TMCM).

This document is also designed to be used in conjunction with the following guides, both of which provide more details about TMCM 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.

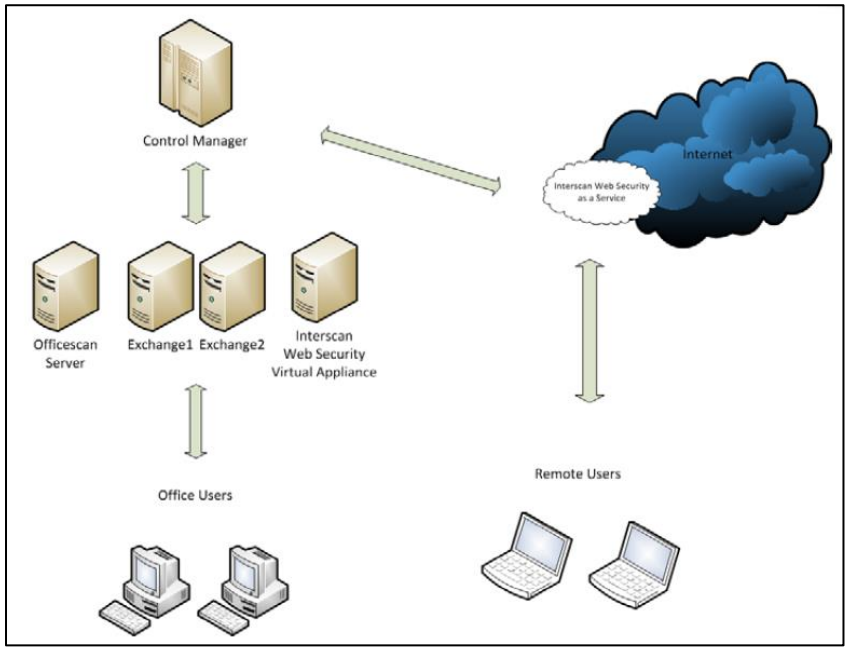
Planning the placement of Control Manager, in conjunction with a target site(s), is a key step.

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 TMCM server on multiple sites:

- The hardware features of the servers hosting TMCM and Microsoft™ SQL Server™ must be powerful enough.
- The firewall ports must be open to ensure connectivity between the TMCM server and agents on managed products. For details, see http://esupport.trendmicro.com/solution/en-US/1038211.aspx.
- TMCM 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 TMCM server has Internet connectivity.

This allows TMCM to download updates and use the License Extension feature. Hosting TMCM 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.

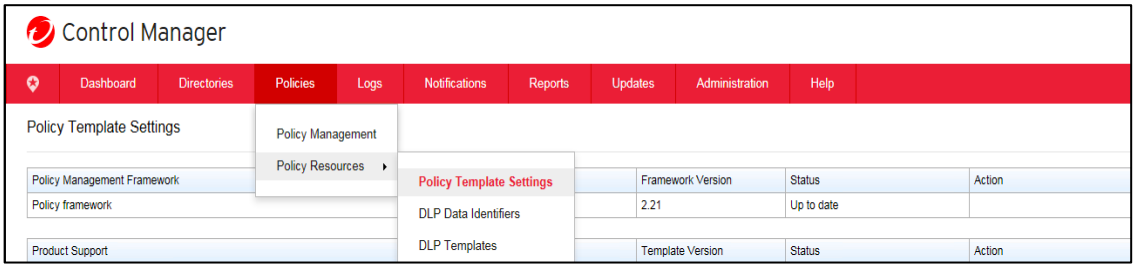
3.1. Planning Policy Management per Product

3.1.1. Get an overview of the settings available

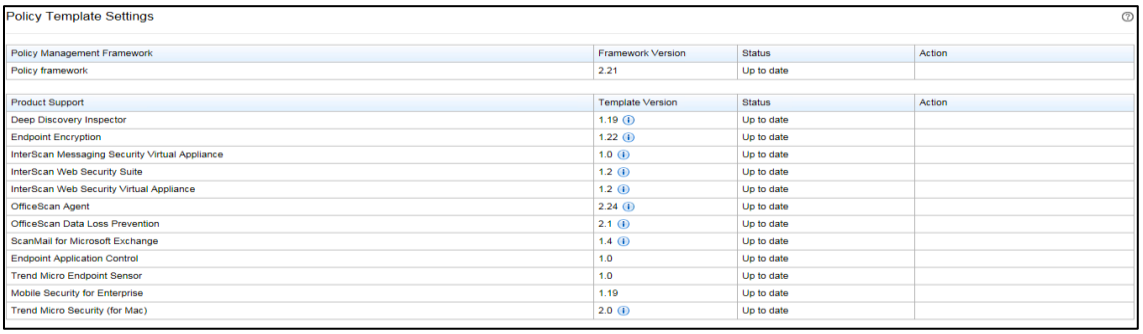
Which products support policy Management

The first important step in planning the Policy Management is to see the settings which can actually 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	Action
Policy framework	2.21	Up to date	

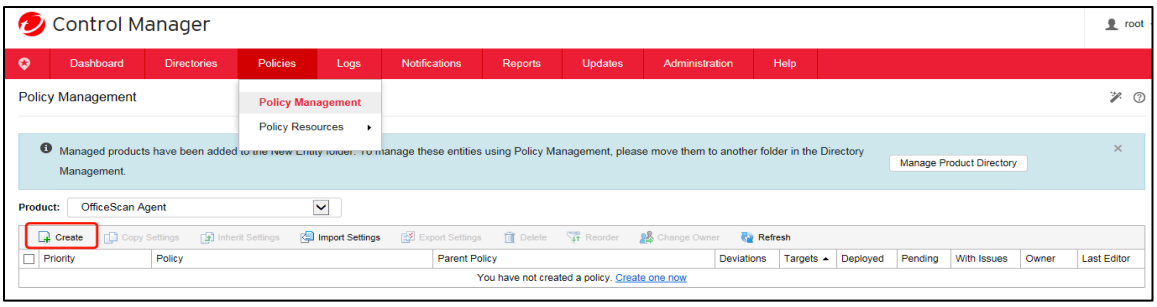
Product Support	Template Version	Status	Action
Deep Discovery Inspector	1.19	Up to date	
Endpoint Encryption	1.22	Up to date	
InterScan Messaging Security Virtual Appliance	1.0	Up to date	
InterScan Web Security Suite	1.2	Up to date	
InterScan Web Security Virtual Appliance	1.2	Up to date	
OfficeScan Agent	2.24	Up to date	
OfficeScan Data Loss Prevention	2.1	Up to date	
ScanMail for Microsoft Exchange	1.4	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	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.

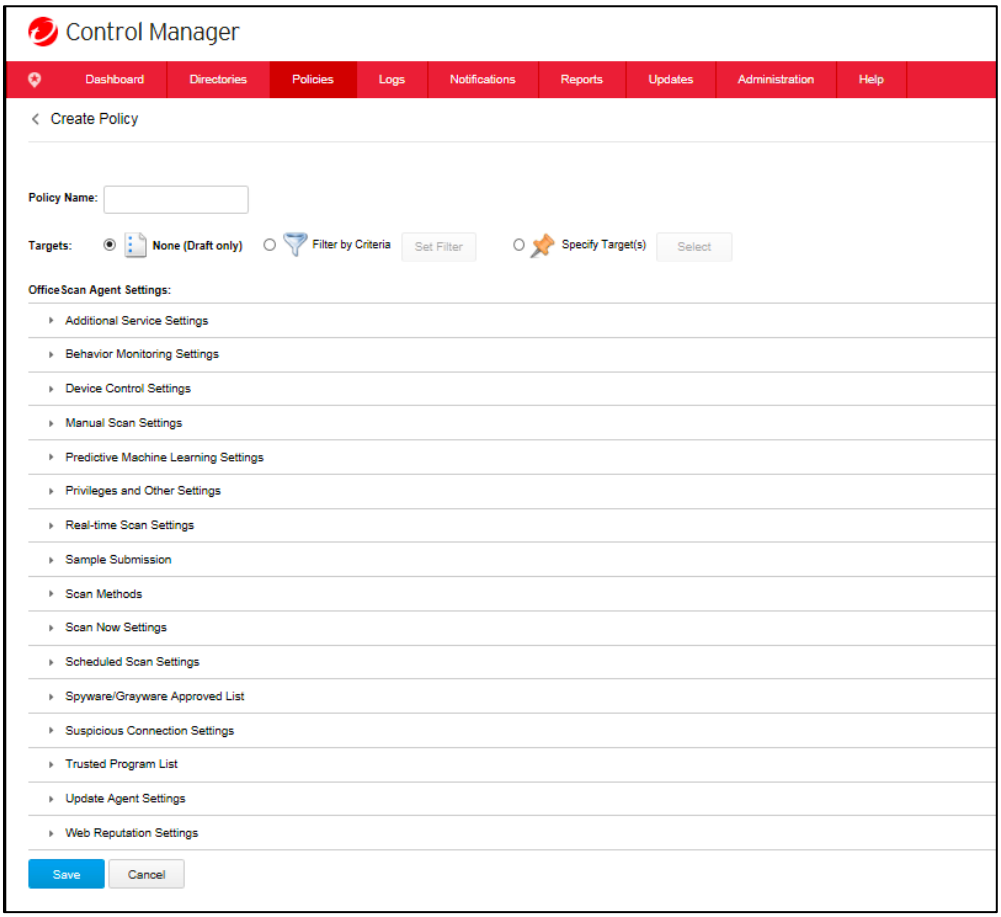
Which settings are available

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.



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:

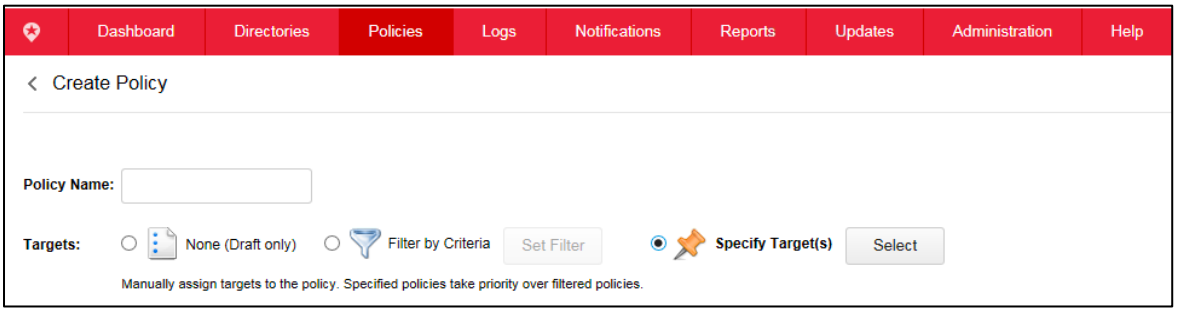
1. A Specified Policy takes precedence over a Filtered Policy.
2. A Specified Policy does not have a Priority number and only shows "Locked". When an entity is assigned a Specified Policy, it is locked to that machine.

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.

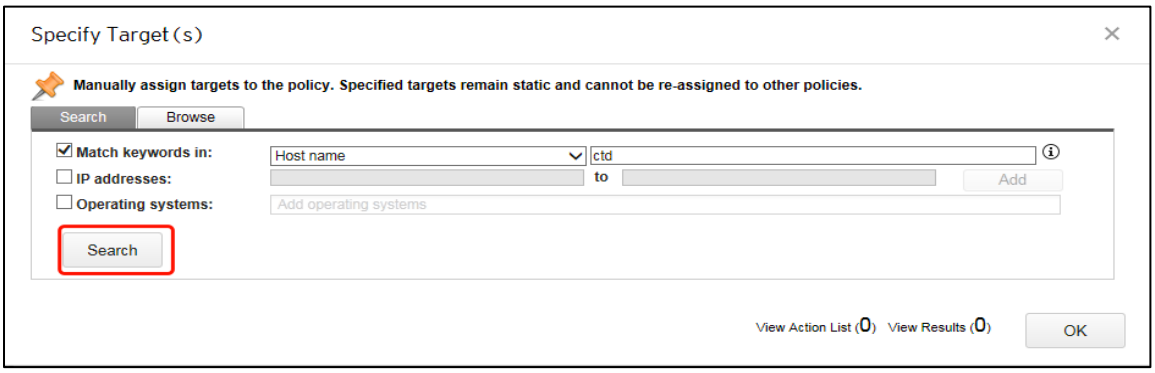
Specified Policies are policies where the "Targets" are specified. This indicates that the machines are already present in the environment.

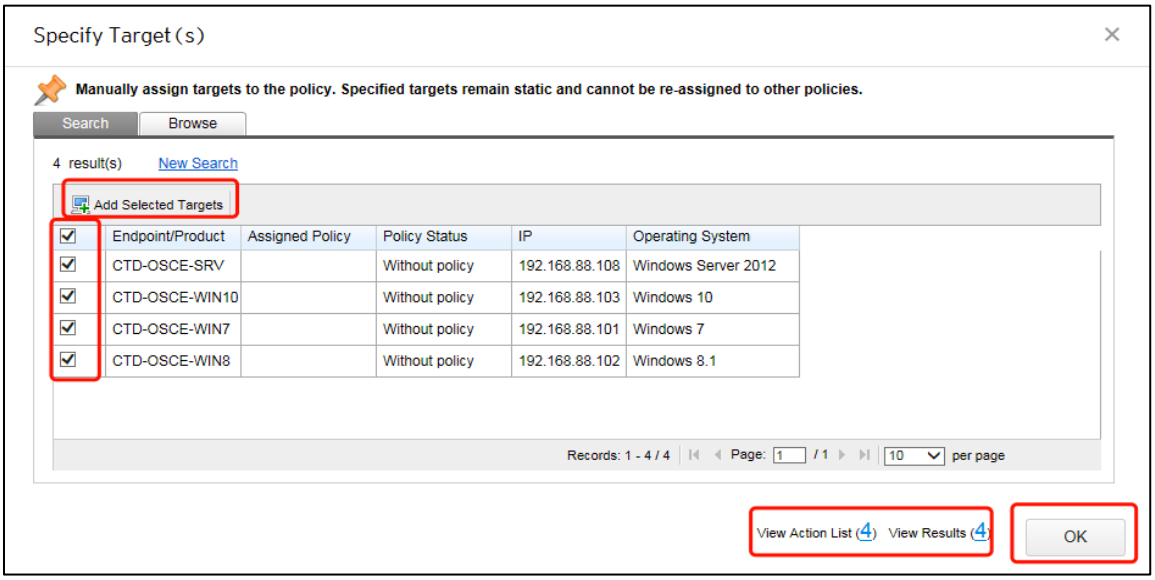


Unlike the Filtered Policy, a Specified policy targets allows users to search for the endpoints or Entities where the policy is to be applied. As indicated, the entity must already be in the Control Manager server to be able to use a Specified Policy on it. By finding the entity or endpoint, administrators 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.

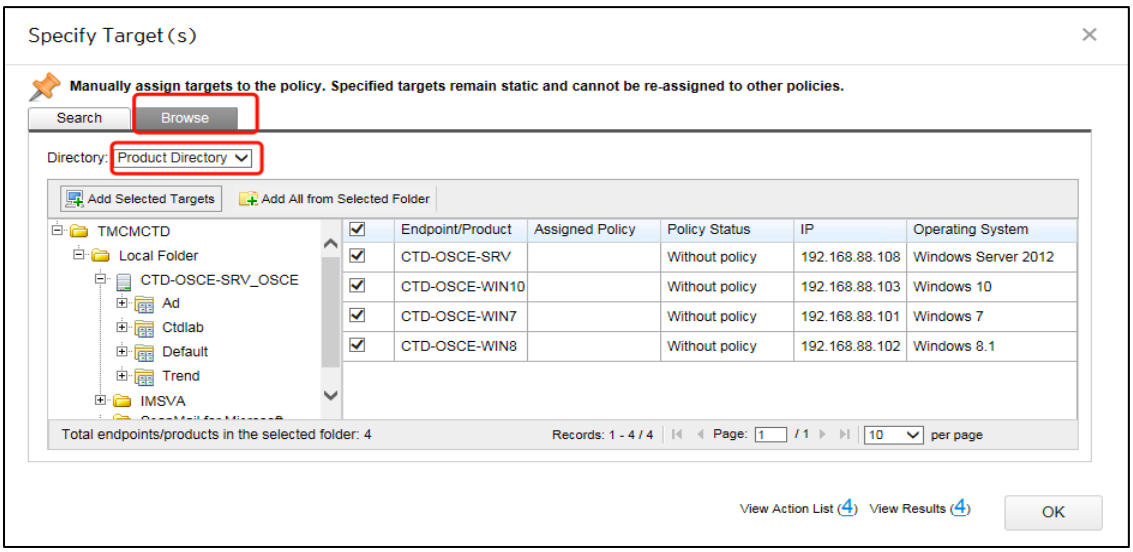
An example of which is running a search for "Host name" TMCM.

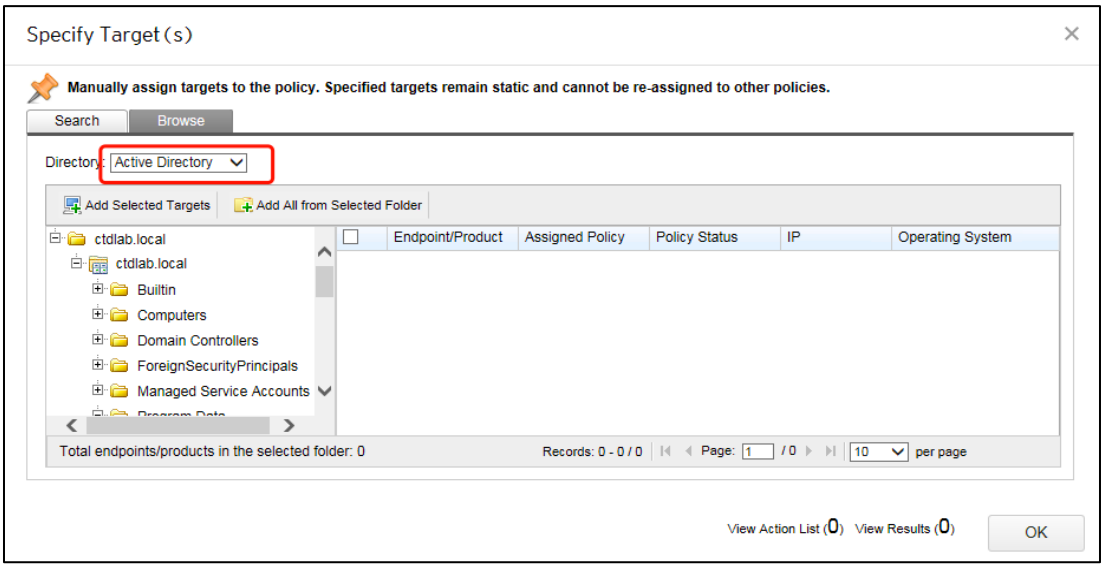




Only by selecting the entity and clicking Add Selected Targets will the policy take effect on the endpoint.

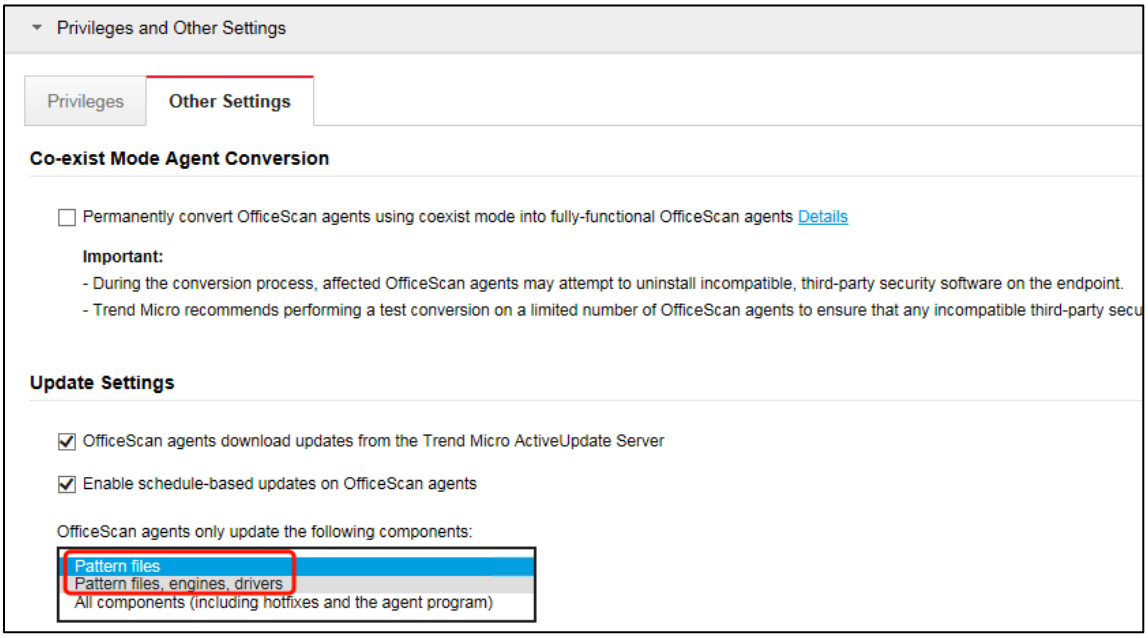
However, the main difference is the section for Product Directory and Active Directory. It is in a separate tab called "Browse". Using the browse tab, it is possible to specify directly the machines to apply, either from the Active Directory (if Active Directory integration is activated), or by browsing 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

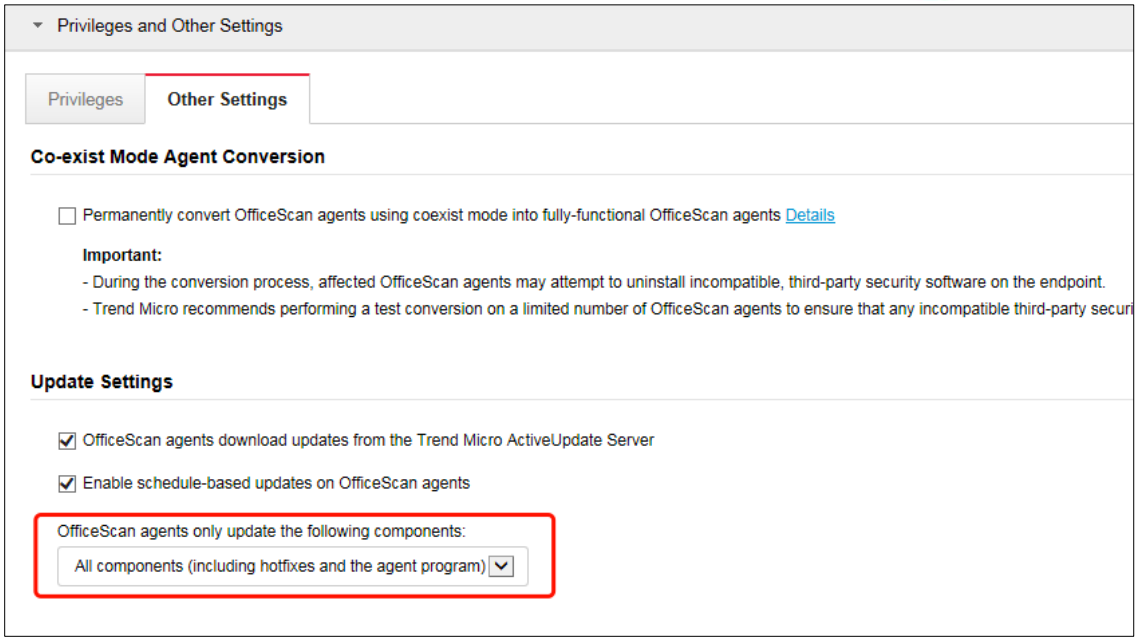
The Trendy-A company has already created two Filtered Policies, one for users in the United States, and one for users in Germany. Every new computer that they add immediately receives the policy that disables deployment of OfficeScan hotfixes and program upgrades. This allows them to prevent a large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



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.



