Apex Central 2019

Best Practice Guide

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

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

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 Apex Central 2019 Best Practices Guide. This document is designed to help resellers and customers develop a set of best practices when deploying and managing the Apex Central 2019.

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

- Apex Central 2019 Installation Guide
- Apex Central 2019 Administrator's Guide

1 Product Description

Apex Central 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 Preparation

2.1 Installation

Please refer Installation and Upgrade Guide and System Requirements .

2.2 Site Planning

In this document, you will learn about deployment methods for Apex Central, 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 Apex Central, in conjunction with a target site(s), is a key step.

In most deployments, a single Apex Central server is sufficient for most regions. Having a single Apex Central server in one site is the primary application of central management. A Apex Central server is required for organizations with multiple Trend Micro products installed. With one site, the communication between Apex Central 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 Apex Central server and registered managed products located in different datacenters. For details, refer to http://esupport.trendmicro.com/solution/en-US/1038211.aspx.

2.2.1 Single Site

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

- Small enterprise
  - A single Apex One/Office Scan 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

2.2.2 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 Apex Central server.

The biggest advantage of having a single Apex Central 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 Apex Central 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.

2.3 Considerations

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

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

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

2.4 Apex One Endpoint Sensor deployment

Apex Central newly integrates with Apex One Endpoint Sensor for Endpoint Detection Response. (EDR). Before Endpoint Sensor deployment, please confirm system requirement and related settings.

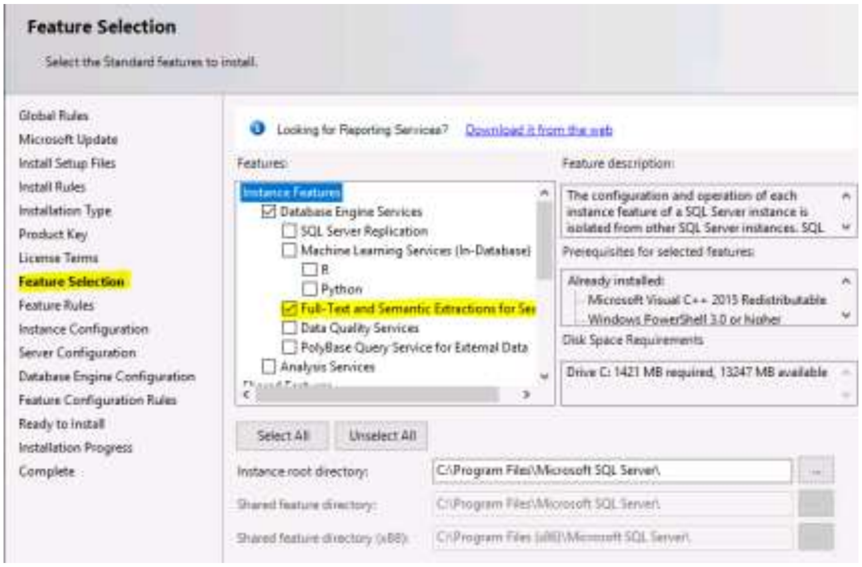
2.4.1 System Requirements

- ✓ Apex One server should be installed on Windows 2012, 2016 or 2019 Server.
- ✓ Endpoint Sensor only support

  SQL 2016 SP1 standard or enterprise

  SQL 2017 standard or above
- ✓ Endpoint Sensor doesn't support SQL Express

✓ SQL server has to enable “Full-Text and semantic Extractions for Search” function in advance.



Feature Selection

Select the Standard features to install.

Global Rules
Microsoft Update
Install Setup Files
Install Rules
Installation Type
Product Key
License Terms
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Looking for Reporting Services? Download it from the web

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication
  - □ Machine Learning Services (In-Database)
    - □ R
    - □ Python
  - ☑ Full-Text and Semantic Extractions for Sea
  - □ Data Quality Services
  - □ PolyBase Query Service for External Data
- □ Analysis Services

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL

Prerequisites for selected features:

Already installed:
- Microsoft Visual C++ 2015 Redistributable
- Windows PowerShell 3.0 or higher

Disk Space Requirements

Drive C: 1421 MB required, 13247 MB available

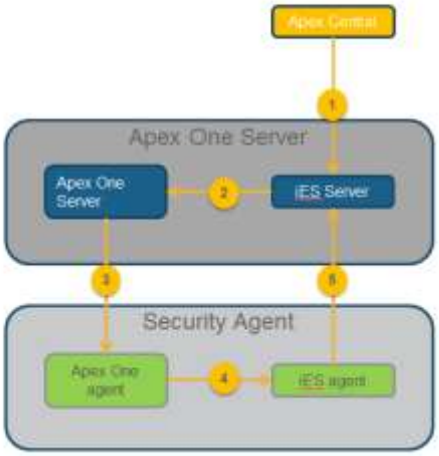
Select All | Unselect All

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

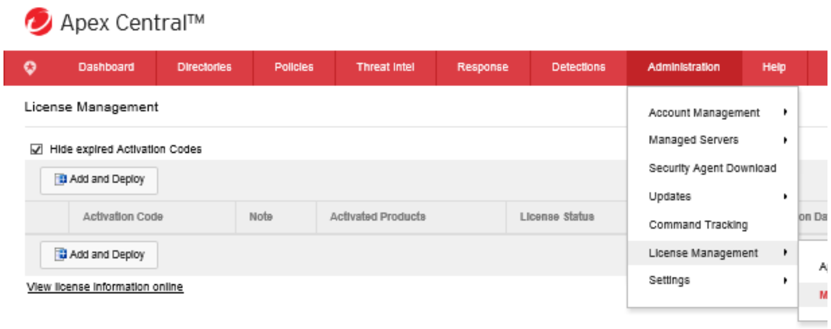
Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

2.4.2 How to enable Apex One Endpoint Sensor



Architecture for Apex One Endpoint Sensor

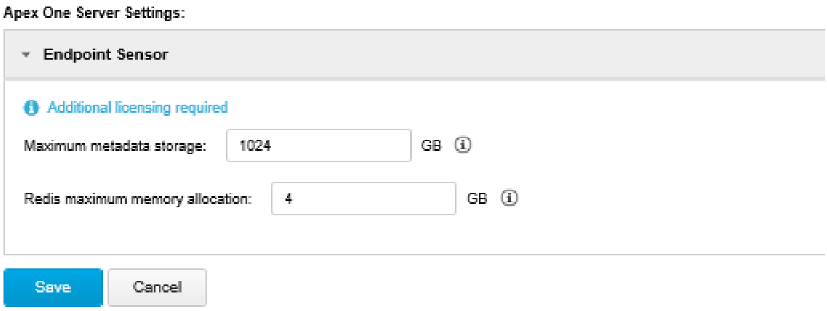
1. Install Apex One with supported OS and SQL version.
2. Install Apex Central.
3. Apex One Endpoint Sensor has individual Activation Code, and Apex Central can activate it from **Administration > License Management > Managed Products**



License Management

☑ Hide expired Activation Codes

4. Deploy Apex One Server policy with enabling Endpoint Sensor.



Apex One Server Settings:

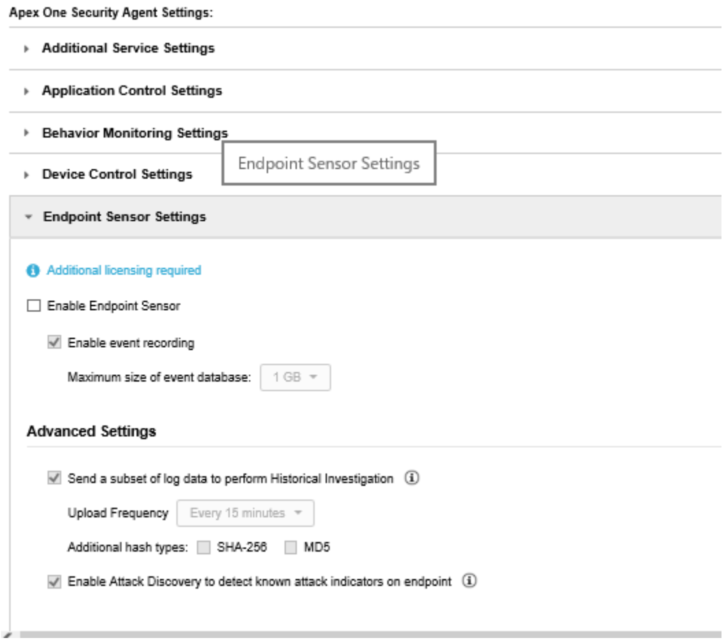
Endpoint Sensor

Additional licensing required

Maximum metadata storage: 1024 GB

Redis maximum memory allocation: 4 GB

5. Deploy Apex One Security Agent policy with enabling Endpoint Sensor.


Additional Service Settings
Application Control Settings
Behavior Monitoring Settings
Device Control Settings
Endpoint Sensor Settings

Apex One Security Agent Settings:

Endpoint Sensor Settings

Additional licensing required

☐ Enable Endpoint Sensor

☑ Enable event recording

Maximum size of event database: 1 GB

Advanced Settings

☑ Send a subset of log data to perform Historical Investigation

Upload Frequency: Every 15 minutes

Additional hash types: ☐ SHA-256 ☐ MD5

☑ Enable Attack Discovery to detect known attack indicators on endpoint

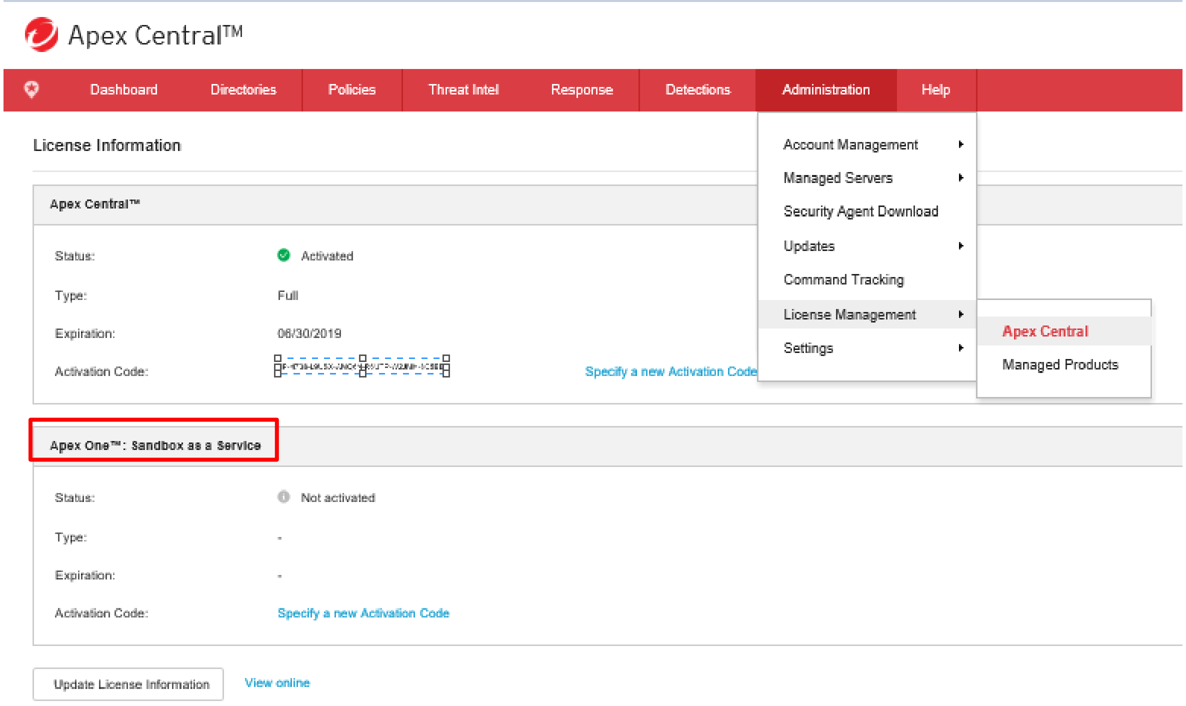
6. Wait until policy is delivered to Apex One server and security agent. After that, iES agent in Apex one agent PC starts collecting following meta data, and Endpoint Sensor function start working.

- ✓ Host (Including host name and IP records)
- ✓ File name and path
- ✓ SHA-1 hash value

- ✓ User account
- ✓ Windows registry (auto-run related)
- ✓ Command lines

2.5 Apex One Sandbox as a Service

Apex Central newly integrates with Apex One Sandbox as a Service. This function needs individual Activation Code, and Apex Central allows to input it from **Administration > License Management > Apex Central**.



License Information

Apex Central™

Status: Activated

Type: Full

Expiration: 06/30/2019

Activation Code: [illegible] Specify a new Activation Code

Apex One™: Sandbox as a Service

Status: Not activated

Type: -

Expiration: -

Activation Code: Specify a new Activation Code

Update License Information View online

2.6 Sizing data

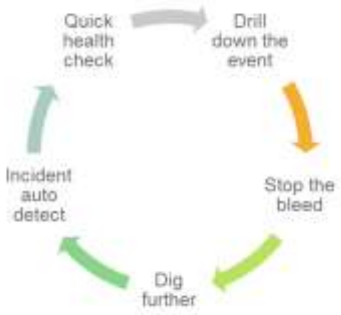
Please refer sizing guide in detail.

- Medium enterprise
  - A single or multiple Apex One/Office Scan 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 Apex One/Office Scan 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 Apex Central with third-party SIEM system

3 Protect your environment

This section describes how to detect your environment

3.1 Protection Steps



0. Set policy

   Please enable necessary functions and add some setting for managed products and endpoints.

1. Quick health check

   Firstly you need to realize malicious events like malware, possible threat, suspicious traffic or unexpected behavior in your environment.

2. Drill down the event

   When you find possible issues, you need to confirm if the event is actual threat or not.

3. Stop the bleed

   When the event is actual threat, you need to stop the threat.

4. Dig further

   After step 3, you need to confirm the threat impact and minimize the threat impact.

5. Incident auto detect

   Based on experience from step 1 to step4, you need to consider how to detect the similar incident automatically.

6. Review and update policy and scheduled investigation.

   To find possible threat earlier and protect your environment well next time, please consider product settings and investigation tasks.

7. Keep Trend Micro product and update components

8. Conduct from step 0 to step 5 continuously.

3.2 Major Functions

Below are the major functions of Apex Central:

0. Set policy (Section 4)

1. Quick health check

   ✓ Notify alert or information by email (SMTP), SNMP, Syslog, Windows event log and Trigger Application Settings.(Section 5)

   ✓ Dashboard can show current threat status

   ✓ Generate report with managed product information (Section 6)

   ✓ Execute malware scan for managed product

2. Drill down the event

   ✓ Collect and query managed product logs (Section 7)

   ✓ Single Sign On for the managed product (Section 8)

3. Stop the bleed

   ✓ Isolate infected PC and recover from isolation, once issue is solved [with Apex One] (Section 9)

4. Dig further

   ✓ Investigate threat in your network [with DDAN or Apex One Sandbox as a Service] (Section 10)

   ✓ Conduct root cause analysis to review the sequence of events (Section 10)

5. Incident auto detect

   ✓ Analyze threat impact for your network regularly [with Apex One Sandbox as a Service] (Section 10)

   ✓ Receive or share suspicious object (SO) between Apex Central and managed product to minimize threat impact (Section 11)

6. Review and update policy and scheduled investigation (Section 2 and Section 10.2.4)

7. Keep Trend Micro product and update components

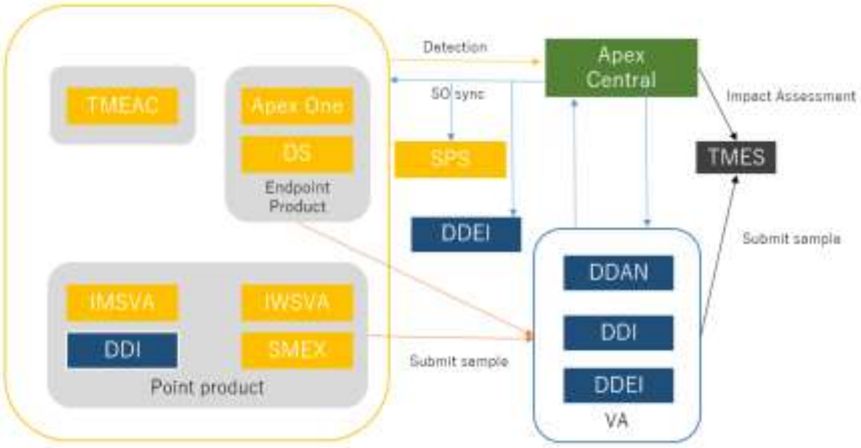
   ✓ Deliver latest pattern and engine (Section 12)

   ✓ Check and update product license status

8. Conduct from step 0 to step 7 continuously.

3.3 Related Trend Micro products

To protect your environment, Apex Central co-work with listed product closely.



- Products in the Virtual Analyzer (VA) group (DDAN, DDI and DDEI) send SOs to Apex Central, also get Exception lists from Apex Central.
- Apex Central and Apex One can newly integrate with internal Endpoint Sensor. Apex Central can also be able to integrate with "Apex One Sandbox as a Service". Trend Micro Endpoint Sensor (TMES) agents submit samples to the Deep Discovery Analyzer (DDAN), and received requests for IOC or SO Impact Assessment from Apex Central as same as TMCM.
- The Endpoint Products, Point Products, and TMEAC get SOs from Apex Central and send back detection information to Apex Central.
- Point and Endpoint Products submit samples for analysis to DDAN.
- Smart Protection Server (SPS) gets SOs from Apex Central
- Deep Discovery Email Inspector (DDEI) gets SOs from Apex Central and also submits samples to DDAN for analysis.

4 Policy Management

This chapter deals with Best Practices for Policy Management. Policy Management is a powerful functionality in Apex Central 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.

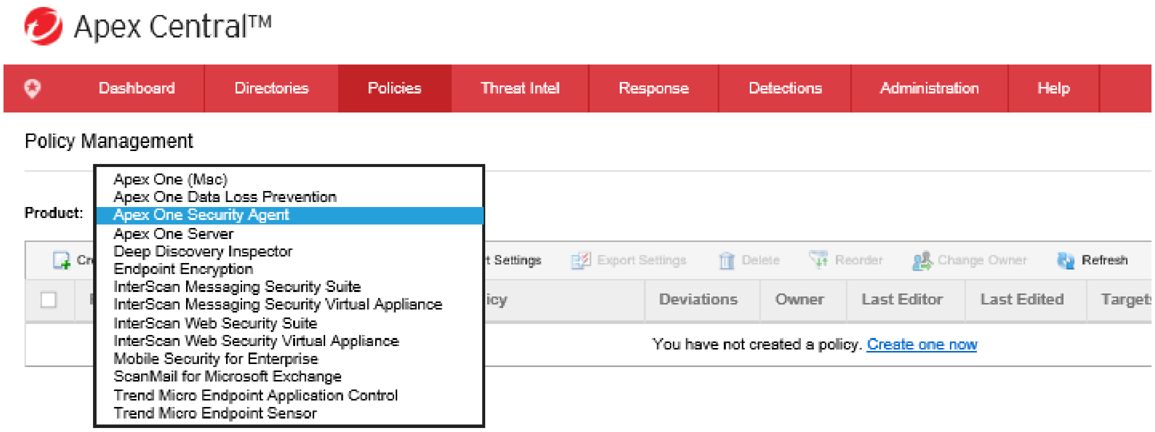
4.1 Planning Policy Management per Product

4.1.1 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 Apex Central console. Just go to **Policies -> Policy Management.**



Policy Management

Product:

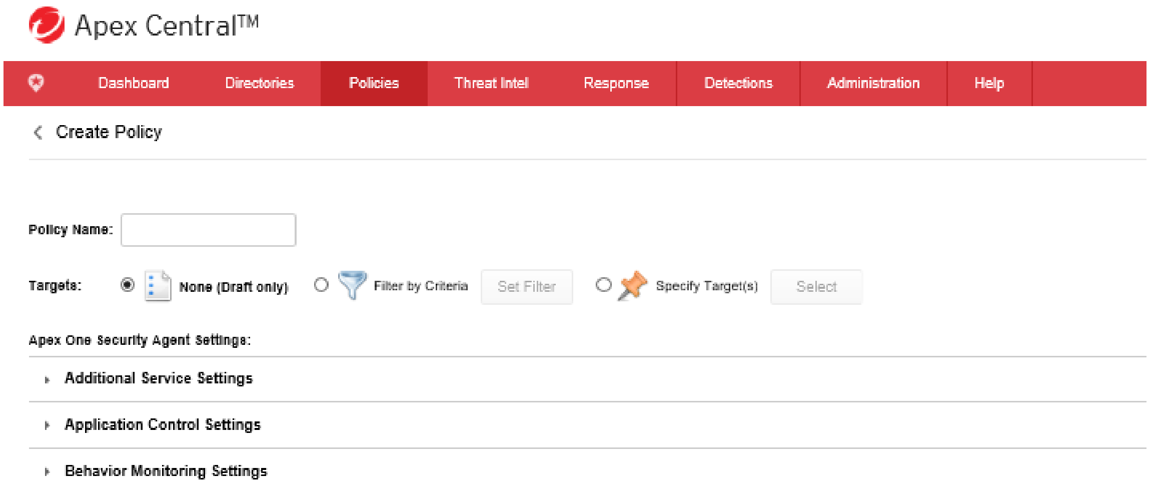
- Apex One (Mac)
- Apex One Data Loss Prevention
- Apex One Security Agent
- Apex One Server
- Deep Discovery Inspector
- Endpoint Encryption
- InterScan Messaging Security Suite
- InterScan Messaging Security Virtual Appliance
- InterScan Web Security Suite
- InterScan Web Security Virtual Appliance
- Mobile Security for Enterprise
- ScanMail for Microsoft Exchange
- Trend Micro Endpoint Application Control
- Trend Micro Endpoint Sensor

You have not created a policy. Create one now

4.1.2 Which settings are available

Please select template from candidates, and click the **Create** button.

This is sample for Apex One Security Agent policy.



Create Policy

Policy Name:

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

Apex One Security Agent Settings:

- Additional Service Settings
- Application Control Settings
- Behavior Monitoring Settings

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.

4.1.3 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.

4.1.4 Planning policy for specific machines (Specified Policy)

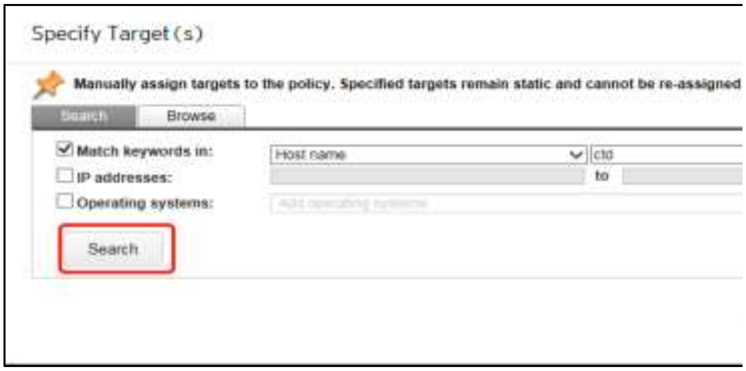
In some situations, customers would want to set a policy only for a specific set of computers. These computers would deviate from the Filtered policy which would normally take effect. Specified Policies are then ideal for these situations.

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 Apex Central 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” Apex Central.



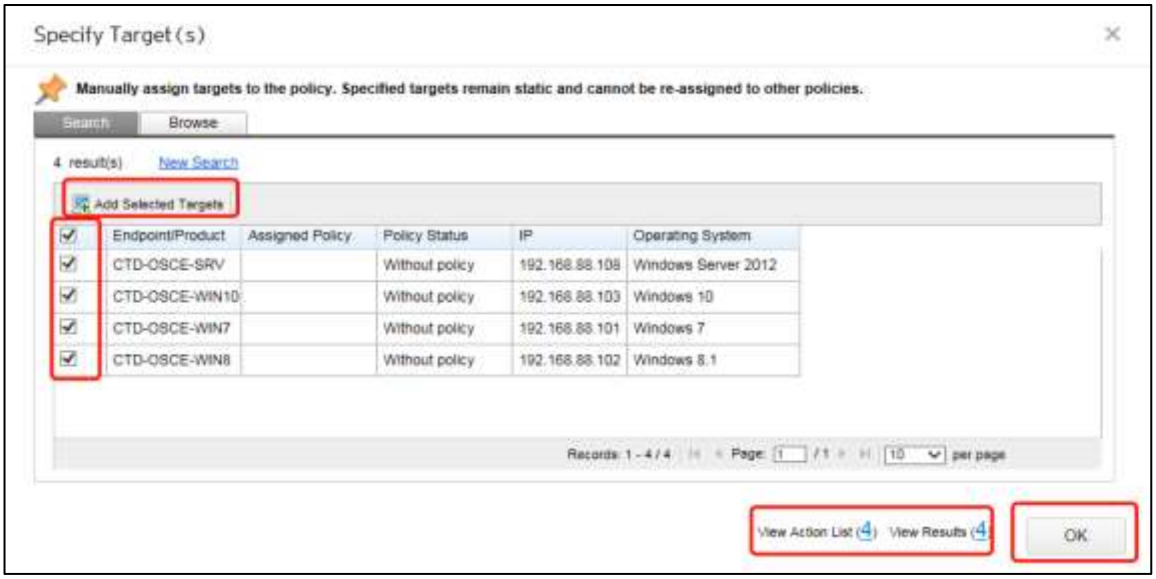
Specify Target(s)

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

☑ Match keywords in: Host name ctd

□ IP addresses: to

□ Operating systems: Add operating systems



Specify Target(s)

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

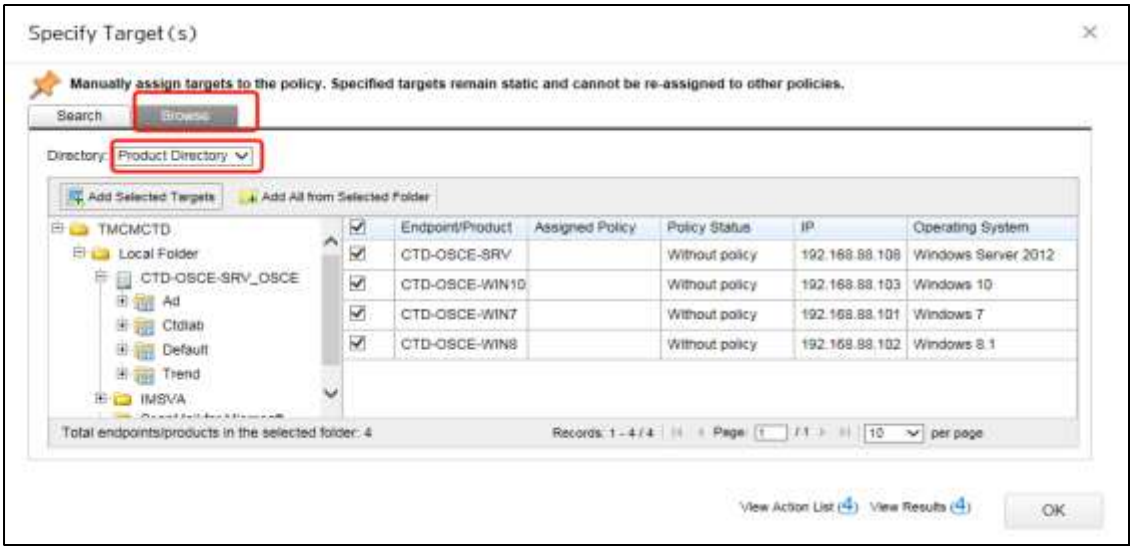
4 result(s) New Search

☑	Endpoint/Product	Assigned Policy	Policy Status	IP	Operating System
☑	CTD-OSCE-SRV		Without policy	192.168.88.108	Windows Server 2012
☑	CTD-OSCE-WIN10		Without policy	192.168.88.103	Windows 10
☑	CTD-OSCE-WIN7		Without policy	192.168.88.101	Windows 7
☑	CTD-OSCE-WIN8		Without policy	192.168.88.102	Windows 8.1

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

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.



