Trend Micro Apex Central™ - Change Management Guide

8th March 2019

OVERVIEW

This document is intended to help aid customers fulfill their change request procedure in upgrading their Trend Micro Control Manager (TMCM) to Trend Micro Apex Central. After a change is planned and scheduled, the change request is set to a status of Scheduled for Review. The change manager or change coordinator has the opportunity to review change plans, schedules, and so on, before moving the change to the Implementation Approval phase. They make recommendations based on the impact on existing services, the cost of the change, and other relevant factors.

APEX CENTRAL ON-PREMISE

Description

Trend Micro centralized visibility and control delivered by Trend Micro Apex Central (formerly known as Trend Micro Control Manager) on-premise and as a service for SaaS deployments. The functionality from Apex Central and Apex Central as a Service are very close. A major difference is that Apex Central on-premise will interface with other on-premise Trend Micro products—while Apex Central as a Service will only interface with Cloud Sandbox and Apex One as a Service.

What's New	Release Date	Size (MB)
• Syslog forwarder in UI • Additional API for UDSO-Hash • New alert type of ADE detection • Virtual Analyzer and product grouping for Sample Submission • Windows Server 2019 support • Endpoint Sensor Integration • Application Control Integration • Vulnerability Protection Integration • Apex One™ Sandbox as a Service Integration • Customized Threat Intelligence • Managed Detection and Response	18th March 2019	614

Supported Operating System

Version	Supported Edition	IIS Version	Required Windows Role or Features (If lack of anyone, install flow would be blocked)		Required Windows Hotfix (Install flow would be blocked if missing)
Windows 2012 x64	Standard | DataCenter	8.0	Web Server Role (IIS) • IIS Windows authentication • IIS 6 Management Compatibility • IIS ASP • IIS CGI Message Queuing	ASP .NET 4.5 .NET Extensibility 4.5	KB2999226
Windows 2012 R2 x64		8.5			KB2919355, KB2919442
Windows 2016 x64		10.0		ASP .NET 4.6 .NET Extensibility 4.6	None
Windows 2019 x64				ASP .NET 4.7 .NET Extensibility 4.7	

Change Summary

Summary Description	Upgrade Control Manager to Apex Central	
Change Reason	Upgrade	
Change Type	Normal	Standard - routinary low risk pre-authorised changes Normal - in-between standard and emergency. Requires multi-level approval Emergency - high priority immediate implementation with CAB approval
Priority	Medium	Low - change leads to minor improvements. Medium - change requires consultation and planning High - change request is crucial and requires immediate attention
Risk Level	Moderate	Low - Low impact Moderate - Moderately acceptable risk with controllable impact High - Significant impact with high possibility of failure

Product Activation Code (AC) Guide

Activation Key Types	Entitlement Scope
Trend Micro Control Manager (TMCM) Key	AC will still work on Apex Central.
Apex One Full Feature Key	Covers all Apex One 2019 features except for Apex One Endpoint Sensor (iES) & Apex One Sandbox as a Service. Please contact Trend Micro Sales to purchase add-on features.
Apex One Endpoint Sensory Key	Covers Apex One Endpoint Sensor feature for both Apex One & Apex One (Mac)
Trend Micro Endpoint Application Control (TMEAC) Key	AC will work on Apex One to activate Application Control Integration (iAC) feature but must be deployed via Apex Central.
Trend Micro Endpoint Sensor (TMVP) Key	AC will work on Apex One to activate Vulnerability Protection Integration (iVP) feature but must be deployed via Apex Central.
Trend Micro Endpoint Sensor (TMES) Key	AC will work on Apex One to activate Endpoint Sensor (iES) feature but must be deployed via Apex Central.

Implementation, Test and Backout Plan

Implementation Plan
Prerequisites: ● 10 GB free disk space ● Window Server 2012 or above version. See **Supported Operating System** ● SQL server 2008 or above version ● .NET Framework 4.6.1 or higher version ● Supported Upgrade Path: ○ TMCM 6.0 SP3 Patch 3 ○ TMCM 7.0 ○ TMCM 7.0 Patch 1 Reminder: ● It is recommended to upgrade during off hours. Avoid upgrading during the system's peak usage times. In-place Upgrade of TMCM to Apex Central 1. Download the Apex Central installation package 2. Double-click the installer on the Control Manager server to start the installation process

3. The installer setup will check for installed .NET Framework version 4.6.1 or higher on the server. If none, the setup will install missing .NET module. Reboot is required after .NET installation. Otherwise, the installation will proceed normally.
4. Follow the installation procedure
5. Once installation finished, the services will be restarted.
6. Functional verification of test plan