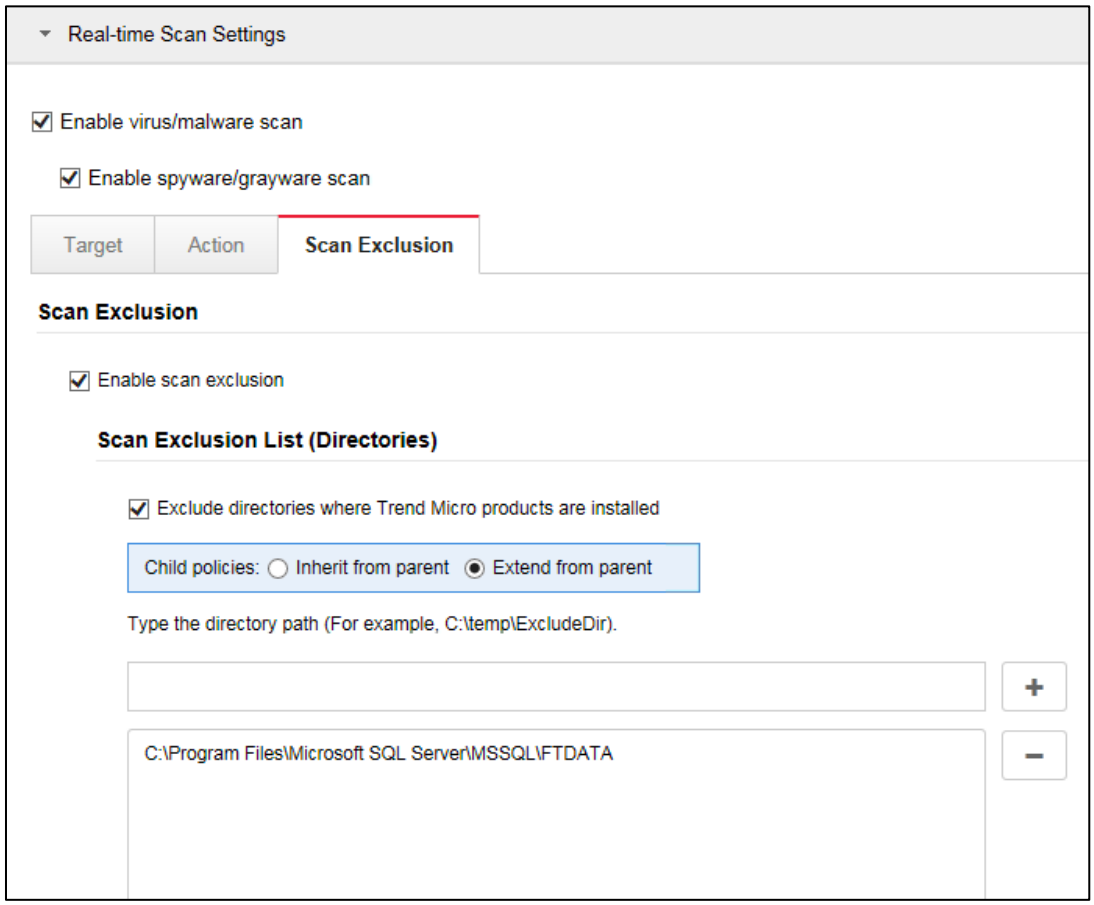
3. After making the changes, it is now possible to set the Target to "Specify Targets" and manually assign the OfficeScan clients chosen to be upgraded.
4. Please take note of the following:
    - If the previous policy was a Specified Policy, then the clients will be removed from the previous Specified 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.

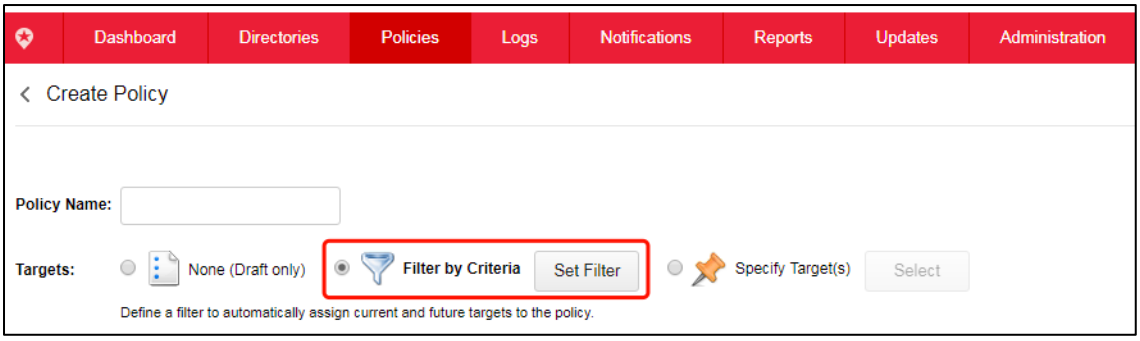
1. Create a copy of the policy you want to modify and set the Target first to **None (Draft only)**. This allow administrators to plan properly the policy, but make sure that it does not apply first.
2. In the Scan Exclusion, the SQL Server paths for exclusion can be added.



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.

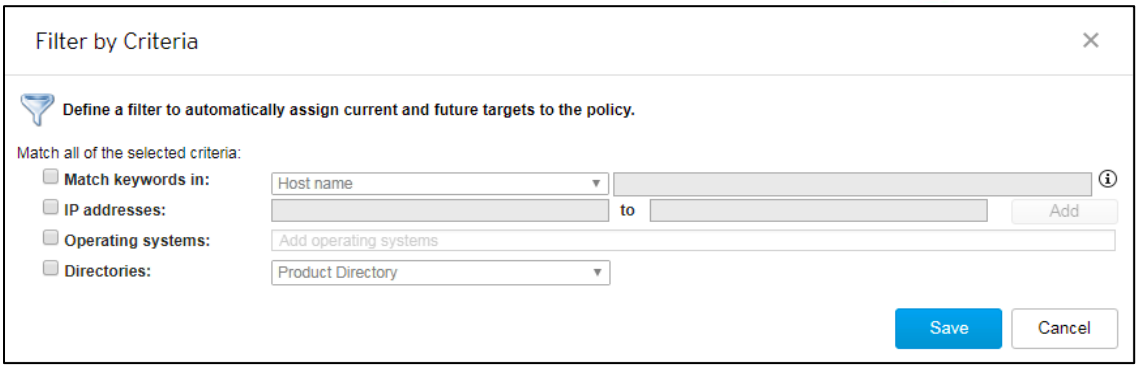
Filtered Policies are ideal for the following scenarios:

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.

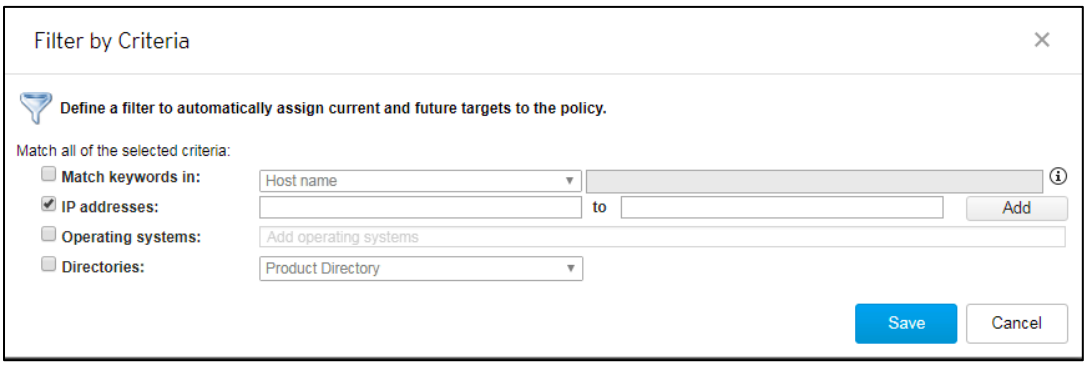


Important to note are as follows:

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

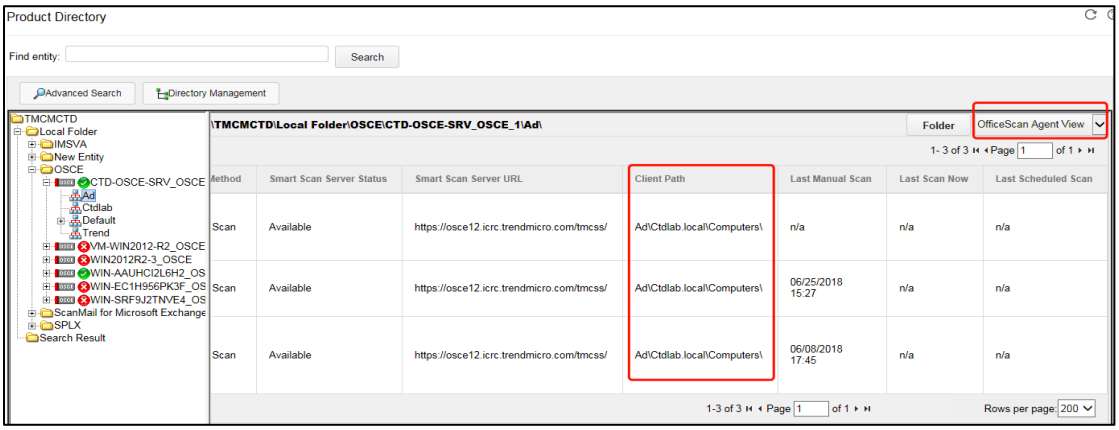
Solution: In this case, the administrators can use the IP addresses criteria to set the criteria to make sure that the Filtered policy applies to the IP address range.

Example 2: Using OfficeScan Multi-layer domain

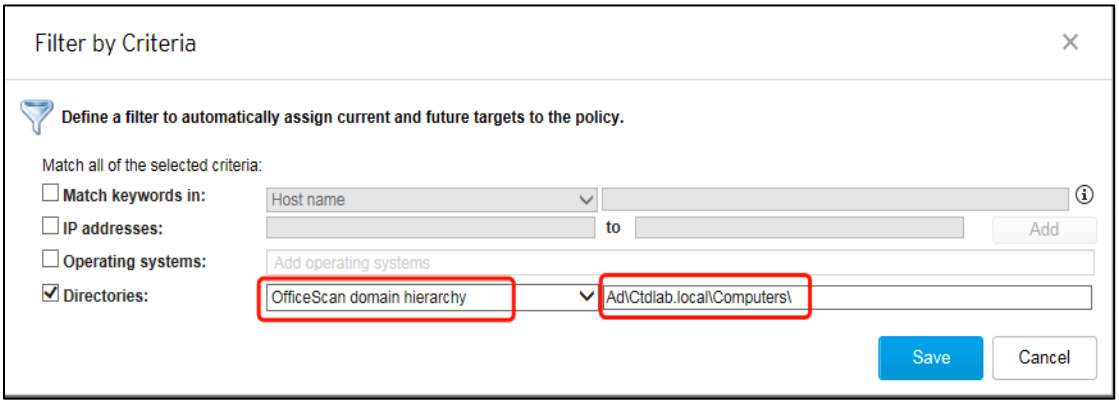
Scenario: The Trendy-B company wants uses OfficeScan Client Grouping to reorder the OfficeScan clients into the multiple layer Domains. The company decided that Control Manager must automatically create a configuration for all sub domains and also change them using the policy.

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.



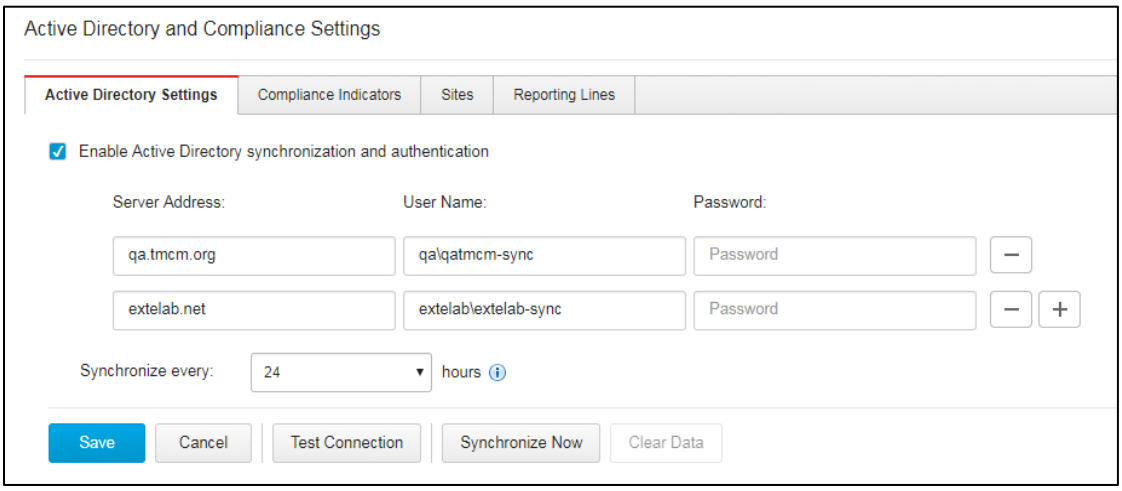
As you can see, the format is actually: layer1\layer2\layer3. As such, it is possible to set the criteria to be "layer1\layer2\layer3" or specify only "layer2\layer3". Note that wildcards are not supported.

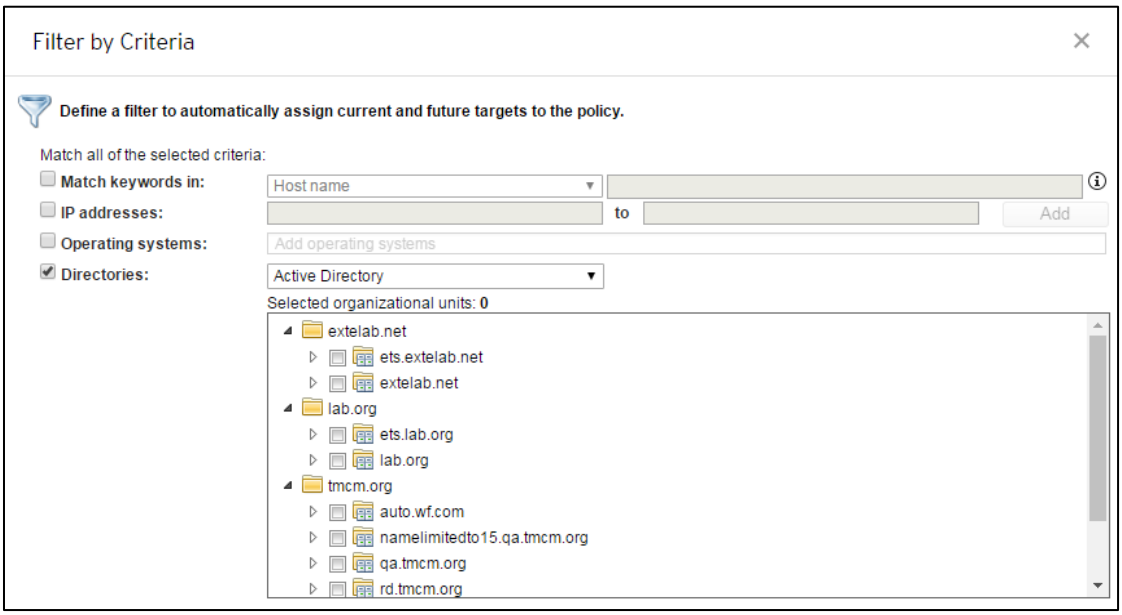


New OfficeScan clients added to this domain will automatically take the policy.

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.





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.

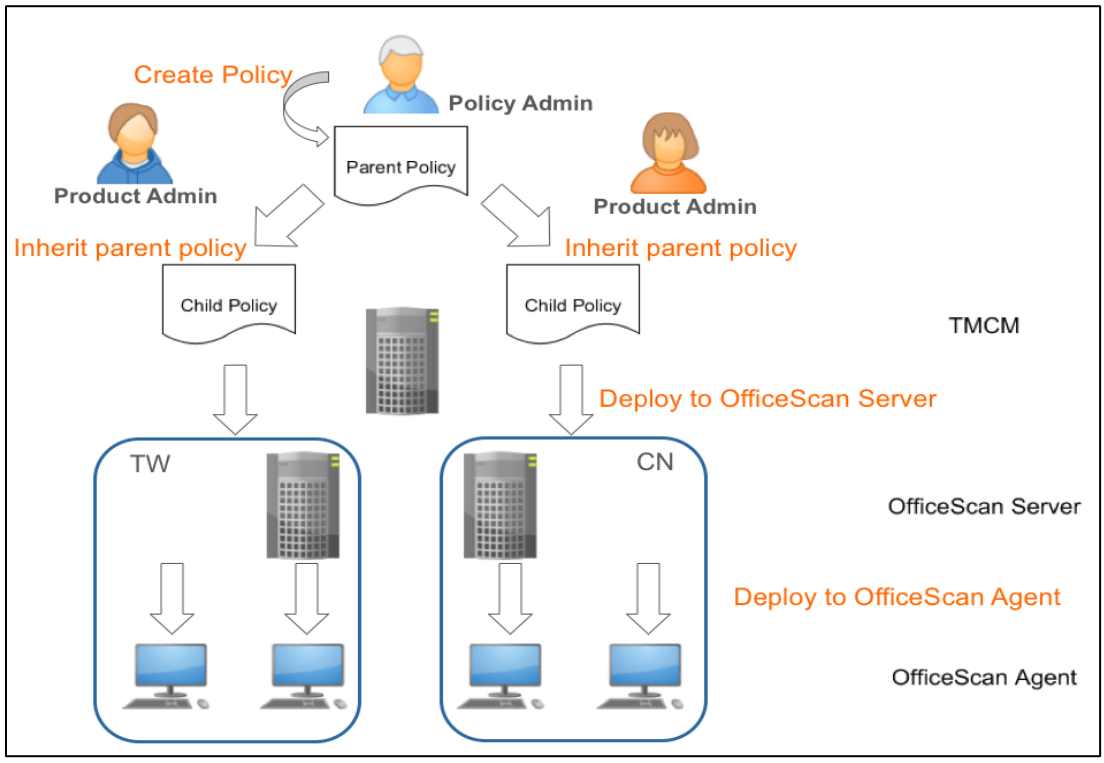
Another thing to note is that any specific policies we create are copies of the Filtered policies. This allows administrators to copy the original settings from old policies, and make minor deviations.

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.

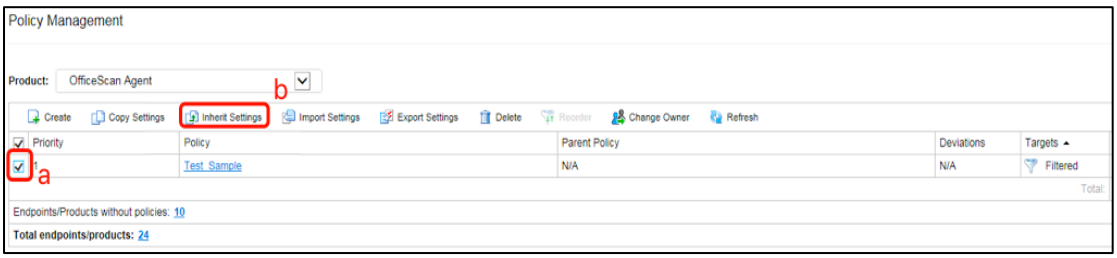
Our customer can benefit from the Policy inheritance feature.

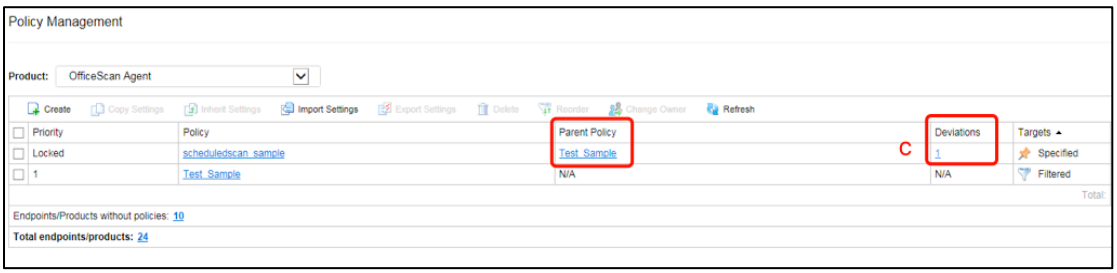
This flow chart shows how policy inheritance works:

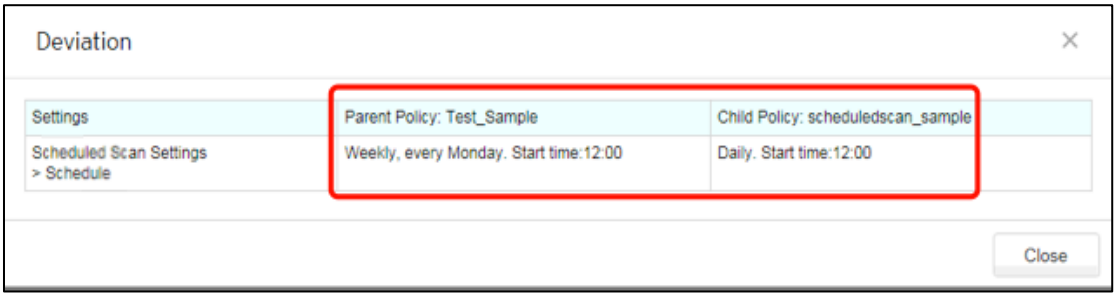


Note: The Policy Inheritance is applicable to OfficeScan only.

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.



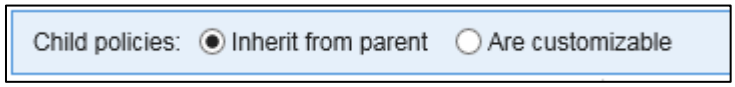




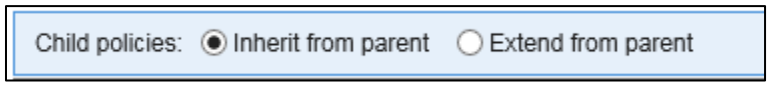
If the policy admin wants to change any of the settings for all OfficeScan agents, he can just edit the parent policy. The changes will affect all its child policies and be deployed to all the target agents.