Specify Target (s)

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

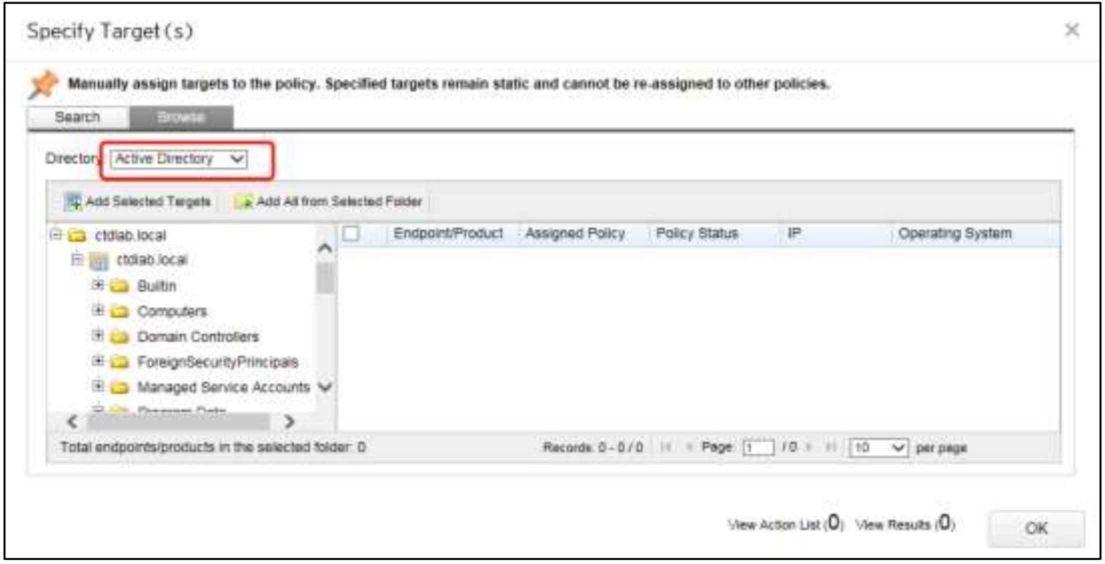
Directory: Product Directory

☑	Endpoint/Product	Assigned Policy	Policy Status	IP	Operating System
☑	CTD-OSCE-SRV		Without policy	192.168.88.108	Windows Server 2012
☑	CTD-OSCE-WIN10		Without policy	192.168.88.103	Windows 10
☑	CTD-OSCE-WIN7		Without policy	192.168.88.101	Windows 7
☑	CTD-OSCE-WIN8		Without policy	192.168.88.102	Windows 8.1

Total endpoints/products in the selected folder: 4

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

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



Specify Target (s)

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

Directory: Active Directory

Add Selected Targets
Add All from Selected Folder
ctdlab.local
ctdlab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts

□	Endpoint/Product	Assigned Policy	Policy Status	IP	Operating System

Total endpoints/products in the selected folder: 0

Records: 0 - 0 / 0 Page: 1 / 0 10 per page

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

Example 1: Enabling hotfix update for Apex One/Office Scan 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 Apex One/Office Scan hotfixes and program upgrades. This allows them to prevent a large amount of network bandwidth.

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

To do this using Specified Policies:

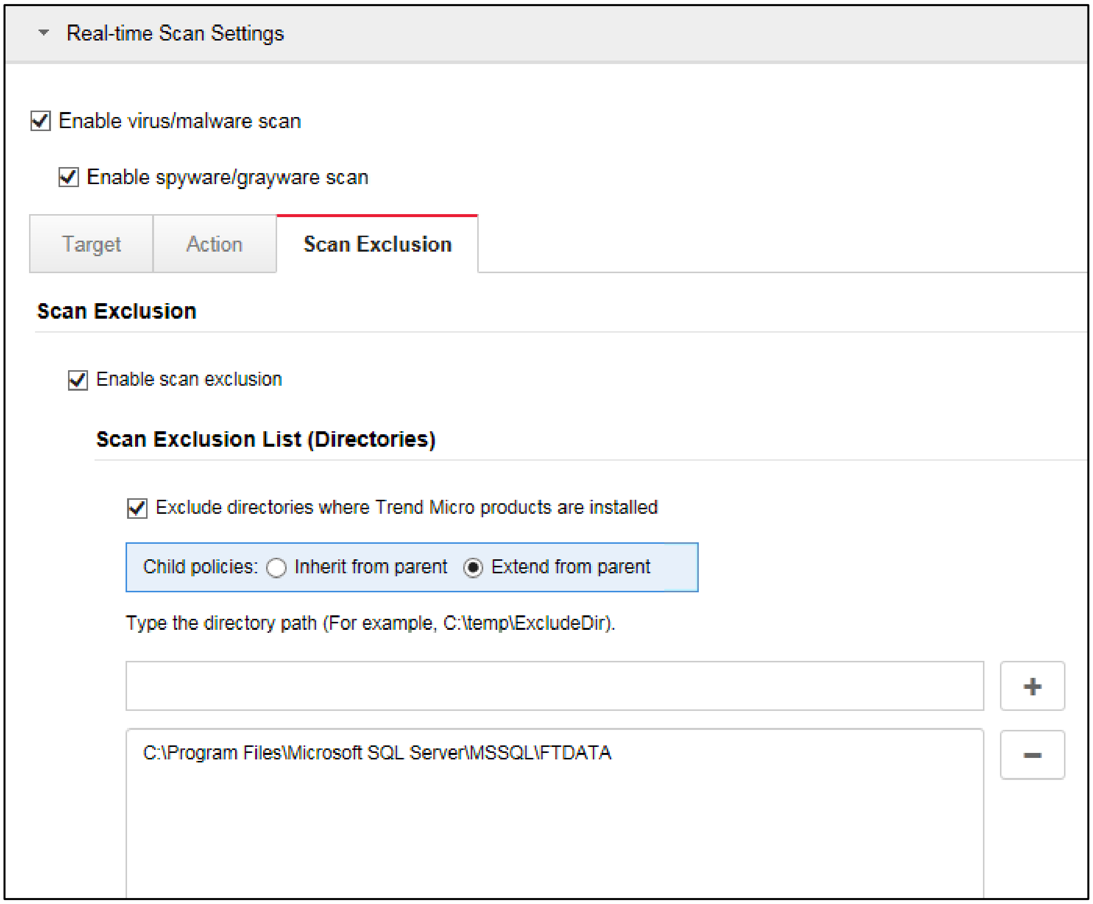
1. Create a copy of the policy you want to modify and set the Target first to **None (Draft only)**. This allows administrators to plan properly the policy, but make sure that it does not apply first.
2. It is now possible to update the setting.
3. After making the changes, it is now possible to set the Target to "Specify Targets" and manually assign the Apex One/Office Scan 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 Apex One/Office Scan clients have finished applying the hotfixes or Service Packs, customer can now check if the Apex One/Office Scan client should be added again to the older specified Policies. This will allow the Apex One/Office Scan clients to restore old policies.
    a. Assign the Apex One/Office Scan clients to "Specified Policies" if they are meant to be under previous "Specified Policies."
    b. The Apex One/Office Scan clients will be sorted into previous Filtered Policies automatically, once the "Specified Policy" is removed.
6. Once all Apex One/Office Scan 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.



Real-time Scan Settings

☑ Enable virus/malware scan

☑ Enable spyware/grayware scan

Scan Exclusion

☑ Enable scan exclusion

Scan Exclusion List (Directories)

☑ Exclude directories where Trend Micro products are installed

Child policies: ○ Inherit from parent ● Extend from parent

Type the directory path (For example, C:\temp\ExcludeDir).

C:\Program Files\Microsoft SQL Server\MSSQL\FTDATA

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.

4.1.5 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 Apex Central 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.

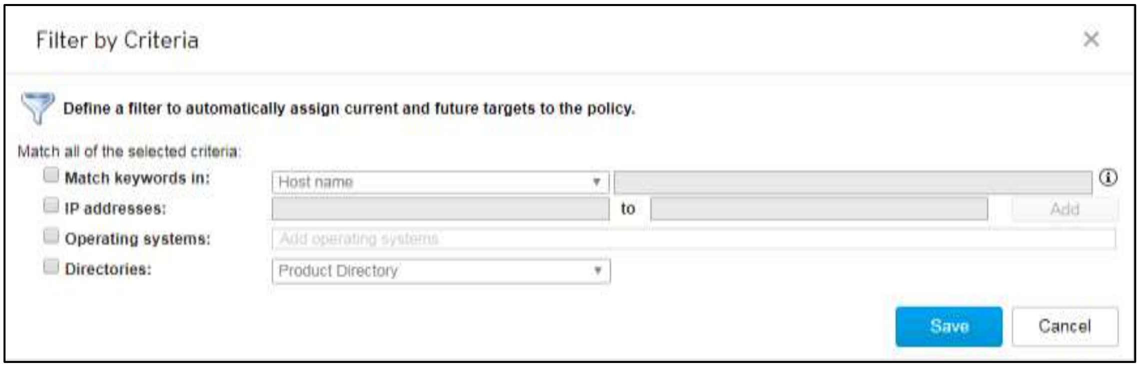
Filtered Policies are ideal for the following scenarios:

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 Apex One/Office Scan client is not yet installed, but once installed, and the criteria matches, the policy is automatically deployed.

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

Understanding the Filters for Filtered Policy

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



Filter by Criteria ×

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

Match all of the selected criteria:

□ Match keywords in: Host name ▾

□ IP addresses: to Add

□ Operating systems: Add operating systems

□ Directories: Product Directory ▾

Save Cancel

Important to note are as follows:

1. When specifying this option, all criteria must match.

2. When a naming convention is available, it is also possible to use the Match keywords in: for Hostname.

3. Tree Paths are also available for Apex One/Office Scan 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.

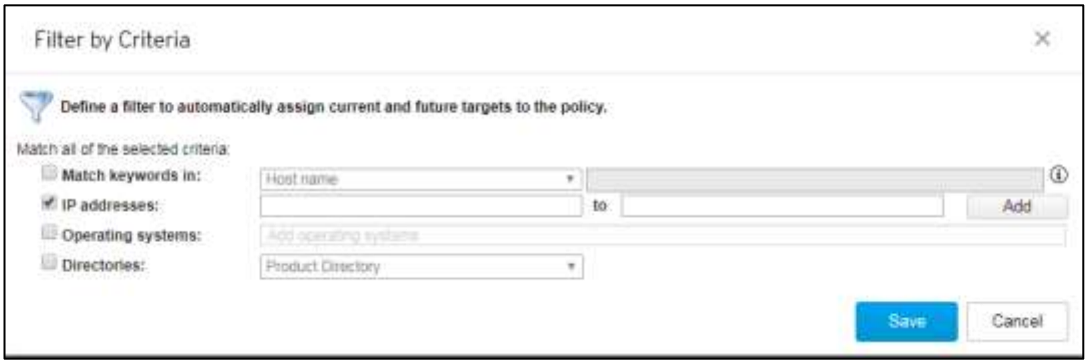
5. Policies can be based on the Product Directory. This allows administrators to define policies for an entire folder within the Apex Central tree.

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 “Apex One/Office Scan 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:



Filter by Criteria

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

Match all of the selected criteria:

☐ Match keywords in: Host name

☑ IP addresses: to

☐ Operating systems: Add operating systems

☐ Directories: Product Directory

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

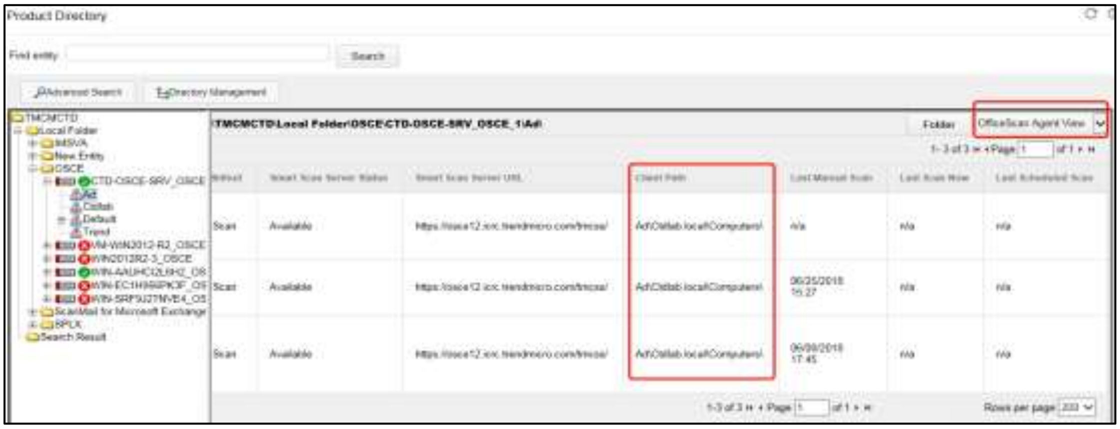
Solution: In this case, the administrators can use the IP addresses criteria to set the criteria to make sure that the Filtered policy applies to the IP address range.

Example 2: Using Apex One/Office Scan Multi-layer domain

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

Solution: Apex Central is only able to display the first layer domain. This is a current limitation of Apex Central. 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:

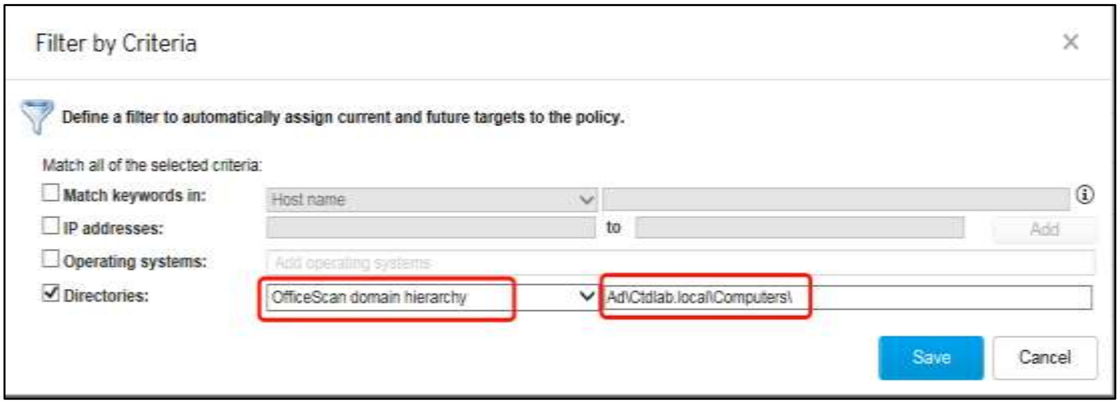
Once "Apex One/Office Scan domain hierarchy" has been specified in Directories, the Client Path of the Apex One/Office Scan client can be seen in the Apex One/Office Scan client view from the Apex Central console.



\TMCMCTD\Local Folder\OSCE\CTD-OSCE-SRV_OSCE_1\Ad\

Method	Smart Scan Server Status	Smart Scan Server URL	Client Path	Last Manual Scan	Last Scan Now	Last Scheduled Scan
Scan	Available	https://osce12.ioc.trendmicro.com/tmcss/	Ad\Ctdlab.local\Computers\	n/a	n/a	n/a
Scan	Available	https://osce12.ioc.trendmicro.com/tmcss/	Ad\Ctdlab.local\Computers\	06/25/2018 15:27	n/a	n/a
Scan	Available	https://osce12.ioc.trendmicro.com/tmcss/	Ad\Ctdlab.local\Computers\	06/08/2018 17:45	n/a	n/a

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.



Filter by Criteria

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

Match all of the selected criteria:

☐ Match keywords in: Host name

☐ IP addresses: to

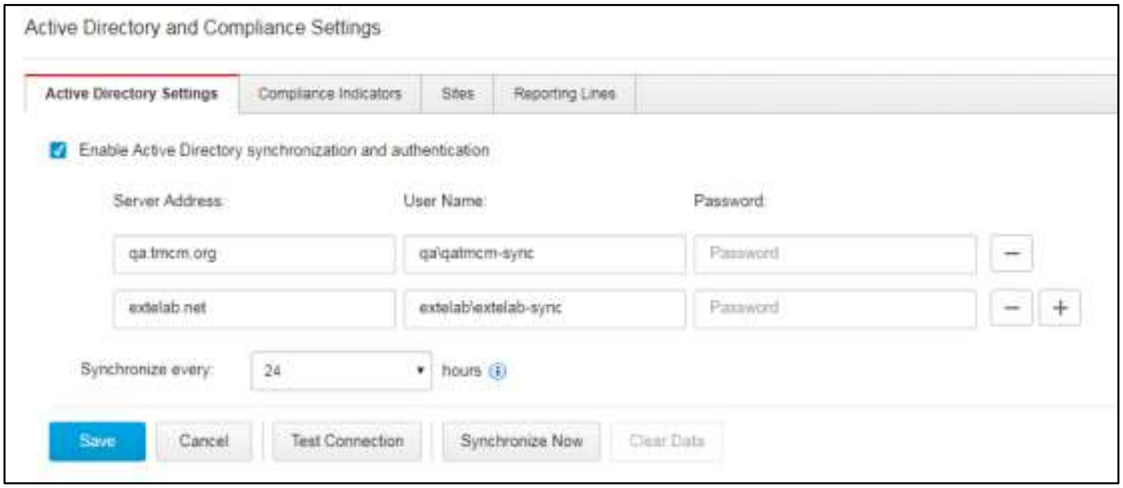
☐ Operating systems: Add operating systems

☑ Directories: OfficeScan domain hierarchy Ad\Ctdlab.local\Computers\

New Apex One/Office Scan 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.

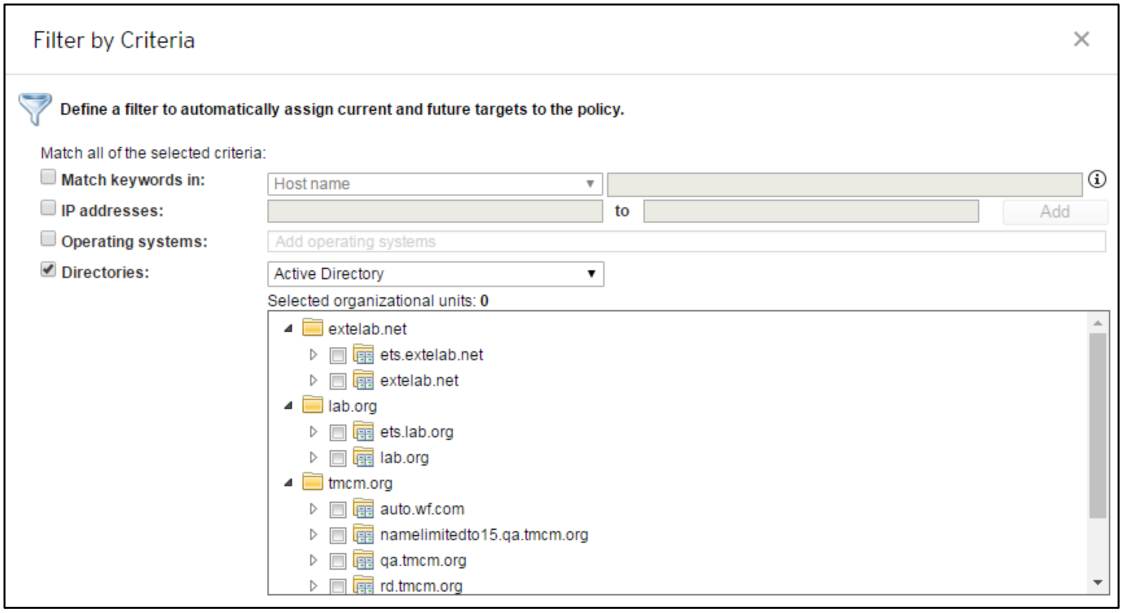


Active Directory and Compliance Settings

☑ Enable Active Directory synchronization and authentication

Server Address:	User Name:	Password:
qa.tmcm.org	qa\qatmcm-sync	Password
extelab.net	extelab\extelab-sync	Password

Synchronize every: 24 hours



Filter by Criteria

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

Match all of the selected criteria:

☐ Match keywords in: Host name

☐ IP addresses: to

☐ Operating systems: Add operating systems

☑ Directories: Active Directory

Selected organizational units: **0**

- extelab.net
  - ☐ ets.extelab.net
  - ☐ extelab.net
- lab.org
  - ☐ ets.lab.org
  - ☐ lab.org
- tmcm.org
  - ☐ auto.wf.com
  - ☐ namelimitedto15.qa.tmcm.org
  - ☐ qa.tmcm.org
  - ☐ rd.tmcm.org

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.

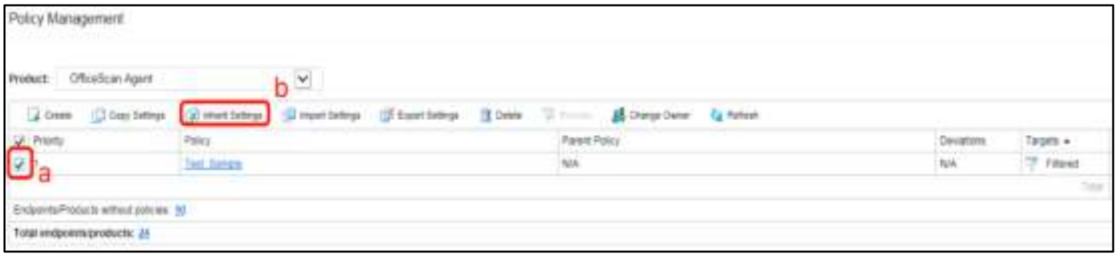
Another thing to note is that any specific policies we create are copies of the Filtered policies. This allows administrators to copy the original settings from old policies, and make minor deviations.

4.2 Central Management and Policy inheritance

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

Our customer can benefit from the Policy inheritance feature. The Policy Inheritance is applicable to Apex One/Office Scan 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 Apex One/Office Scan server and agents.



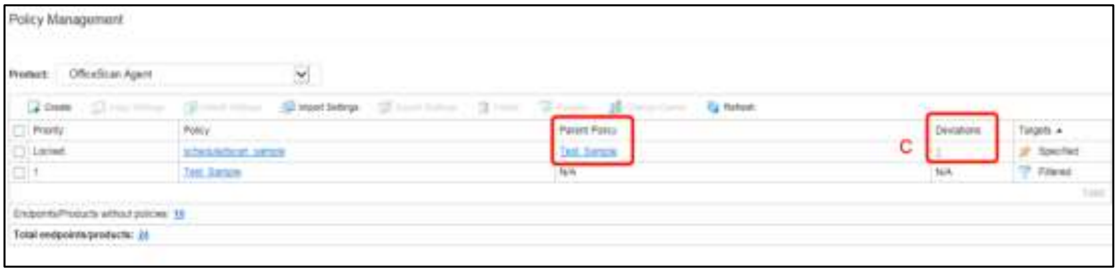
Policy Management

Product: OfficeScan Agent

	Priority	Policy	Parent Policy	Deviations	Targets ▲
☑		Test_Sample	N/A	N/A	Filtered

Endpoints/Products without policies: 10

Total endpoints/products: 24



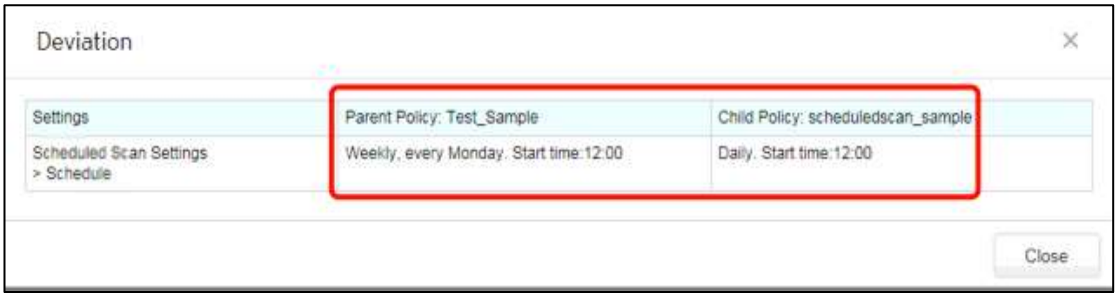
Policy Management

Product: OfficeScan Agent

	Priority	Policy	Parent Policy	Deviations	Targets ▲
□	Locked	scheduledscan_sample	Test_Sample	1	Specified
□	1	Test_Sample	N/A	N/A	Filtered

Endpoints/Products without policies: 18

Total endpoints/products: 24



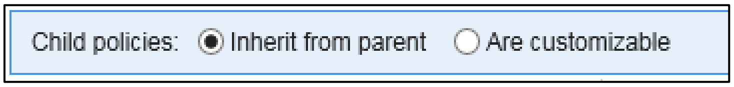
Deviation

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

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

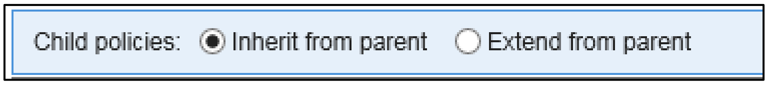
There are three inheritance types:

- Customizable



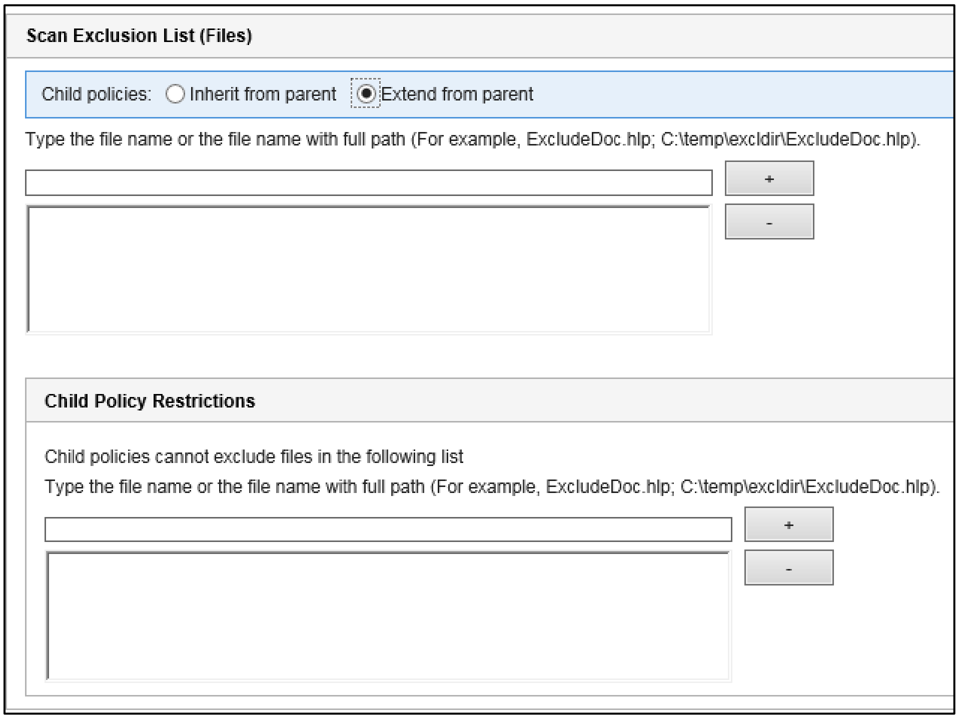
Child policies: ● Inherit from parent ○ Are customizable

- Extend from parent



Child policies: ● Inherit from parent ○ Extend from parent

- Extend from parent + Neutralize List



Scan Exclusion List (Files)

Child policies: ○ Inherit from parent ● Extend from parent

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

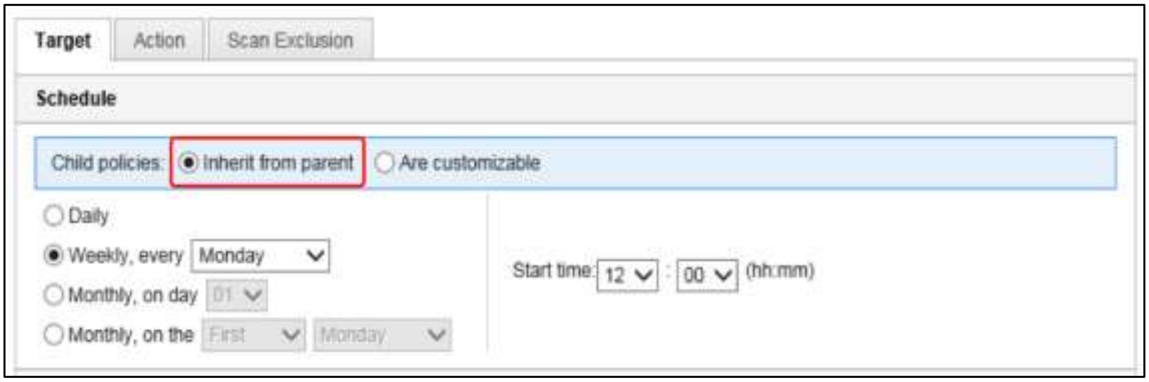
Child Policy Restrictions

Child policies cannot exclude files in the following list

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

Below are things to note per policy type:

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



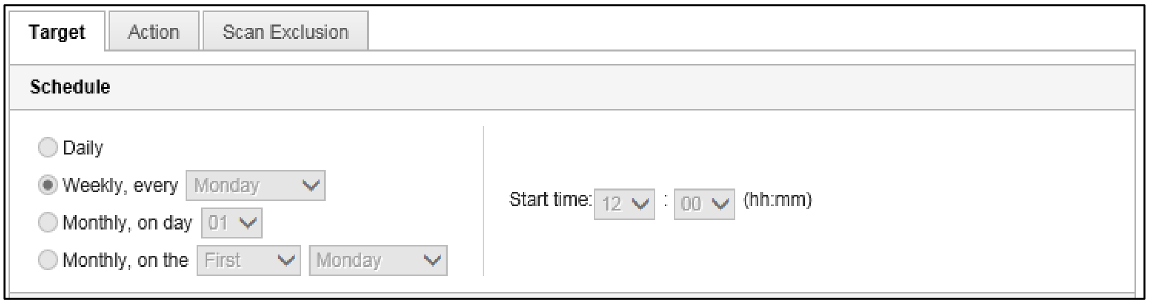
Schedule

Child policies: ● Inherit from parent ○ Are customizable

○ Daily
● Weekly, every Monday
○ Monthly, on day 01
○ Monthly, on the First Monday

Start time: 12 : 00 (hh:mm)