Test Plan

1. Apex Central console can be accessed without issue
2. Apex Central version 2019 is showing in the Help > About console page
3. All Apex Central services are running- Trend Micro Apex Central & Trend Micro Management Infrastructure services exist and status are running
4. Original TMCM settings are migrated and intact in the new Apex Central
5. All agents are showing in the console

Post-Migration Settings

Move policy setting from Apex One into Apex Central

1. Export policy from Apex One Server
    a. Open Apex One Web Console, and go to Administration > Settings >Server Migration
    b. Download Apex One Settings Export Tool
    c. Copy the tool to the Apex One Server Computer, and double-click the ApexOneSettingsExportTool.exe to start the export
    d. Copy the export packages (zip files) to a location which could access the Apex Central Server

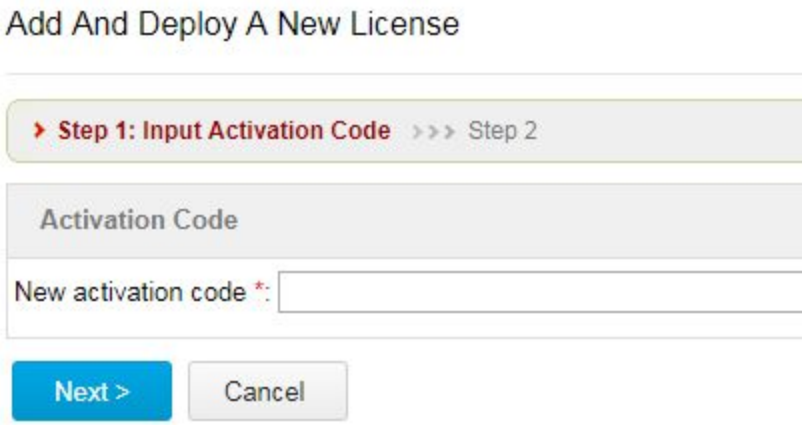
2. Import policy into Apex Central Server
    a. Open Apex Central Web console, and go to Policies ➔ Policy Management
    b. Choose Apex One Security Agent from product list, then click "Import Settings" and import the exported policy
    c. Edit the policy, set targets (either choose "Filter by Criteria" or "Specify Target(s)") and click deploy. (This step can combined with the following Endpoint sensor, Application Control and Vulnerability Protection Settings)

Enable Application Control & Vulnerability Protection feature in Apex One security agent.

Note: If the Apex One server is not activated with Apex One full feature key, deploy TMEAC or TMVP keys to managed Apex One server

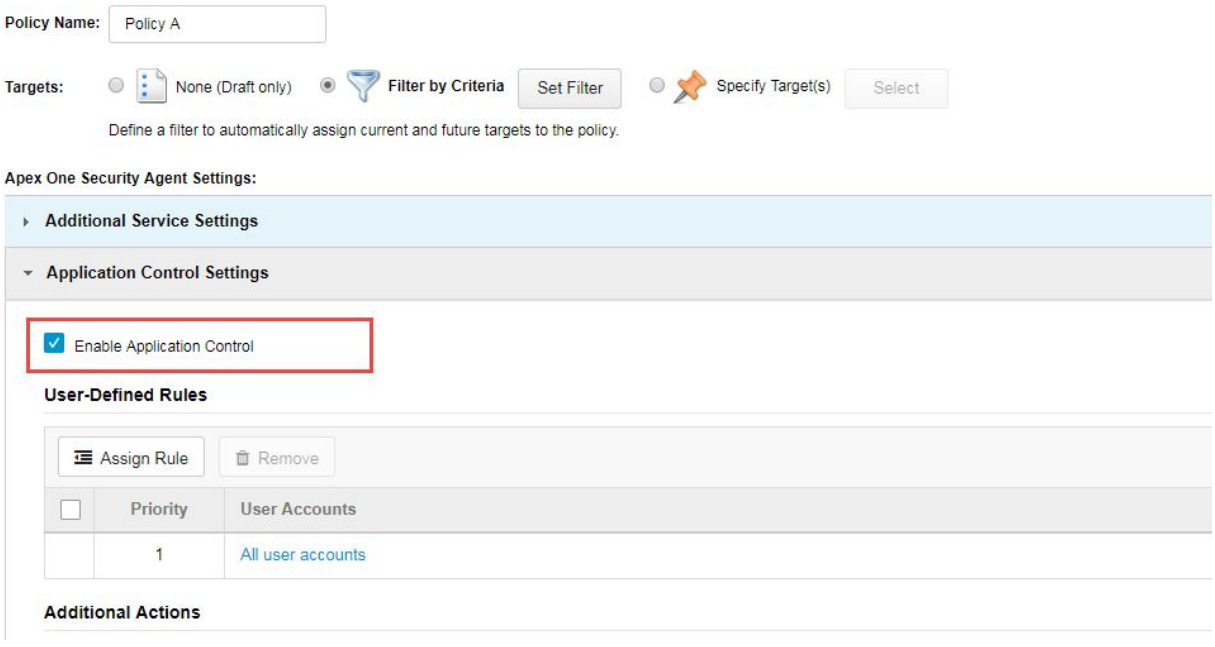
1. Deploy TMEAC and TMVP keys to the managed Apex One server

    a. Go to Administration ➔ License Management ➔ Managed Products, click "Add and Deploy" and input the TMEAC and TMVP keys separately.