There are three inheritance types:

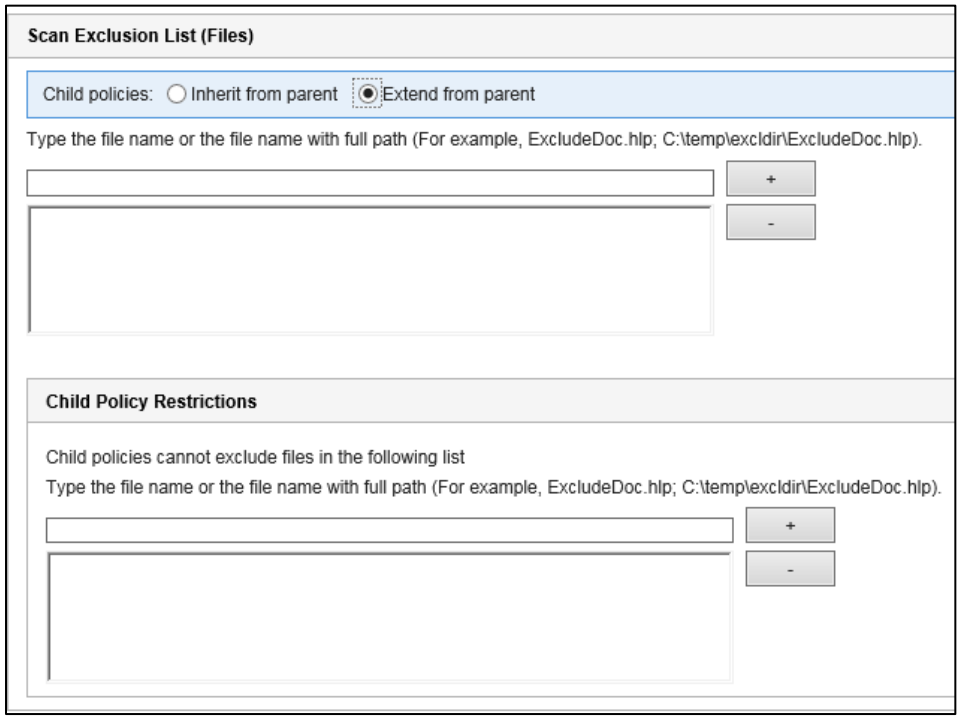
- Customizable



- Extend from parent



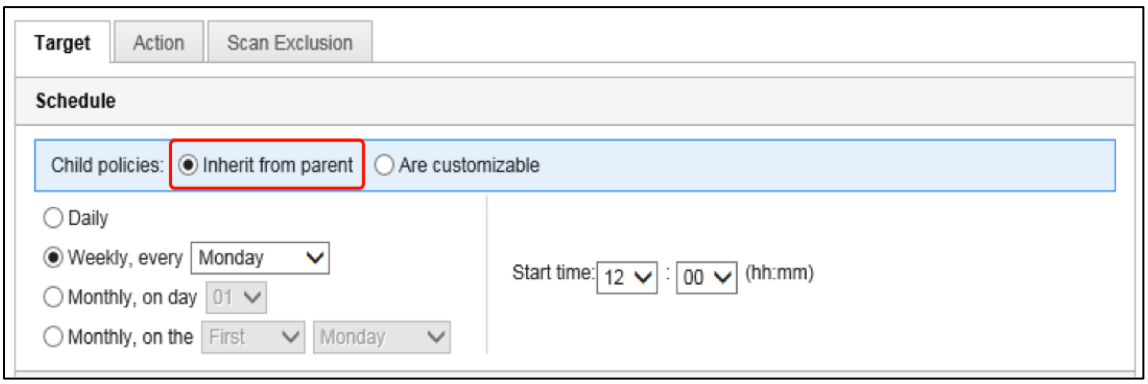
- Extend from parent + Neutralize List



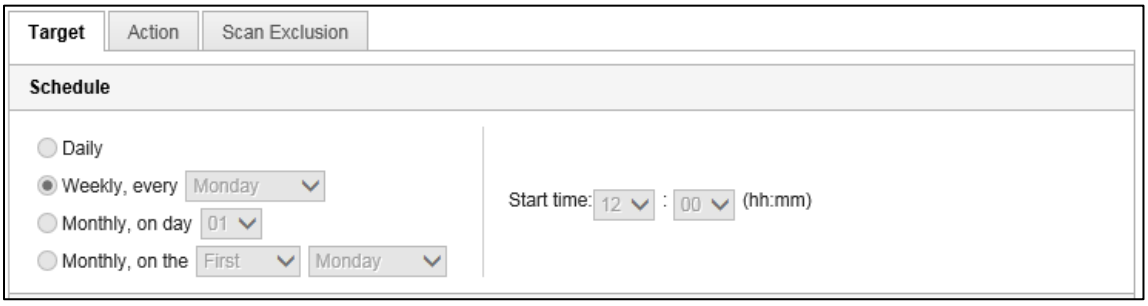
Below are things to note per policy type:

- 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

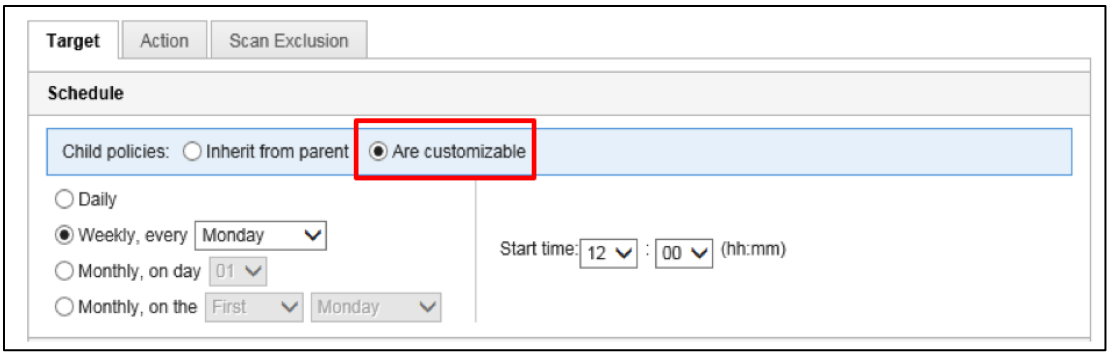


– Child Policy (options are grey, which means you cannot edit them)

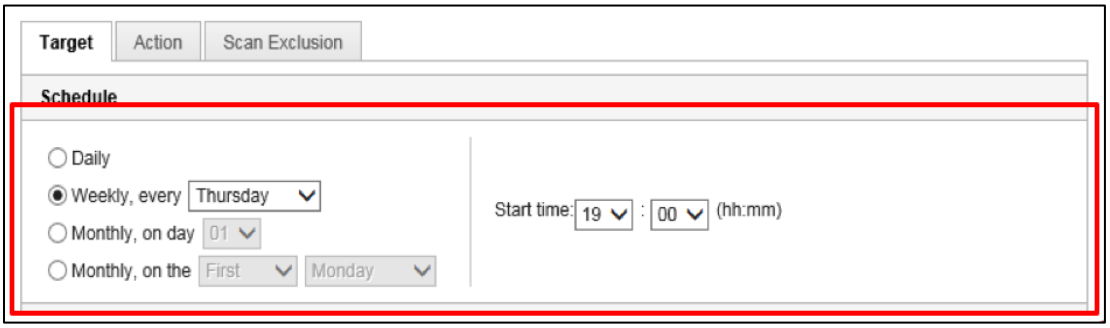


If the settings have been set to "Are customizable", the value of settings can be changed in child policy.

– Parent Policy

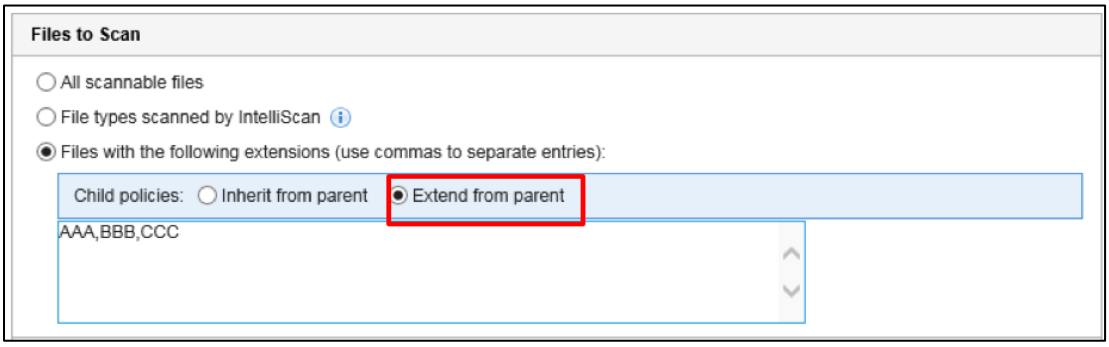


– Child Policy

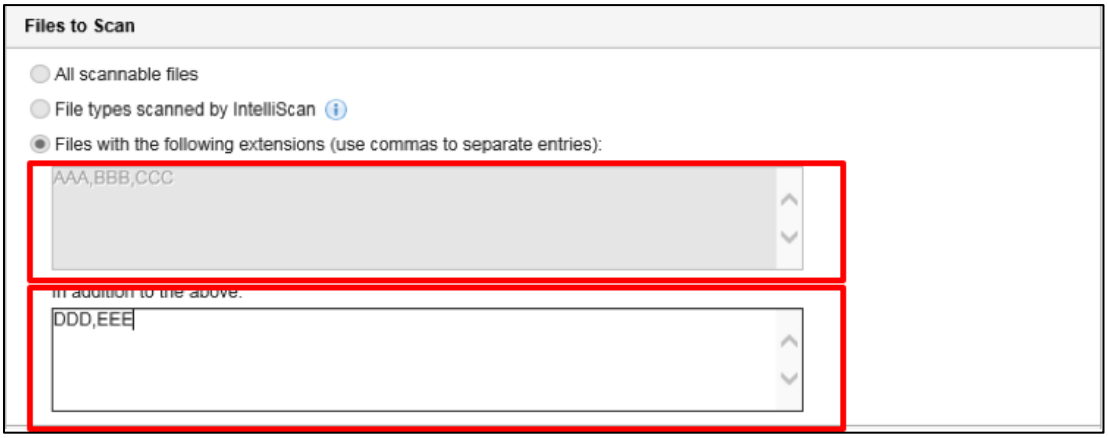


- For "Extend from policy" type:
  If you choose "Extend from parent", you can extend the configuration to the child policy

  – Parent policy



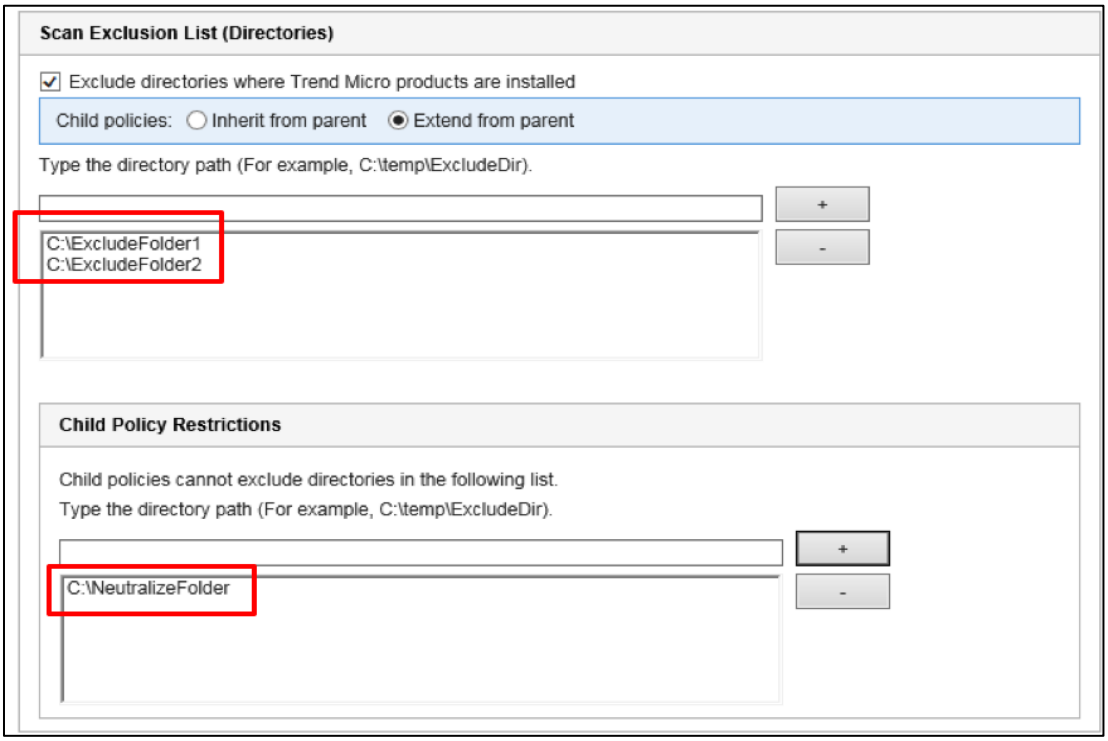
  – Child policy



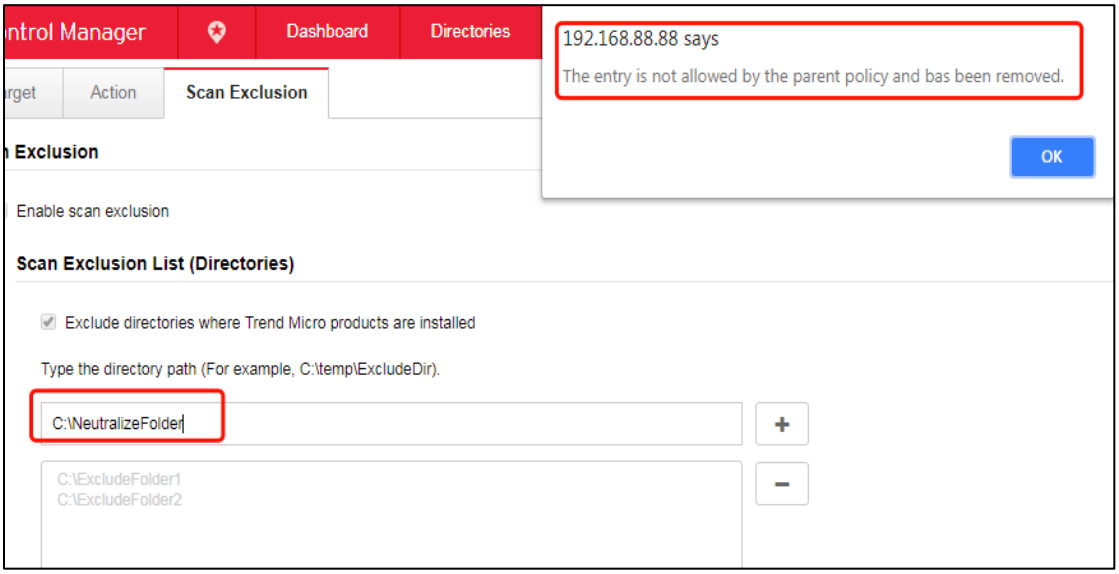
- For Extend from parent + Neutralize List type:
  "Extend from parent with neutralize list" settings can restrict the extend the settings of child policy.

  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



– Child policy



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

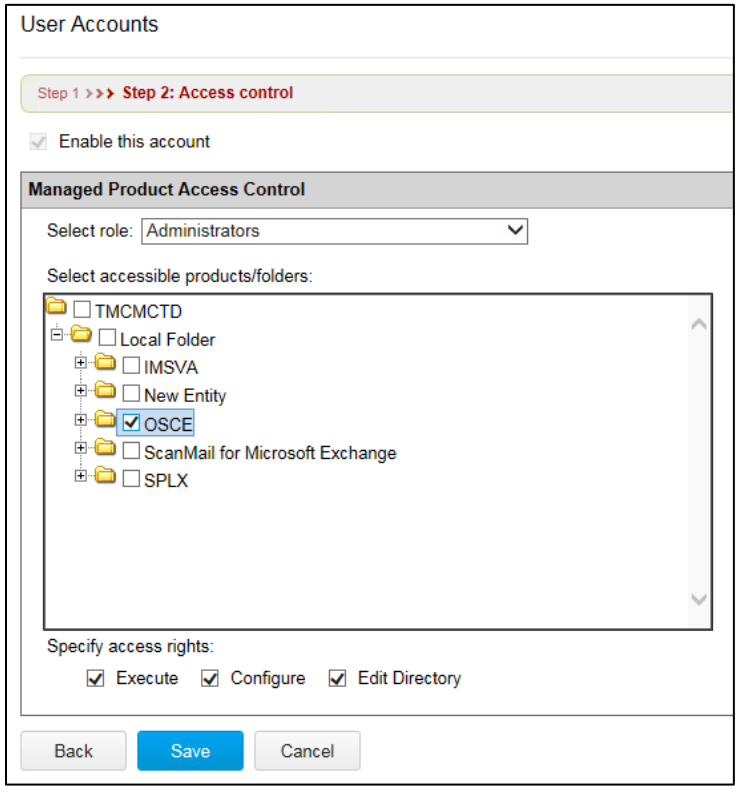
It is worth noting that the Policy can only cover endpoints where the Control Manager user has access. As such, it becomes important also to plan who will create the Policy.

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.

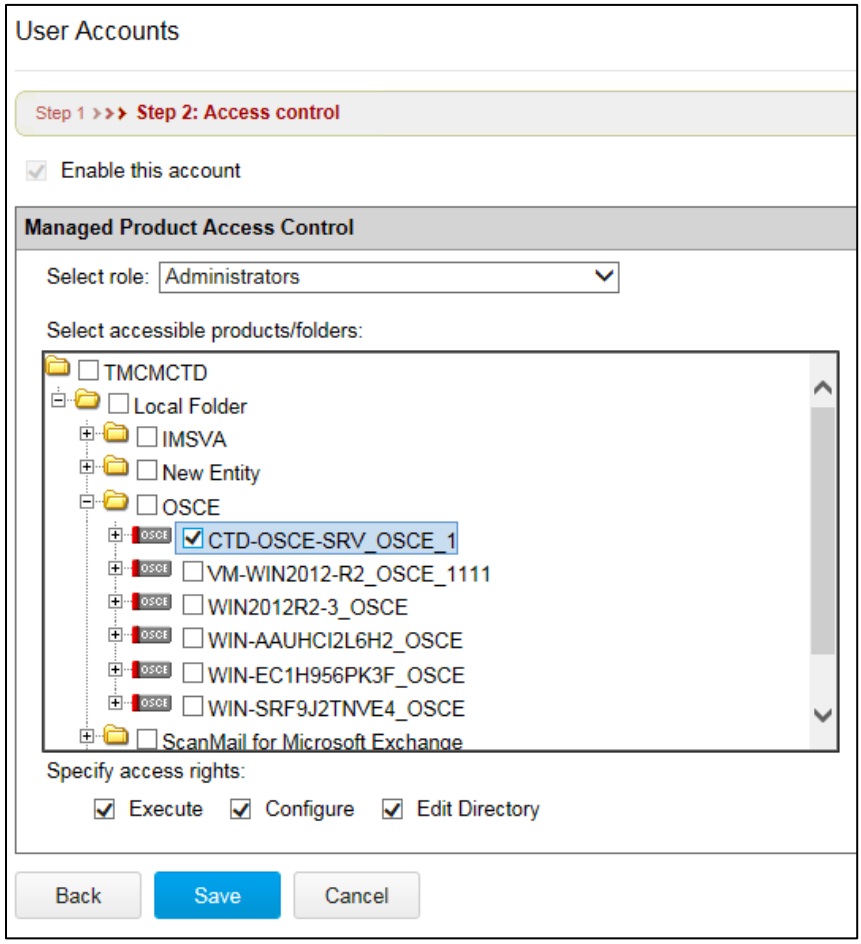
In the example shown below, the user "CTDLAB\TMCMADM" only has access to the entity under the "OSCE" folder. The user will not be able to apply any policy to entities or endpoints under the other folders.



Scenario 2: Security Coverage based on Products

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

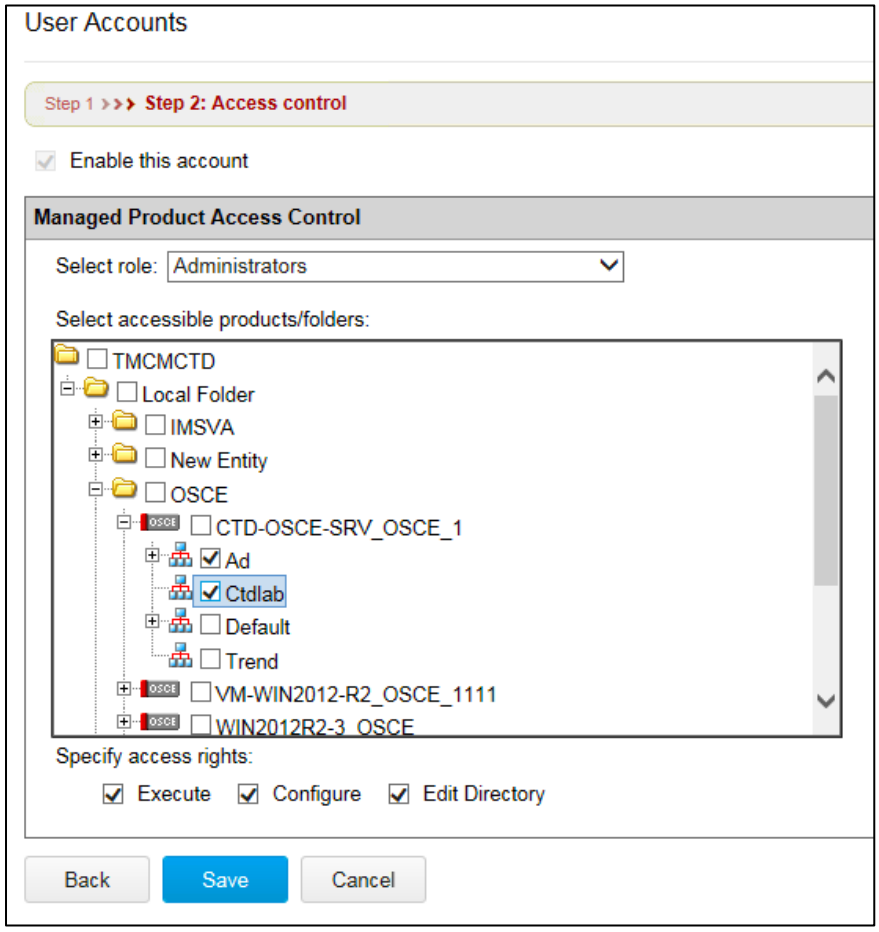
In the example below, it can be seen that the account has access to the CTD-OSCE-SRV_OSCE_1. Because of this, the account is only able to apply policies to the CTD-OSCE-SRV_OSCE_1.



Scenario 3: Security Coverage based on OfficeScan Subdomains

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

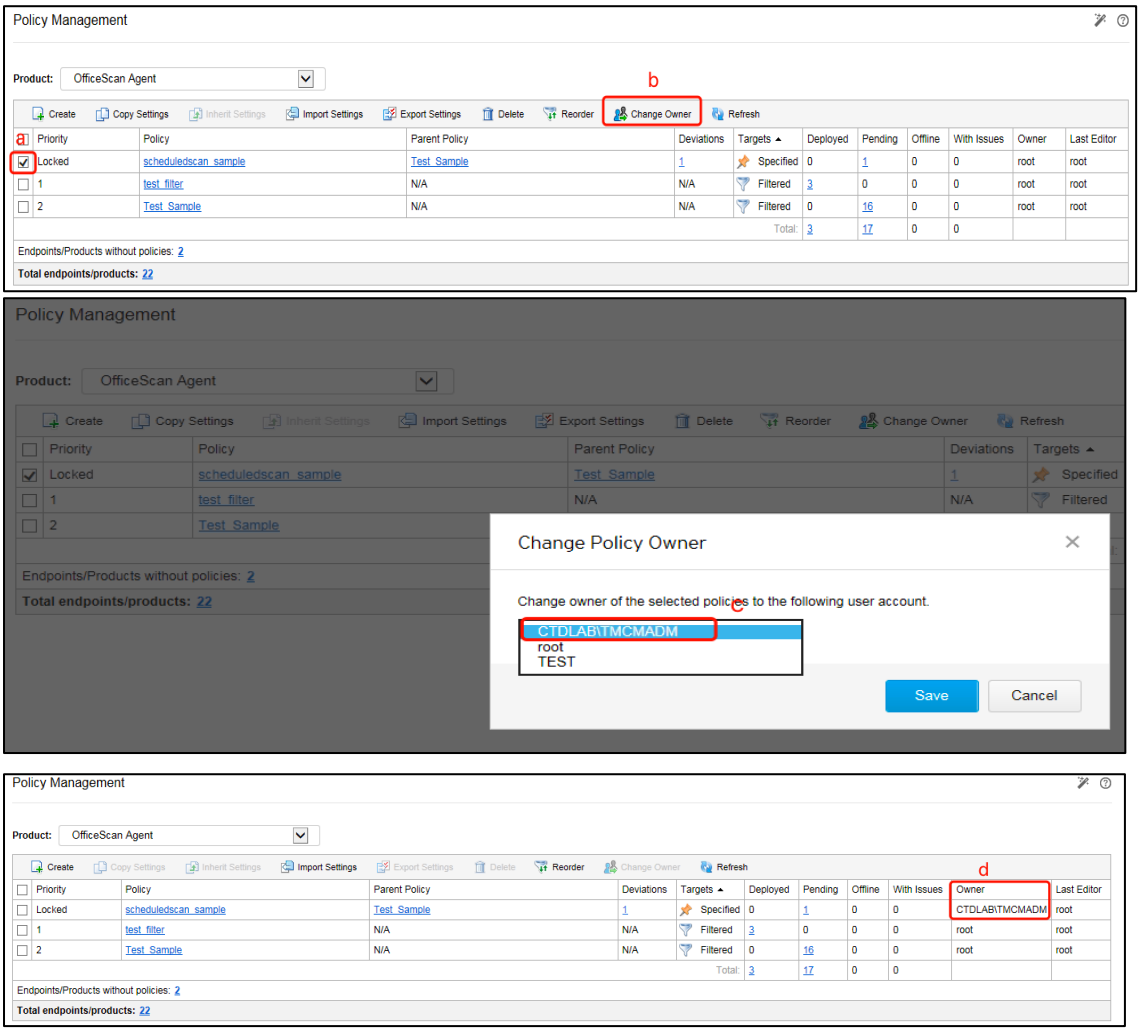
In the example below, the account has access to two domains – Ad and Ctdlab. In this kind of setup, the account is restricted from applying policies to other domains.