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



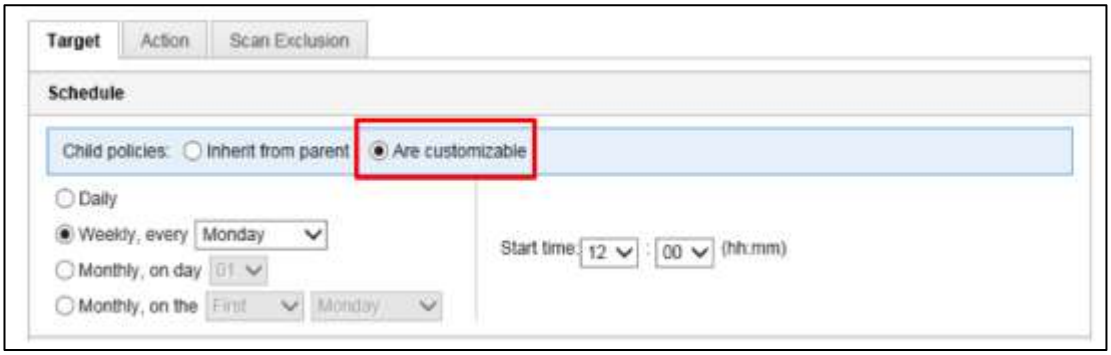
Schedule

○ Daily
● Weekly, every Monday
○ Monthly, on day 01
○ Monthly, on the First Monday

Start time: 12 : 00 (hh:mm)

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

- Parent Policy



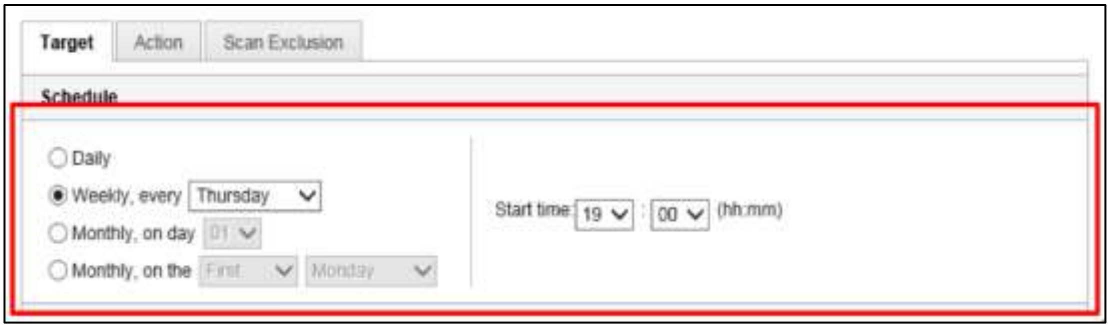
Schedule

Child policies: ○ Inherit from parent ● Are customizable

○ Daily
● Weekly, every Monday
○ Monthly, on day 01
○ Monthly, on the First Monday

Start time 12 : 00 (hh:mm)

- Child Policy

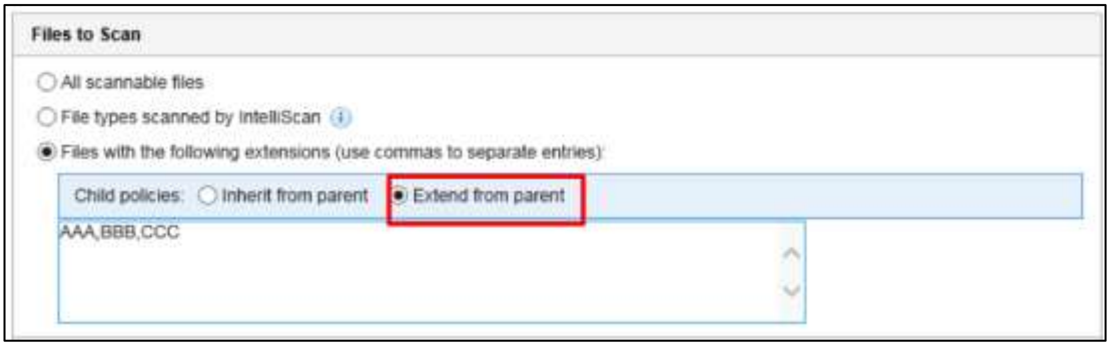


Schedule

○ Daily
● Weekly, every Thursday
○ Monthly, on day 01
○ Monthly, on the First Monday

Start time 19 : 00 (hh:mm)

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



Files to Scan

○ All scannable files

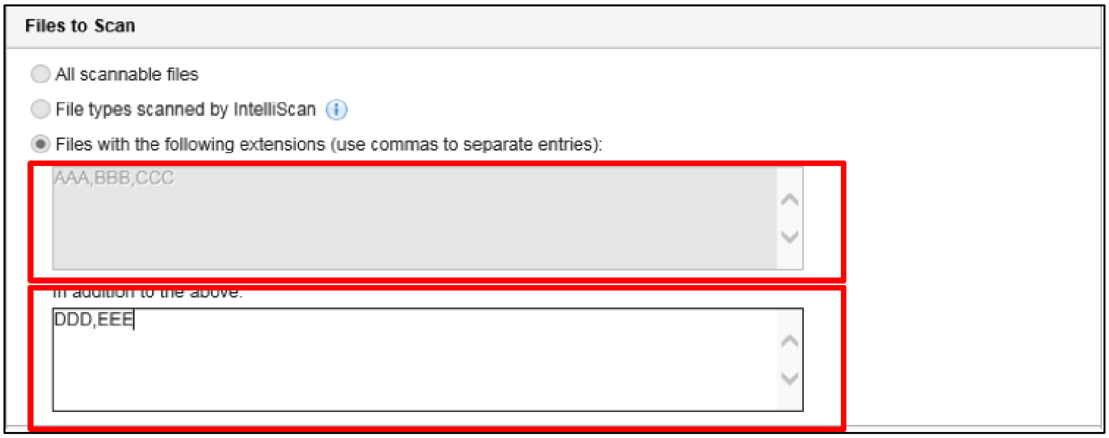
○ File types scanned by IntelliScan

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

Child policies: ○ Inherit from parent ● Extend from parent

AAA,BBB,CCC

  - Child policy



Files to Scan

○ All scannable files

○ File types scanned by IntelliScan

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

AAA,BBB,CCC

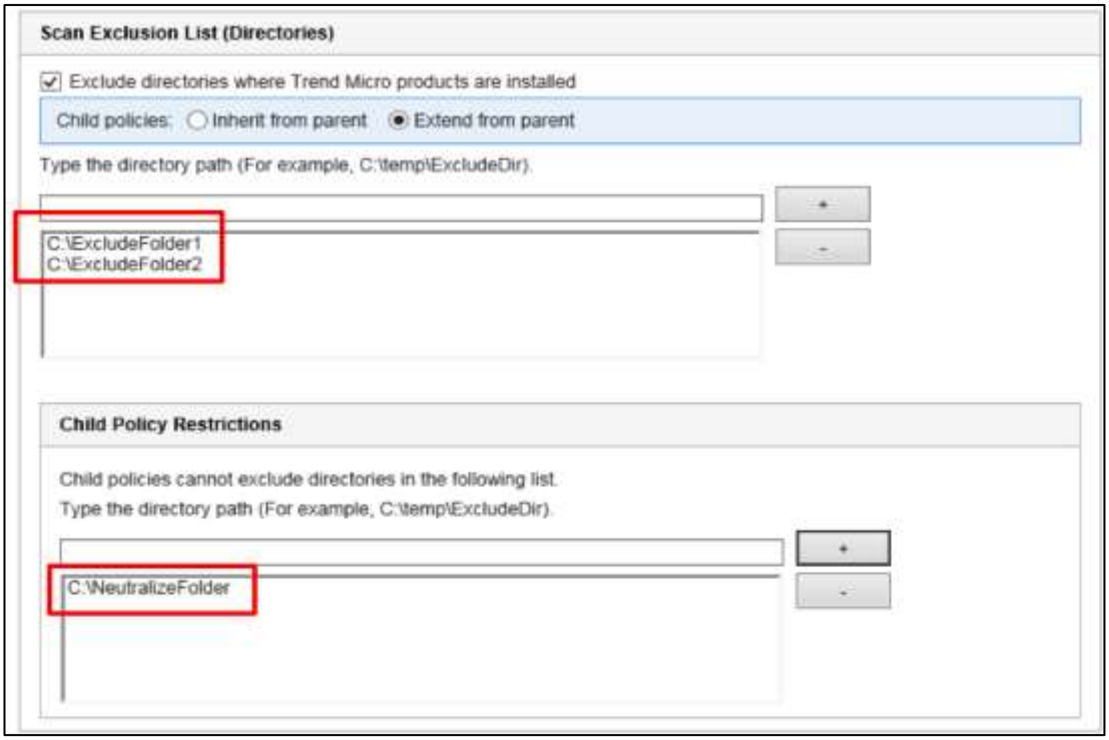
In addition to the above:

DDD,EEE

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

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

  – Parent policy



Scan Exclusion List (Directories)

☑ Exclude directories where Trend Micro products are installed

Child policies: ○ Inherit from parent ● Extend from parent

Type the directory path (For example, C:\temp\ExcludeDir).

C:\ExcludeFolder1
C:\ExcludeFolder2

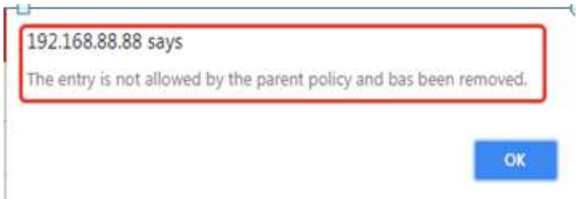
Child Policy Restrictions

Child policies cannot exclude directories in the following list.

Type the directory path (For example, C:\temp\ExcludeDir).

C:\NeutralizeFolder

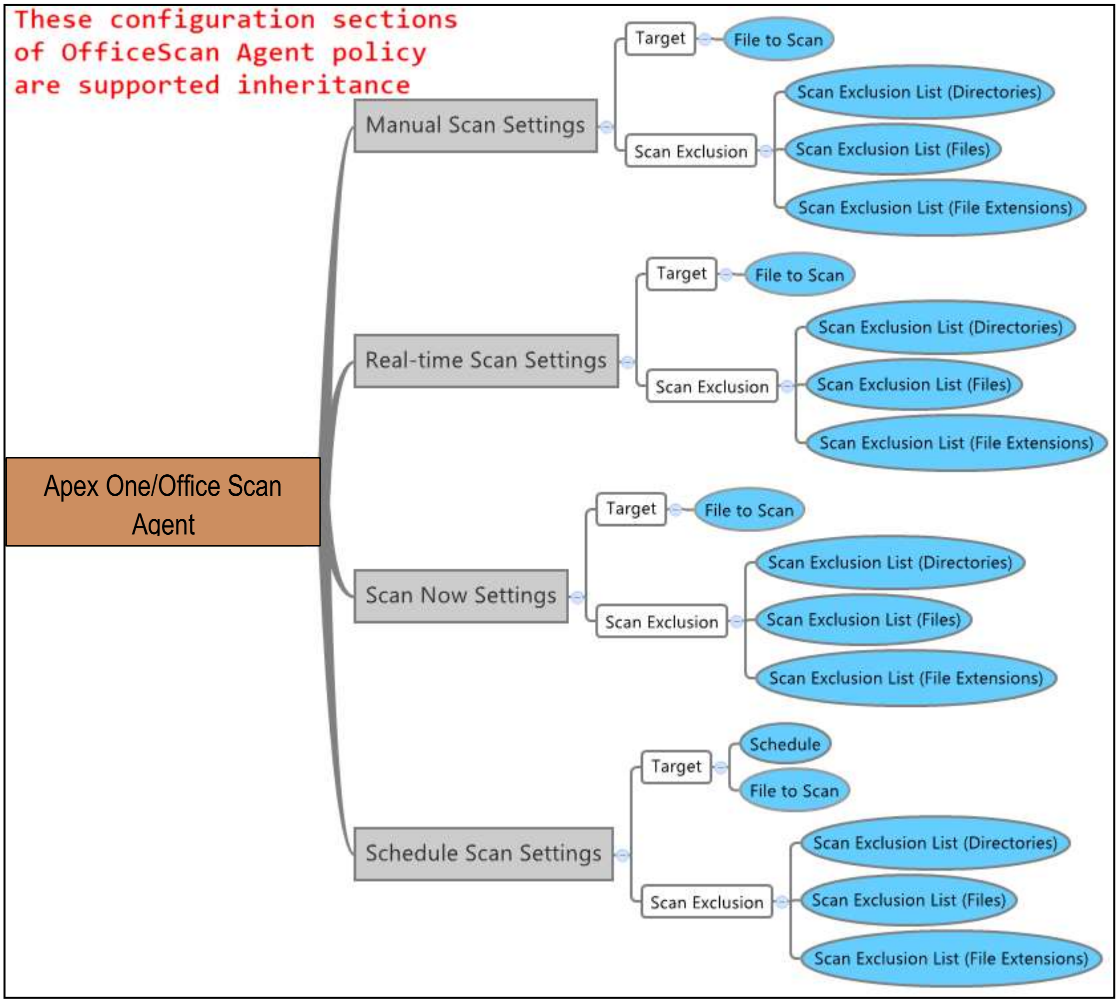
– Child policy



192.168.88.88 says

The entry is not allowed by the parent policy and bas been removed.

Below are the configuration sections of Apex One/Office Scan Agent policies that supports inheritance:



These configuration sections of OfficeScan Agent policy are supported inheritance

Apex One/Office Scan Agent
Manual Scan Settings
Target
File to Scan
Scan Exclusion
Scan Exclusion List (Directories)
Scan Exclusion List (Files)
Scan Exclusion List (File Extensions)
Real-time Scan Settings
Target
File to Scan
Scan Exclusion
Scan Exclusion List (Directories)
Scan Exclusion List (Files)
Scan Exclusion List (File Extensions)
Scan Now Settings
Target
File to Scan
Scan Exclusion
Scan Exclusion List (Directories)
Scan Exclusion List (Files)
Scan Exclusion List (File Extensions)
Schedule Scan Settings
Target
Schedule
File to Scan
Scan Exclusion
Scan Exclusion List (Directories)
Scan Exclusion List (Files)
Scan Exclusion List (File Extensions)

4.3 Effects of removing Policies

When a policy is removed, Apex Central 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.

4.4 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

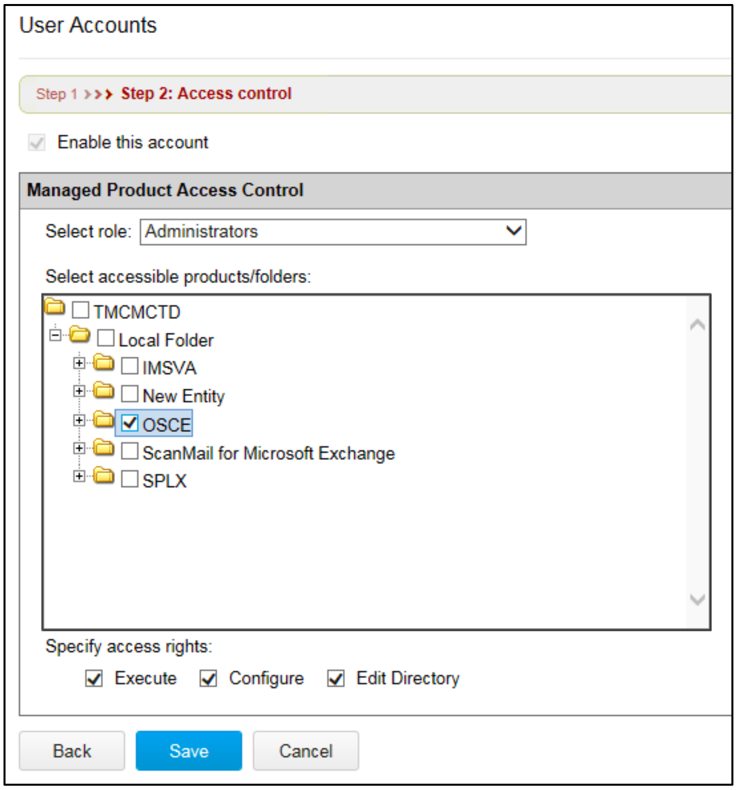
It is worth noting that the Policy can only cover endpoints where the Apex Central user has access. As such, it becomes important also to plan who will create the Policy.

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 Apex Central 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¥ApexCentralADM" only has access to the entity under the "Apex One/Office Scan" folder. The user will not be able to apply any policy to entities or endpoints under the other folders.



User Accounts

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

☑ Enable this account

Managed Product Access Control

Select role: Administrators

Select accessible products/folders:

- □ TMCMCTD
- □ Local Folder
  - □ IMSVA
  - □ New Entity
  - ☑ OSCE
  - □ ScanMail for Microsoft Exchange
  - □ SPLX

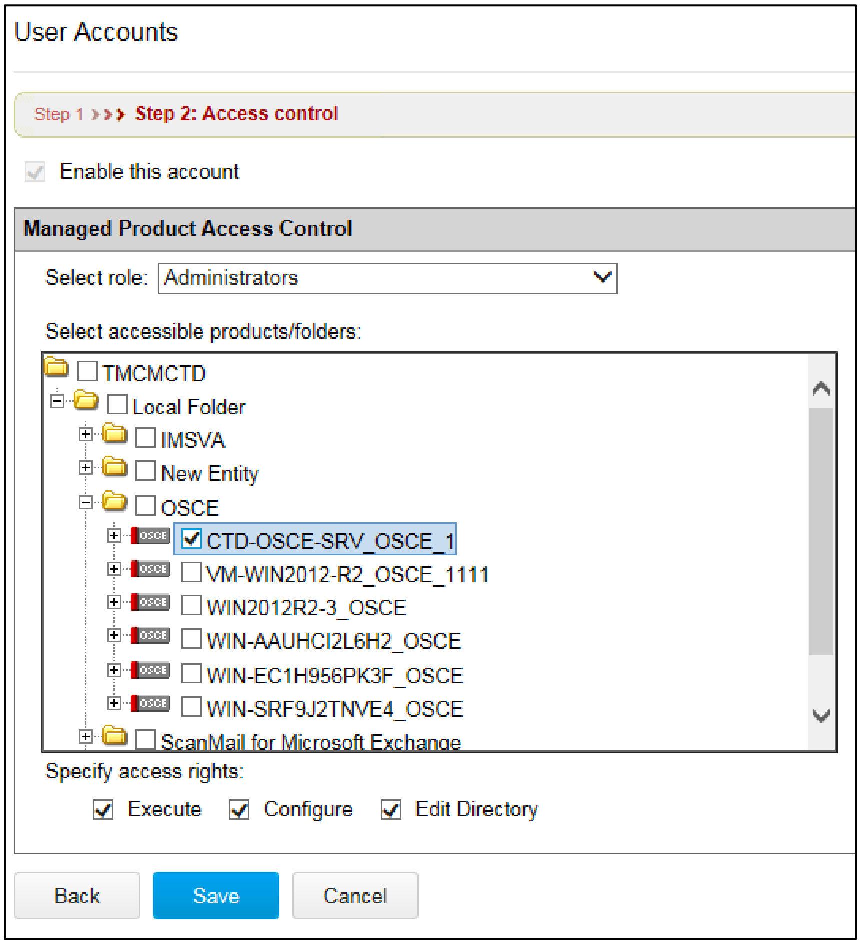
Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

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-Apex One/Office Scan-SRV_Apex One/Office Scan_1. Because of this, the account is only able to apply policies to the CTD-Apex One/Office Scan-SRV_Apex One/Office Scan_1.



User Accounts

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

☑ Enable this account

Managed Product Access Control

Select role: Administrators

Select accessible products/folders:

- □ TMCMCTD
- □ Local Folder
  - □ IMSVA
  - □ New Entity
  - □ OSCE
    - ☑ CTD-OSCE-SRV_OSCE_1
    - □ VM-WIN2012-R2_OSCE_1111
    - □ WIN2012R2-3_OSCE
    - □ WIN-AAUHCI2L6H2_OSCE
    - □ WIN-EC1H956PK3F_OSCE
    - □ WIN-SRF9J2TNVE4_OSCE
  - □ ScanMail for Microsoft Exchange

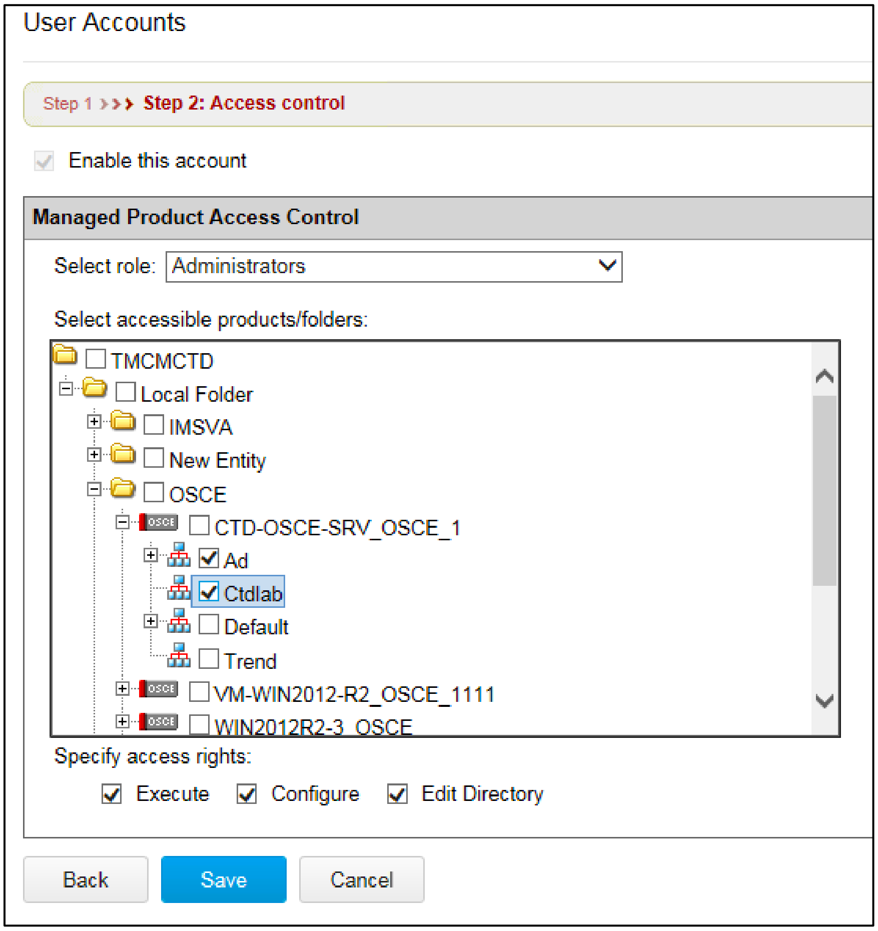
Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

Scenario 3: Security Coverage based on Apex One/Office Scan Subdomains

Administrators may also create policies that are based on Apex One/Office Scan domains.

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



User Accounts

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

☑ Enable this account

Managed Product Access Control

Select role: Administrators

Select accessible products/folders:

- □ TMCMCTD
  - □ Local Folder
    - □ IMSVA
    - □ New Entity
    - □ OSCE
      - □ CTD-OSCE-SRV_OSCE_1
        - ☑ Ad
        - ☑ Ctdlab
        - □ Default
        - □ Trend
      - □ VM-WIN2012-R2_OSCE_1111
      - □ WIN2012R2-3_OSCE

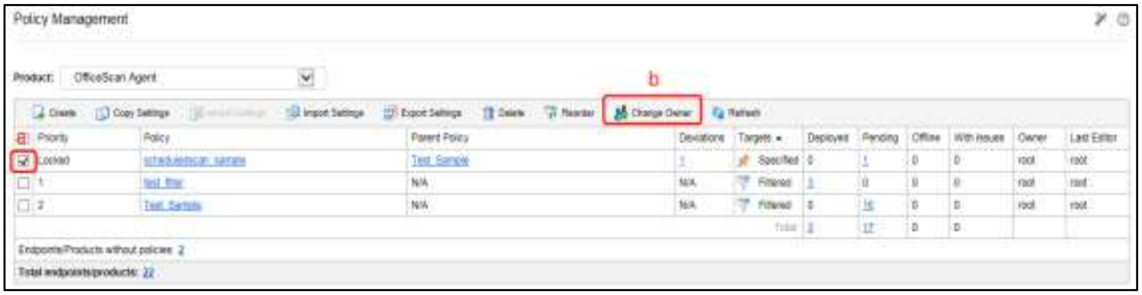
Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

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".



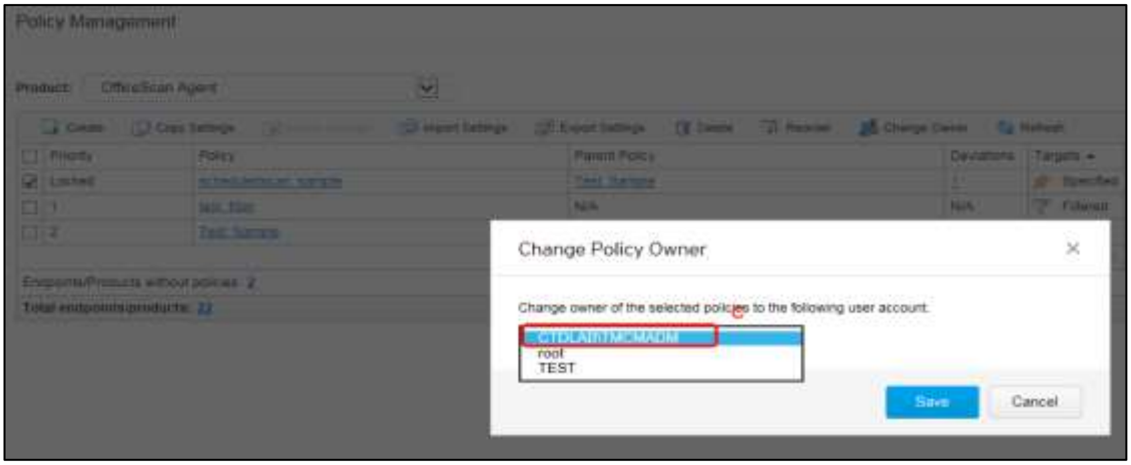
Policy Management

Product: OfficeScan Agent

	Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With issues	Owner	Last Editor
☑	Locked	scheduledscan_sample	Test_Sample	1	Specified	0	1	0	0	root	root
□	1	test_filter	N/A	N/A	Filtered	1	0	0	0	root	root
□	2	Test_Sample	N/A	N/A	Filtered	0	16	0	0	root	root
					Total	1	17	0	0		

Endpoints/Products without policies: 2

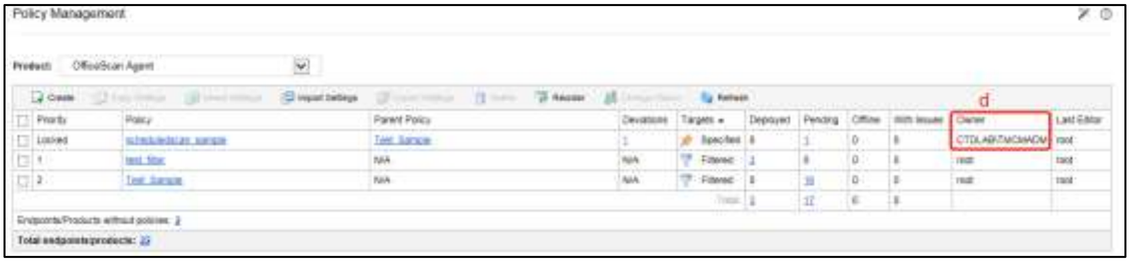
Total endpoints/products: 22



Change Policy Owner

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

CTDLAB\TMCMADM
root
TEST



Policy Management

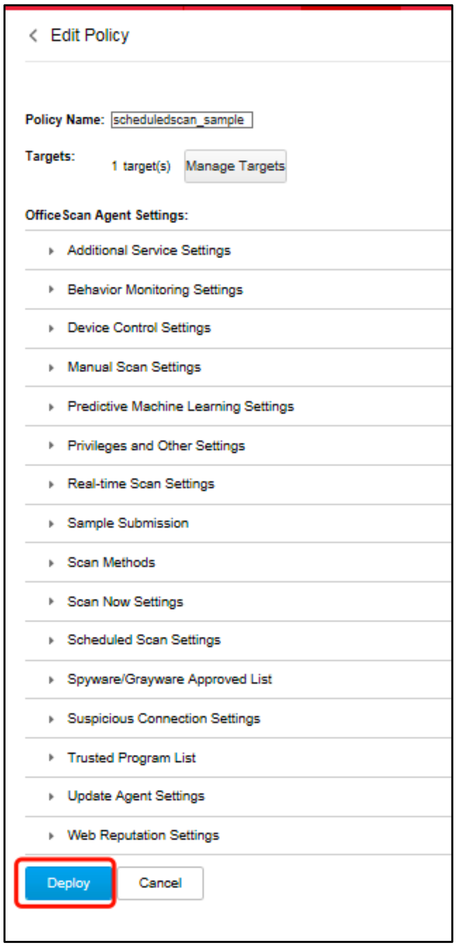
Product: OfficeScan Agent

	Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With issues	Owner	Last Editor
□	Locked	scheduledscan_sample	Test_Sample	1	Specified	0	1	0	0	CTDLAB\TMCMADM	root
□	1	test_filter	N/A	N/A	Filtered	1	0	0	0	root	root
□	2	Test_Sample	N/A	N/A	Filtered	0	16	0	0	root	root
					Total	1	17	0	0		

Endpoints/Products without policies: 2

Total endpoints/products: 22

Here is an admin whose account is “CTDLAB¥admin1” belongs to this AD group. When they login to the Apex Central web console with this account “CTDLAB¥admin1”, he is able to edit this policy “scheduledscan_sample”.



< Edit Policy

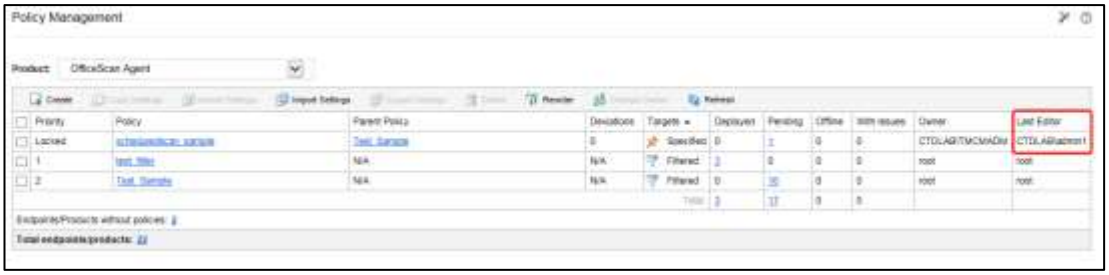
Policy Name: scheduledscan_sample

Targets: 1 target(s) Manage Targets

OfficeScan Agent Settings:

- Additional Service Settings
- Behavior Monitoring Settings
- Device Control Settings
- Manual Scan Settings
- Predictive Machine Learning Settings
- Privileges and Other Settings
- Real-time Scan Settings
- Sample Submission
- Scan Methods
- Scan Now Settings
- Scheduled Scan Settings
- Spyware/Grayware Approved List
- Suspicious Connection Settings
- Trusted Program List
- Update Agent Settings
- Web Reputation Settings

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



Policy Management

Product: OfficeScan Agent

□	Priority	Policy	Parent Policy	Deviations	Targets	Deployed	Pending	Offline	With issues	Owner	Last Editor
□	Locked	scheduledscan_sample	Test_Sample	0	Specified	0	1	0	0	CTDLAB\TMCMADM	CTDLAB\admin1
□	1	test_filter	N/A	N/A	Filtered	1	0	0	0	root	root
□	2	Test_Sample	N/A	N/A	Filtered	0	16	0	0	root	root
					Total	1	17	0	0		

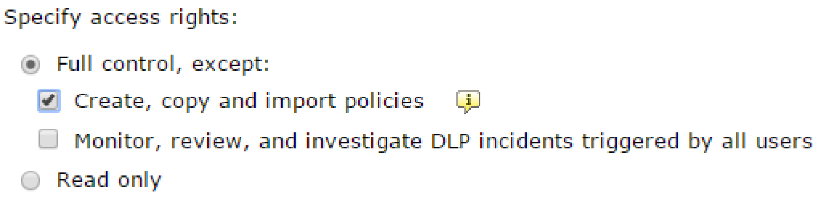
Endpoints/Products without policies: 1

Total endpoints/products: 22

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

The user can’t perform “Change Owner” operation if:

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



Specify access rights:

● Full control, except:

☑ Create, copy and import policies

☐ Monitor, review, and investigate DLP incidents triggered by all users

○ Read only

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

4.5 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 Apex Central to Apex One/Office Scan based on the user accounts.

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

First, the customer needs to integrate Apex Central server with AD.

Second, the Apex One/Office Scan server needs to be registered to Apex Central server.

Third, we can select the endpoint and configure the AD account, device permission from Apex Central web console and deploy the policy to the Apex One/Office Scan agent.

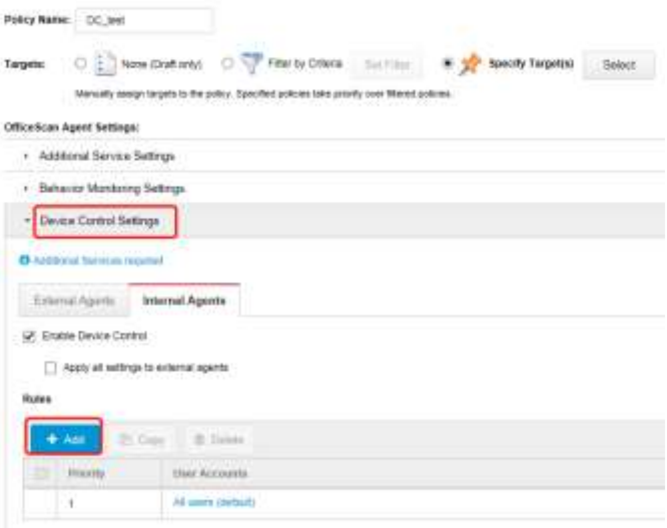
Finally, the users will get different device permissions base on which account they logon to the Windows OS with.

Policy deployment:

a. Select the target AD user

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

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



Policy Name: DC_test

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

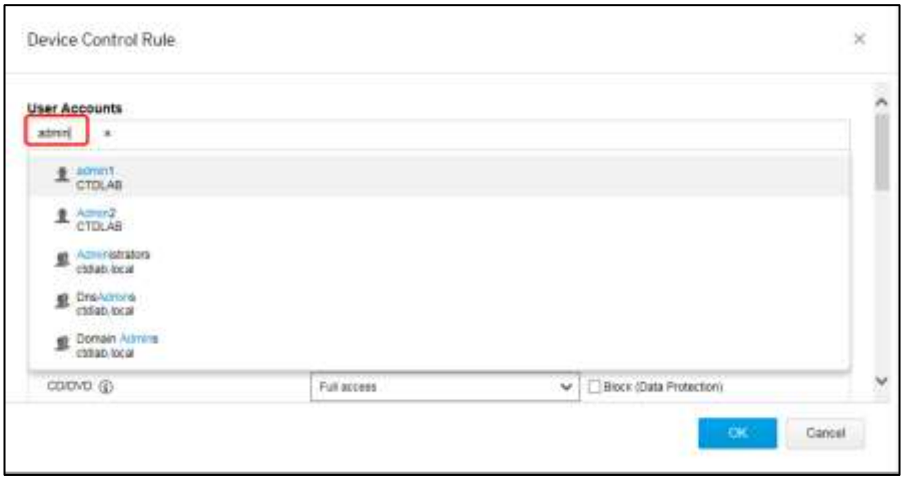
Manually assign targets to the policy. Specified policies take priority over filtered policies.

OfficeScan Agent Settings:

☑ Enable Device Control

□ Apply all settings to external agents

	Priority	User Accounts
	1	All users (default)



Device Control Rule

User Accounts

admin|

admin1 CTDLAB

Admin2 CTDLAB

Administrators ctdlab.local

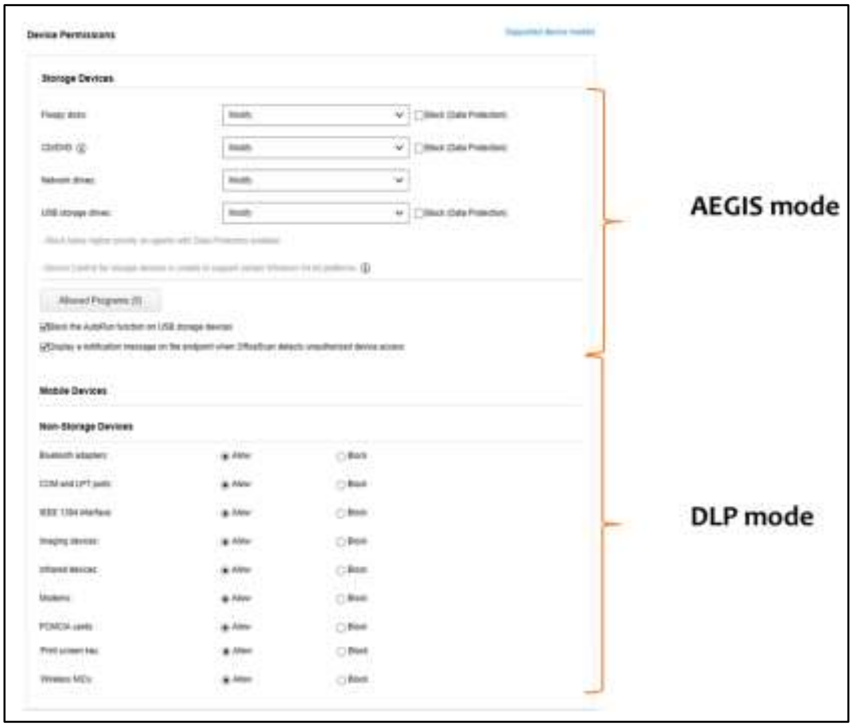
DnsAdmins ctdlab.local

Domain Admins ctdlab.local

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

b. Configure the Device Control permission

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



Device Permissions

Supported device models

Storage Devices

Floppy disks:	Modify	□ Block (Data Protection)
CD/DVD:	Modify	□ Block (Data Protection)
Network drives:	Modify	
USB storage drives:	Modify	□ Block (Data Protection)

Allowed Programs (0)

☑ Block the AutoRun function on USB storage devices

☑ Display a notification message on the endpoint when OfficeScan detects unauthorized device access

Mobile Devices

Non-Storage Devices

Bluetooth adapters:	● Allow	○ Block
COM and LPT ports:	● Allow	○ Block
IEEE 1394 interface:	● Allow	○ Block
Imaging devices:	● Allow	○ Block
Infrared devices:	● Allow	○ Block
Modems:	● Allow	○ Block
PCMCIA cards:	● Allow	○ Block
Print screen key:	● Allow	○ Block
Wireless NICs:	● Allow	○ Block

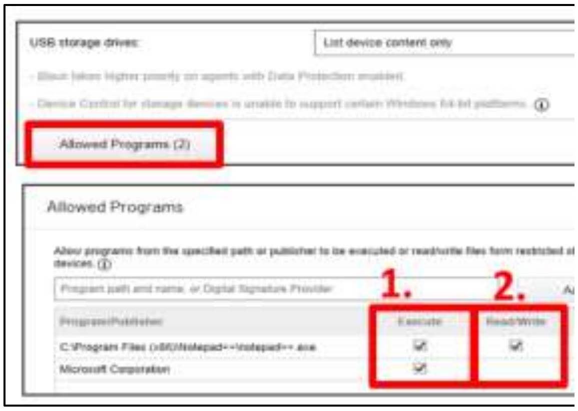
c. Configure the Device Control exception list

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.



USB storage drives: List device content only

- Block takes higher priority on agents with Data Protection enabled.
- Device Control for storage devices is unable to support certain Windows 64-bit platforms.

Allowed Programs (2)

Allowed Programs

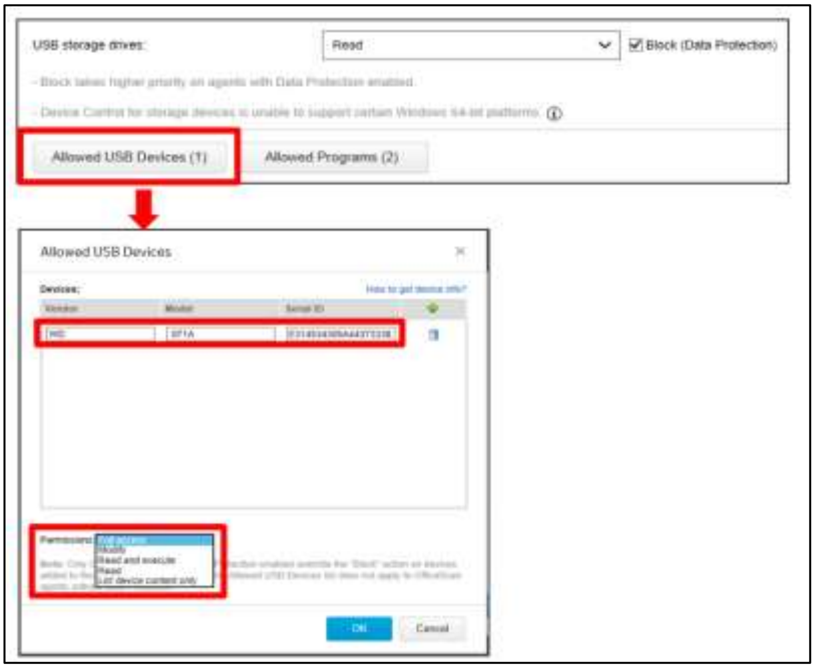
Allow programs from the specified path or publisher to be executed or read/write files form restricted st devices.

Program path and name, or Digital Signature Provider

Program/Publisher	Execute	Read/Write
C:\Program Files (x86)\Notepad++\notepad++.exe	☑	☑
Microsoft Corporation	☑	

- 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.



USB storage drives: Read ☑ Block (Data Protection)

- Block takes higher priority on agents with Data Protection enabled.
- Device Control for storage devices is unable to support certain Windows 64-bit platforms.

Allowed USB Devices (1) Allowed Programs (2)

Allowed USB Devices

Devices: How to get device info?

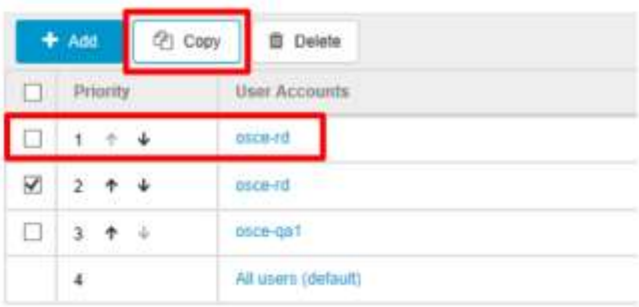
Vendor	Model	Serial ID
WD	0F1A	[illegible]

Permissions: Full access / Modify / Read and execute / Read / List device content only

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.

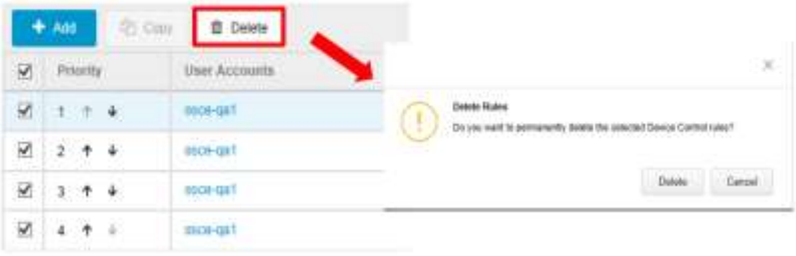


□	Priority	User Accounts
□	1 ↑ ↓	osce-rd
☑	2 ↑ ↓	osce-rd
□	3 ↑ ↓	osce-qa1
	4	All users (default)

- Delete

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

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



☑	Priority	User Accounts
☑	1 ↑ ↓	osce-qa1
☑	2 ↑ ↓	osce-qa1
☑	3 ↑ ↓	osce-qa1
☑	4 ↑ ↓	osce-qa1

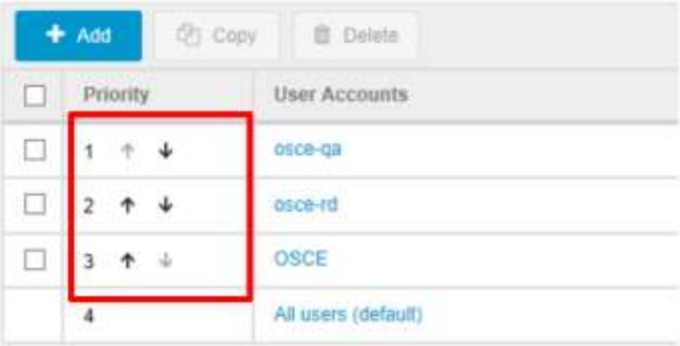
Delete Rules

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

- Adjust priority

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

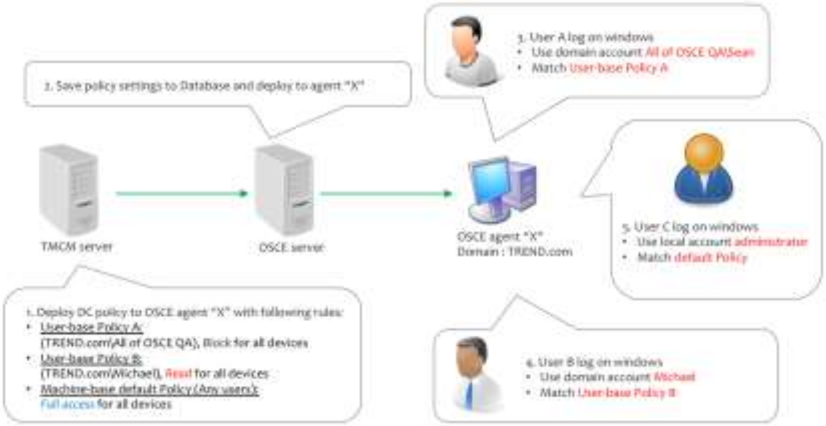
  The higher priority of the policy rule will override the lower policy if the same users are in the different policy rules.



□	Priority	User Accounts
□	1 ↑ ↓	osce-qa
□	2 ↑ ↓	osce-rd
□	3 ↑ ↓	OSCE
	4	All users (default)

e. Policy matching:

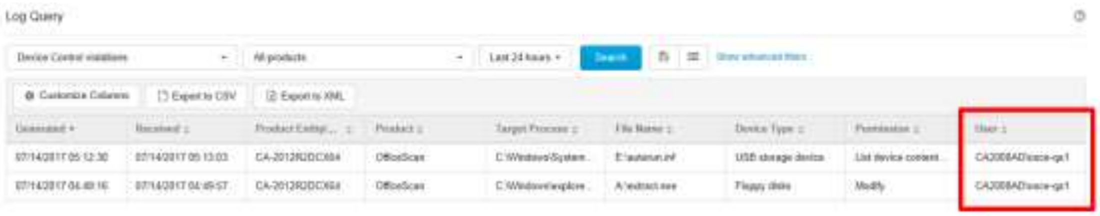
Here is an example workflow for policy matching.


2. Save policy settings to Database and deploy to agent "X"
3. User A log on windows
• Use domain account All of OSCE QA\Sean
• Match User-base Policy A
TMCM server
OSCE server
OSCE agent "X"
Domain : TREND.com
5. User C log on windows
• Use local account administrator
• Match default Policy
1. Deploy DC policy to OSCE agent "X" with following rules:
• User-base Policy A:
(TREND.com\All of OSCE QA), Block for all devices
• User-base Policy B:
(TREND.com\Michael), Read for all devices
• Machine-base default Policy (Any users):
Full access for all devices
4. User B log on windows
• Use domain account Michael
• Match User-base Policy B

f. Check the violation log

The domain user info will be recorded in the violation log on Apex Central's web console.

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



Generated	Received	Product Entity/...	Product	Target Process	File Name	Device Type	Permission	User
07/14/2017 05:12:30	07/14/2017 05:13:03	CA-2012R2DC604	OfficeScan	C:\Windows\System...	E:\autorun.inf	USB storage device	List device content...	CA2008AD\osce-qa1
07/14/2017 04:49:16	07/14/2017 04:49:57	CA-2012R2DC604	OfficeScan	C:\Windows\explore...	A:\extract.exe	Floppy disks	Modify	CA2008AD\osce-qa1

4.6 Apex One Endpoint Sensor

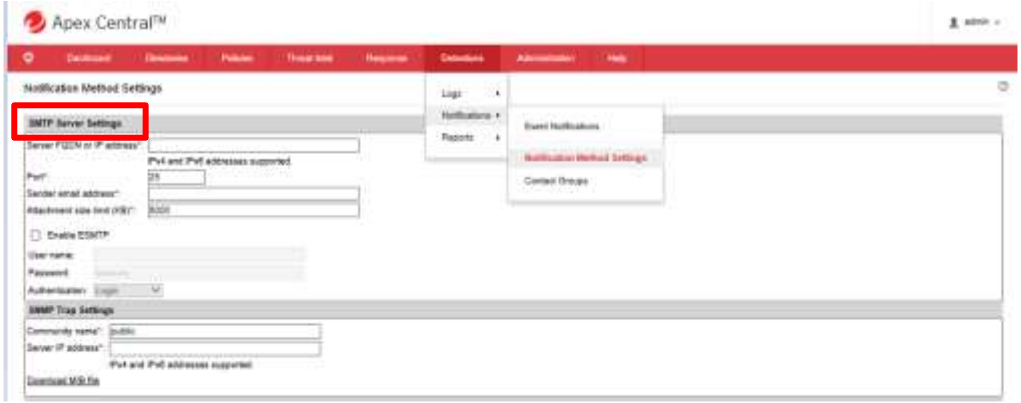
Apex Central newly integrates with Apex One Endpoint Sensor for Endpoint Detection Response. (EDR). Please refer Section 2.4.

5. Notify alert or information by email (SMTP), SNMP, Syslog, Windows event log and Trigger Application Settings.

5.1 Event Notifications

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

a. Configure the SMTP Server Settings.



Notification Method Settings

SMTP Server Settings

Server FQDN or IP address*:

IPv4 and IPv6 addresses supported.

Port*: 25

Sender email address*:

Attachment size limit (KB)*: 5000

□ Enable ESMTP

User name:

Password:

Authentication: Login

SNMP Trap Settings

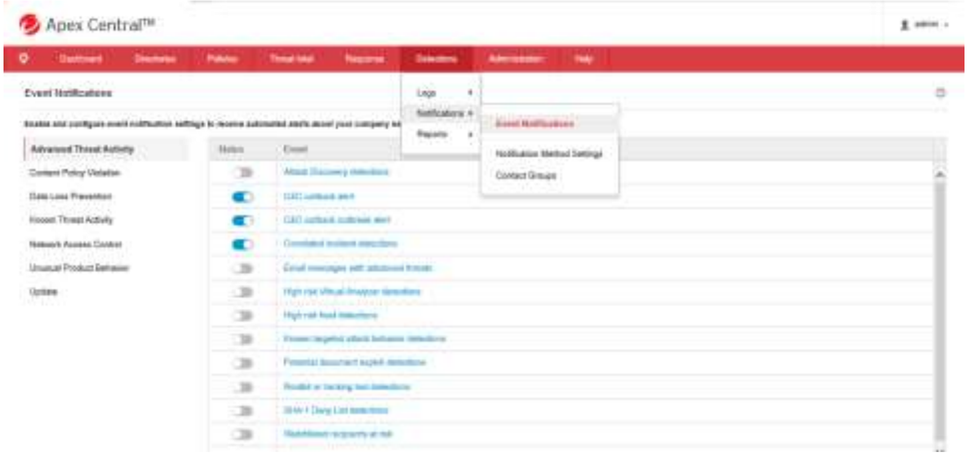
Community name*: public

Server IP address*:

IPv4 and IPv6 addresses supported.

Download MIB file

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



Event Notifications

Enable and configure event notification settings to receive automated alerts about your company ne

Advanced Threat Activity

Content Policy Violation

Data Loss Prevention

Known Threat Activity

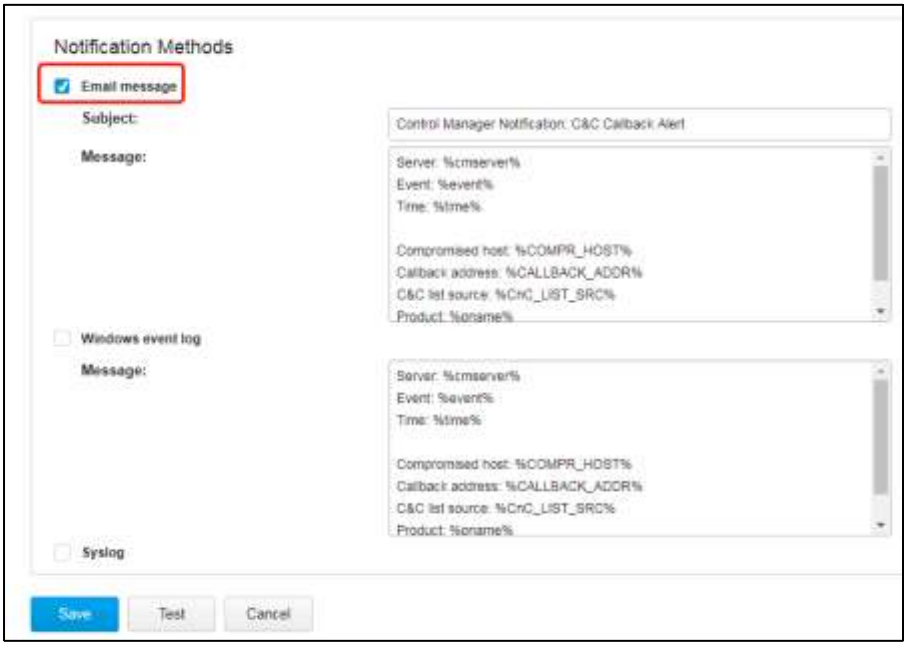
Network Access Control

Unusual Product Behavior

Update

Status	Event
○	Attack Discovery detections
●	C&C callback alert
●	C&C callback outbreak alert
●	Correlated incident detections
○	Email messages with advanced threats
○	High risk Virtual Analyzer detections
○	High risk host detections
○	Known targeted attack behavior detections
○	Potential document exploit detections
○	Rootkit or hacking tool detections
○	SHA-1 Deny List detections
○	Watchlisted recipients at risk

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



Notification Methods

☑ Email message

Subject: Control Manager Notification: C&C Callback Alert

Message:

```
Server: %cmserver%
Event: %event%
Time: %time%

Compromised host: %COMPR_HOST%
Callback address: %CALLBACK_ADDR%
C&C list source: %CnC_LIST_SRC%
Product: %pname%
```

☐ Windows event log

Message:

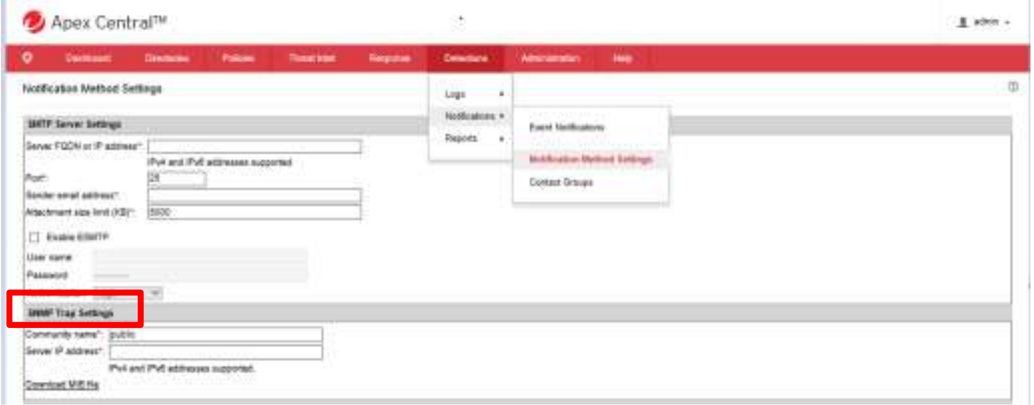
```
Server: %cmserver%
Event: %event%
Time: %time%

Compromised host: %COMPR_HOST%
Callback address: %CALLBACK_ADDR%
C&C list source: %CnC_LIST_SRC%
Product: %pname%
```

☐ Syslog

d. Click **Save**.

✓ SNMP

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



Notification Method Settings

SMTP Server Settings

Server FQDN or IP address*:

IPv4 and IPv6 addresses supported

Port: 25

Sender email address*:

Attachment size limit (KB)*: 5000

☐ Enable ESMTP

User name

Password

SNMP Trap Settings

Community name*: public

Server IP address*:

IPv4 and IPv6 addresses supported.

Download MIB file

In the SNMP Trap Settings section, specify the following:

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

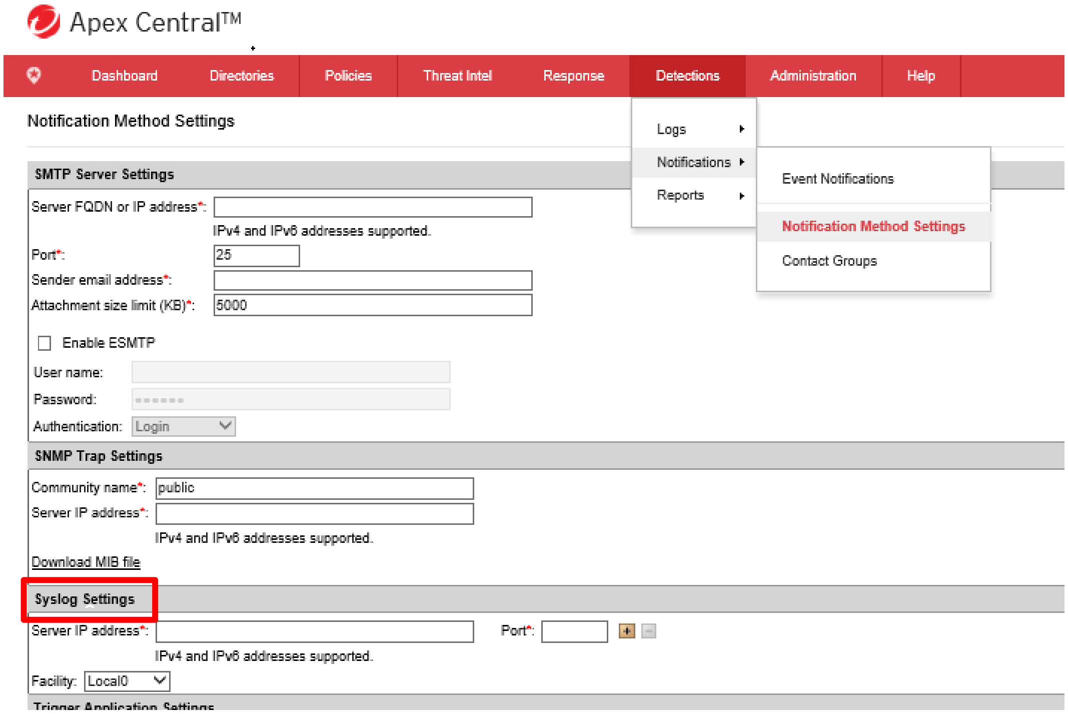
b. **Server IP address**: Type the IPv4 or IPv6 address of the SNMP server.