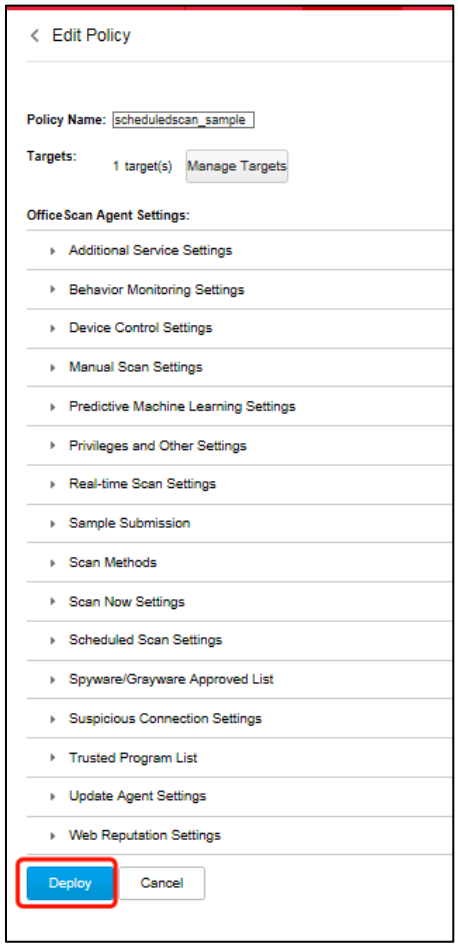
Scenario 4: Change the policy owner to another User Account or AD Group

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.

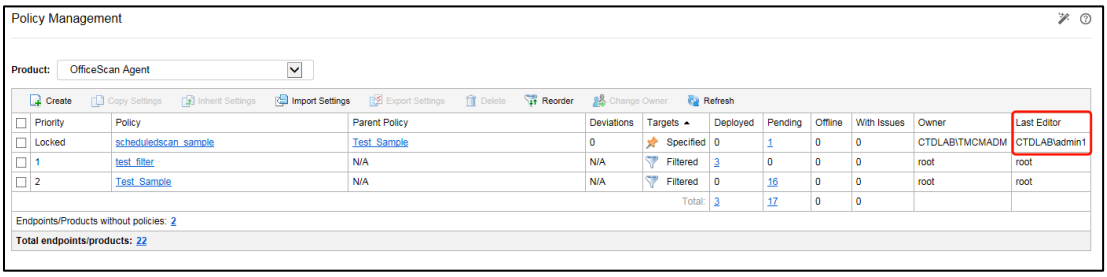
As an example, users may click the "Change Owner" to change the owner of policy "scheduledscan_sample" from "root" to "CTDLAB\TMCMADM".



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".



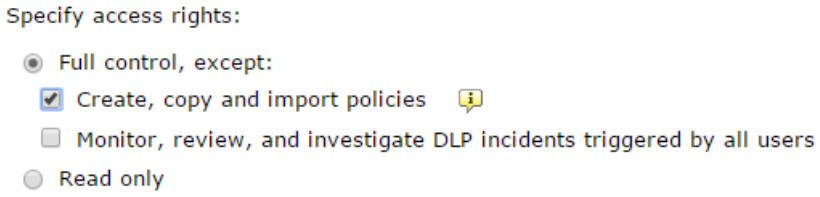
Once he modifies and deploys a policy, his account name will be recorded in the the Last Editor column.



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].



- 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.

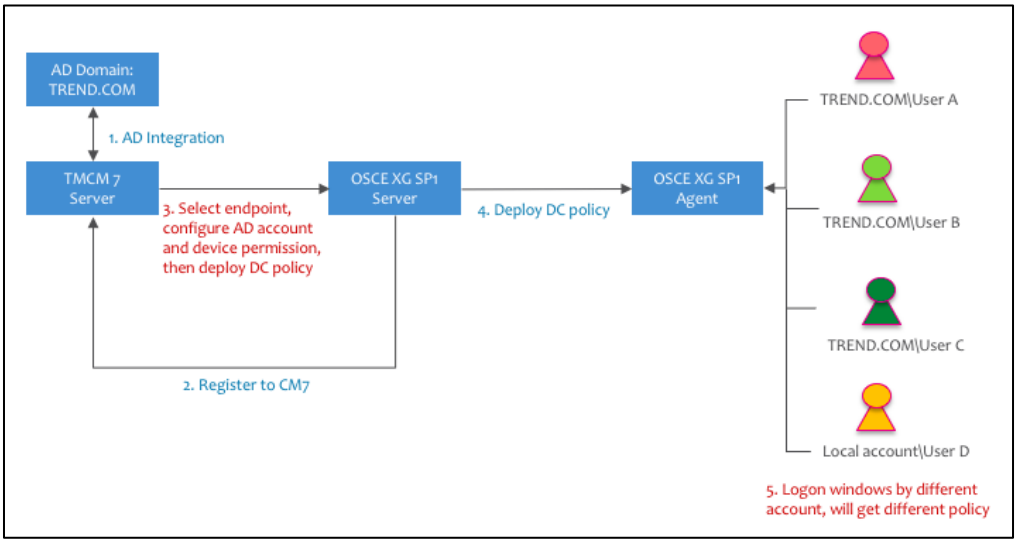
Scenario: The customer wants to apply different policies by individual AD account on the endpoint

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.

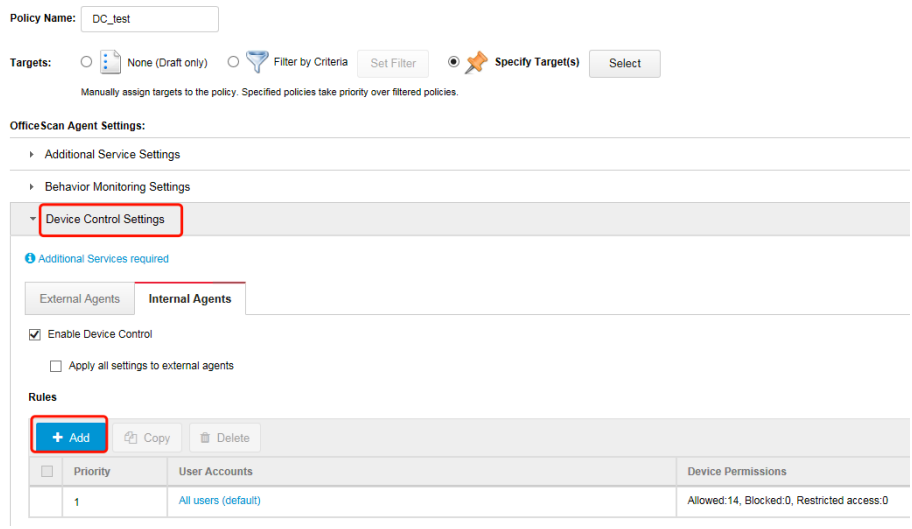


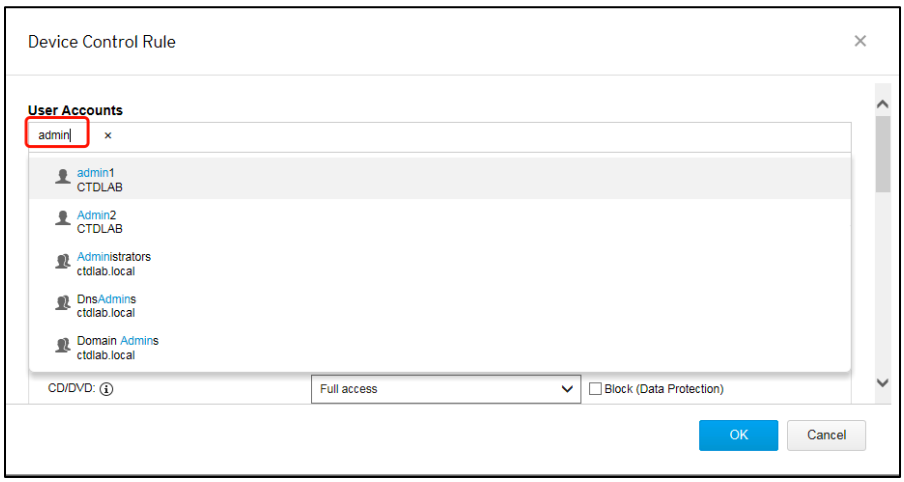
Policy deployment:

a. Select the target AD user

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

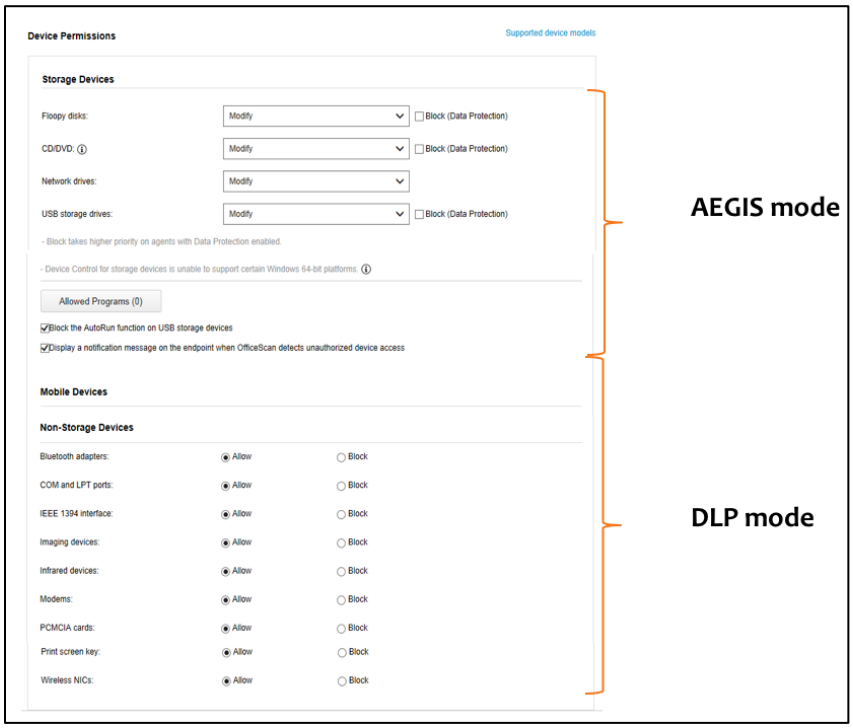
- Show the first 5 matching tokens in searching result list.
- The maximum token count is 30.





b. Configure the Device Control permission

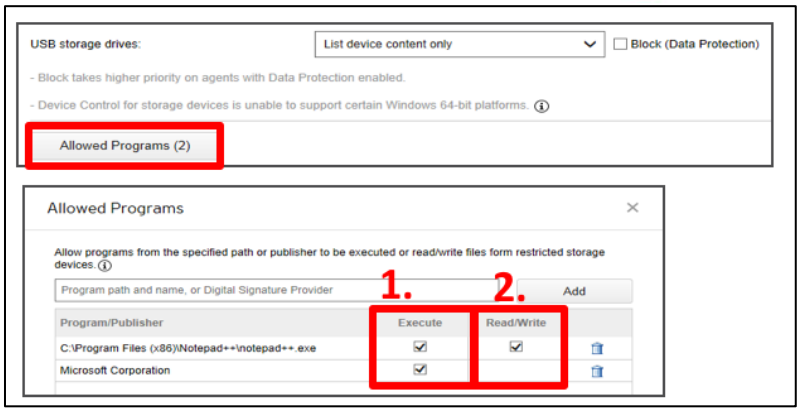
The admin can configure AEGIS and DLP Device Control permission in the same UI.



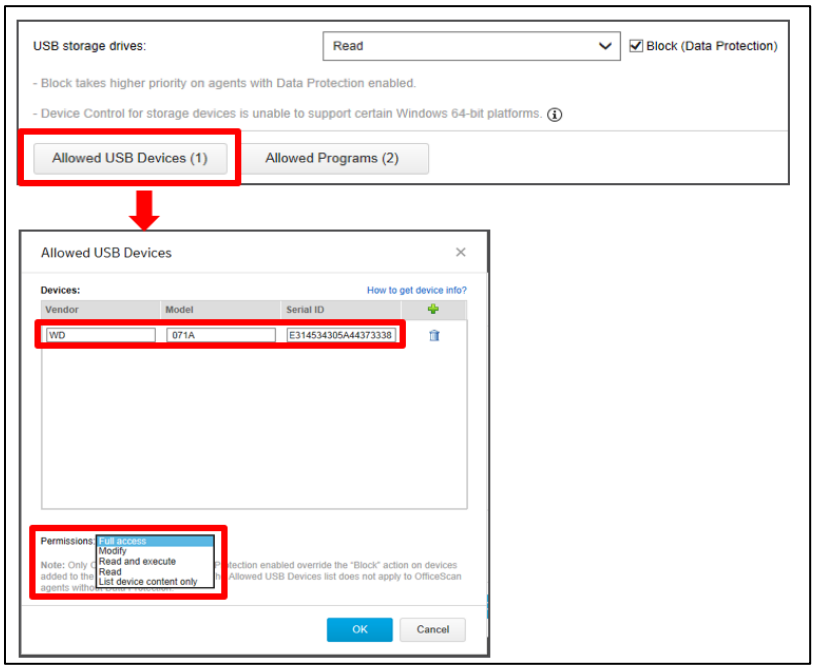
c. Configure the Device Control exception list

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.



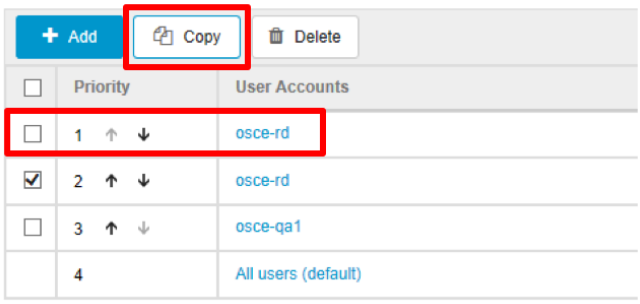
- Allowed USB Devices.
  If the admin set USB storage permission in Block, but they want to allow some specified USB drive to READ, you can add the Vendor, model and Serial ID into USB device list. The specified USB drive will be allowed to access.



d. Manage the Device Control policies

- Copy

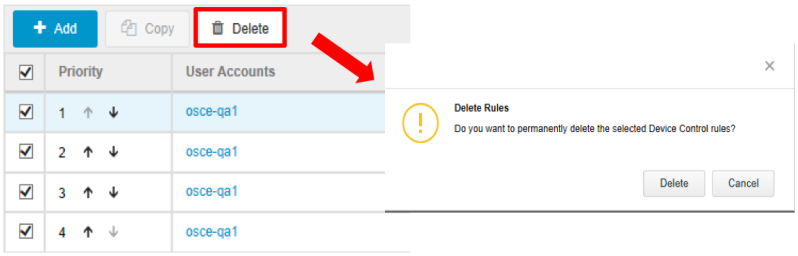
  The admin can copy any existing customized policy rules. However the default machine-based rule "All users" cannot be duplicated.



- Delete

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

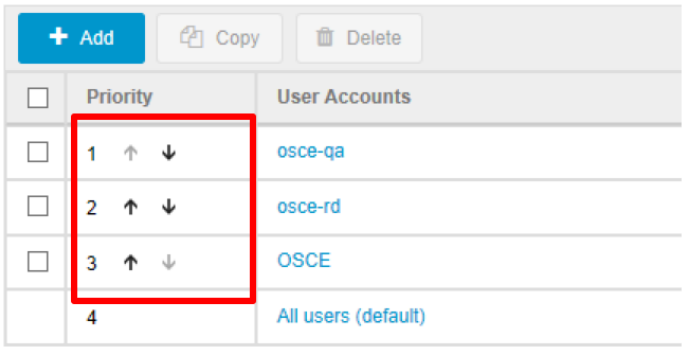
  The default machine-based rule "All users" cannot be deleted.



- Adjust priority

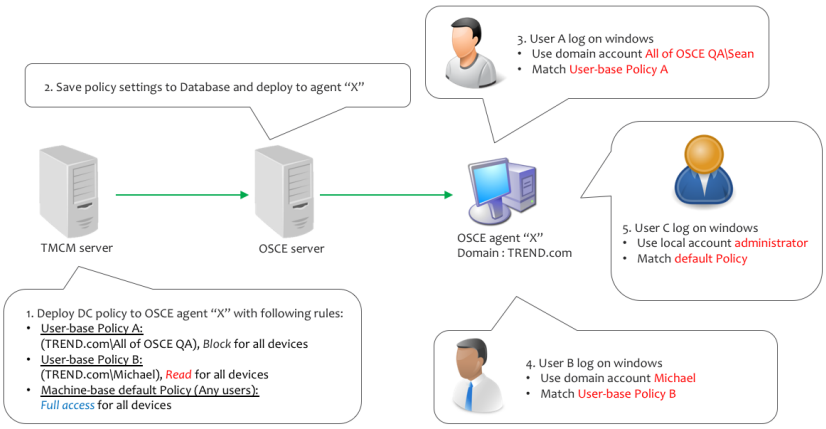
  The admin can adjust priority for customized policy rules. But we can NOT adjust the priority for machine-based rule "All users".

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



e. Policy matching:

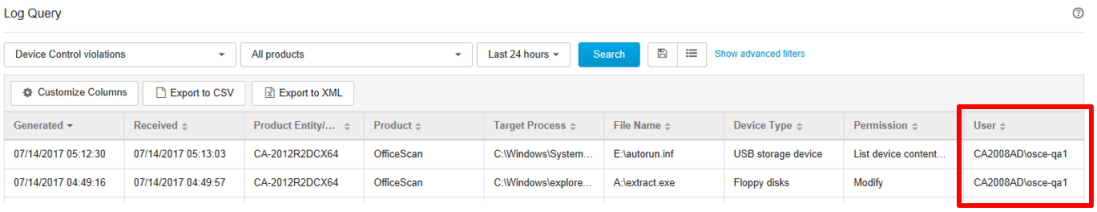
Here is an example workflow for policy matching.



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



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:

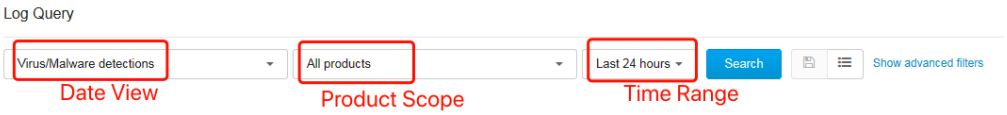
- Use advanced filters to narrow log query search results.
- Configure log aggregation settings to reduce network traffic when sending log data from managed products to the Control Manager server.
- Manually delete log entries by type or configure automatic log deletion.

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 TMCM 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 TMCM 7.0.

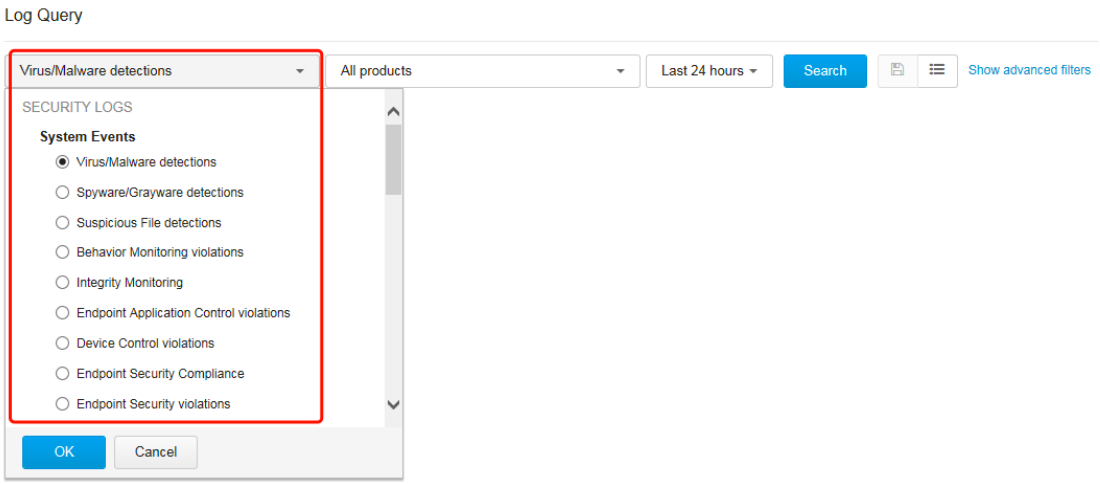
The new design in TMCM 7.0 for Log Query distinguishes itself from Reports to reduce the similar functions between different features. Thus users should query summary data results in Reports, and query raw logs in **Log Query**.



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.

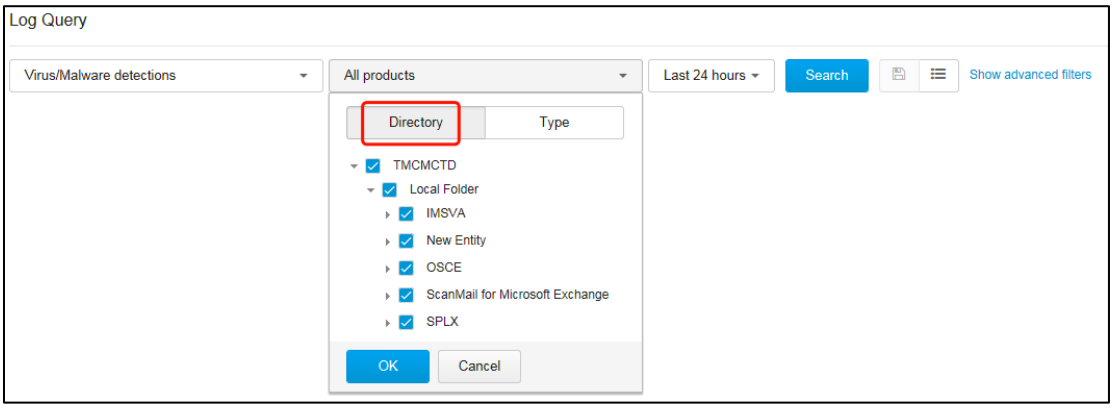
For example, the product scope will be disabled if you select Command Tracking in Data View, because command tracking belongs to TMCM only.

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

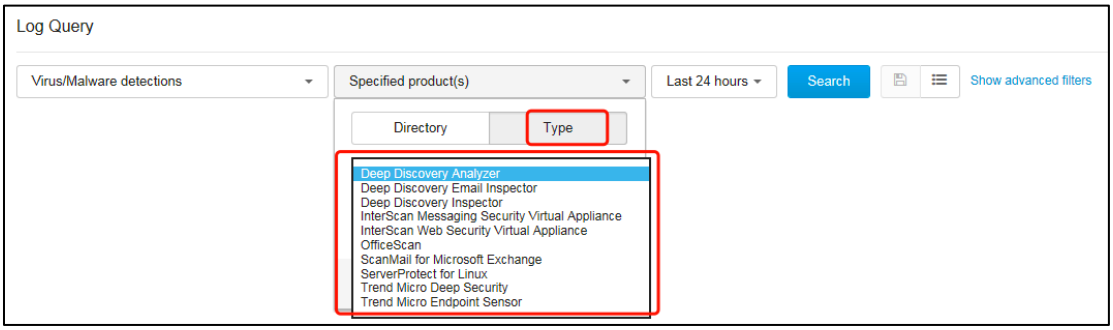
4.2.2. Basic Filters – Product Scope

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.

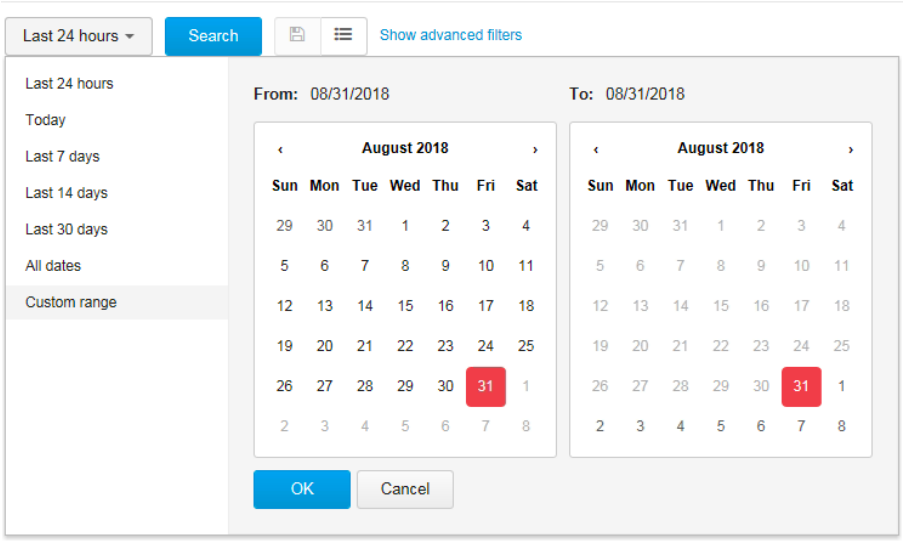


The product **Type** dropdown list only shows the products registered to TMCM.



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.



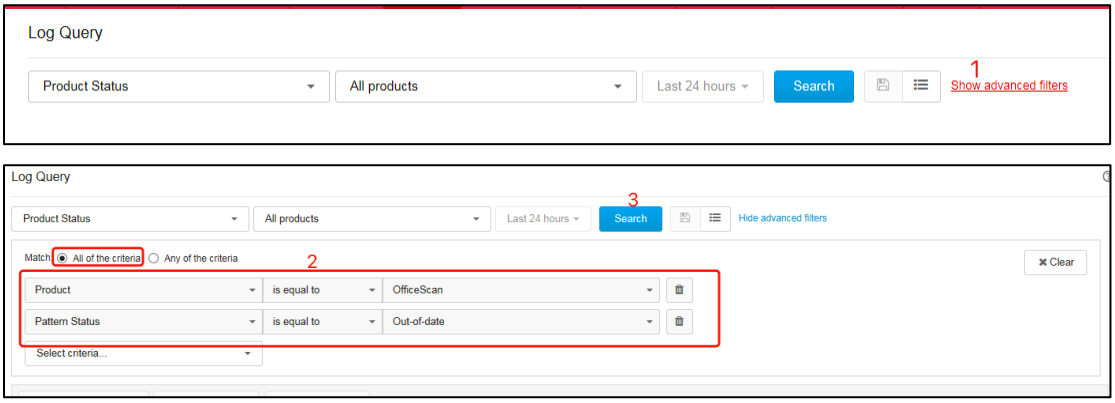
4.2.4. Advanced Filters

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**".

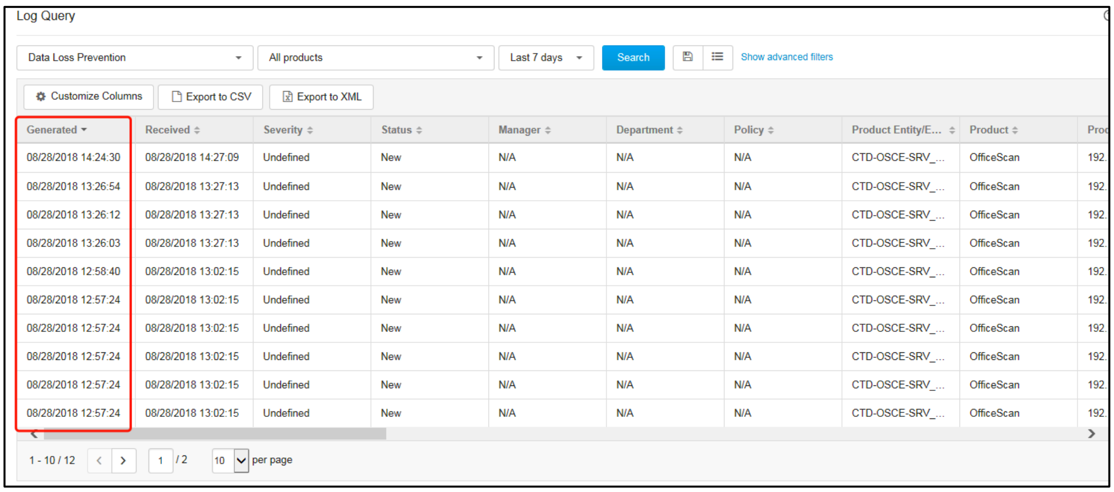
For example, you want to filter out how many OfficeScan Agents' pattern are out of date.



4.2.5. Query Results

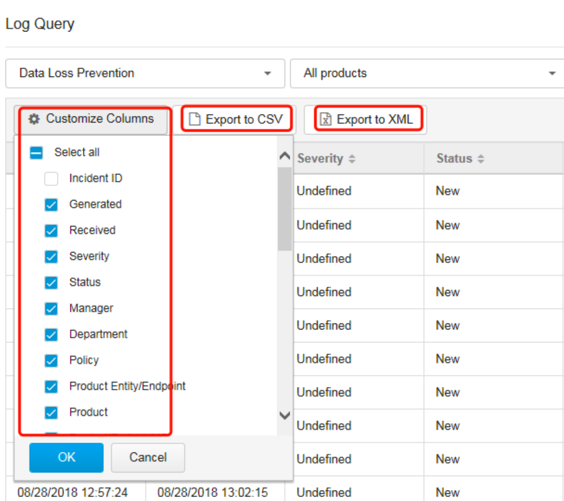
After configuring the advanced filters and clicking **Search**, the query result is shown as a table, with the results shown in the order of log generation time (Generated column) as the default sorting column, instead of the log received time (**Received**) as used in the older versions of TMCM.

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 TMCM server received the logs from the product side.



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.

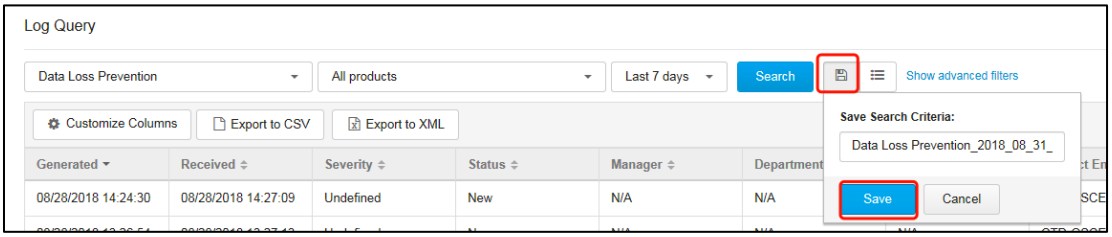


By default, the maximum number of entries which can be displayed in a query result is 10000, but this can be modified by editing the following key in the ..*Program Files\Trend Micro\Control Manager\SystemConfiguration.xml* file:

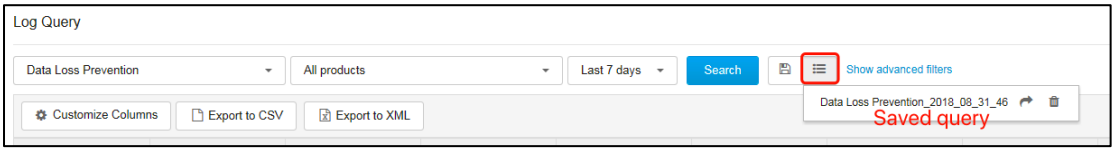
P Name="m_iAdhocQueryUIMaxResultSize" Value="

4.2.6. Save and Share the Query Results

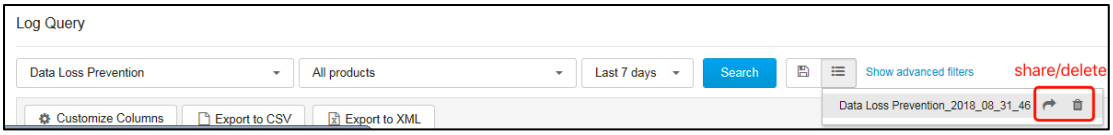
After performing a Query/Search, the Save Query button (floppy disk icon) becomes clickable. Users can click **Save** to save query.

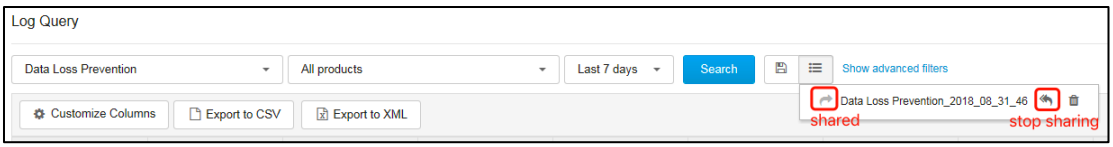


When at least one query has been saved, user can click the Saved queries button to view a list of saved queries.

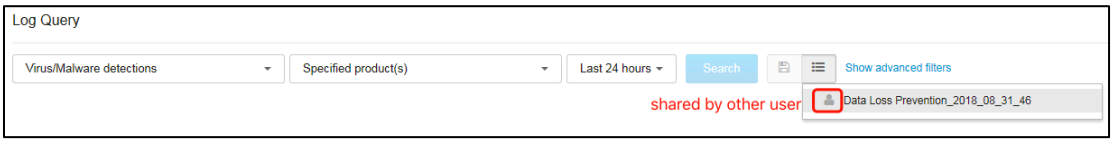


The user can share the saved queries to others. Read-only users can also save and share queries.





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 gray portrait reveals the sharer's username.



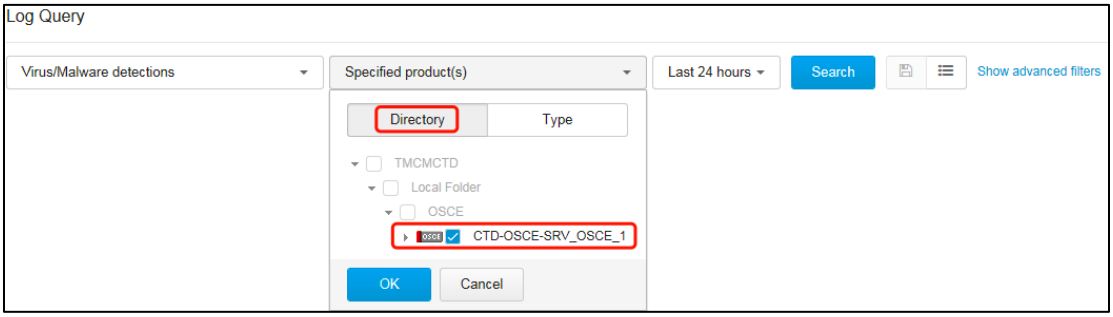
4.3. Role-Based Access Control Log Queries

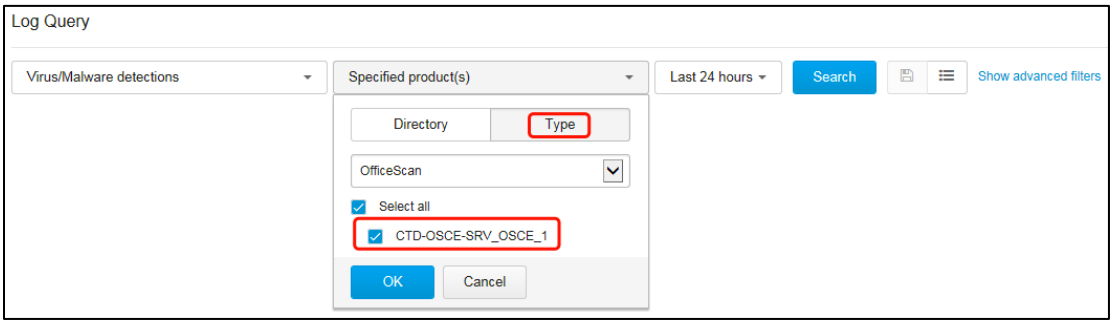
In Log Query, the following parts are controlled by Role-Based Access Control (RBAC):

- 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.





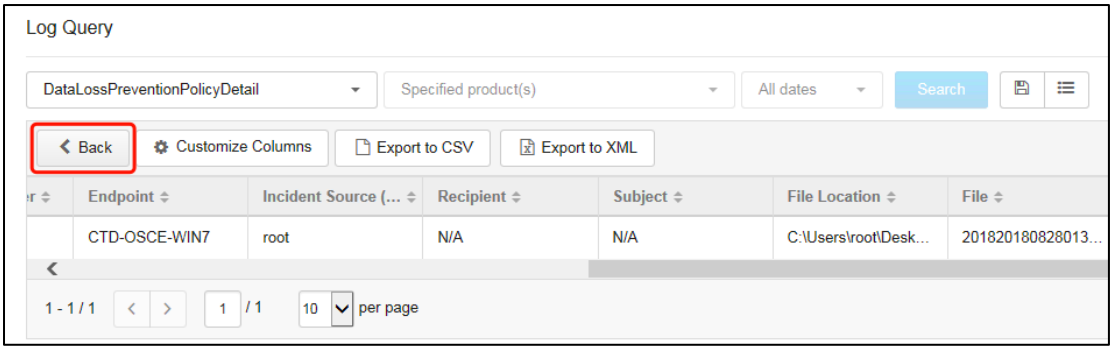
4.4. Drill-down Query Views

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.

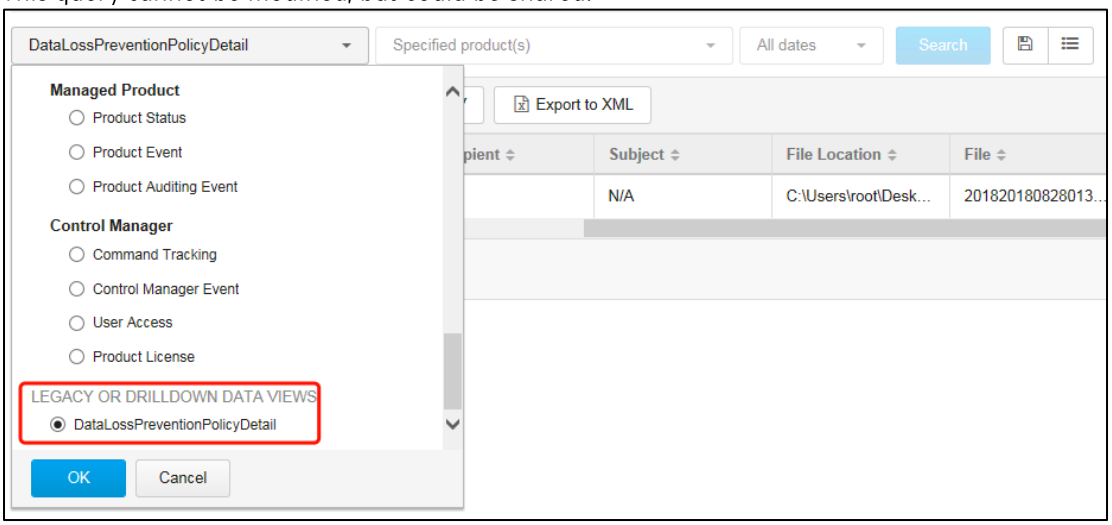
In TMCM 7.0, we can drill down to Log Query from the following:

- 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 TMCM 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.

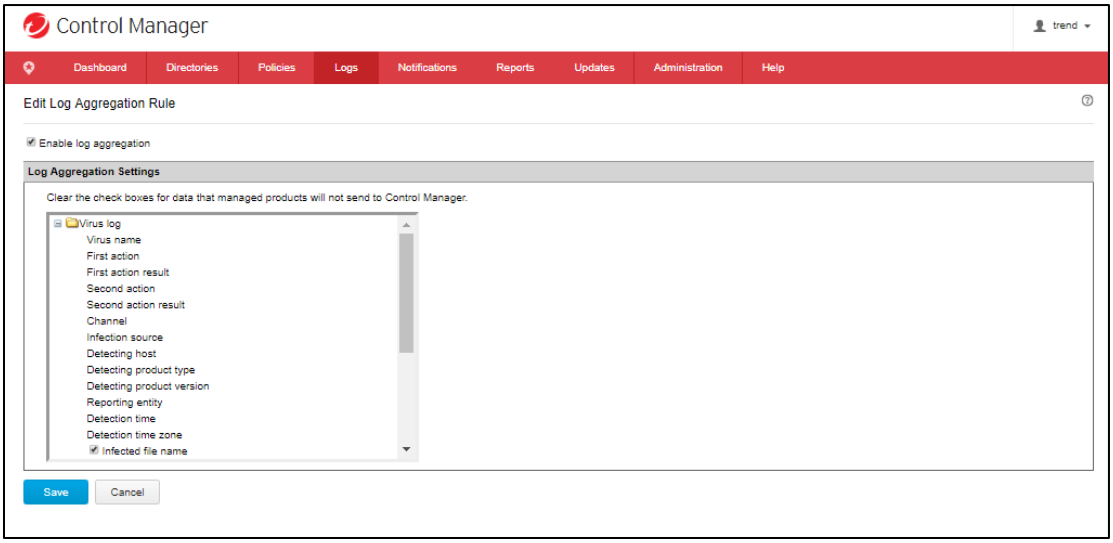


4.5. How to Aggregate Logs

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

Log Name	Log Entries	Maximum Log Entries	Purge Offset	Maximum Log Age	
Virus/Spyware/Grayware log	35	1000000 logs	1000 logs	90 days old	Delete All
Product event log	0	1000000 logs	1000 logs	90 days old	Delete All
Security log	0	1000000 logs	1000 logs	90 days old	Delete All
Web security log	32	1000000 logs	1000 logs	90 days old	Delete All
Network virus log	0	1000000 logs	1000 logs	90 days old	Delete All
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

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

By default, TMCM 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 TMCM 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

TMCM 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
System Events:		
Virus/Malware	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
Spyware/Grayware	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
Suspicious File	Detailed Suspicious File Information	Provides specific information about suspicious files detected on your network
Behavior Monitoring	Detailed Behavior Monitoring Information	Provides specific information about Behavior Monitoring events on your network
Integrity Monitoring	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
Endpoint Application Control violations	Detailed Endpoint Application Control Violation Information	Provides specific information about endpoint application violations on your network, such as the violated policy and rule name
Device Control violations	Device Access Control Information	Provides specific information about Device Access Control events on your network
Endpoint Security Compliance	Detailed Endpoint Security Compliance Information	Provides specific information about endpoint security compliance on your network

Endpoint Security violations	Detailed Endpoint Security Violation Information	Provides specific information about endpoint security violations on your network
Detailed Predictive Machine Learning Information	Detailed Predictive Machine Learning Information	Provides specific information about advanced unknown threats detected by Predictive Machine Learning
Virtual Analyzer Detections	Detailed Virtual Analyzer Detection Information	Provides specific information about advanced unknown threats detected by Virtual Analyzer
Network Events:		
Spam Connection	Spam Connection Information	Provides specific information about the source of spam on your network
Content Violation	Detailed Content Violation Information	Provides specific information about content violations on your network
Email Messages with Advanced Threats	Email Messages with Advanced Threats	Provides specific information about email messages with suspicious and malicious behavior patterns
Web Reputation	Detailed Web Reputation Information	Provides security threat information about policy or rule violations detected by Web Reputation Services
Web Violation	Detailed Web Violation Information	Provides specific information about web violations on your network
Firewall Violation	Detailed Firewall Violation Information	Provides specific information about firewall violations on your network
Network Content Inspection	Network Content Inspection Information	Provides specific information about network content violations on your network
Intrusion Prevention	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
C&C Callback	Detailed C&C Callback Information	Provides specific information about C&C callback events detected on your network
Suspicious Threat	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
Application Activity	Detailed Application Activity	Displays specific information about application activities that violate network security policies
Mitigation	Detailed Mitigation Information	Provides specific information about tasks carried out by mitigation servers to resolve threats on your network

Correlation	Detailed Correlation Information	Provides specific information about detailed threat analyses and remediation recommendations
Data Protection Events:		
Data Loss Prevention	DLP Incident Information	Displays specific information about incidents detected by Data Loss Prevention
Data Discovery	Data Discovery Data Loss Prevention Detection Information	Displays specific information about incidents detected by Data Discovery
Managed Product:		
Product Status	Product Status Information	Displays specific information about managed products registered to the Control Manager server
Product Event	Product Event Information	Displays specific information about managed product events
Product Auditing Event	Product Auditing Event Log	Displays auditing information related to managed products
Control Manager:		
Command Tracking	Command Tracking Information	Displays specific information about commands issued to managed products
Control Manager Event	Control Manager Event Information	Displays specific information about Control Manager server events
User Access	User Access Information	Displays Control Manager user access and the activities users perform while logged on to Control Manager
Product License	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 TMCM. This is based on the design of the product being a centralized management platform for Trend Micro business products.

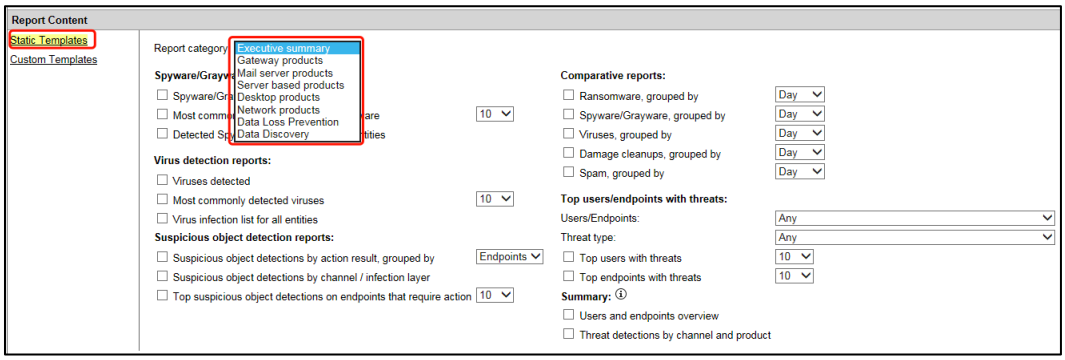
5.1. Static template and Custom template

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

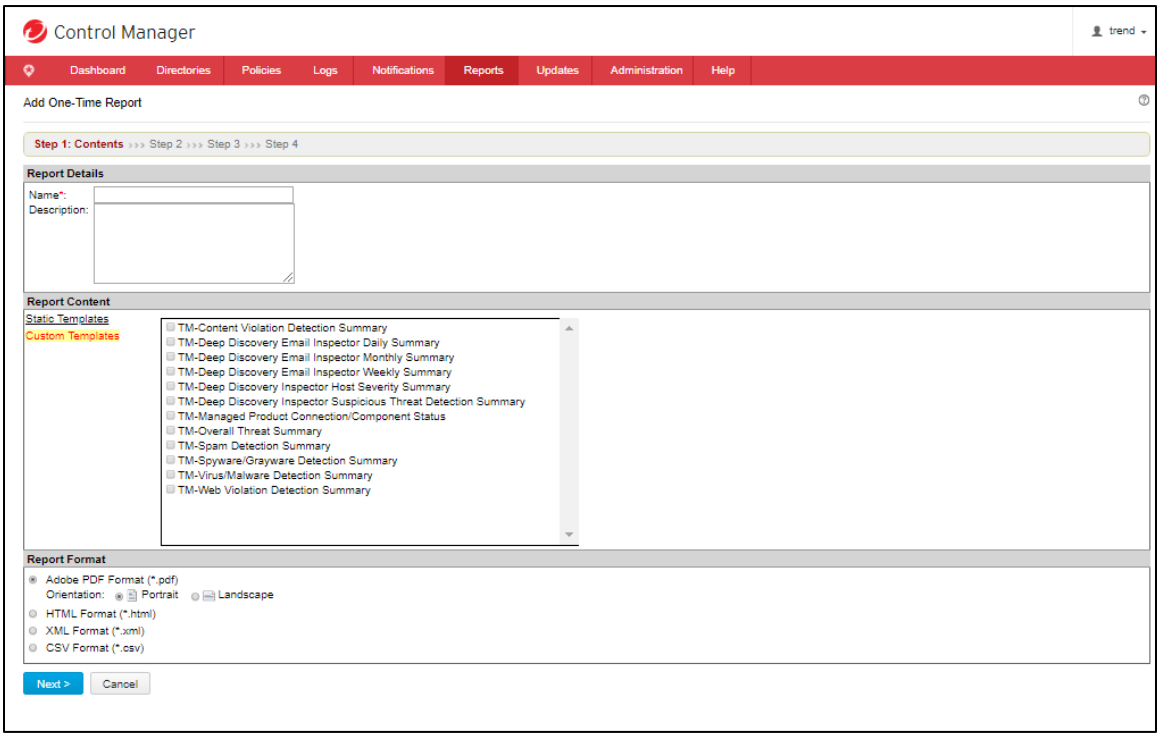
- Custom Templates (Formerly TMCM 5.0 Templates)
- Static Templates (Formerly TMCM 3.0 Templates)
- TMCM 2.5 Templates(hidden by default)

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:



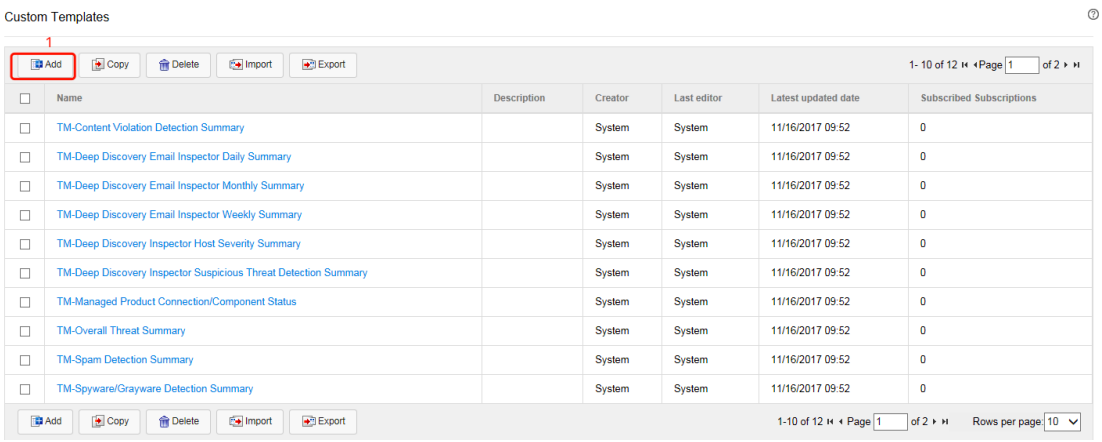
Custom Templates:



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.