Check if the SNMP trap is supported.

5.2 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



Notification Method Settings

SMTP Server Settings

Server FQDN or IP address*:
IPv4 and IPv6 addresses supported.
Port*: 25
Sender email address*:
Attachment size limit (KB)*: 5000

☐ Enable ESMTP

User name:
Password: ••••••
Authentication: Login

SNMP Trap Settings

Community name*: public
Server IP address*:
IPv4 and IPv6 addresses supported.

Syslog Settings

Server IP address*: Port*:
IPv4 and IPv6 addresses supported.
Facility: Local0

Trigger Application Settings

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.

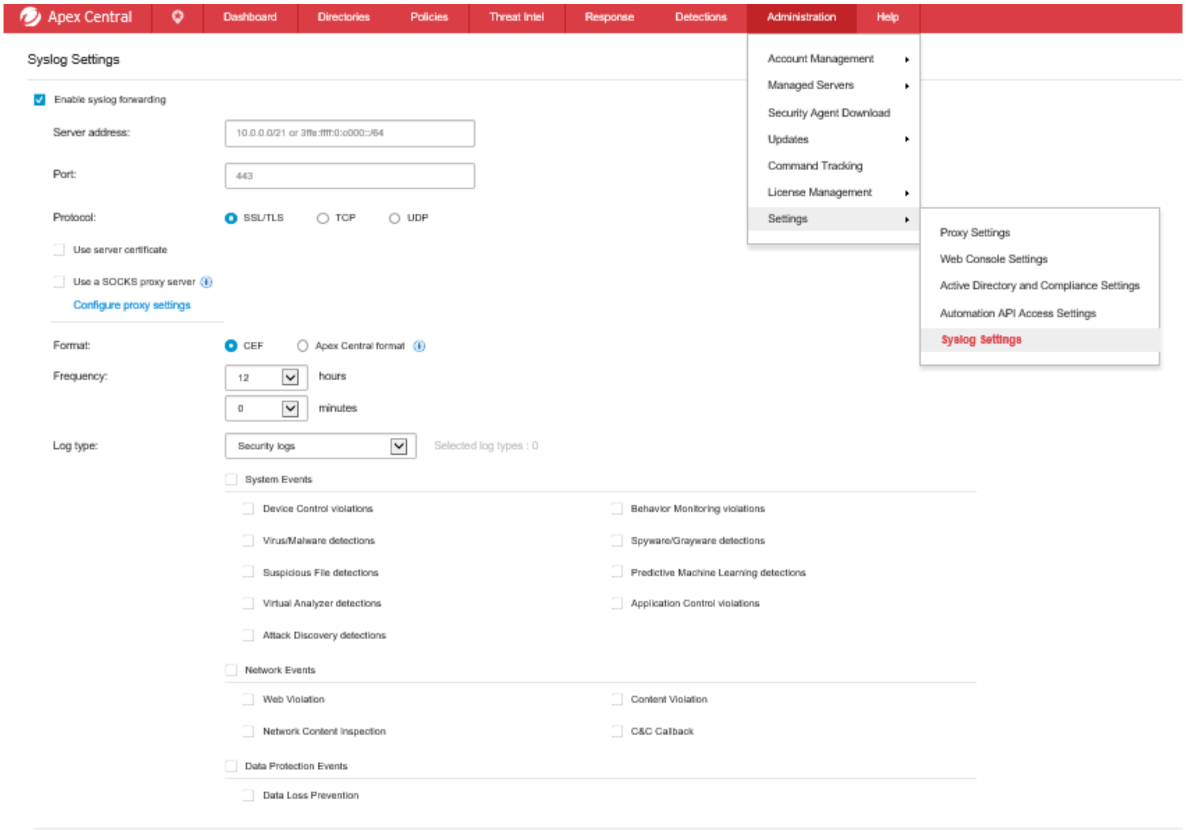
This table shows which event is supported by syslog.

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

5.3 Syslog forwarding setting

Apex Central allows syslog forwarding settings from **Administration > Settings > Syslog settings** instead of LogForwarder Tool. So, please use Apex Central management console setting.



Syslog Settings

☑ Enable syslog forwarding

Server address: 10.0.0.0/21 or 3ffe:ffff:0:c000::/64

Port: 443

Protocol: ● SSL/TLS ○ TCP ○ UDP

□ Use server certificate

□ Use a SOCKS proxy server

Configure proxy settings

Format: ● CEF ○ Apex Central format

Frequency: 12 hours
0 minutes

Log type: Security logs   Selected log types : 0

□ System Events

□ Device Control violations   □ Behavior Monitoring violations
□ Virus/Malware detections   □ Spyware/Grayware detections
□ Suspicious File detections   □ Predictive Machine Learning detections
□ Virtual Analyzer detections   □ Application Control violations
□ Attack Discovery detections

□ Network Events

□ Web Violation   □ Content Violation
□ Network Content Inspection   □ C&C Callback

□ Data Protection Events

□ Data Loss Prevention

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

The following are the types of logs that Apex Central supports:

Log types	CEF	Apex Central
Application Control	**Yes**	No
Behavior Monitoring	**Yes**	**Yes**
Contents Security	**Yes**	No
C&C Callback	**Yes**	No
Data Loss Prevention	**Yes**	**Yes**
Device Access Control	**Yes**	**Yes**

Engine Update status	**Yes**	**Yes**
Network Connection Inspection	**Yes**	No
Pattern Update status	**Yes**	**Yes**
Predictive Machine Learning	**Yes**	No
Virus/Malware	**Yes**	No
Sandbox Detection logs	**Yes**	No
Spyware/Grayware	**Yes**	No
Suspicious File	**Yes**	No
Web Security	**Yes**	No
Web Security	**Yes**	No
Predictive Machine Learning	**Yes**	No

Apex Central only supports UDP protocol.

5.3.1 Configuring syslog forwarding Settings

a. Enable syslog forwarding.

- Configure the Log Receiver settings.
  IP address: Syslog server IP address
- Port: Syslog server port number
- Protocol: SSL/TLS, TCP or UDP
- Check if server certification is necessary
- Check if SOCKS proxy server is used

b. Configure the **Log Forwarding Settings**.

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

c. Click **Test Connection** or **Start**.

6. Report

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

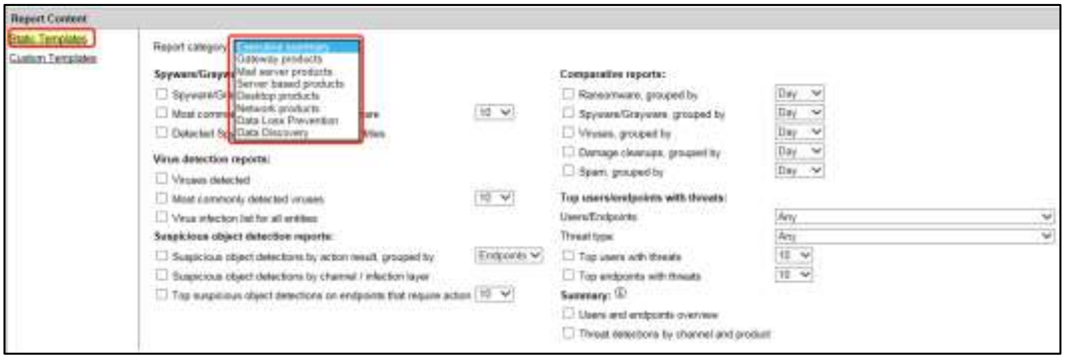
6.1 Static template and Custom template

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

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

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

Static Templates:



Report Content

Static Templates
Custom Templates

Report category: Executive summary

- Executive summary
- Gateway products
- Mail server products
- Server based products
- Desktop products
- Network products
- Data Loss Prevention
- Data Discovery

Spyware/Grayw

☐ Spyware/Gr
☐ Most comm ...are: 10
☐ Detected Sp ...ities

Virus detection reports:

☐ Viruses detected
☐ Most commonly detected viruses: 10
☐ Virus infection list for all entities

Suspicious object detection reports:

☐ Suspicious object detections by action result, grouped by: Endpoints
☐ Suspicious object detections by channel / infection layer
☐ Top suspicious object detections on endpoints that require action: 10

Comparative reports:

☐ Ransomware, grouped by: Day
☐ Spyware/Grayware, grouped by: Day
☐ Viruses, grouped by: Day
☐ Damage cleanups, grouped by: Day
☐ Spam, grouped by: Day

Top users/endpoints with threats:

Users/Endpoints: Any
Threat type: Any
☐ Top users with threats: 10
☐ Top endpoints with threats: 10

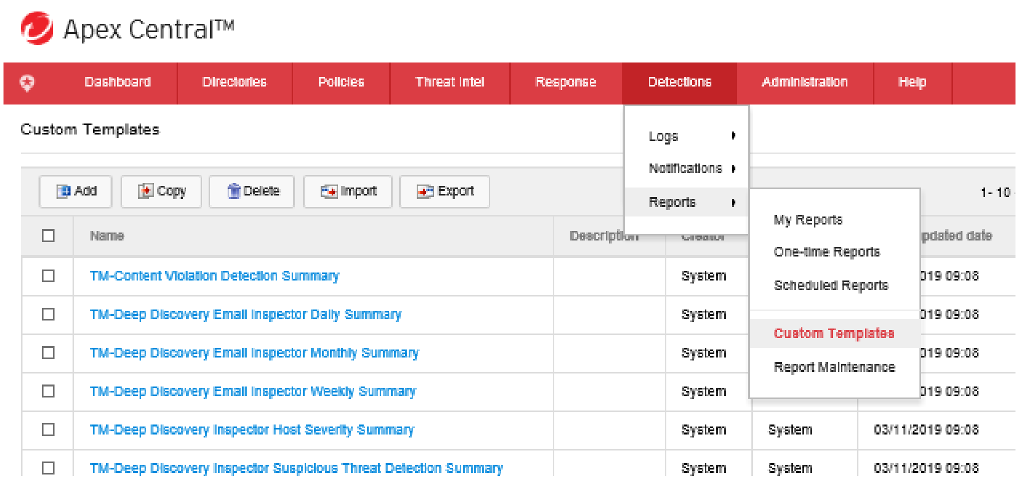
Summary: ⓘ

☐ Users and endpoints overview
☐ Threat detections by channel and product

Custom Templates:

You can edit or add your own customer template via **Detections > Reports > Custom Templates**.

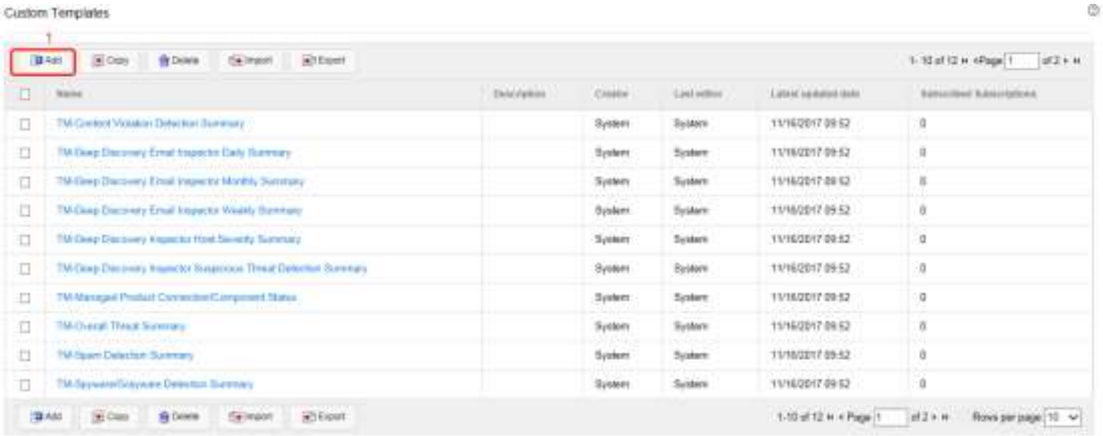
For example, the users can create a template of the managed product’s pattern and engine status.



Custom Templates

□	Name	Description	Creator		pdated date
□	TM-Content Violation Detection Summary		System		019 09:08
□	TM-Deep Discovery Email Inspector Daily Summary		System		019 09:08
□	TM-Deep Discovery Email Inspector Monthly Summary		System		019 09:08
□	TM-Deep Discovery Email Inspector Weekly Summary		System		019 09:08
□	TM-Deep Discovery Inspector Host Severity Summary		System	System	03/11/2019 09:08
□	TM-Deep Discovery Inspector Suspicious Threat Detection Summary		System	System	03/11/2019 09:08

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


1
Add
Copy
Delete
Import
Export
1- 10 of 12 « ‹Page 1 of 2 › »
1-10 of 12 « ‹ Page 1 of 2 › »
Rows per page 10

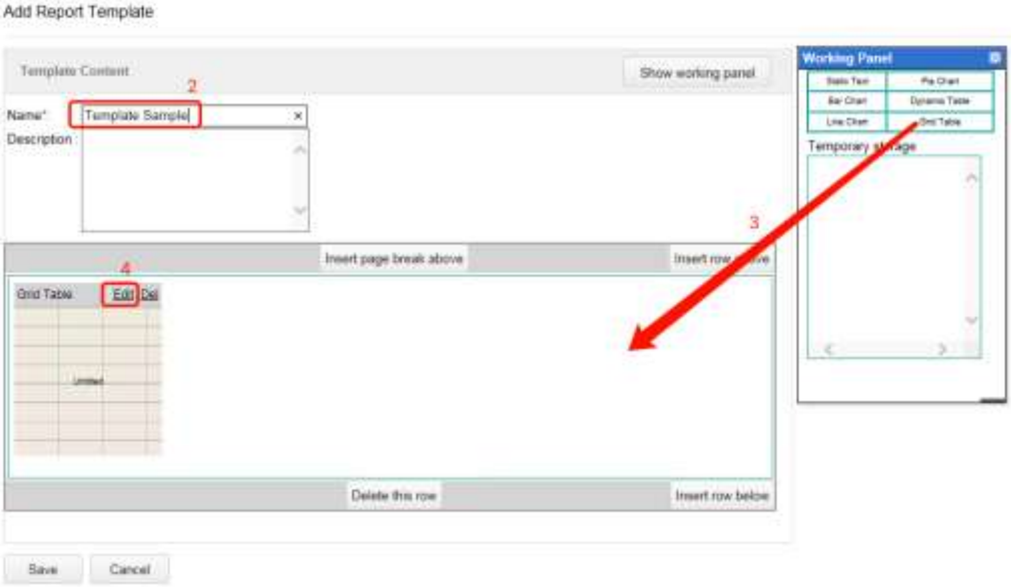
Custom Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	TM-Content Violation Detection Summary		System	System	11/16/2017 09:52	0
□	TM-Deep Discovery Email Inspector Daily Summary		System	System	11/16/2017 09:52	0
□	TM-Deep Discovery Email Inspector Monthly Summary		System	System	11/16/2017 09:52	0
□	TM-Deep Discovery Email Inspector Weekly Summary		System	System	11/16/2017 09:52	0
□	TM-Deep Discovery Inspector Host Severity Summary		System	System	11/16/2017 09:52	0
□	TM-Deep Discovery Inspector Suspicious Threat Detection Summary		System	System	11/16/2017 09:52	0
□	TM-Managed Product Connection/Component Status		System	System	11/16/2017 09:52	0
□	TM-Overall Threat Summary		System	System	11/16/2017 09:52	0
□	TM-Spam Detection Summary		System	System	11/16/2017 09:52	0
□	TM-Spyware/Grayware Detection Summary		System	System	11/16/2017 09:52	0

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

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

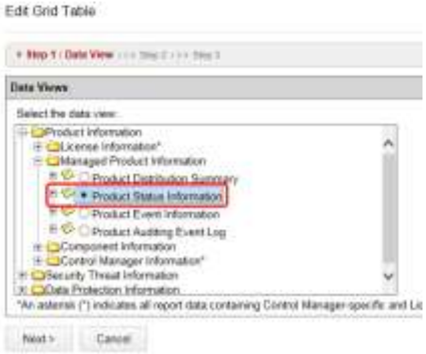
For example, you choose the "Grid Table".



Add Report Template

Name*: Template Sample

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



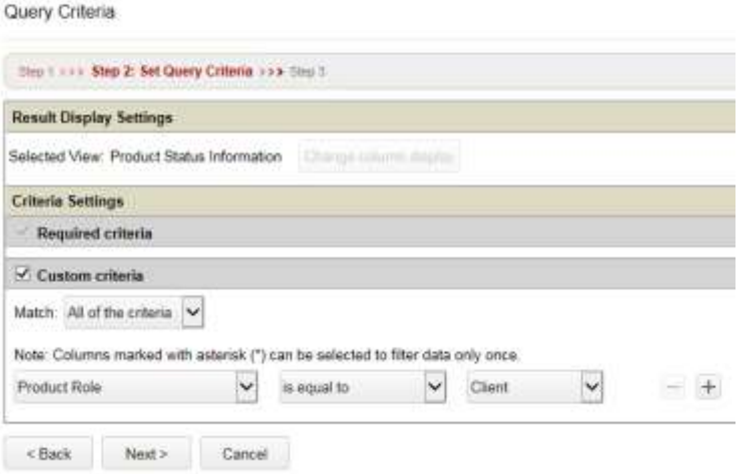
Edit Grid Table

Select the data view: ● Product Status Information

*An asterisk (*) indicates all report data containing Control Manager-specific and Li

Step 1 : Data View >>> Step 2 >>> Step 3
Data Views
Product Information
License Information*
Managed Product Information
Product Distribution Summary
Product Status Information
Product Event Information
Product Auditing Event Log
Component Information
Control Manager Information*
Security Threat Information
Data Protection Information
Next >
Cancel

4. Set the custom criterial if needed.



Query Criteria

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

Result Display Settings

Selected View: Product Status Information

Criteria Settings

Required criteria

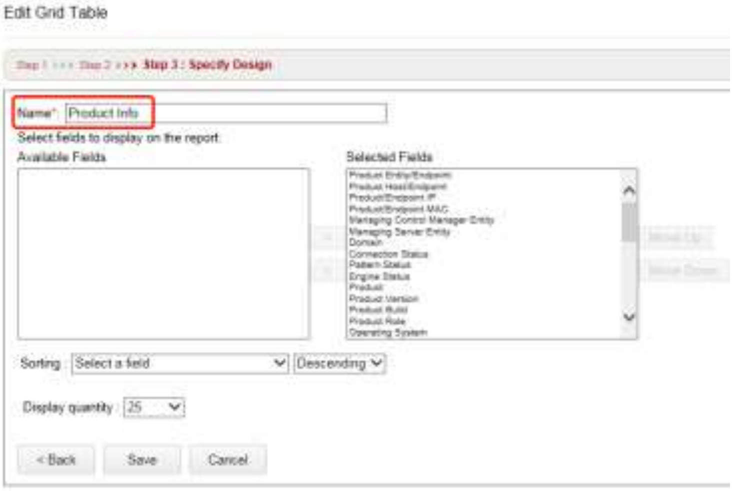
☑ **Custom criteria**

Match: All of the criteria

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

Product Role | is equal to | Client

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



Edit Grid Table

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

Name*: Product Info

Select fields to display on the report.

Available Fields

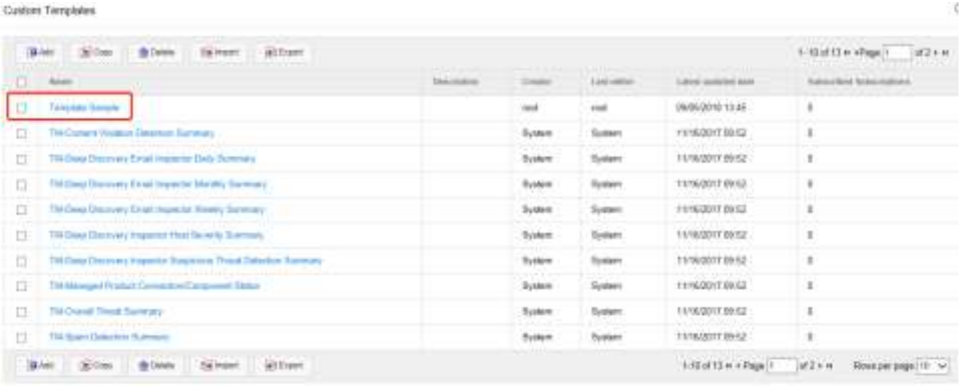
Selected Fields

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

Sorting : Select a field | Descending

Display quantity : 25

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



Custom Templates

1-10 of 13 Page 1 of 2

☐	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
☐	Template Sample		root	root	09/05/2019 13:45	0
☐	TM Content Violation Detection Summary		System	System	11/16/2017 09:52	0
☐	TM Deep Discovery Email Inspector Daily Summary		System	System	11/16/2017 09:52	0
☐	TM Deep Discovery Email Inspector Monthly Summary		System	System	11/16/2017 09:52	0
☐	TM Deep Discovery Email Inspector Weekly Summary		System	System	11/16/2017 09:52	0
☐	TM Deep Discovery Inspector Host Severity Summary		System	System	11/16/2017 09:52	0
☐	TM Deep Discovery Inspector Suspicious Threat Detection Summary		System	System	11/16/2017 09:52	0
☐	TM Managed Product Connection/Component Status		System	System	11/16/2017 09:52	0
☐	TM Overall Threat Summary		System	System	11/16/2017 09:52	0
☐	TM Spam Detection Summary		System	System	11/16/2017 09:52	0

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

Control Manager 2.5 Templates

With the release of Control Manager 5.0 report sets, Control Manager 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 …¥ControlManager¥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.

6.1.1 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

6.1.2 Report format

- ✓ 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)

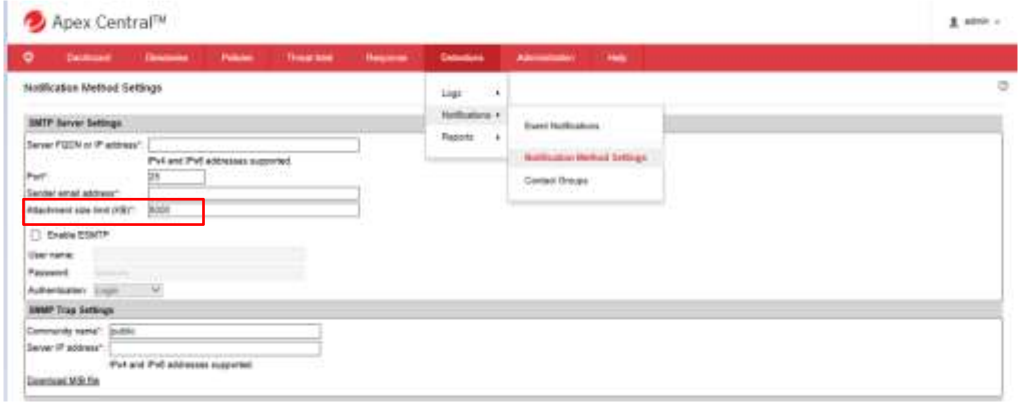
- ✓ After migration to Apex Central, the format in next scheduled report will be converted.
  - ▪ Rich text (*.rtf) -> Microsoft Word format (*.docx)
  - ▪ Other -> Adobe PDF format (*.pdf)

6.2 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 **Detections > 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 Apex Central console. After log-on, the report will be downloaded. This was added due to issues when Apex Central reports would not be sent when the attachment size exceeds the SMTP server attachment size limitations.



Notification Method Settings

SMTP Server Settings

Server FQDN or IP address*:

IPv4 and IPv6 addresses supported.

Port*: 25

Sender email address*:

Attachment size limit (KB)*: 5000

□ Enable ESMTP

User name:

Password:

Authentication: Login

SNMP Trap Settings

Community name*: public

Server IP address*:

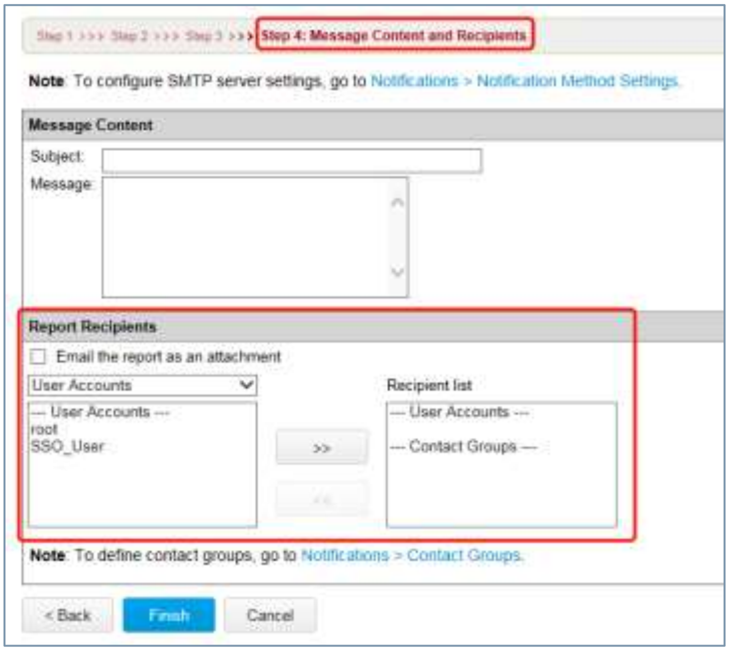
IPv4 and IPv6 addresses supported.

Download MIB file

This setting can be altered to confirm to the limits set on the domain’s SMTP server.

1.1. Access Control List

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



Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Message Content and Recipients**

Note: To configure SMTP server settings, go to Notifications > Notification Method Settings.

Message Content

Subject:

Message:

Report Recipients

□ Email the report as an attachment

User Accounts

--- User Accounts ---
root
SSO_User

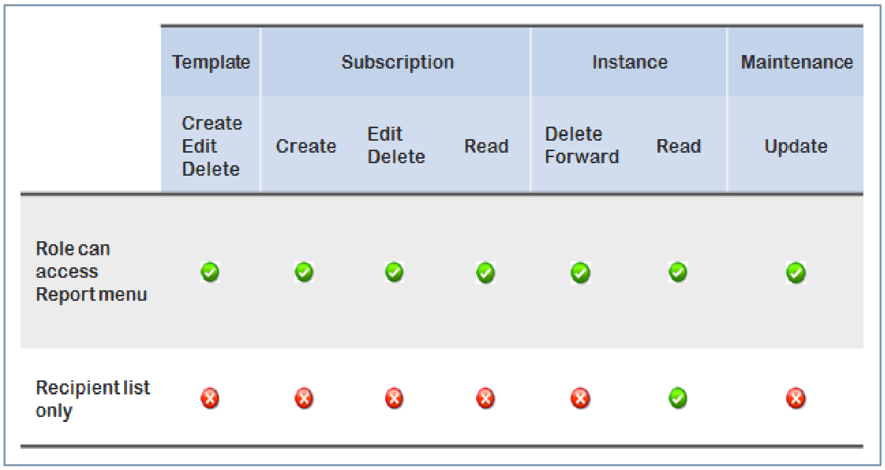
Recipient list

--- User Accounts ---

--- Contact Groups ---

Note: To define contact groups, go to Notifications > Contact Groups.

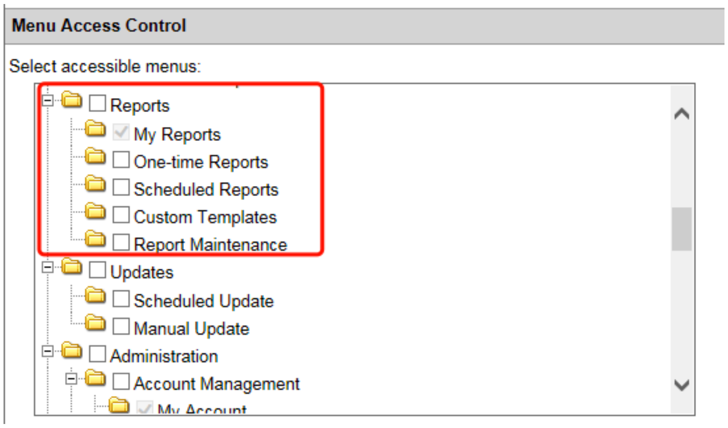
This configuration, together with the role's menu access control, dictates the operations that a specific user can perform to report related items.