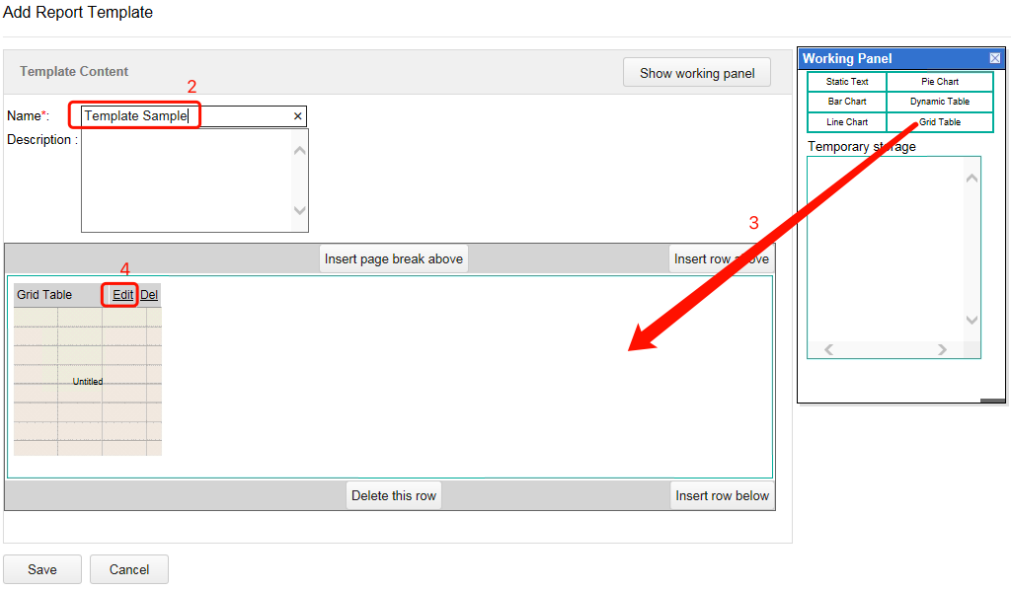
1. Click **Add** to create a new custom template.



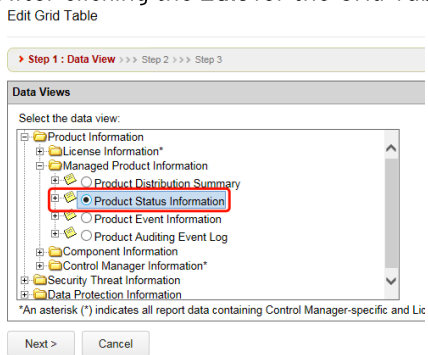
2. Type in a name for the template and drag the needed content unit from the working panel. Six types of content unit are available:

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".

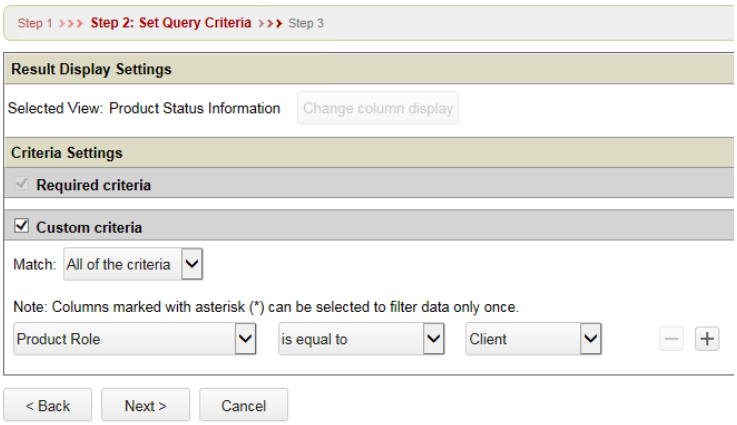


3. After clicking the **Edit** for the Grid Table, you need to choose the specific date view.



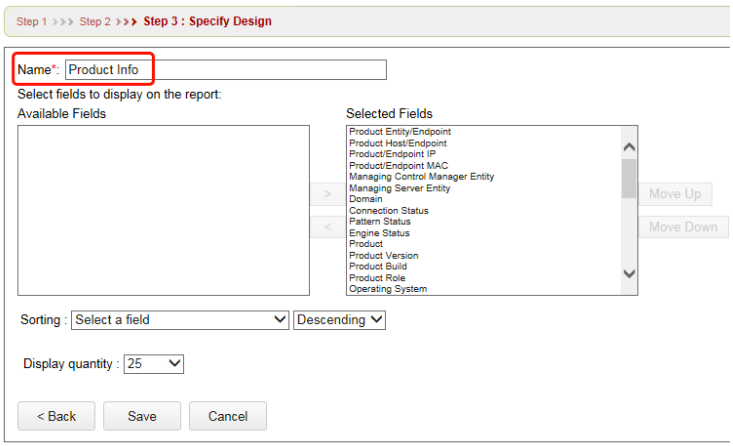
4. Set the custom criterial if needed.

Query Criteria



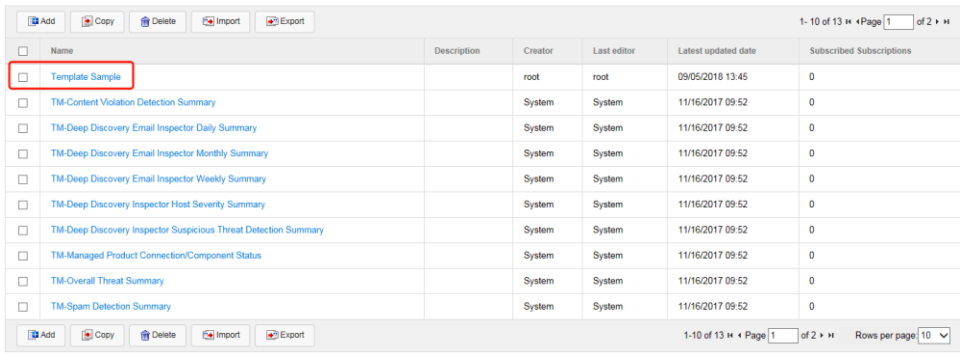
5. Type in the name of this Grid Table, choose the needed fields, and then click **Save**.

Edit Grid Table



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

Custom Templates



Control Manager 2.5 Templates

With the release of TMCM 5.0 report sets, TMCM 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="CrystalImageCleaner-AutoStart" value="true" />
<add key="CrystalImageCleaner-Sleep" value="60000" />
<add key="CrystalImageCleaner-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)

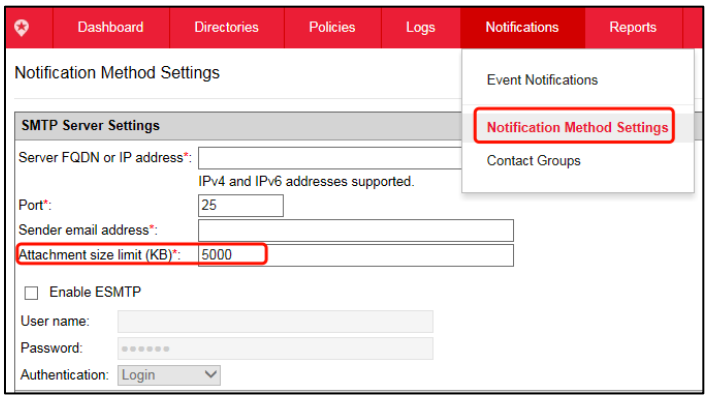
- ✓ After migration to TMCM7.0, the format in next scheduled report will be converted.
  - Rich text (*.rtf) -> Microsoft Word format (*.docx)
  - Other -> Adobe PDF format (*.pdf)

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.**

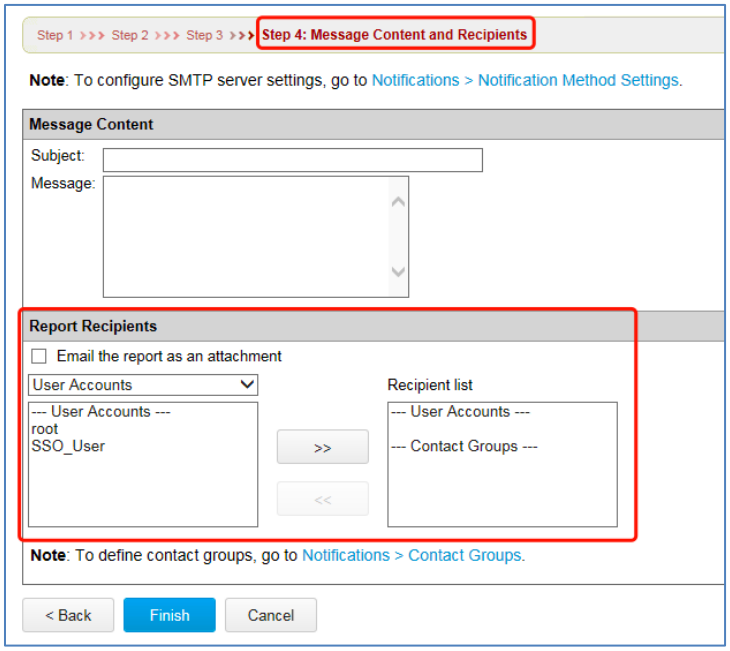
A setting for attachment file size limit has been added, and is set to 5000 KB by default. If notification reports exceed the size limit, then the report is sent as a download link in the email instead of as an attachment. Clicking the link redirects to the TMCM console. After log-on, the report will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



This setting can be altered to confirm 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.

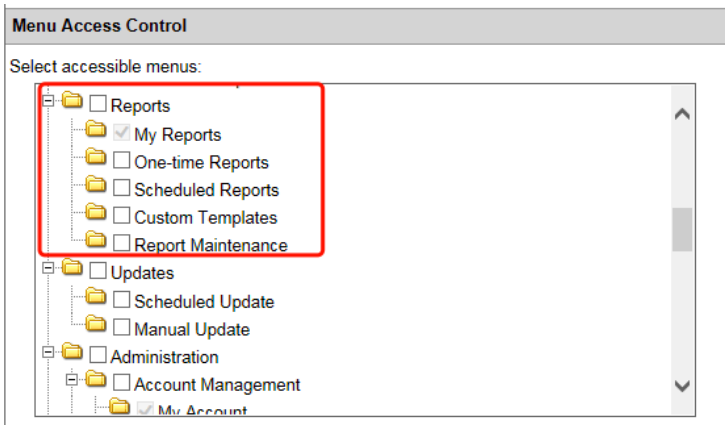


This configuration, together with the role's menu access control, dictates the operations that a specific user can perform to report related items.

	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)

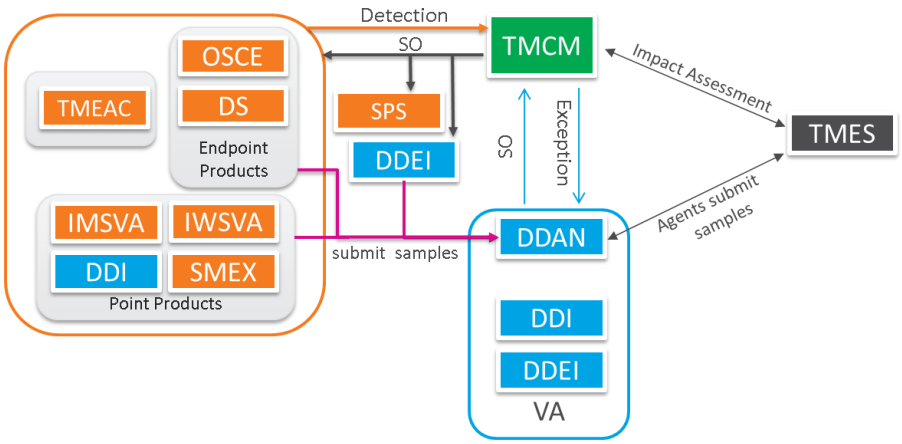
To help customers locate and mitigate these threats, Trend Micro introduced Connected Threat Defense (CTD), which provides a comprehensive and more complete solution to this problem.

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
- TMCM 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	

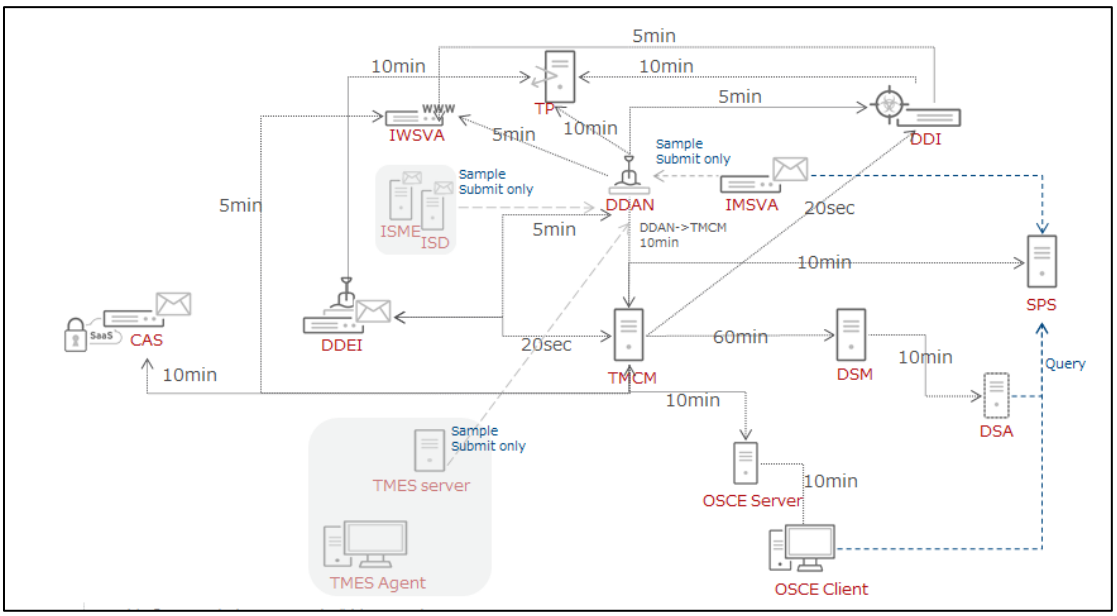
Domain	Log Block	✓ Only VASO can be added into exception list. ✓ Wild card is suppoted	
File (UDSO)	Log Block Quarantine	✓ UDSO has the highest priority ✓ CM will still display the detection log on the UDSO page even if it matches to the wildcard exception list	

6.2.2. Suspicious Object Sync Interval

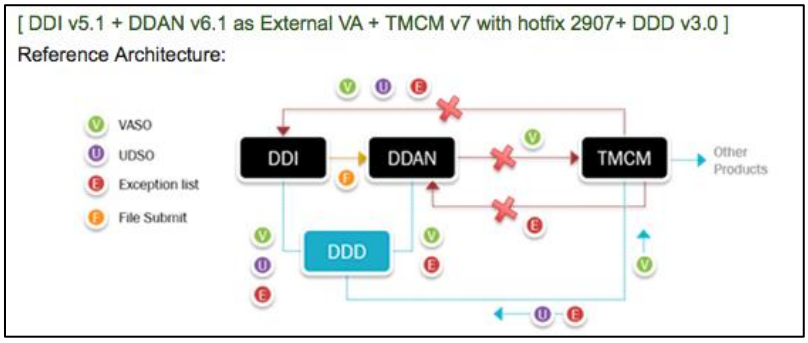
DDAN, DDEI and DDI can be the VASO source, and TMCM can deliver them to OSCE, DSM, TP, IWSVA, SPS and CAS.

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

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



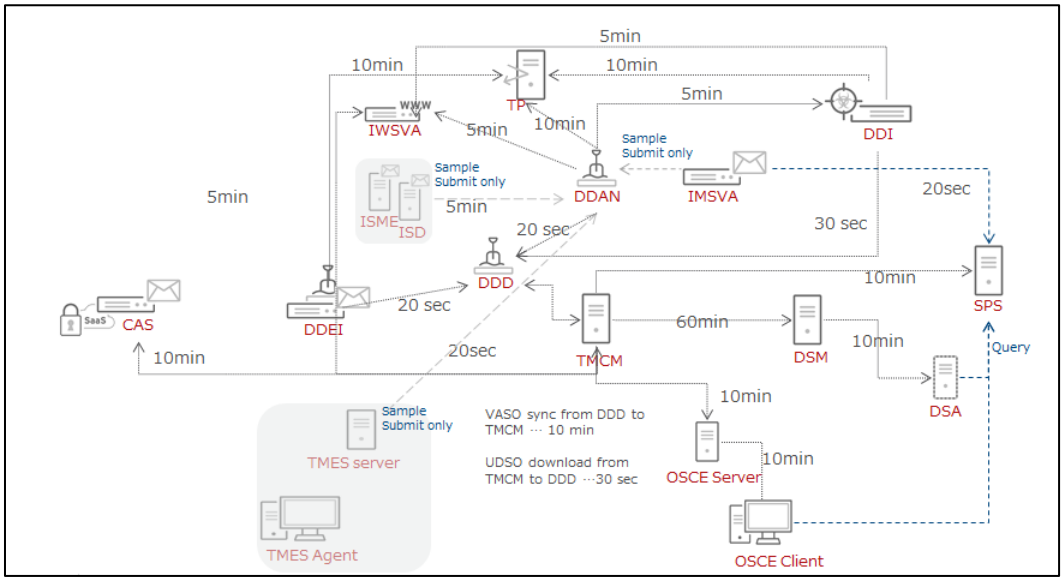
DDD V3.0 has the ability to do suspicious object synchronization among managed Deep Discovery products (DDI v5.1, DDAN v6.1, and DDEI v3.1).



After registering DDD to TMCM, TMCM will issue the following requests to DDD every 10 minutes:

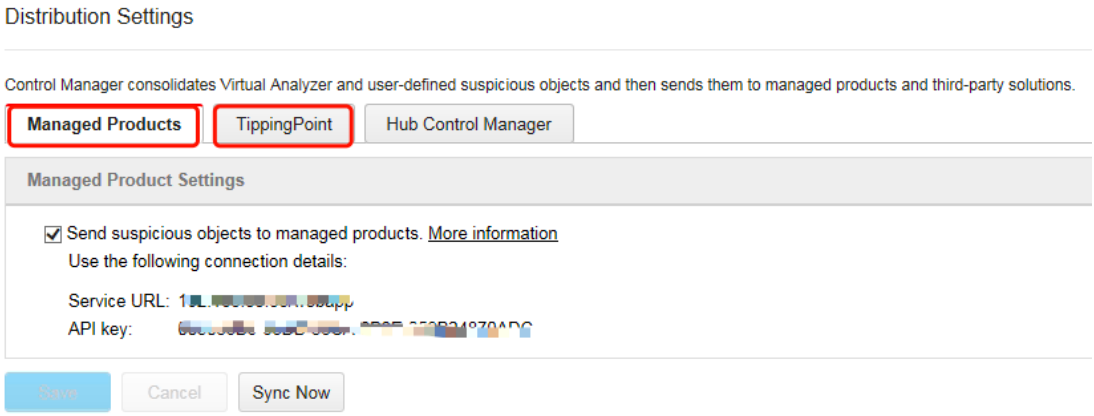
- Upload Virtual Analyzer Suspicious Object (VASO) to TMCM.
- Push full exception list if there is an item changed (e.g.: Add/Delete from TMCM console).

As for the User-Defined Suspicious Object (UDSO), DDD will download them every 30 seconds.



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.



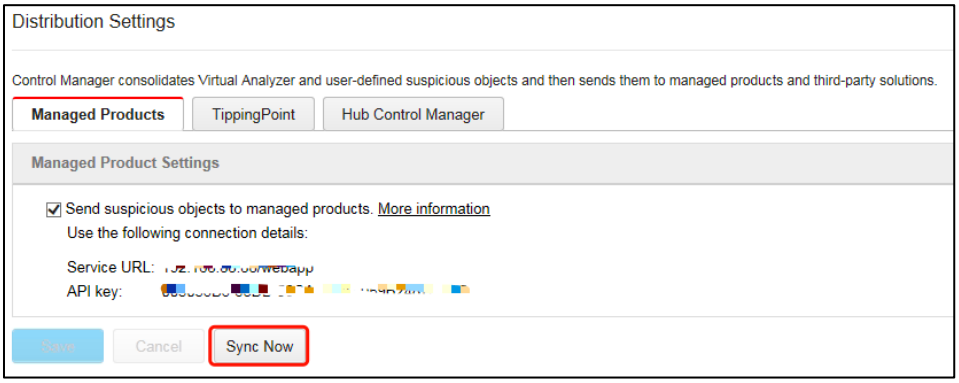
Normally, we can automatically deploy two kinds of API keys: the **DDAN API key** and the **TMCM API key.**

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

2. Consolidate the SO in TMCM
3. Notify products to sync SO
4. Products attempt to synchronize SO with TMCM. 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

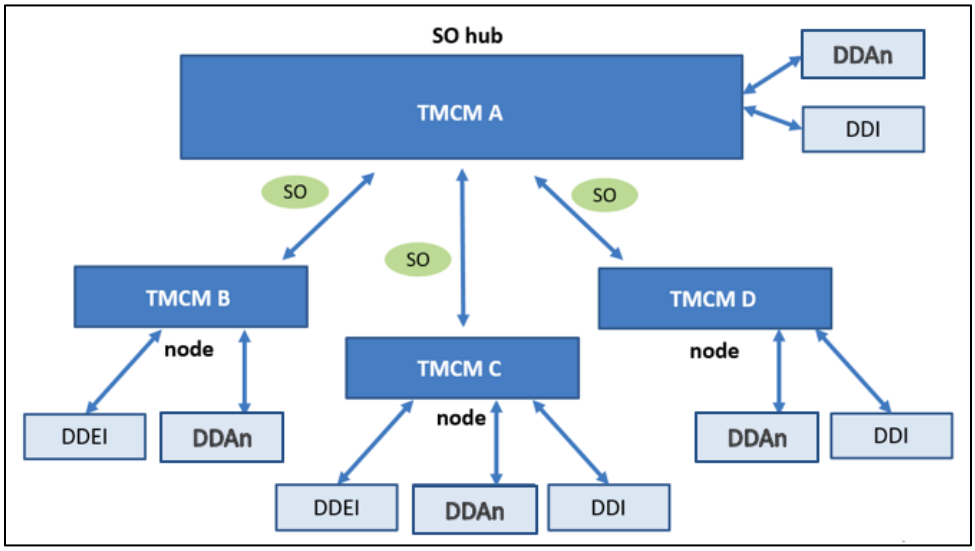
6.3. Hub and Node TMCM

6.3.1. Hub and Node

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

The SO can be synced between Hub and Nodes.

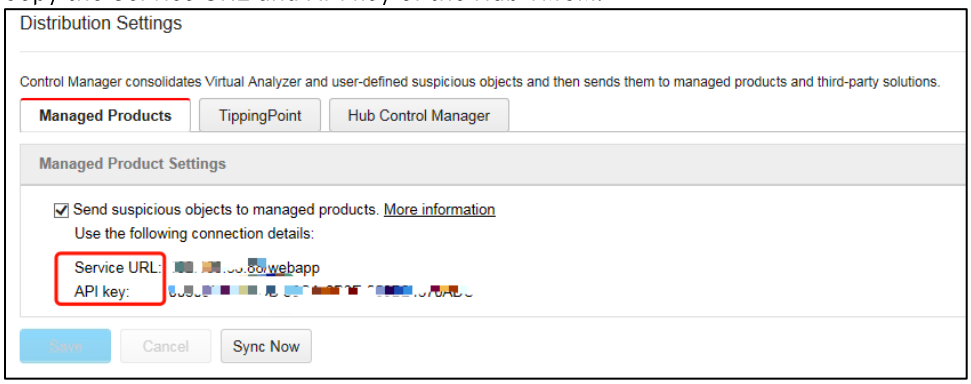
All the TMCM servers will have the same VASOs and UDSOs.



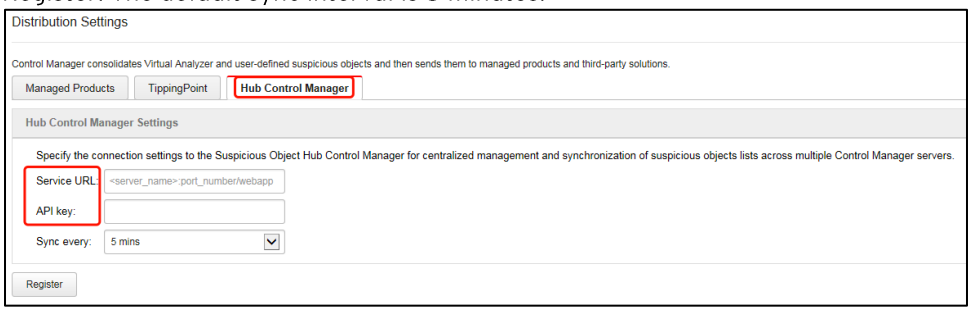
6.3.2. How to register Hub and Node TMCM

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

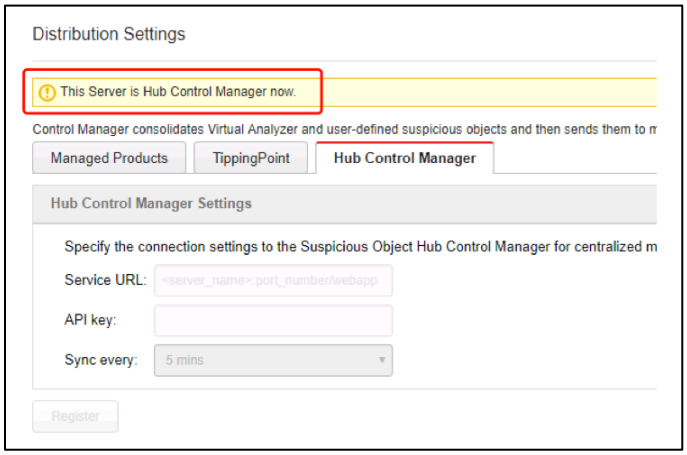
1. Go to **Administration** -> **Suspicious Objects** -> **Distribution Settings.**
2. Copy the Service URL and API key of the Hub TMCM.