	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.



Menu Access Control

Select accessible menus:

- □ Reports
  - ✓ My Reports
  - □ One-time Reports
  - □ Scheduled Reports
  - □ Custom Templates
  - □ Report Maintenance
- □ Updates
  - □ Scheduled Update
  - □ Manual Update
- □ Administration
  - □ Account Management
    - ✓ My Account

- 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.

1.2. 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.

7 Log Query

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

7.1 Log Query summary

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

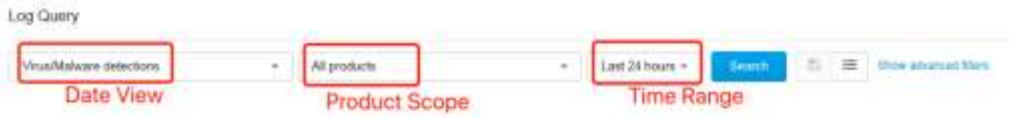
Apex Central also allows you to:

- 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 Apex Central server.
- Manually delete log entries by type or configure automatic log deletion.

7.2 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.

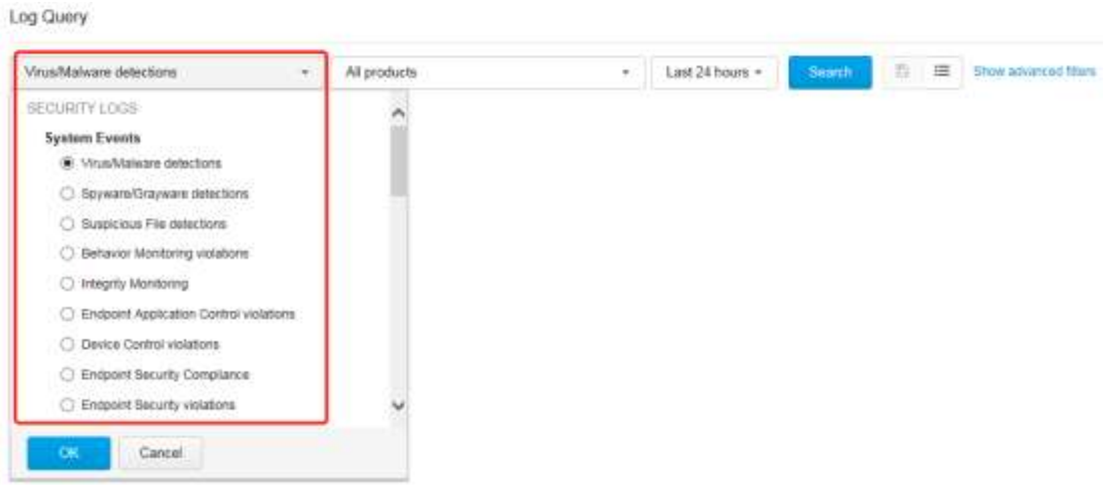
Apex Central shows collected logs and allow to query logs from **Detections > Logs > Log Query**.



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

7.2.2 Basic Filters – Data View

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

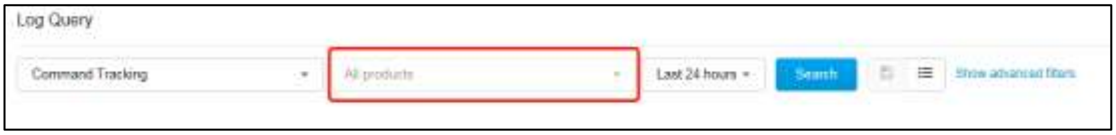

Log Query
Virus/Malware detections
All products
Last 24 hours
Search
Show advanced filters
SECURITY LOGS
System Events
● Virus/Malware detections
○ Spyware/Grayware detections
○ Suspicious File detections
○ Behavior Monitoring violations
○ Integrity Monitoring
○ Endpoint Application Control violations
○ Device Control violations
○ Endpoint Security Compliance
○ Endpoint Security violations
OK
Cancel

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

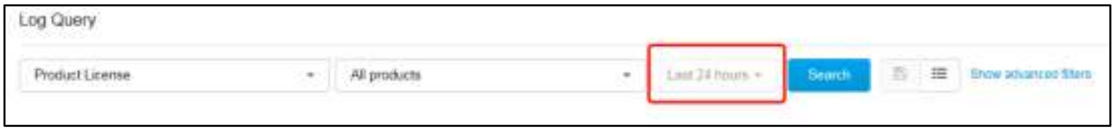
- The following are new Data Views that have been added:
- Detailed Predictive Machine Learning Information
- Virtual Analyzer Detections (sandbox detection)
- Detailed Virtual Analyzer Suspicious Object Impact Information

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 Apex Central only.



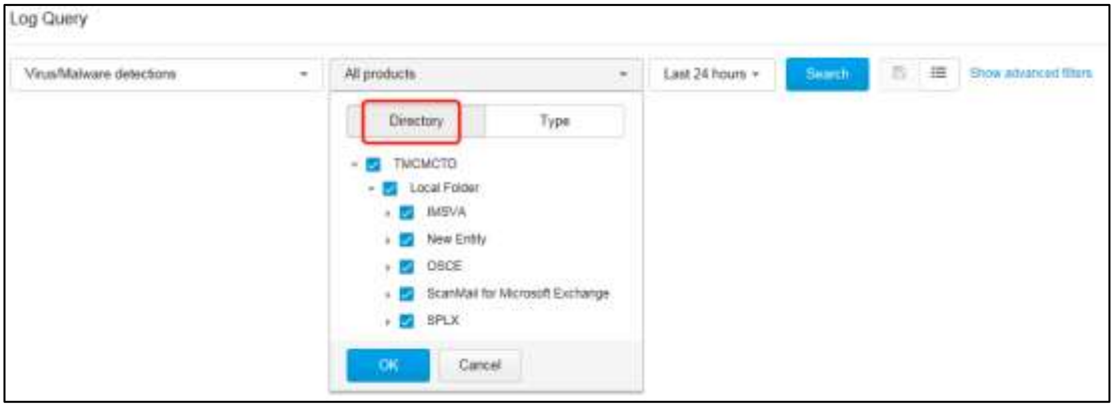
If you select Product License as the Data View, the Time Range will be disabled because it is not required criteria.



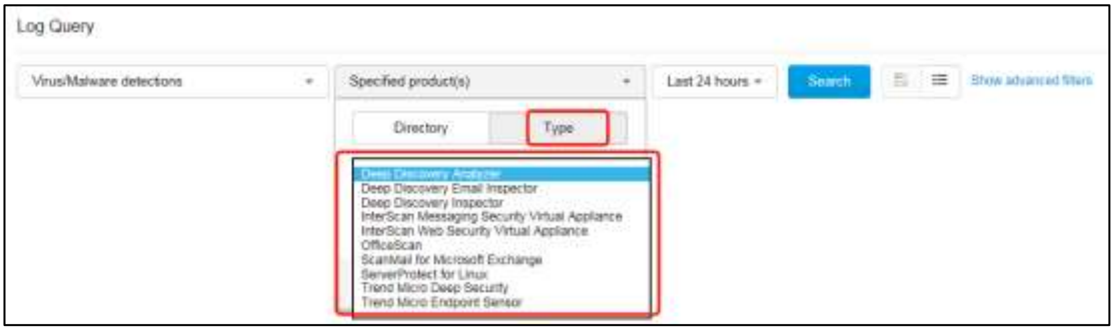
7.2.3 Basic Filters – Product Scope

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.

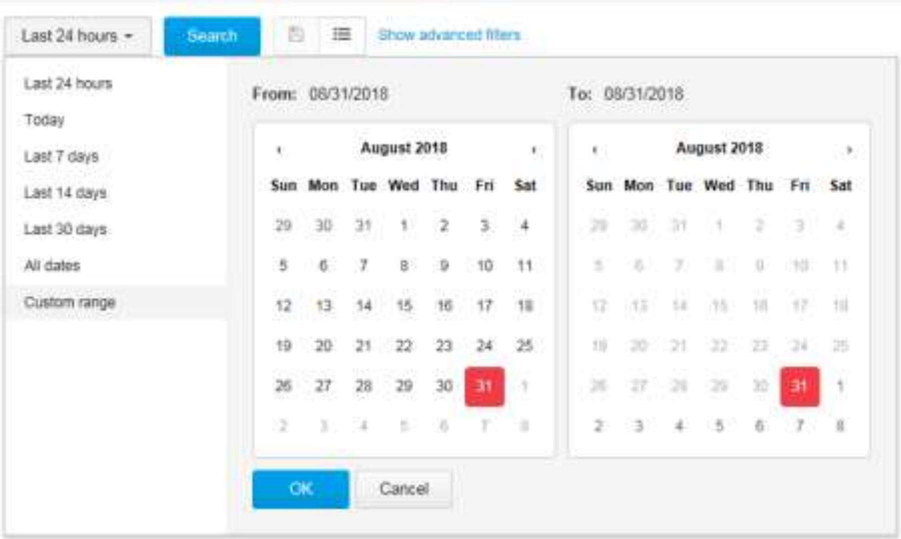


The product **Type** dropdown list only shows the products registered to Apex Central.


Log Query
Virus/Malware detections
Specified product(s)
Last 24 hours
Search
Show advanced filters
Directory
Type
Deep Discovery Analyzer
Deep Discovery Email Inspector
Deep Discovery Inspector
InterScan Messaging Security Virtual Appliance
InterScan Web Security Virtual Appliance
OfficeScan
ScanMail for Microsoft Exchange
ServerProtect for Linux
Trend Micro Deep Security
Trend Micro Endpoint Sensor

7.2.4 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.



From: 08/31/2018

To: 08/31/2018

August 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

August 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

7.2.5 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.

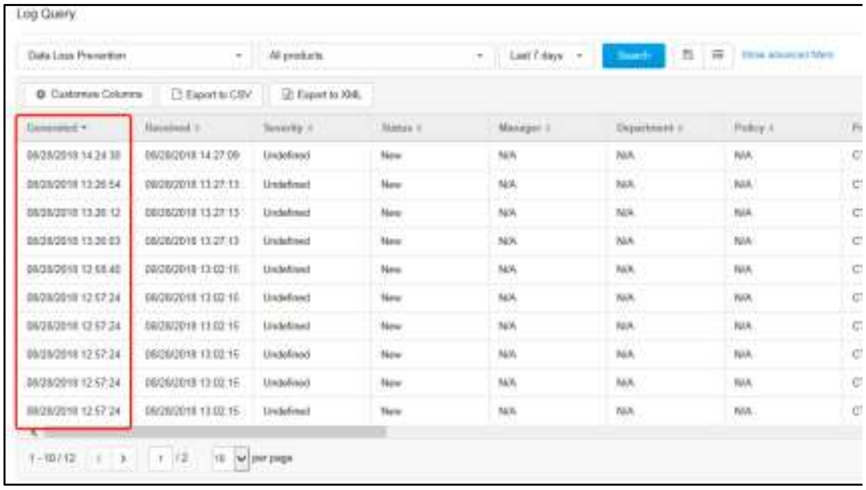
Same as with Ad hoc queries, you can select that these filters are applied by matching "**All of the criteria**" or "**Any of the criteria**".

For example, you want to filter out how many Apex One/Office Scan Agents' pattern are out of date.

7.2.6 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 Apex Central.

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 Apex Central server received the logs from the product side.

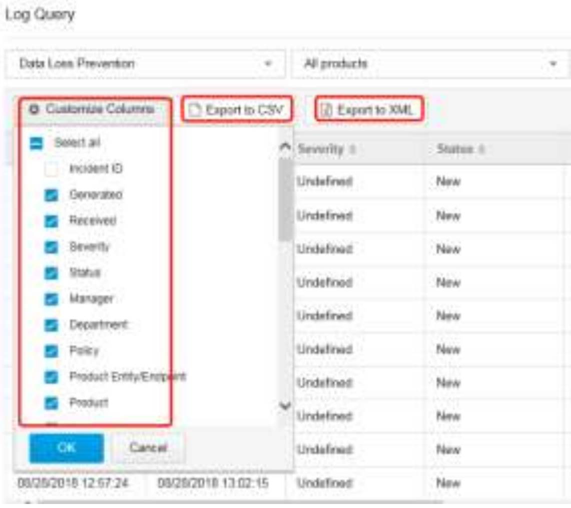


Log Query

Generated	Received	Severity	Status	Manager	Department	Policy
08/28/2018 14:24:38	08/28/2018 14:27:09	Undefined	New	N/A	N/A	N/A
08/28/2018 13:26:54	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A
08/28/2018 13:26:12	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A
08/28/2018 13:26:03	08/28/2018 13:27:13	Undefined	New	N/A	N/A	N/A
08/28/2018 12:58:40	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New	N/A	N/A	N/A

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.



Log Query

- ☐ Select all
- ☐ Incident ID
- ☑ Generated
- ☑ Received
- ☑ Severity
- ☑ Status
- ☑ Manager
- ☑ Department
- ☑ Policy
- ☑ Product Entity/Endpoint
- ☑ Product

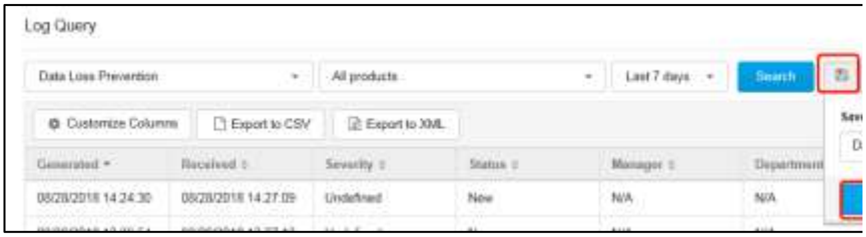
		Severity	Status
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
		Undefined	New
08/28/2018 12:57:24	08/28/2018 13:02:15	Undefined	New

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¥Apex Central¥SystemConfiguration.xml* file:

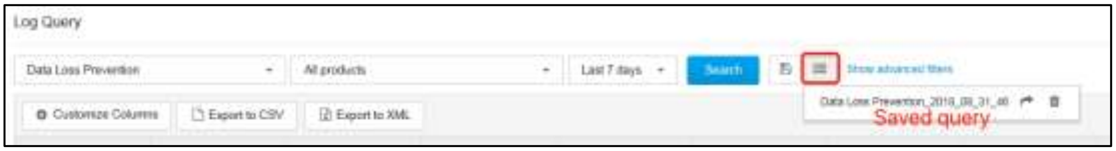
P Name="m_iAdhocQueryUIMaxResultSize" Value="

7.2.7 Save and Share the Query Results

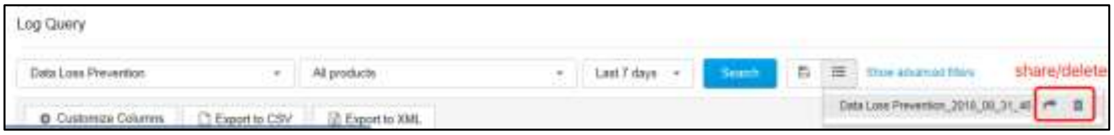
After performing a Query/Search, the Save Query button (floppy disk icon) becomes clickable. Users can click **Save** to save query.

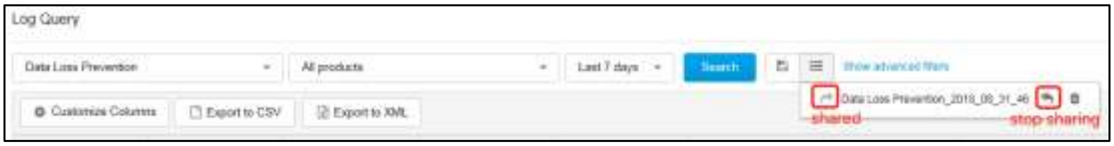


When at least one query has been saved, user can click the Saved queries button to view a list of saved queries.

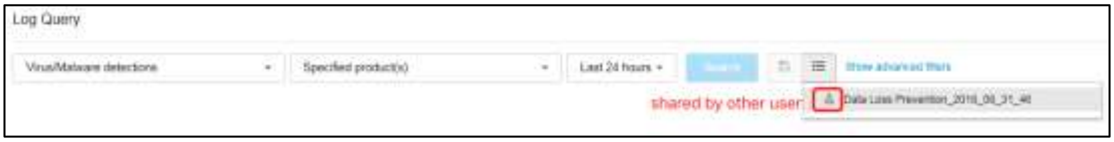


The user can share the saved queries to others. Read-only users can also save and share queries.





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.



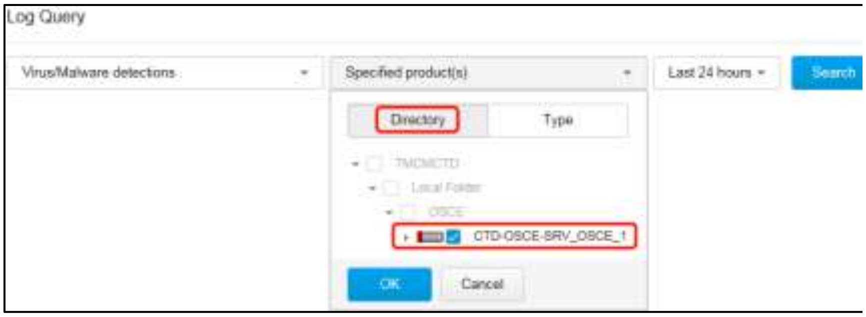
7.3 Role-Based Access Control Log Queries

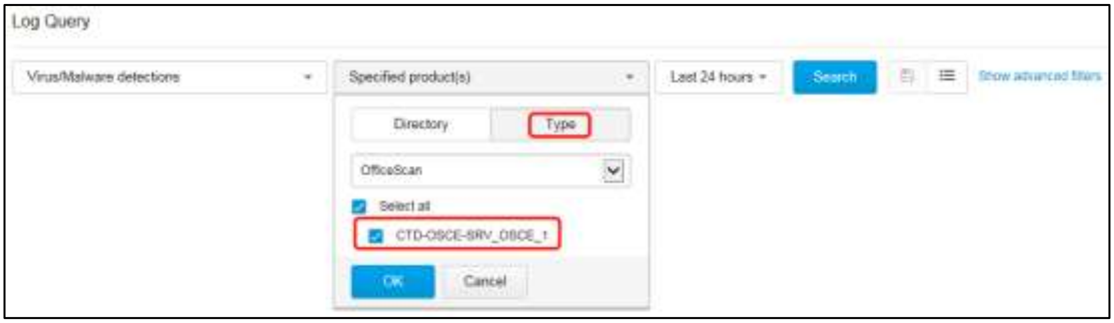
In Log Query, the following parts are controlled by Role-Based Access Control (RBAC):

- 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 Apex One/Office Scan server, their options in both product directory and product type will be limited to the Apex One/Office Scan server that they manage.


Log Query
Virus/Malware detections
Specified product(s)
Last 24 hours
Search
Directory
Type
TMCMCTD
Local Folder
OSCE
CTD-OSCE-SRV_OSCE_t
OK
Cancel


Log Query
Virus/Malware detections
Specified product(s)
Last 24 hours
Search
Show advanced filters
Directory
Type
OfficeScan
Select all
CTD-OSCE-SRV_OSCE_t
OK
Cancel

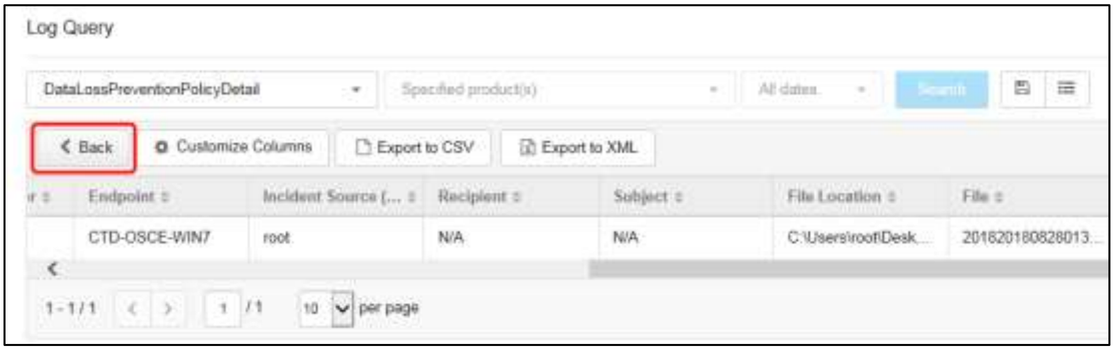
7.4 Drill-down Query Views

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 Apex Central , we can drill down to Log Query from the following:

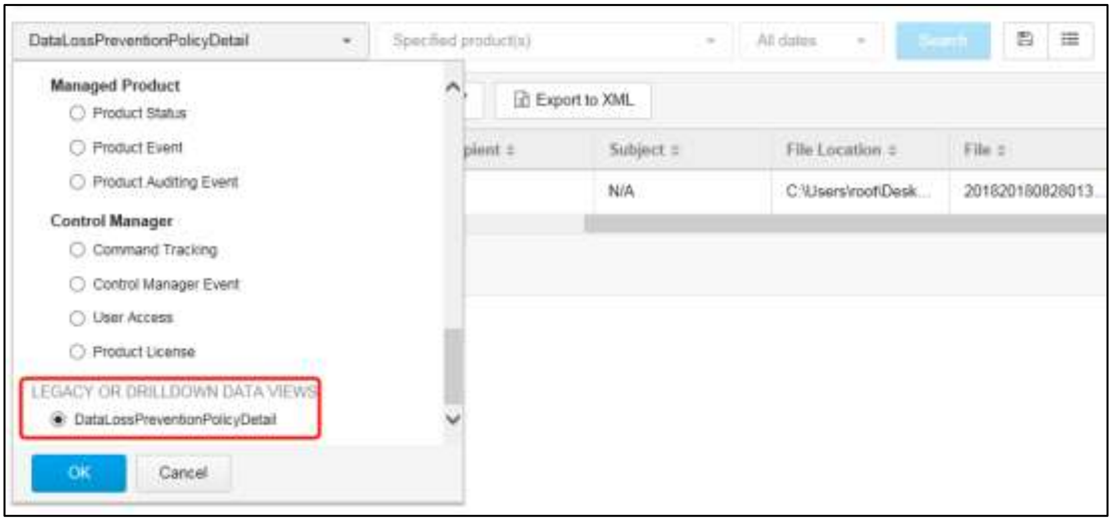
- Default data views in Log Query
- Widgets
- Inventory view
- Policies

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.



r	Endpoint	Incident Source (...	Recipient	Subject	File Location	File
	CTD-OSCE-WIN7	root	N/A	N/A	C:\Users\root\Desk...	201820180828013...

When customers migrate to Apex Central 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.



pient	Subject	File Location	File
	N/A	C:\Users\root\Desk...	201820180828013...

7.5 How to Aggregate Logs

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

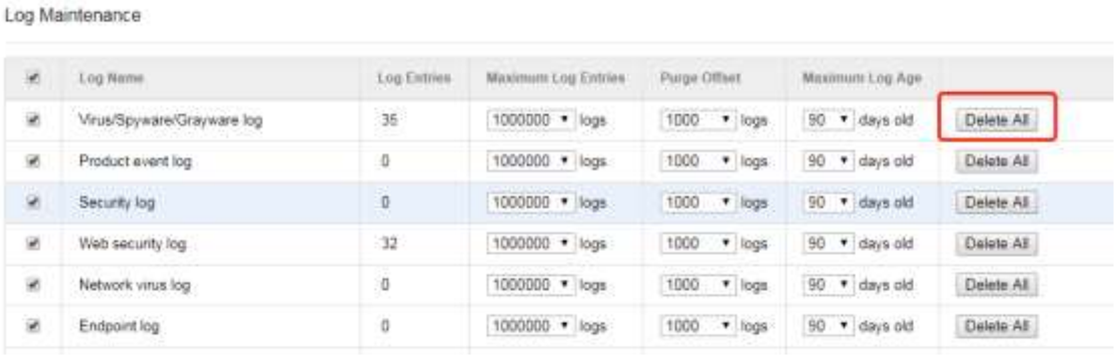
By default the feature is disabled.

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

7.6 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

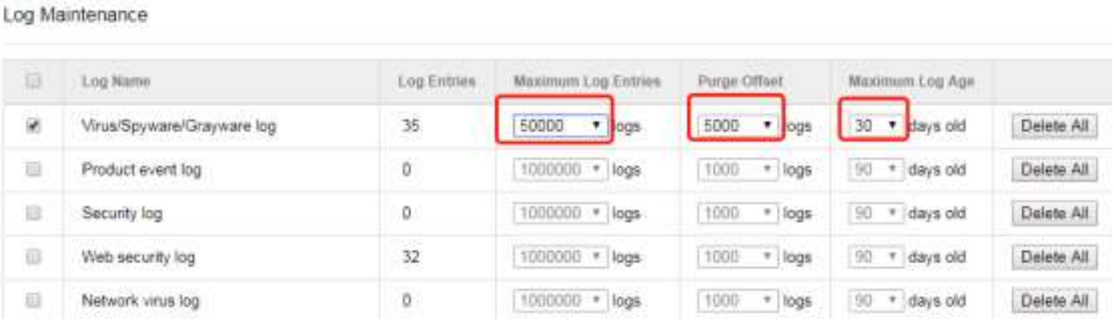
- How to delete the logs automatically

  Select the check box for the log type.

  In the Maximum Log Entries column, specify the maximum number of logs that Apex Central retains.

  In the Purge Offset column, specify the number of logs that Apex Central 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 Apex Central 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, Apex Central 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.

7.7 Log Query Specifications

- 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.

7.8 Log Query Data Views

Apex Central 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 Apex Central 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
Apex Central:		
Command Tracking	Command Tracking Information	Displays specific information about commands issued to managed products
Apex Central Event	Apex Central Event Information	Displays specific information about Apex Central server events
User Access	User Access Information	Displays Apex Central user access and the activities users perform while logged on to Apex Central
Product License	Detailed Product License Information	Displays information about the Activation Code and information on managed products that use the Activation Code

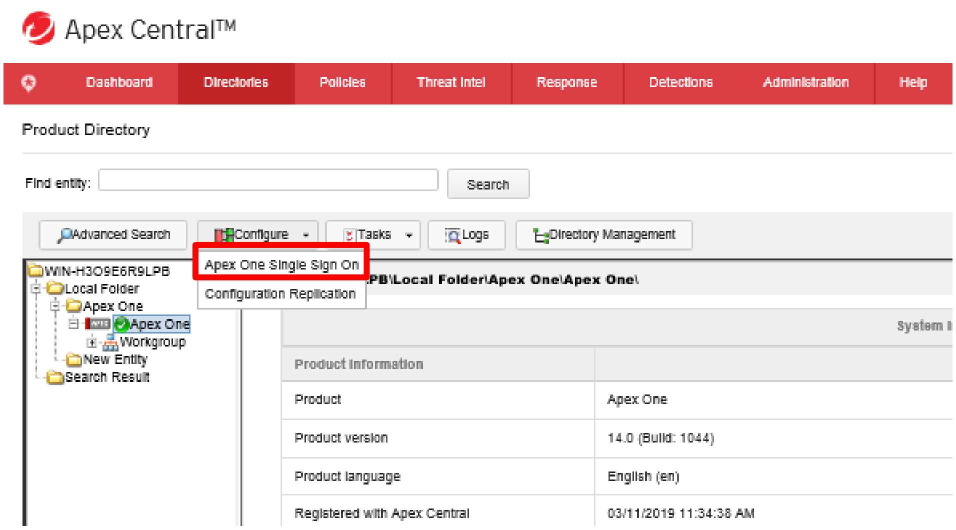
8 Single sign on

This chapter explains how you can log into product console via Apex Central.

8.1 Steps how to log into product console from Apex Central

When product supports Single Sign On from Apex Central, you can login product management console.

1. Access **Directories > Products.**
2. Select server name in Product Directory tree.
3. Click configure, and select Single Sign On.



Product Information	
Product	Apex One
Product version	14.0 (Build: 1044)
Product language	English (en)
Registered with Apex Central	03/11/2019 11:34:38 AM

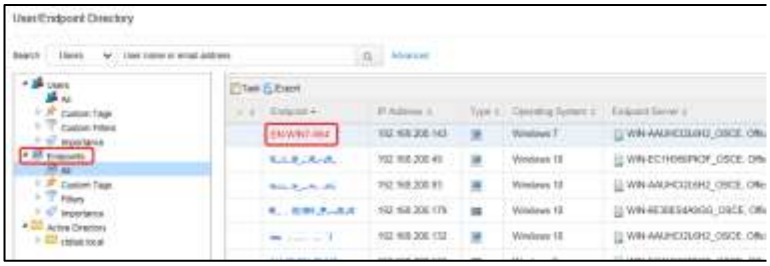
9 Apex One/Office Scan Endpoint Isolation

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 Apex Central Administrator a method of mitigation to prevent further damage.

When you would like to isolate endpoint with Office Scan, you needed to enable Office Scan firewall. However, Apex Central doesn't require to enable Apex One firewall function.