3. Go to **Administration** -> **Suspicious Objects** -> **Distribution Settings.**
4. Go to the **Hub TMCM** tab on the **Node TMCM.**
5. Enter the Service URL and API key that was copied from Hub TMCM 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 TMCM 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 TMCM 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>
```

  The tool looks for certain keyword (Observable, watchlist) in the STIX file, and then places the SO into a CSV file. The user can then use the **ImportSOFromCSV** tool to import the CSV into UDSO.

- 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

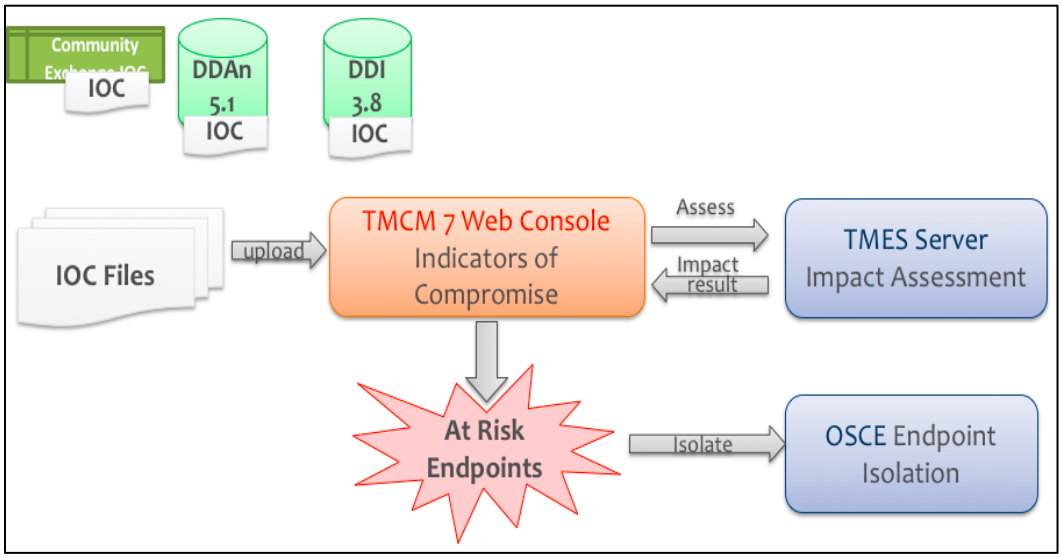
- SOMigrationTool
  This tool exports SOs from CM and import those SOs into a third-party software or other device (i.e. CheckPoint Firewall).
  Please refer to the OLH for details:
  http://docs.trendmicro.com/en-us/enterprise/control-manager-70/tools-and-additional/suspicious-object-mi/using-the-suspicious.aspx

6.5. IOC Management

Indicators-of-Compromise (IOC) Sources:

- DDAn 5.1
- DDI 3.8
- OpenIOC Samples

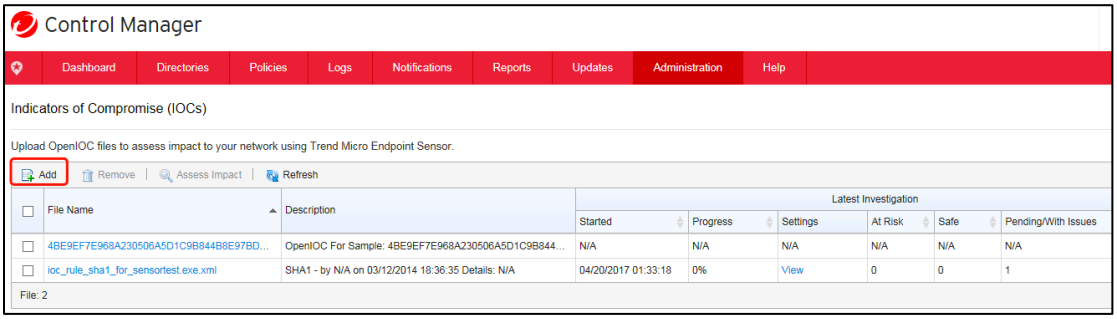
It is recommended to use community IOC as an input for TMCM. Though TMCM supports DDI/DDAn IOC, those DDI/DDAn IOC are automatically converted to SO and sent to TMCM. To avoid redundancy, it is not recommended to use DDI/DDAn IOCs. Once IOC is uploaded to TMCM, the administrator use TMES to perform impact 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

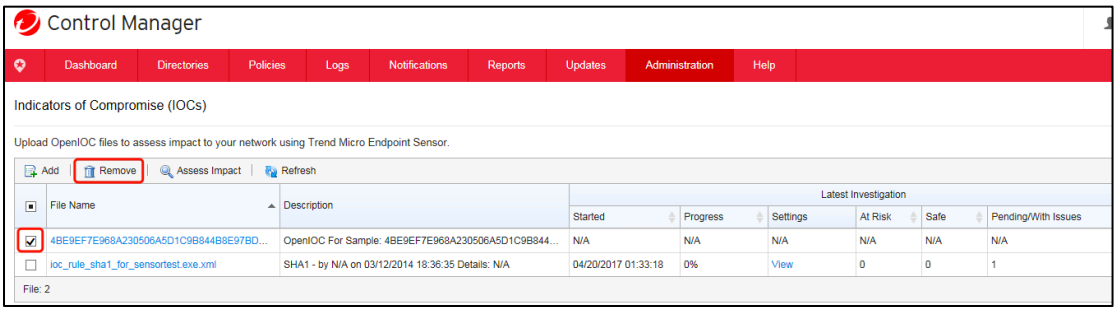
The Add button allows customers to add IOC files from either Deep Discovery Inspector or from OpenIOC samples.

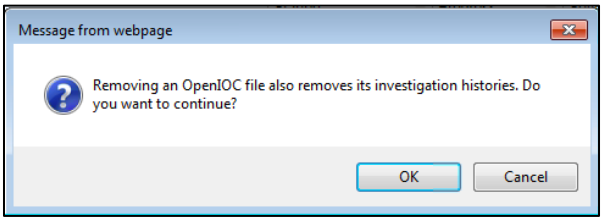
1. Open the TMCM console.
2. Go to **Administration** > **Indicators of Compromise**.



6.5.2. Removing IOCs

The **Remove** button removes IOC files and reports previously added.

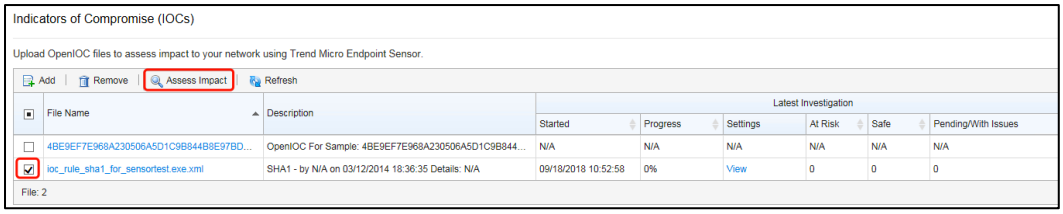


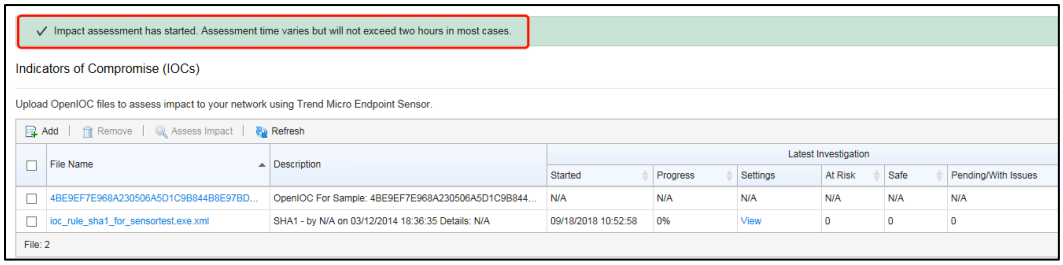


6.5.3. Impact Assessment

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.

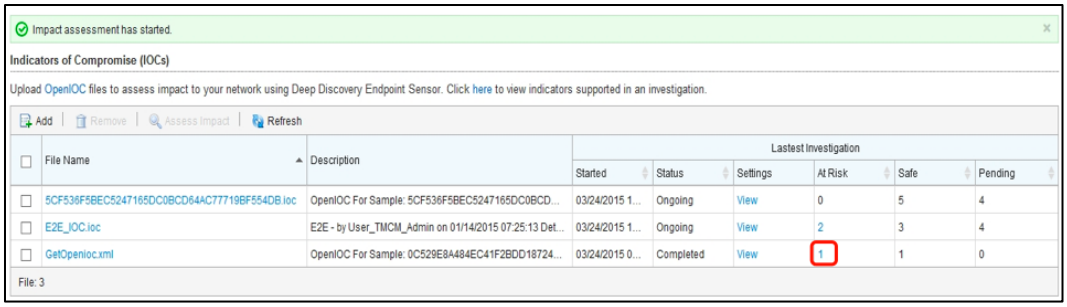
Control Manager initiates a command to Trend Micro Endpoint Sensor (TMES) to assess the endpoints which are at risk.



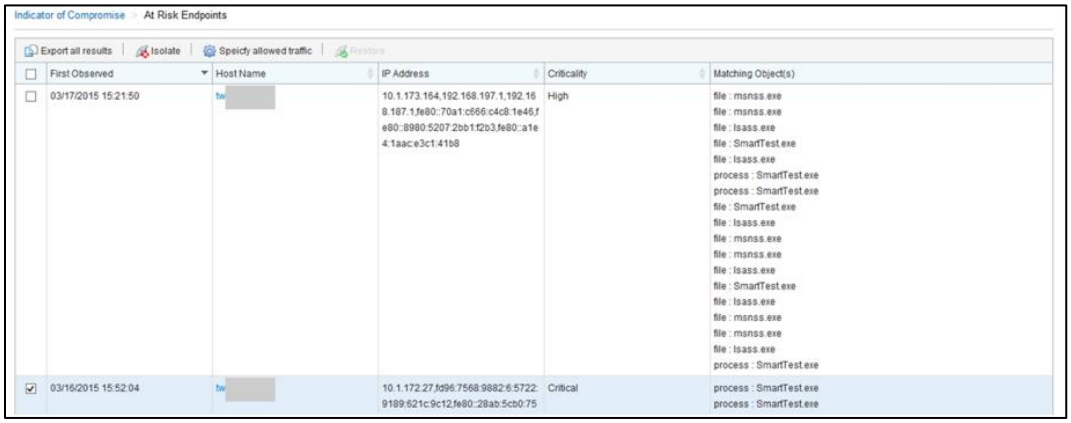


6.5.4. At-risk Endpoints

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



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



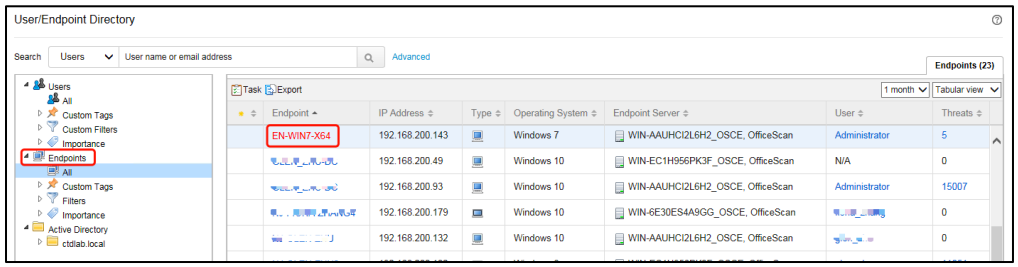
6.5.5. OfficeScan Endpoint Isolation

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 TMCM Administrator a method of mitigation to prevent further damage.

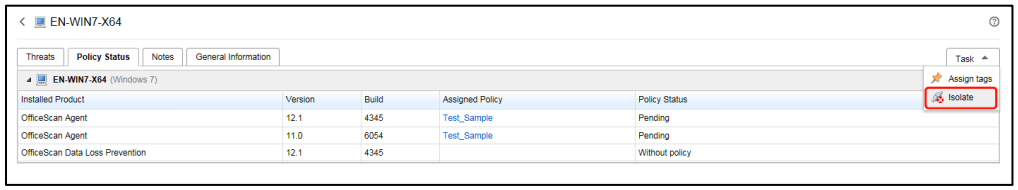
The OfficeScan firewall is used to isolate endpoints at risk. Please also ensure the Single-Sign On for the OSCE server is enabled.

Deploying Endpoint Isolation Task

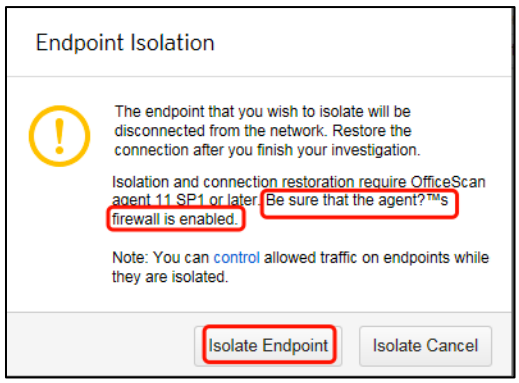
1. Find and select the infected endpoint (e.g. EN-WIN70-X64).



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



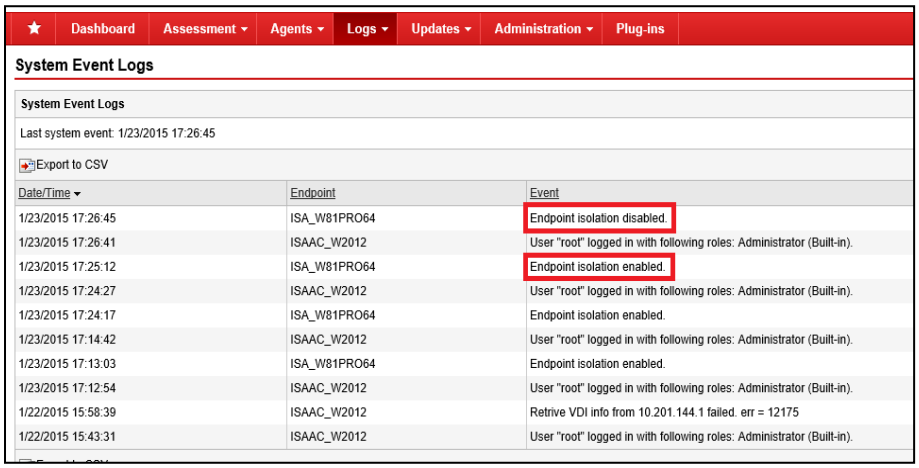
3. Click **Isolate Endpoint.**



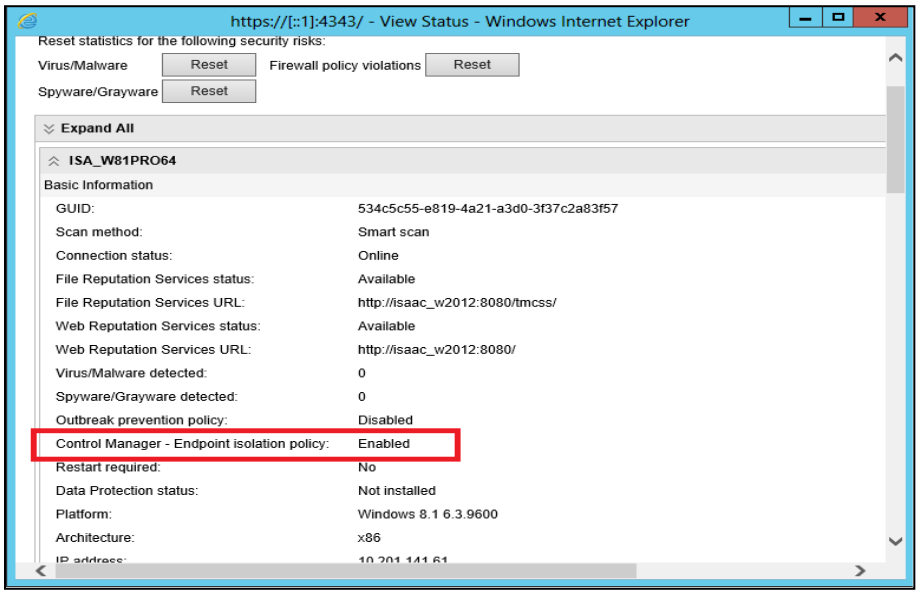
Verifying Endpoint Isolation

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

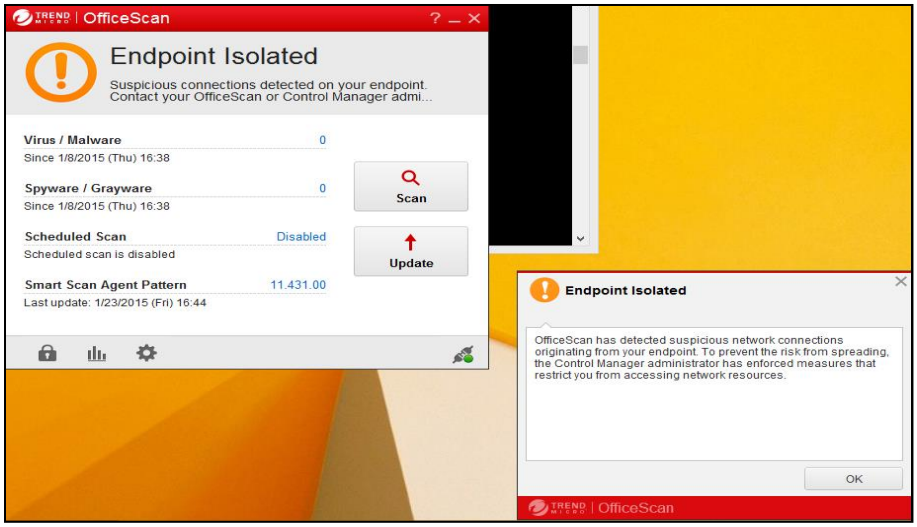
7. OfficeScan Server System Event Logs



8. OfficeScan Server console displaying Client status



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 TMCM 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

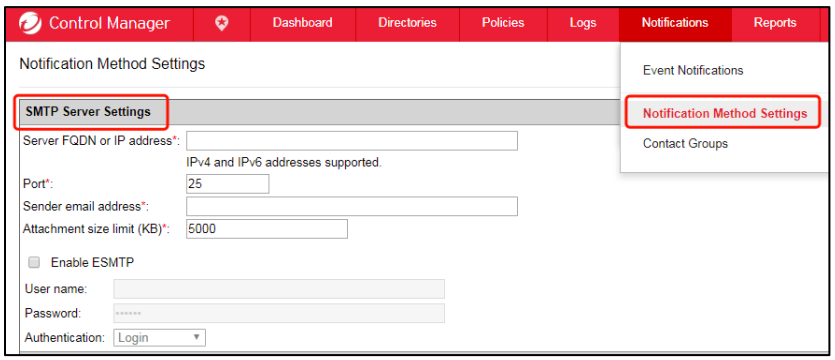
To realize the possible incident earlier, email notification, syslog or SNMP could be enabled by Control Manager.

Event Notifications

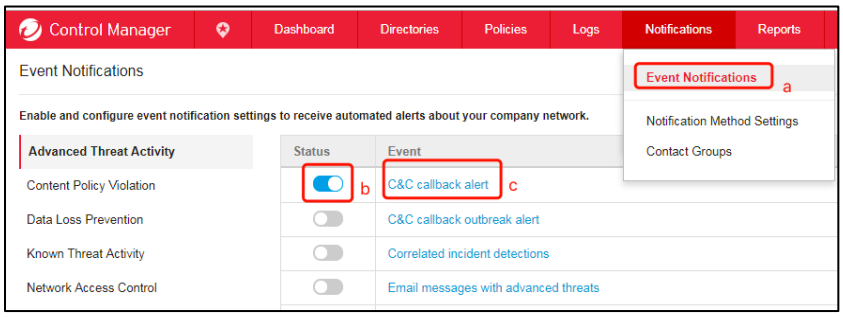
✓ Email notification

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

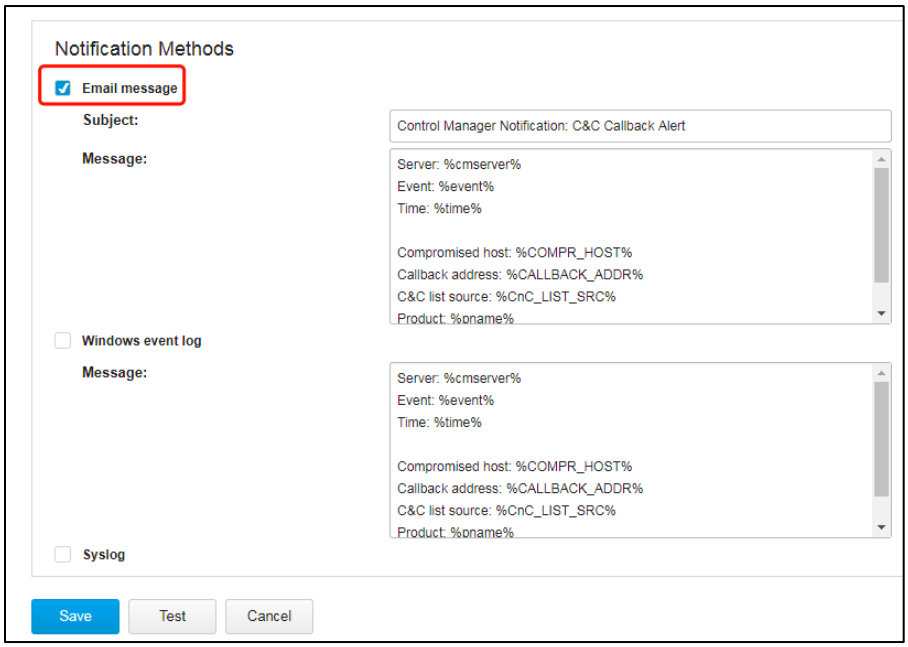
a. Configure the SMTP Server Settings.



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



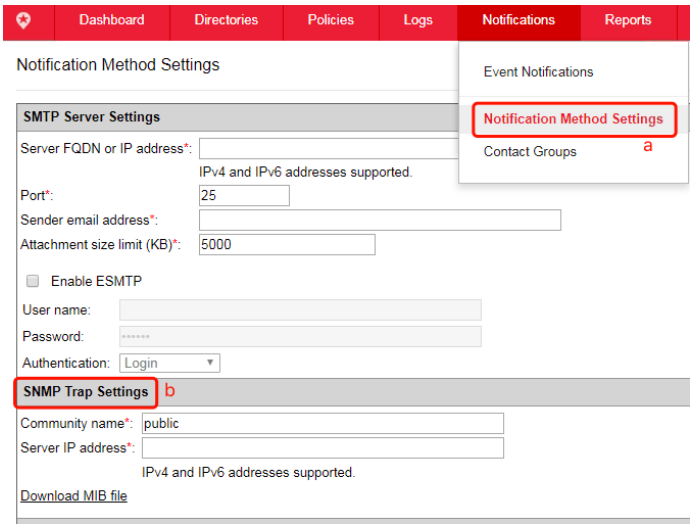
c. Enable **Email message**. Modify the Subject and Message is needed.



d. Click **Save**.

✓ SNMP

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

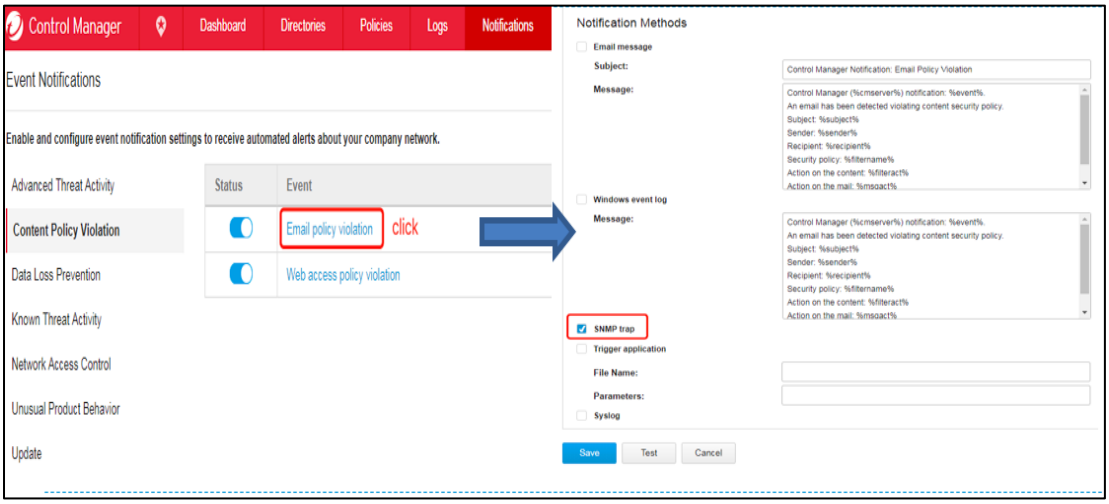


In the SNMP Trap Settings section, specify the following:

a. **Community name**: Type the SNMP community name.

b. **Server IP address**: Type the IPv4 or IPv6 address of the SNMP server.

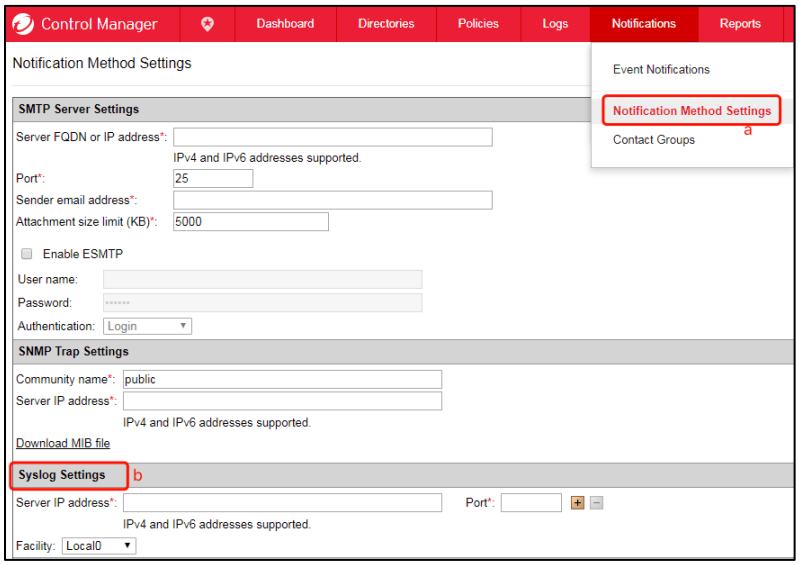
Check if the SNMP trap is supported.



✓ Syslog

The following are the characteristics of the syslog message:

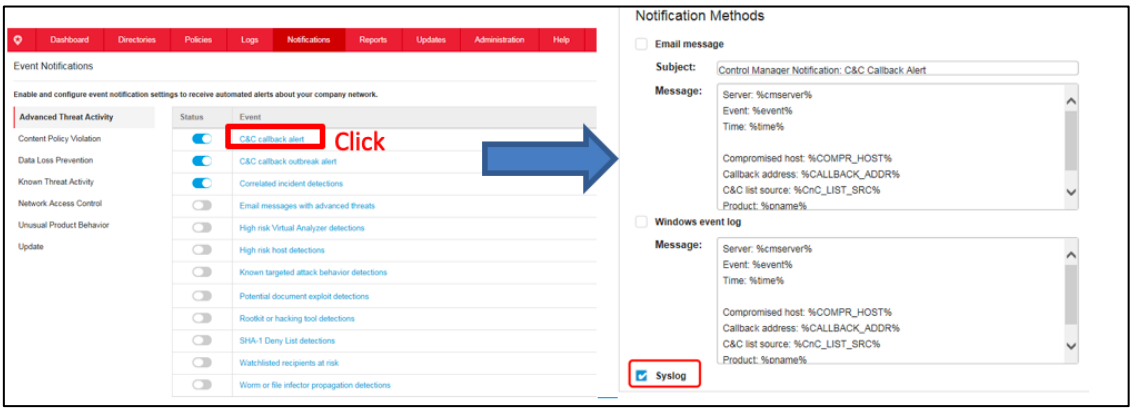
- Easier regular expression parsing
- Enhanced readability
- Uses the name value pair __name = "__value__"
- Follows RFC 3164 for syslog format
- Applies ISO 8601 time format
- Maintains the same event ID with the SNMP message for better consistency



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	Y
	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

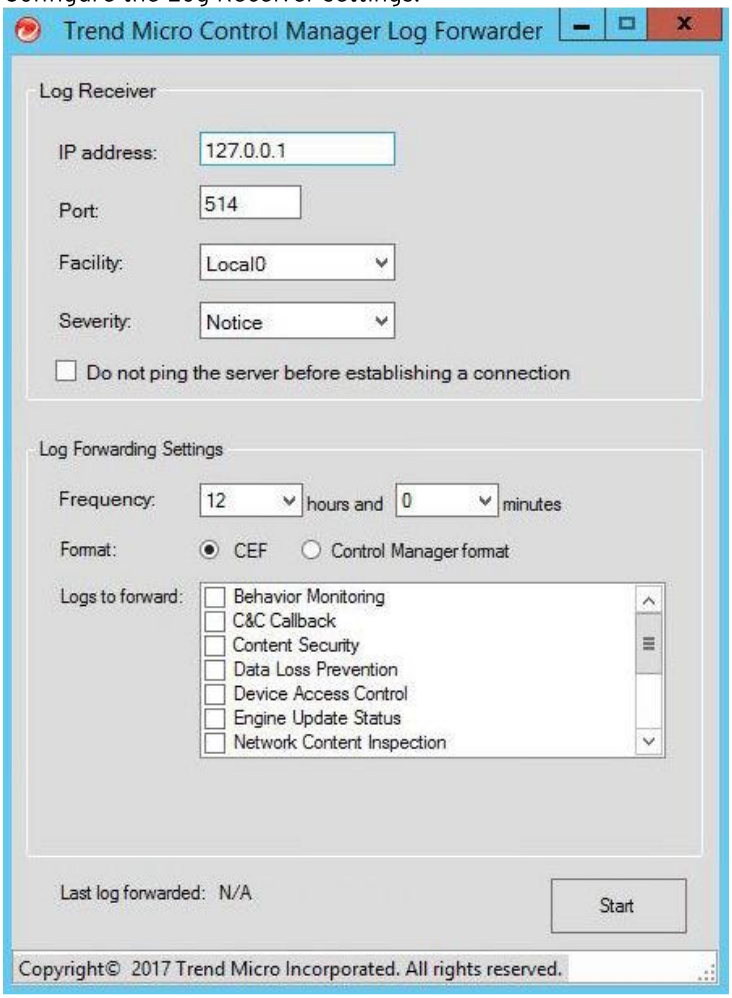
- ✓ TMCM 7.0 discontinues support for the DataExport Tool. Administrators should use the new LogForwarder Tool (LogForwarder.exe).
- ✓ The LogForwarder Tool only supports UDP protocol.

Configuring LogForwarder Settings

a. Go to the TMCM installation directory. By default, the installation directory is C:\Program Files (x86)\Trend Micro\Control Manager.

b. Execute the LogForwarder.exe file using administrator rights (Run as administrator) to open the LogForwarder console.

c. Configure the Log Receiver settings.



- 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

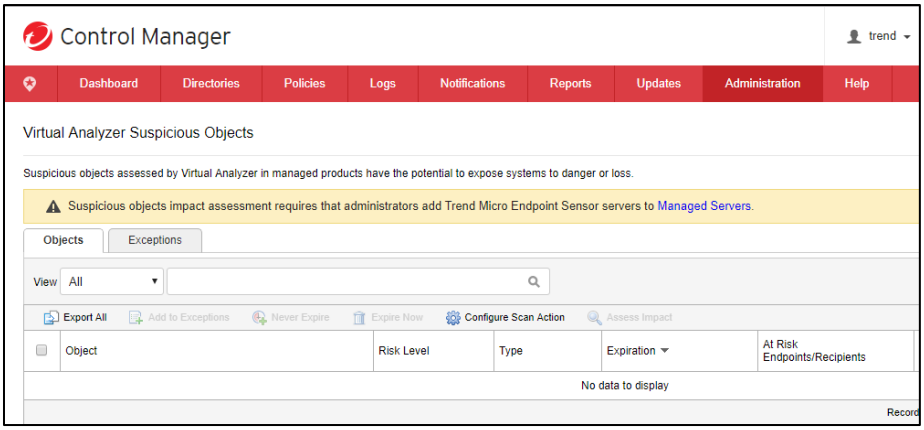
d. Configure the **Log Forwarding Settings**.

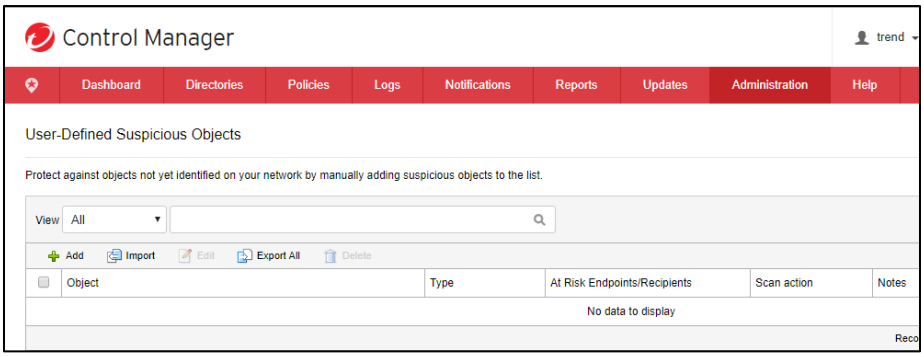
- Frequency: The frequency in which the tool sends logs
- Format: Select whether to use CEF or Control Manager log format
- Logs to forward: Select the log types to forward to Control Manager

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 TMCM services.

7.2. Minimize Threat Influence

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





Note:

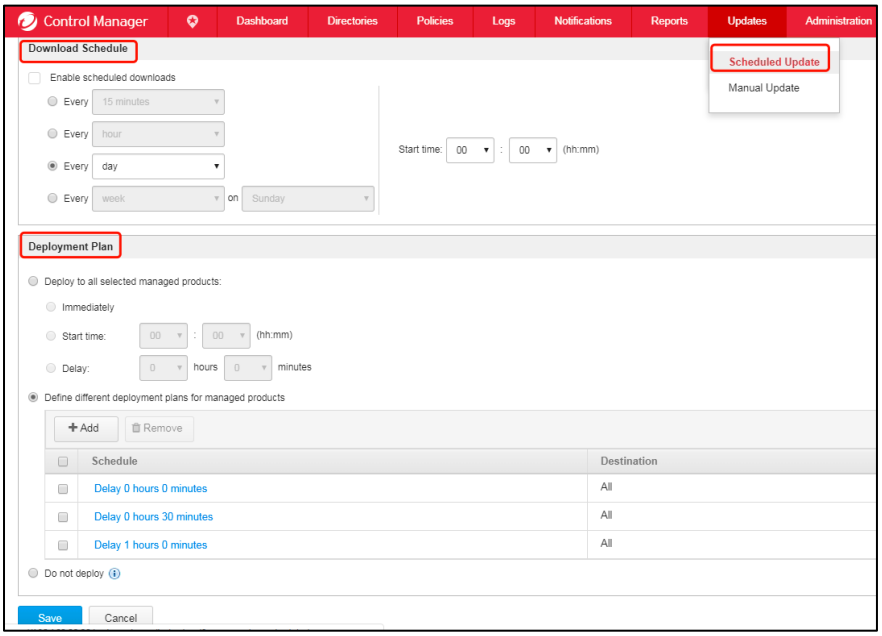
- Expired SO will be deleted every hour.
- From TMCM web console, expiration period can be configure to:
  - Expire now
  - Never expire

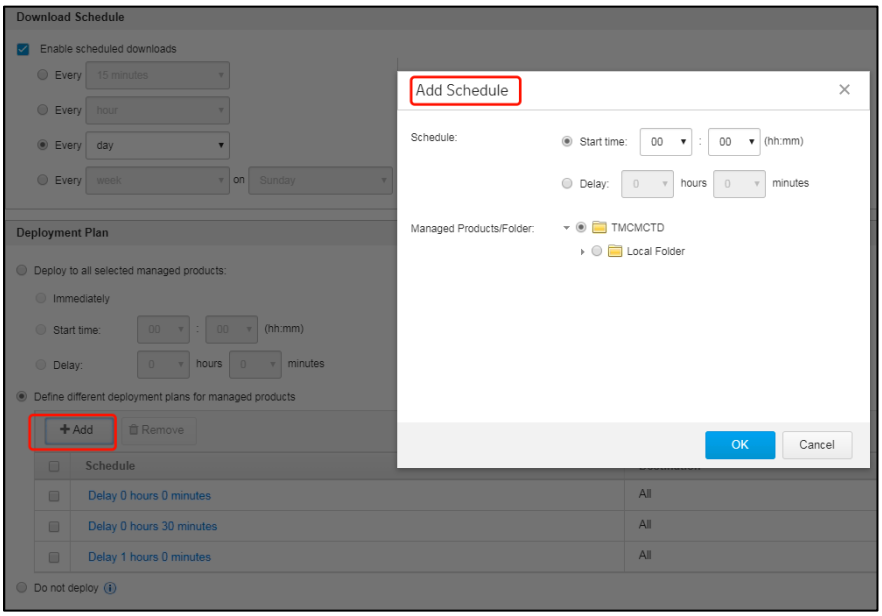
7.3. Deliver latest pattern and engine

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.

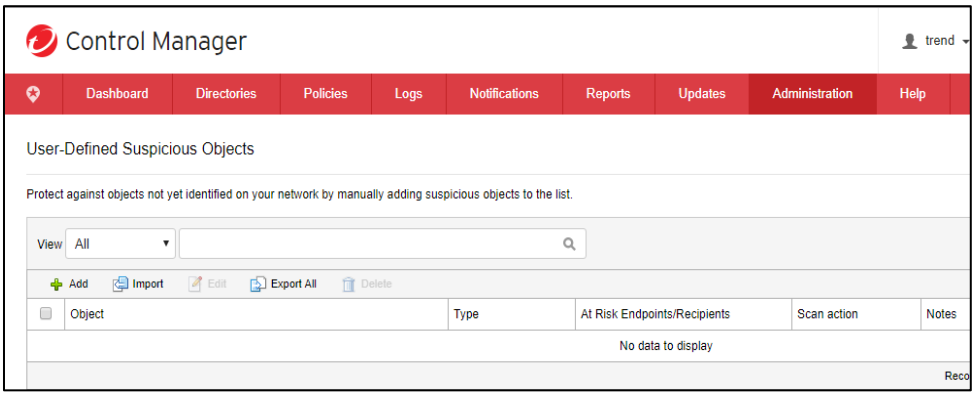




For Manual Update, administrators should consider the reasonable and suitable the Deployment Plan.

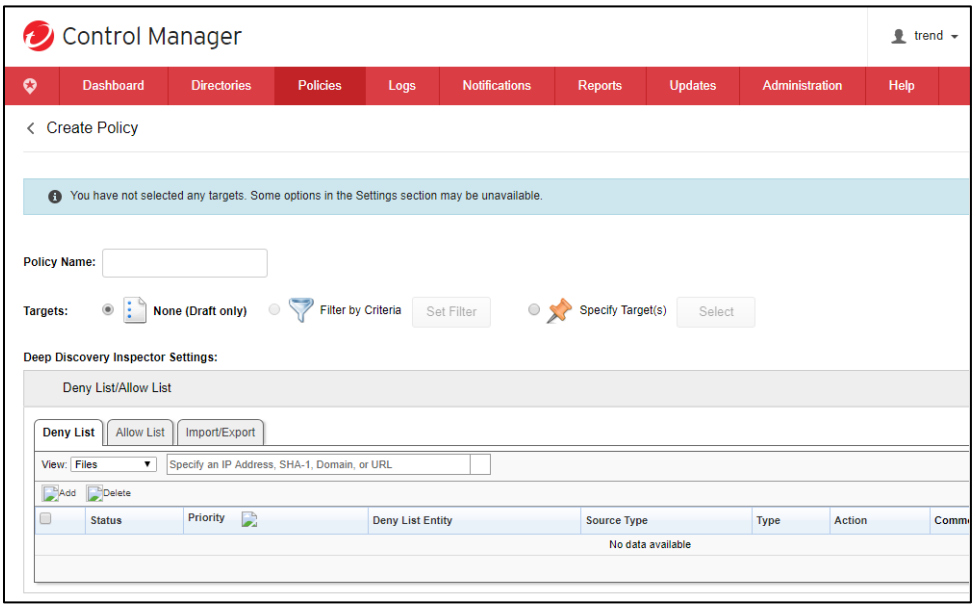
7.4. Minimize false alarm detection

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, TMCM 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 TMCM 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 TMCM 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 TMCM 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 TMCM and the parent TMCM server can be collected. Refer to the information below:

8.1.1. User Accounts and Roles

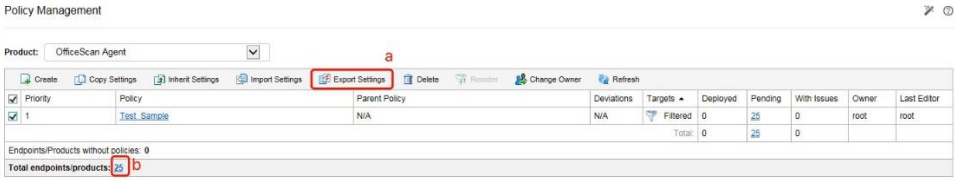
1. Go to **Administration** > **Account Management** > **User Accounts** and take note of the user role and access control for each account.
2. Go to **Administration** > **Account Management** > **User Roles** and take note of the Menu Access Control for customized roles.

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.



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 TMCM 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

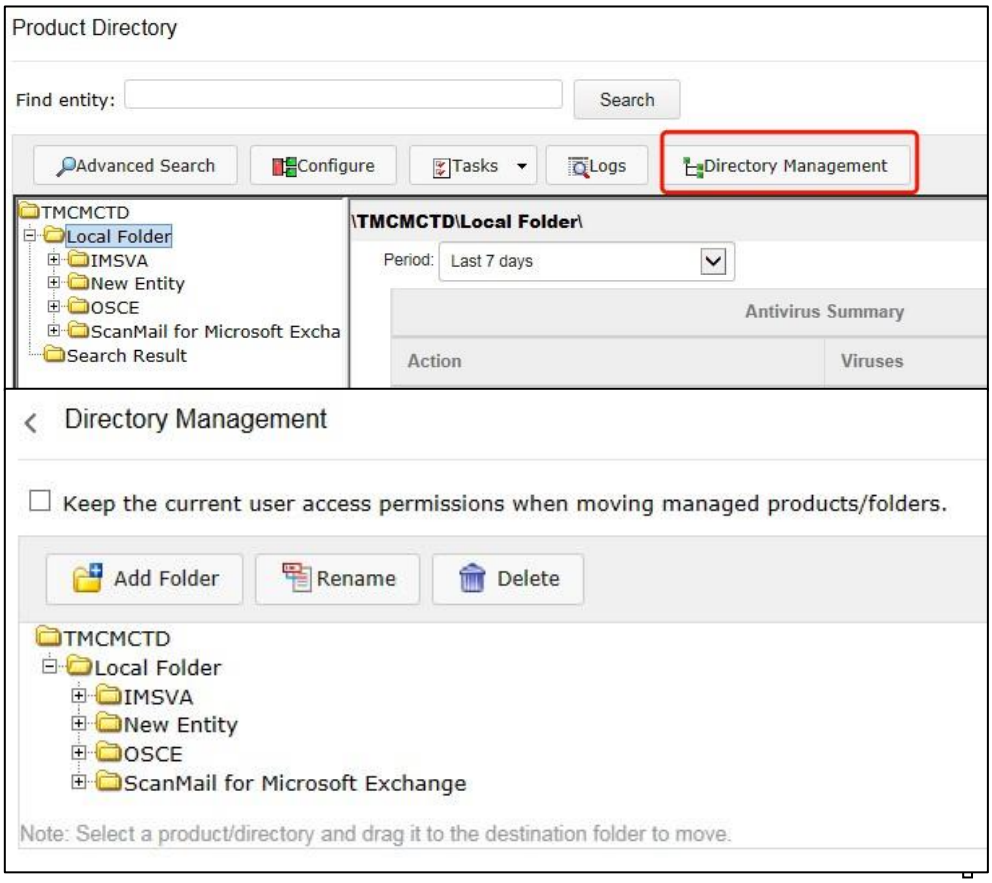
Since all child/parent TMCM users will be merged into one TMCM. Please refer to the questions below to re-design the management model.

8.2.1. Account and Access Control

- Review all accounts and access control scope from all Child/Parent TMCM to remove non-used accounts and leave only necessary accounts and privilege.
- The TMCM 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 TMCM 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 TMCM.
- Design a grouping model for all products (e.g. by geography or by function).
- Use Product Directory Management to sort the products.



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 TMCM 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 TMCM.
  - 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 TMCM, 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, TMCM 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 TMCM, but some products (WSI\SCO) are added on TMCM side.

So, the network connections between TMCM and managed products should be configured to allow two-way communication for TMCM 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 TMCM Server.
- If a monthly or weekly report is required, it needs to be generated before doing a migration.

8.3.2. Install TMCM

- Perform a fresh installation of TMCM 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 TMCM Databases and upgrade the managed products to the version that are supported by TMCM 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 contol manager support for the managed product.

Function	Description	OfficeScan	Office Scan Plug-in	
		11, XG, XG SP1	DLP option	Vulnerability detection
Dashboard	Dashboard can show connection status with managed product	Supported	N/A	N/A
Directory > Product	**Directory** > **Product** 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