Deploying Endpoint Isolation Task

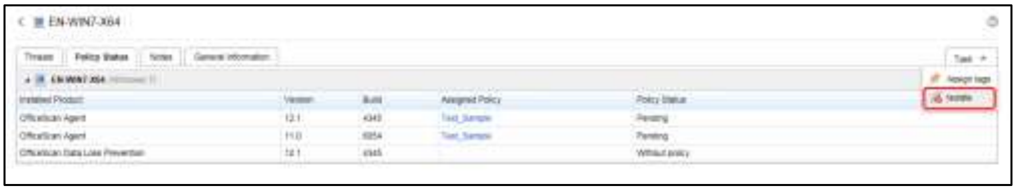
1. Find and select the infected endpoint (e.g. EN-WIN70-X64).



User/Endpoint Directory

Endpoint	IP Address	Type	Operating System	Endpoint Server
EN-WIN7-X64	192.168.200.143		Windows 7	WIN-AAUHCI2L6H2_OSCE_Offi
[illegible]	192.168.200.40		Windows 10	WIN-EC1HD6IPKOF_OSCE_Offi
[illegible]	192.168.200.91		Windows 10	WIN-AAUHCI2L6H2_OSCE_Offi
[illegible]	192.168.200.175		Windows 10	WIN-6E3EES4A9G0_OSCE_Offi
[illegible]	192.168.200.132		Windows 10	WIN-AAUHCI2L6H2_OSCE_Offi

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



EN-WIN7-X64

Installed Product	Version	Build	Assigned Policy	Policy Status
OfficeScan Agent	12.1	4349	Test_Sample	Pending
OfficeScan Agent	11.0	6054	Test_Sample	Pending
OfficeScan Data Loss Prevention	12.1	4345		Without policy

3. Click **Isolate Endpoint**.

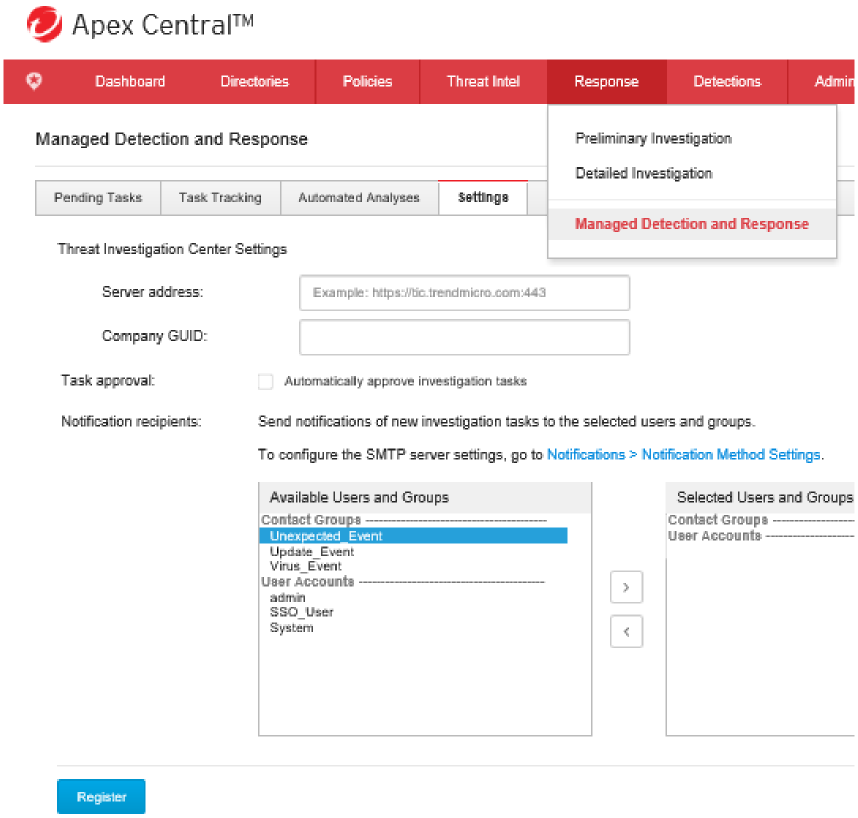
10 Investigate threat in your network

You can investigate threat information with registered DDAN or Apex One Sandbox as a Service.

10.1 Apex One Sandbox as a Service preparation

To use Apex One Sandbox as a Service functions under Response menu, please input Activation Code for Apex One Sandbox as a Service. (Section 2.5)

Then, please input Threat Investigation Server information which you received and Notification recipients.



Managed Detection and Response

Threat Investigation Center Settings

Server address: Example: https://tic.trendmicro.com:443

Company GUID:

Task approval: □ Automatically approve investigation tasks

Notification recipients: Send notifications of new investigation tasks to the selected users and groups.

To configure the SMTP server settings, go to Notifications > Notification Method Settings.

Available Users and Groups
Contact Groups --
Unexpected_Event
Update_Event
Virus_Event
User Accounts --
admin
SSO_User
System

Selected Users and Groups
Contact Groups -------------------
User Accounts -------------------

10.2 How to start investigation and review result

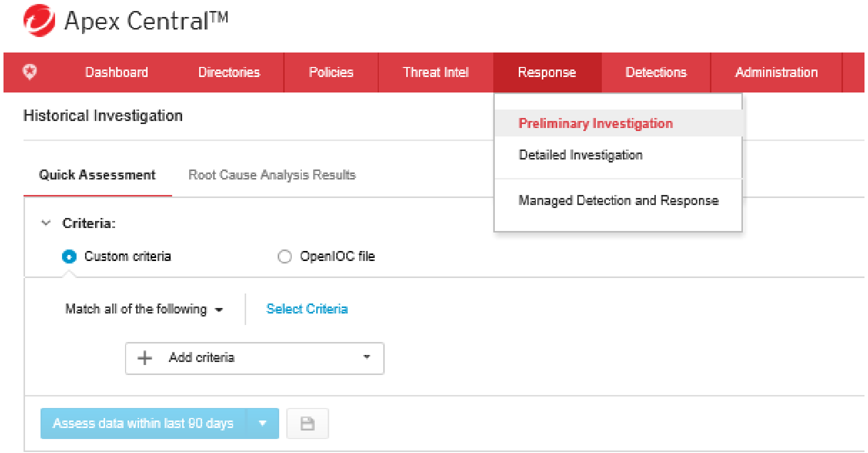
You can start investigation from **Response > Preliminary Investigation** or **Response >Detail Investigation.**

10.2.2 Add criteria manually

You can start investigation from **Response > Preliminary Investigation**.

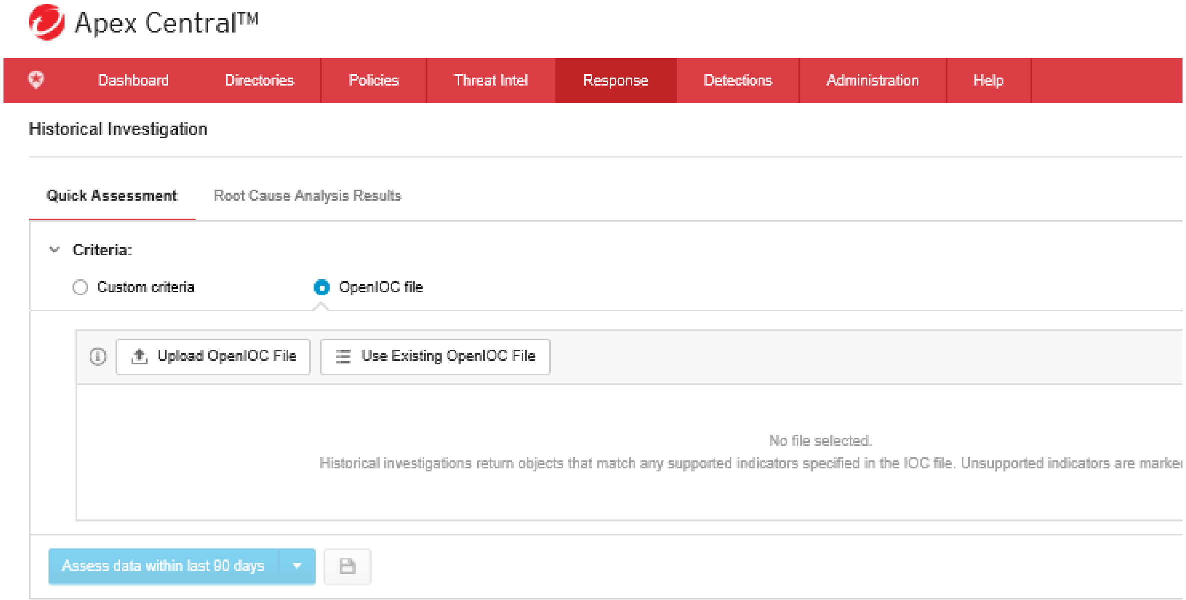
You can add criteria manually.

- ✓ Host Name
- ✓ User account
- ✓ File name
- ✓ File path
- ✓ Hash value
- ✓ Registry key
- ✓ Registry name
- ✓ Registry data
- ✓ Command line



10.2.3 File investigation

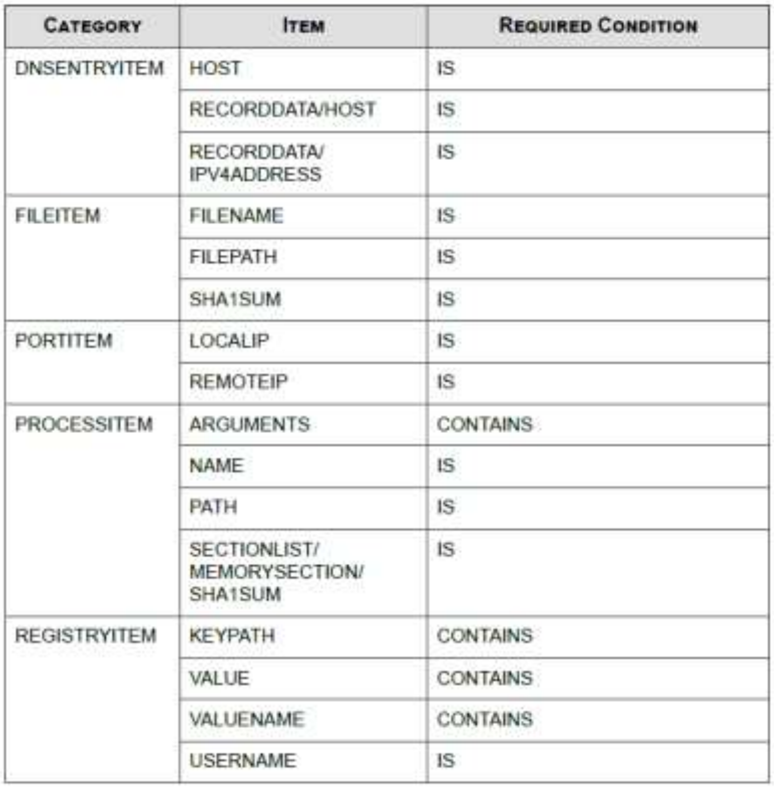
Please select OpenIOC file radio box in Quick Assessment from **Response > Preliminary Investigation**.



No file selected.
Historical investigations return objects that match any supported indicators specified in the IOC file. Unsupported indicators are marke

✓ Disk files: IOC

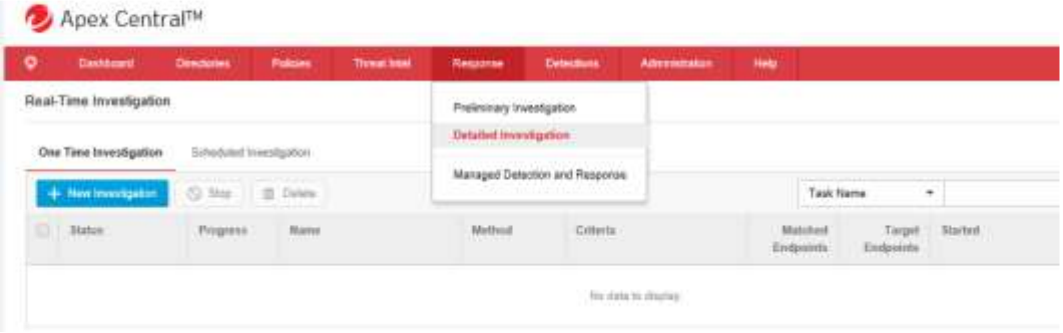
Preliminary investigation allow following IOC indicator



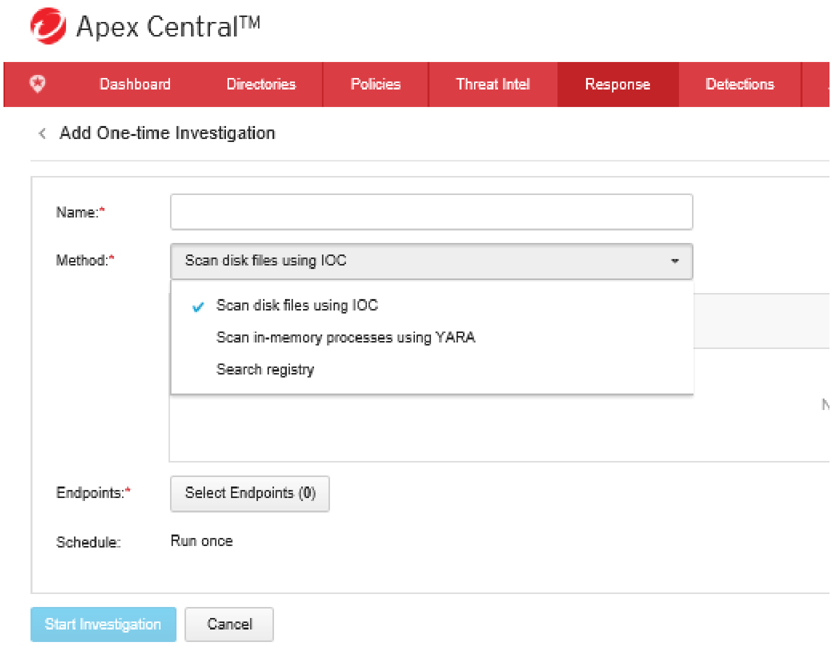
CATEGORY	ITEM	REQUIRED CONDITION
DNSENTRYITEM	HOST	IS
	RECORDDATA/HOST	IS
	RECORDDATA/ IPV4ADDRESS	IS
FILEITEM	FILENAME	IS
	FILEPATH	IS
	SHA1SUM	IS
PORTITEM	LOCALIP	IS
	REMOTEIP	IS
PROCESSITEM	ARGUMENTS	CONTAINS
	NAME	IS
	PATH	IS
	SECTIONLIST/ MEMORYSECTION/ SHA1SUM	IS
REGISTRYITEM	KEYPATH	CONTAINS
	VALUE	CONTAINS
	VALUENAME	CONTAINS
	USERNAME	IS

10.2.4 Detail investigation for file, process or registry key

When you would like to investigate in-memory process or registry key, please select **Response > Detail investigation**.



No data to display



Name:*

Method:* Scan disk files using IOC

✓ Scan disk files using IOC

Scan in-memory processes using YARA

Search registry

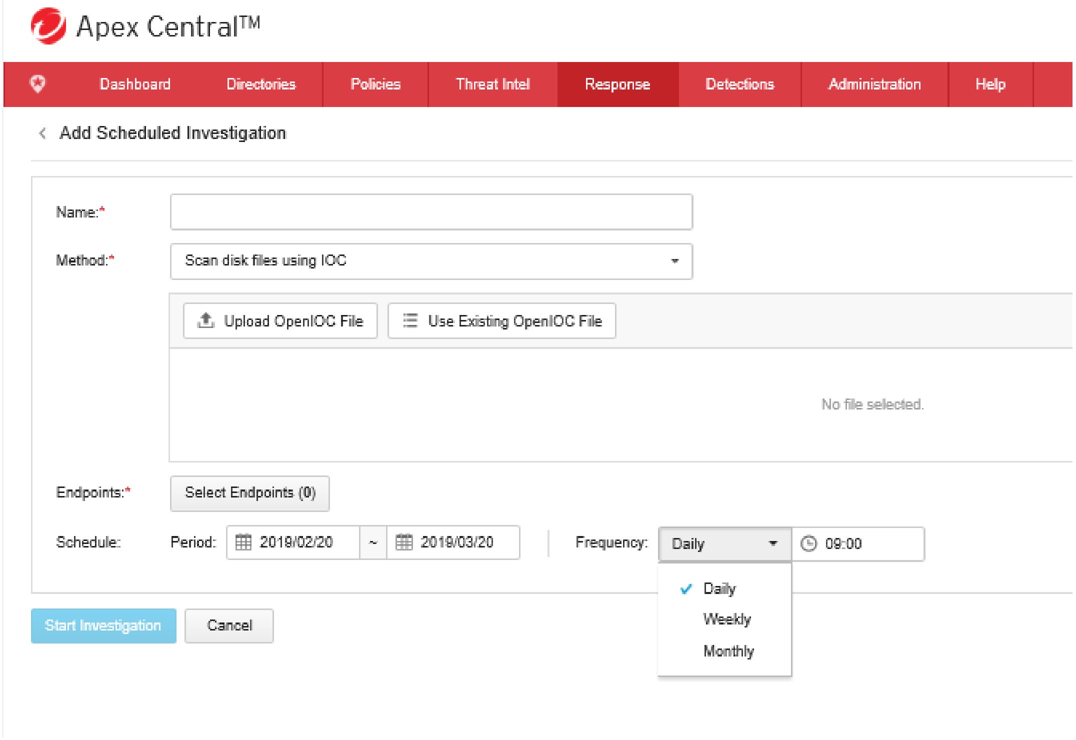
Endpoints:* Select Endpoints (0)

Schedule: Run once

Please select target endpoints for the investigation.

10.2.5 Scheduled investigation for file, process or registry key

When you would like to investigate with certain criteria regularly, please select scheduled investigation in **Response > Detail investigation**.



Name:*

Method:* Scan disk files using IOC

No file selected.

Endpoints:* Select Endpoints (0)

Schedule: Period: 2019/02/20 ~ 2019/03/20 Frequency: Daily 09:00

✓ Daily

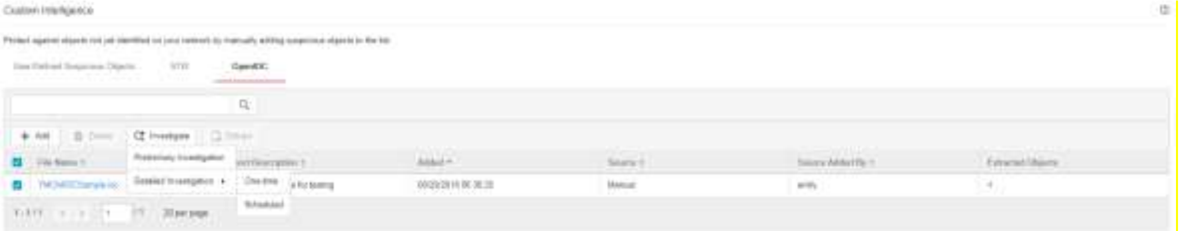
Weekly

Monthly

Please select target endpoints for scheduled investigation.

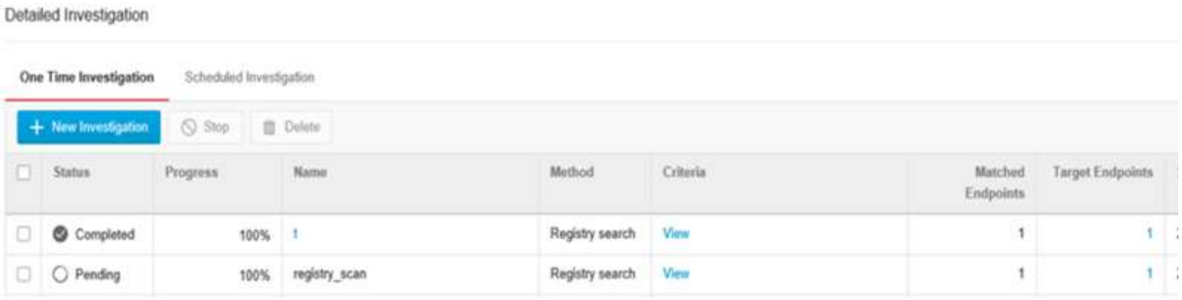
10.2.6 Conduct Root cause analysis

When endpoint matches criteria, you can start root cause analysis to see sequence related to the threat from



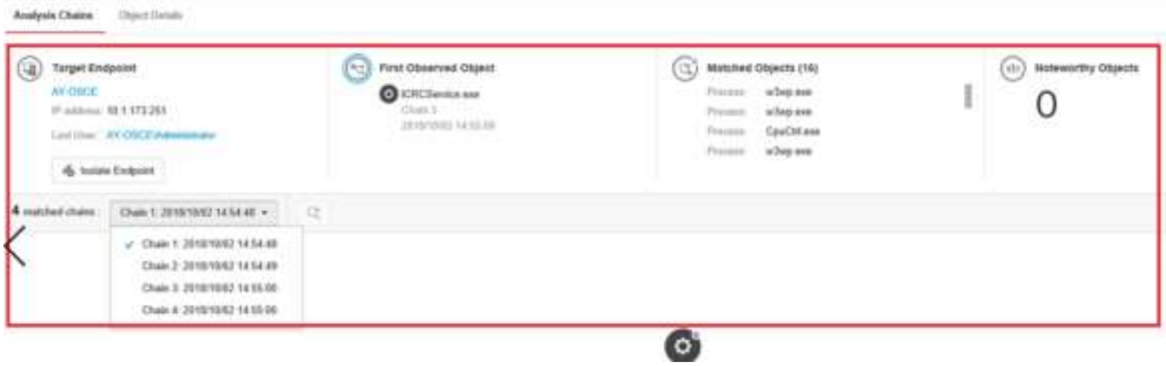
10.2.7 See Root cause analysis result

After root cause analysis is completed, you can see available sequence.



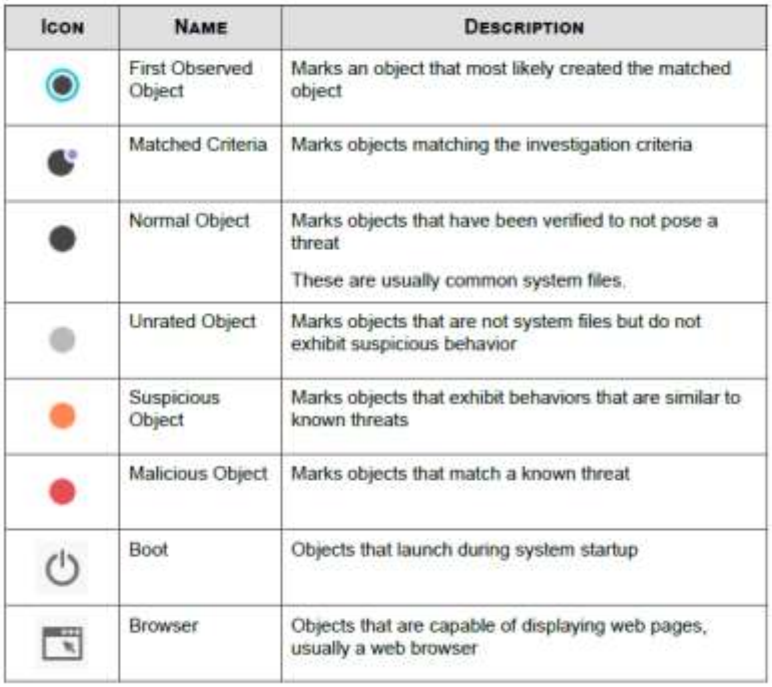
Detailed Investigation

☐	Status	Progress	Name	Method	Criteria	Matched Endpoints	Target Endpoints
☐	Completed	100%	1	Registry search	View	1	1
☐	Pending	100%	registry_scan	Registry search	View	1	1

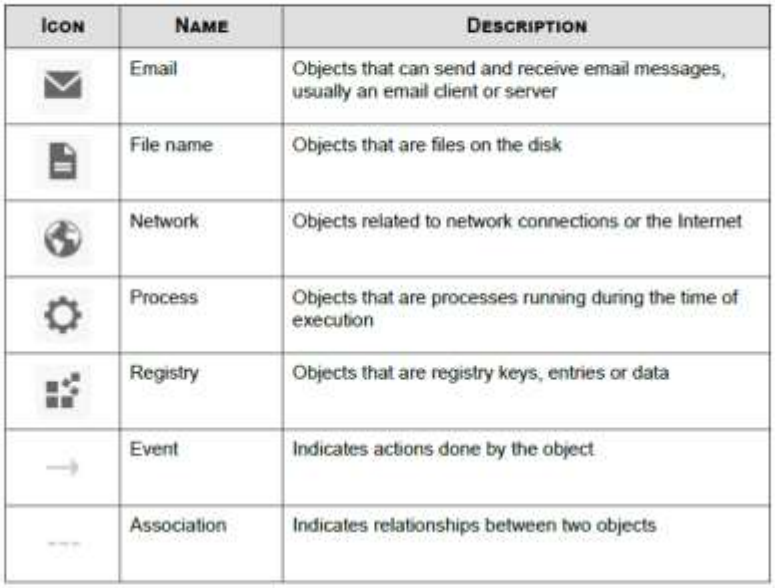


When the endpoint PC is infected or has critical issues, you can isolate the endpoint after you select endpoint.

Icon meaning:



Icon	Name	Description
◉	First Observed Object	Marks an object that most likely created the matched object
●	Matched Criteria	Marks objects matching the investigation criteria
●	Normal Object	Marks objects that have been verified to not pose a threat These are usually common system files.
●	Unrated Object	Marks objects that are not system files but do not exhibit suspicious behavior
🟠	Suspicious Object	Marks objects that exhibit behaviors that are similar to known threats
🔴	Malicious Object	Marks objects that match a known threat
⏻	Boot	Objects that launch during system startup
🗔	Browser	Objects that are capable of displaying web pages, usually a web browser



Icon	Name	Description
✉	Email	Objects that can send and receive email messages, usually an email client or server
🗎	File name	Objects that are files on the disk
🌐	Network	Objects related to network connections or the Internet
⚙	Process	Objects that are processes running during the time of execution
▦	Registry	Objects that are registry keys, entries or data
→	Event	Indicates actions done by the object
- - -	Association	Indicates relationships between two objects

11 Suspicious Object and Custom Intelligence with STIX and OpenIOC

11.1 Virtual Analyzer Suspicious Object (VASO) and User-Defined Suspicious Object (UDSO)

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

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 Apex One/Apex One/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 Apex One/Apex One/Office Scan, file is encrypted.
IP address	Log	✓ Only VASO can be added into exception list.	

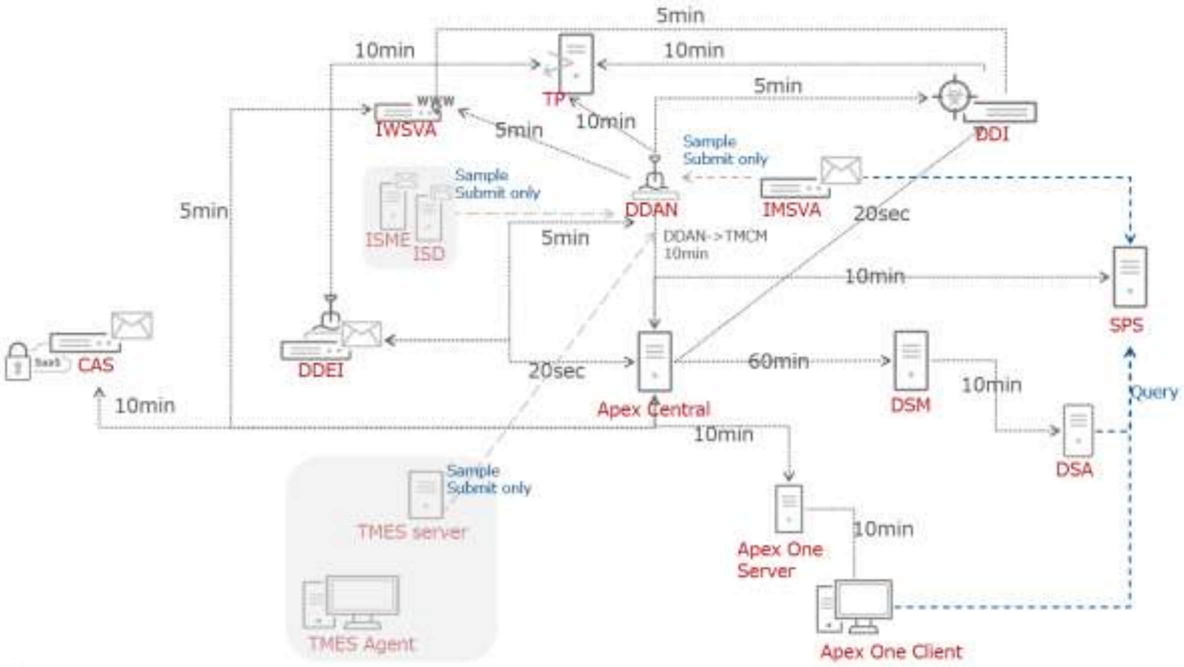
	Block		
URL	Log Block	✓ Only VASO could be added into exception list. ✓ Wild card is supported	
Domain	Log Block	✓ Only VASO can be added into exception list. ✓ Wild card is suppoted	
File (UDSO)	Log Block Quarantine	✓ UDSO has the highest priority ✓ CM will still display the detection log on the UDSO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

11.1.3 Suspicious Object Sync Interval

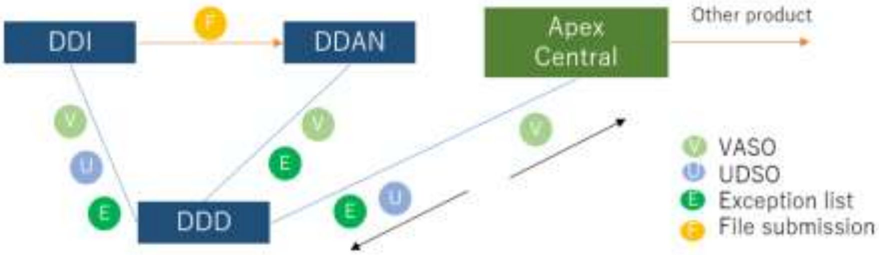
DDAN, DDEI and DDI can be the VASO source, and Apex Central can deliver them to Apex One/Office Scan, DSM, TP, IWSVA, SPS and CAS.

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

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



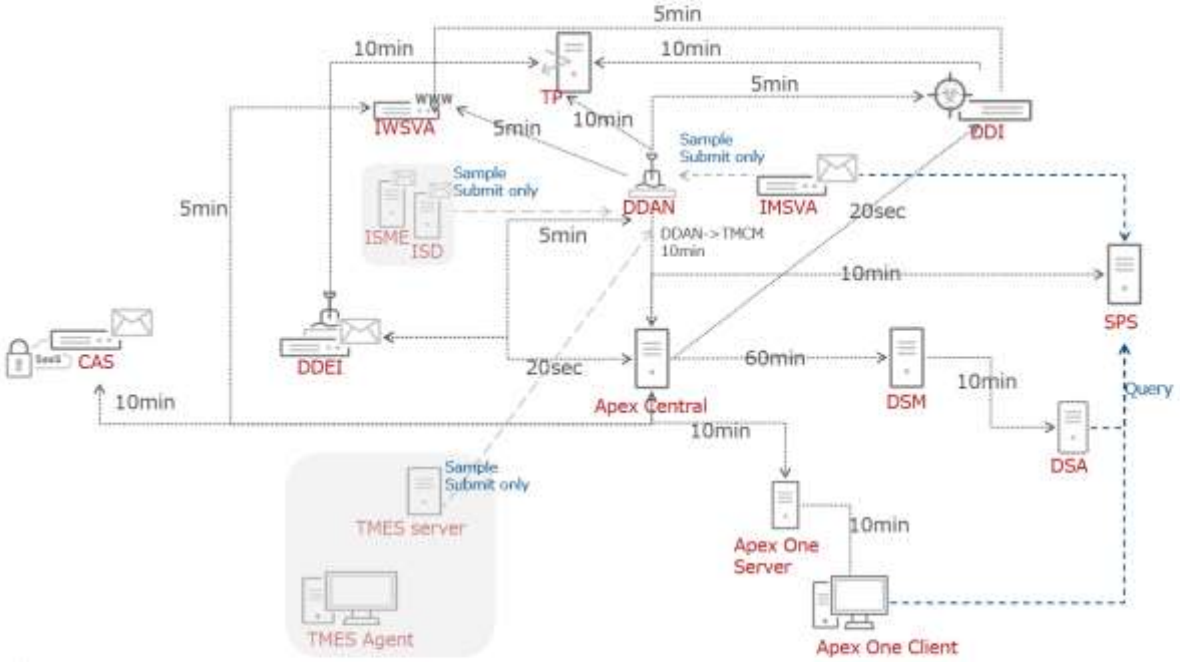
DDD has the ability to do suspicious object synchronization among managed Deep Discovery products



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

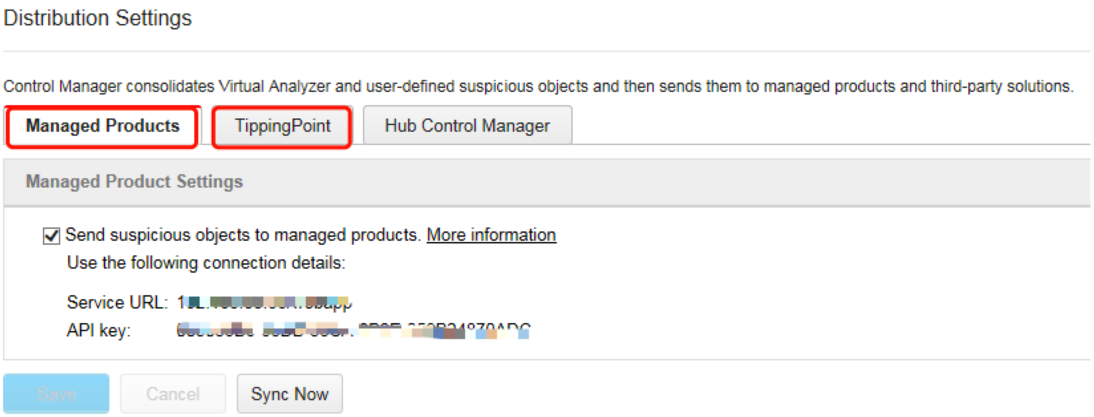
- Upload Virtual Analyzer Suspicious Object (VASO) to Apex Central.
- Push full exception list if there is an item changed (e.g.: Add/Delete from Apex Central console).

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



11.1.4 Suspicious Object Sync Now

Apex Central can sync SO with Trend Micro Managed Product Settings and the TippingPoint from **Treat Intel > Distribution Settings**.



Distribution Settings

Control Manager consolidates Virtual Analyzer and user-defined suspicious objects and then sends them to managed products and third-party solutions.

☑ Send suspicious objects to managed products. More information

Use the following connection details:

Service URL: [redacted]

API key: [redacted]

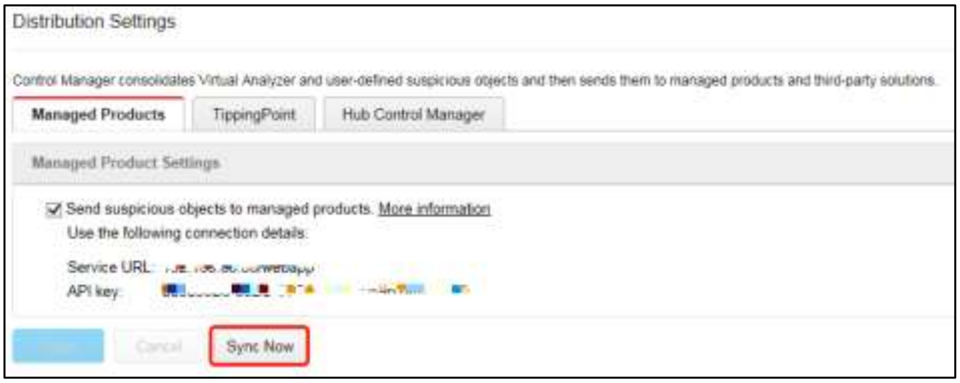
Normally, we can automatically deploy two kinds of API keys: the **DDAN API key** and the **Apex Central API key**.

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 **Treat Intel > Distribution Settings** tab.



Distribution Settings

Control Manager consolidates Virtual Analyzer and user-defined suspicious objects and then sends them to managed products and third-party solutions.

☑ Send suspicious objects to managed products. More information

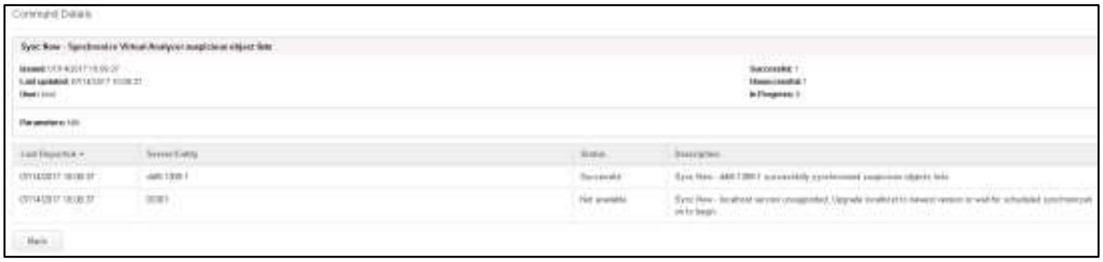
Use the following connection details:

Service URL: [redacted]

API key: [redacted]

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

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



Command Details

Sync Now - Synchronize Virtual Analyzer suspicious object lists

Issued: [illegible]
Last updated: [illegible]
User: [illegible]

Successful: 1
Unsuccessful: 1
In Progress: 0

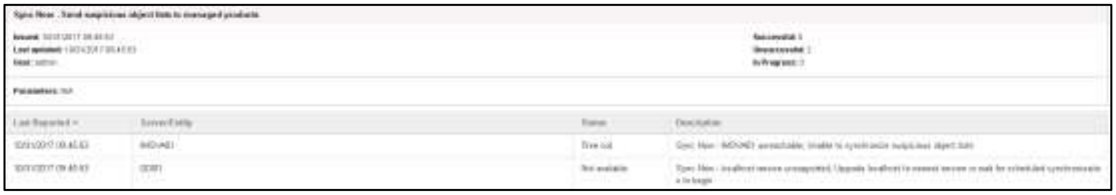
Parameters: N/A

Last Reported ▾	Server/Entity	Status	Description
07/14/2017 18:08:37	[illegible]	Successful	Sync Now - [illegible] successfully synchronized suspicious objects lists
07/14/2017 18:08:37	[illegible]	Not available	Sync Now - localhost version unsupported. Upgrade localhost to newest version or wait for scheduled synchronization to begin.

2. Consolidate the SO in Apex Central

3. Notify products to sync SO

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



Sync Now - Send suspicious object lists to managed products

Issued: [illegible]
Last updated: [illegible]
User: admin

Successful: 1
Unsuccessful: 2
In Progress: 0

Parameters: N/A

Last Reported ▾	Server/Entity	Status	Description
10/31/2017 09:45:03	[illegible]	Time out	Sync Now - [illegible] unreachable; Unable to synchronize suspicious object lists
10/31/2017 09:45:03	[illegible]	Not available	Sync Now - localhost version unsupported. Upgrade localhost to newest version or wait for scheduled synchronization to begin.

11.2 Hub and Node Apex Central

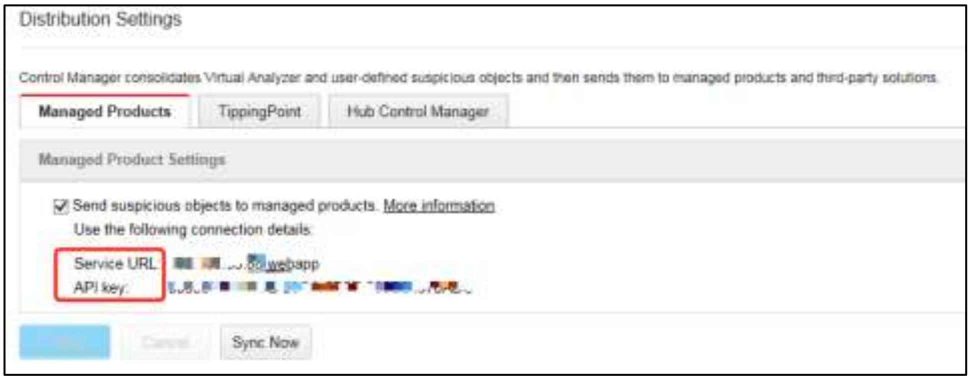
One of Apex Central servers can be set as the hub server, to share Suspicious Object among other Apex Central servers.

The SO can be synced between Hub and Nodes. All the Apex Central servers will have the same VASOs and UDSOs.

11.2.2 How to register Hub and Node Apex Central

Apex Central which should be the Node needs to register to the Hub Apex Central.

1. Go to **Treat Intel > Distribution Settings**.
2. Copy the Service URL and API key of the Hub Apex Central.



Distribution Settings

Control Manager consolidates Virtual Analyzer and user-defined suspicious objects and then sends them to managed products and third-party solutions.

Managed Product Settings

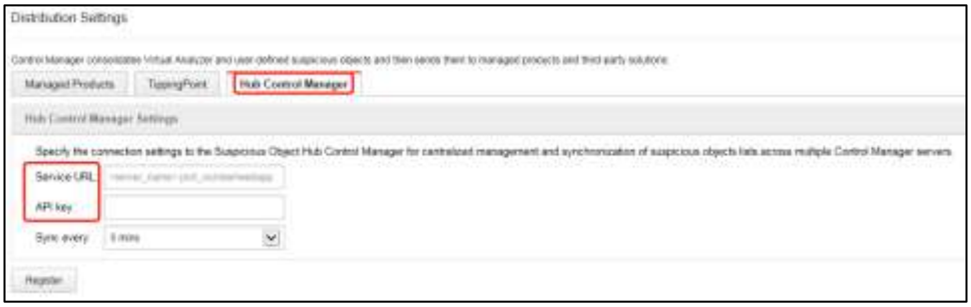
☑ Send suspicious objects to managed products. More information

Use the following connection details:

Service URL: [redacted]webapp

API key: [redacted]

3. Go to the **Hub Apex Central** tab on the **Node Apex Central**.
4. Enter the Service URL and API key that was copied from Hub Apex Central and click Register. The default sync interval is 5 minutes.



Distribution Settings

Control Manager consolidates Virtual Analyzer and user-defined suspicious objects and then sends them to managed products and third-party solutions.

Hub Control Manager Settings

Specify the connection settings to the Suspicious Object Hub Control Manager for centralized management and synchronization of suspicious objects lists across multiple Control Manager servers.

Service URL: server_name:port_number/webapp

API key:

Sync every: 5 mins

After becoming a Hub, the “This Server is Hub Apex Central now” message will be seen on the Hub Apex Central 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.

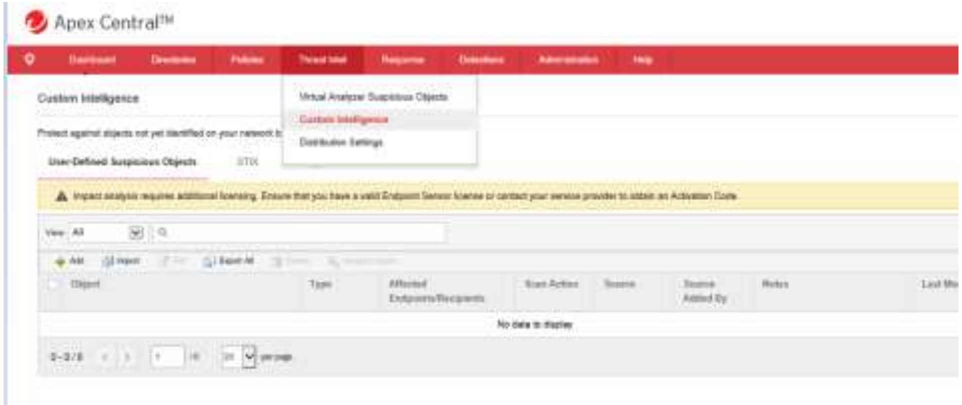
Following steps can enable exception synchronization from Hub to Node manually

1. Edit <CM_ROOT>¥SystemConfiguration.xml on Hub CM.
2. Set m_iApex CentralSoDist_ForceSyncWhitelist to 1.
3. Restart LogProcessor process.

4.

11.3 Import Suspicious Object

You can add file, file SHA-1, IP address, URL or Domain information with Scan action.



Custom Intelligence

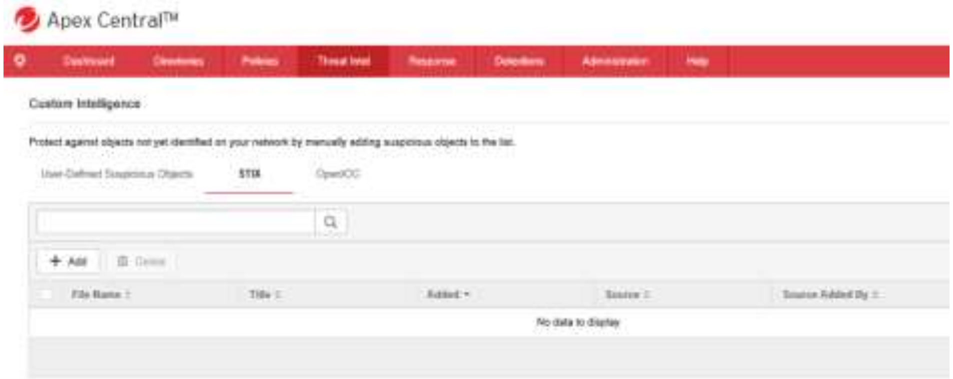
Protect against objects not yet identified on your network b

Impact analysis requires additional licensing. Ensure that you have a valid Endpoint Sensor license or contact your service provider to obtain an Activation Code.

Object	Type	Affected Endpoints/Recipients	Scan Action	Source	Source Added By	Notes	Last Mo
No data to display							

11.4 Import STIX and Open IOC files

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. Apex Central supports STIX v1.2.



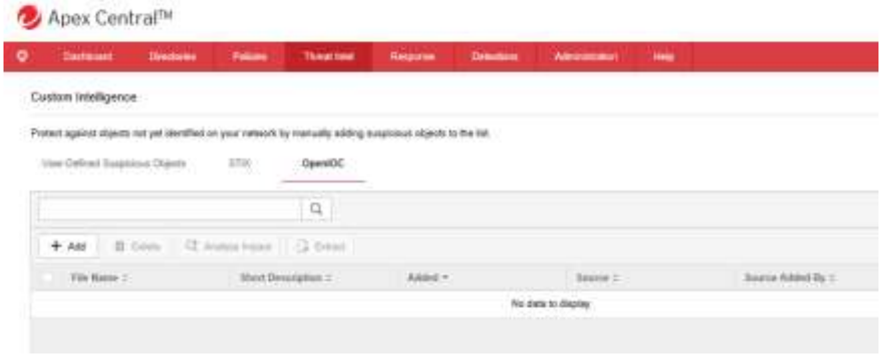
Custom Intelligence

Protect against objects not yet identified on your network by manually adding suspicious objects to the list.

File Name	Title	Added	Source	Source Added By
No data to display				

11.5 Import Open IOC files

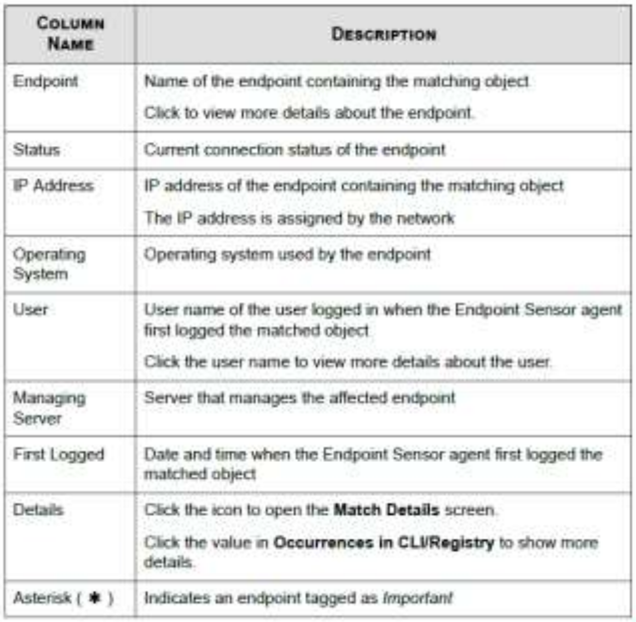
Apex Central also support OpenIOC file to detect possible threat with OpenIOC file.



Custom Intelligence

Protect against objects not yet identified on your network by manually adding suspicious objects to the list.

File Name	Short Description	Added	Source	Source Added By
No data to display				



Column Name	Description
Endpoint	Name of the endpoint containing the matching object Click to view more details about the endpoint.
Status	Current connection status of the endpoint
IP Address	IP address of the endpoint containing the matching object The IP address is assigned by the network
Operating System	Operating system used by the endpoint
User	User name of the user logged in when the Endpoint Sensor agent first logged the matched object Click the user name to view more details about the user.
Managing Server	Server that manages the affected endpoint
First Logged	Date and time when the Endpoint Sensor agent first logged the matched object
Details	Click the icon to open the **Match Details** screen. Click the value in **Occurrences in CLI/Registry** to show more details.
Asterisk (✱)	Indicates an endpoint tagged as *Important*

11.5 IOC Management

Indicators-of-Compromise (IOC) Sources:

- DDAn 6.5
- DDI 5.1
- OpenIOC Samples

It is recommended to use community IOC as an input for Apex Central. Though Apex Central supports DDI/DDAn IOC, those DDI/DDAn IOC are automatically converted to SO and sent to Apex Central. To avoid redundancy, it is not recommended to use DDI/DDAn IOCs. Once IOC is uploaded to Apex Central, the administrator use Apex One Endpoint Sensor or 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.

11.5.1 Adding IOCs

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

1. Go to **Response** > **Historical Investigation**
2. Select **OpenIOC file** in Quick Assessment menu.
3. Select Upload OpenIOC file button and add OpenIOC file for investigation.

11.5.2 Removing IOCs

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

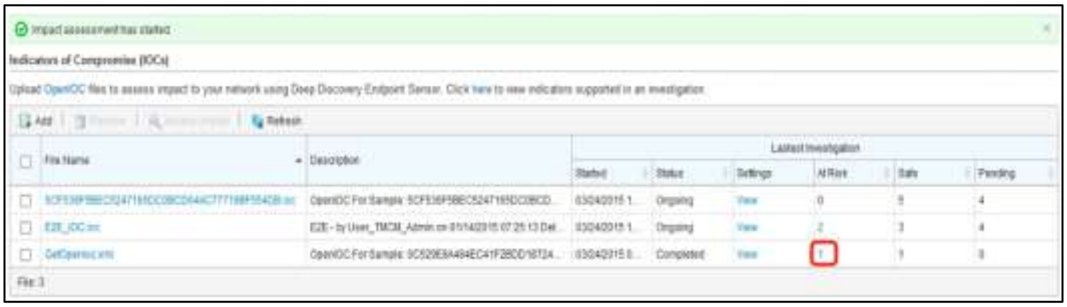
11.5.3 Impact Assessment

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.

Apex Central initiates a command to Apex One Endpoint Sensor or Trend Micro Endpoint Sensor (TMES) to assess the endpoints which are at risk.

11.5.4 At-risk Endpoints

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



Impact assessment has started

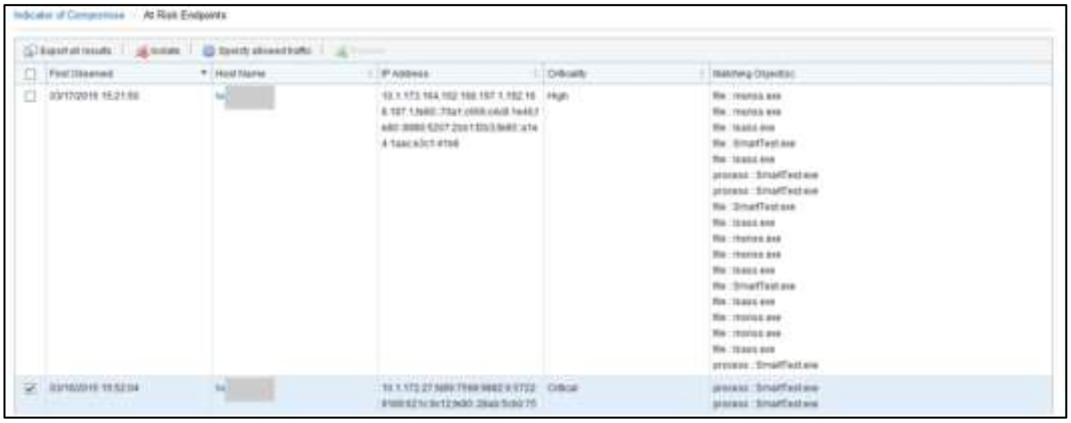
Indicators of Compromise (IOCs)

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

□	File Name	Description	Latest Investigation					
			Started	Status	Settings	At Risk	Safe	Pending
□	5CF536F5BEC5247165DC0BCD[illegible].ioc	OpenIOC For Sample: 5CF536F5BEC5247165DC0BCD...	03/24/2015 1...	Ongoing	View	0	5	4
□	E2E_IOC.ioc	E2E - by User_TMCM_Admin on 01/14/2015 07:25:13 Del...	03/24/2015 1...	Ongoing	View	2	3	4
□	GetOpenioc.xml	OpenIOC For Sample: 9C520E8A484EC41F2BDD18724...	03/24/2015 0...	Completed	View	1	1	0

File: 3

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



Indicator of Compromise > At Risk Endpoints

□	First Observed	Host Name	IP Address	Criticality	Matching Object(s)
□	03/17/2015 15:21:50	[redacted]	[illegible]	High	file : [illegible].exe file : [illegible].exe file : [illegible].exe file : SmartTest.exe file : [illegible].exe process : SmartTest.exe process : SmartTest.exe file : SmartTest.exe file : [illegible].exe file : [illegible].exe file : [illegible].exe file : [illegible].exe file : SmartTest.exe file : [illegible].exe file : [illegible].exe file : [illegible].exe file : [illegible].exe process : SmartTest.exe
☑	03/16/2015 15:52:04	[redacted]	[illegible]	Critical	process : SmartTest.exe process : SmartTest.exe

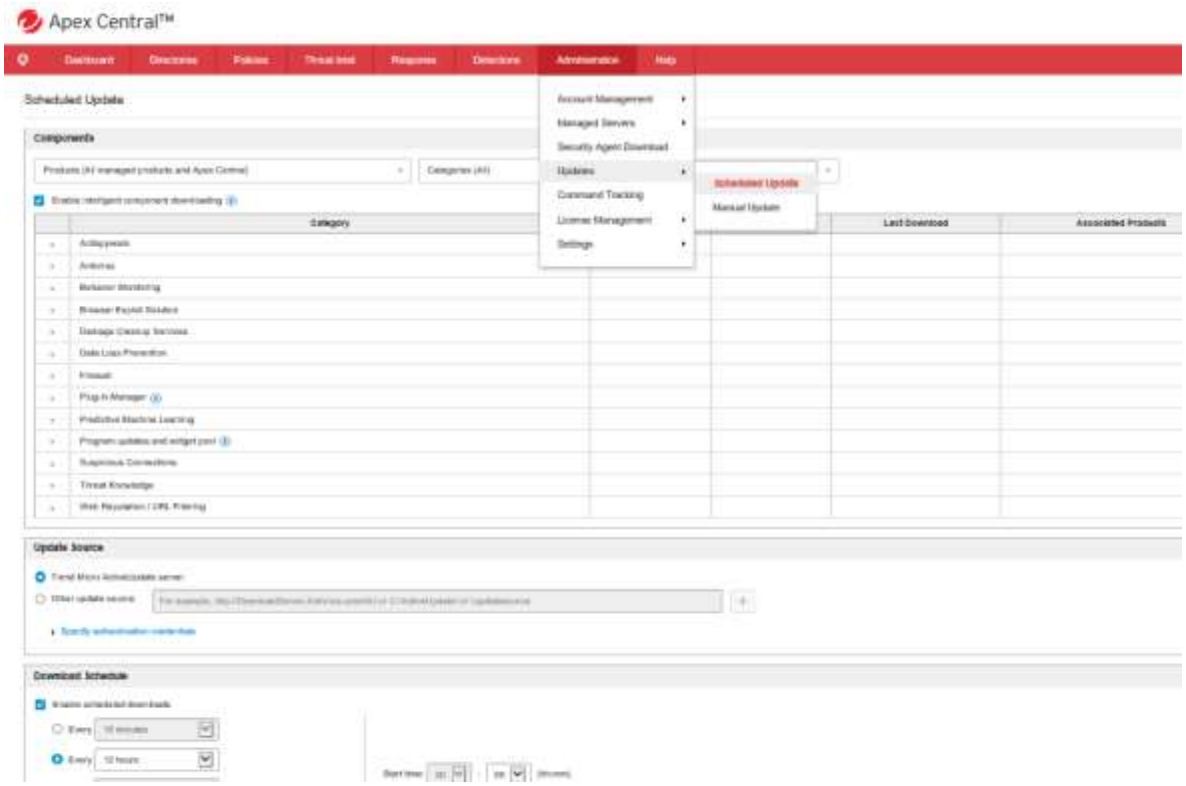
11.5.5 Other tools

- 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/Apex Central-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/Apex Central-70/tools-and-additional/suspicious-object-mi/using-the-suspicious.aspx

12 Deliver latest pattern and engine

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

Scheduled Update the Manual Update is available.



Scheduled Update

Components

Products (All managed products and Apex Central)

Categories (All)

☑ Enable intelligent component downloading

Category	Last Download	Associated Products
Antispyware		
Antivirus		
Behavior Monitoring		
Browser Exploit Solution		
Damage Cleanup Services		
Data Loss Prevention		
Firewall		
Plug-in Manager		
Predictive Machine Learning		
Program updates and widget pool		
Suspicious Connections		
Threat Knowledge		
Web Reputation / URL Filtering		

Update Source

● Trend Micro ActiveUpdate server

○ Other update source: [illegible]

Specify authentication credentials

Download Schedule

☑ Enable scheduled downloads

○ Every 15 minutes

● Every 12 hours

Start time: [illegible] : [illegible] (hh:mm)