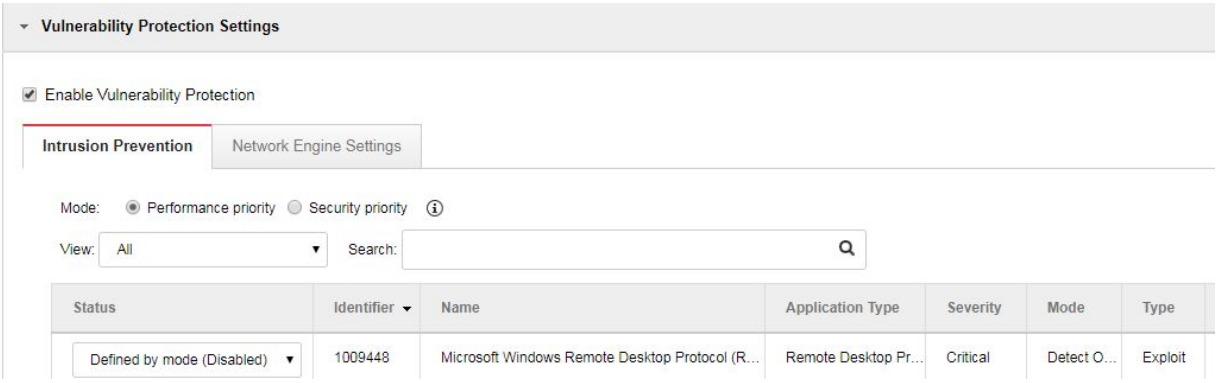


b. Choose target Apex One server to deploy the AC key
c. Back to Managed Products page, and wait for few minutes until the product applied the license. (The activated products should be greater than 0)

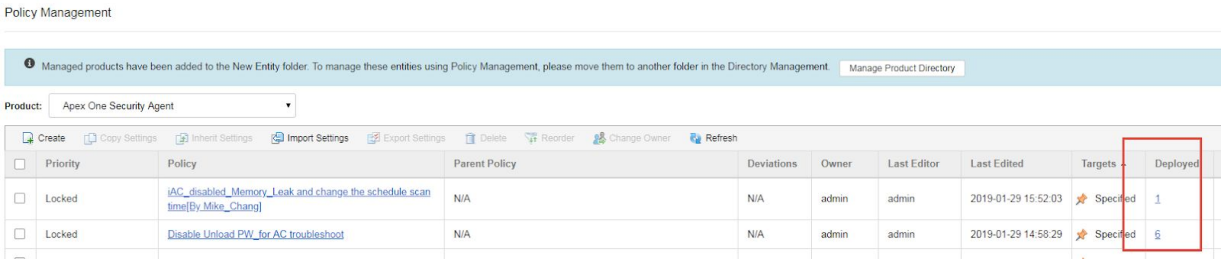
2. Go to Policy Management, choose products Apex One security agent, and create or edit policy to security agents with Application Control & Vulnerability Protection enabled
    a. Enable Application Control



b. Enable Vulnerability Protection

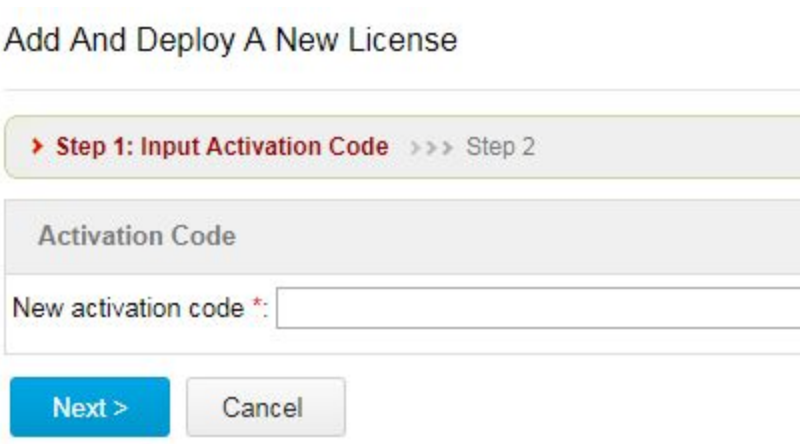


3. Wait for a few minutes until policy status become deployed



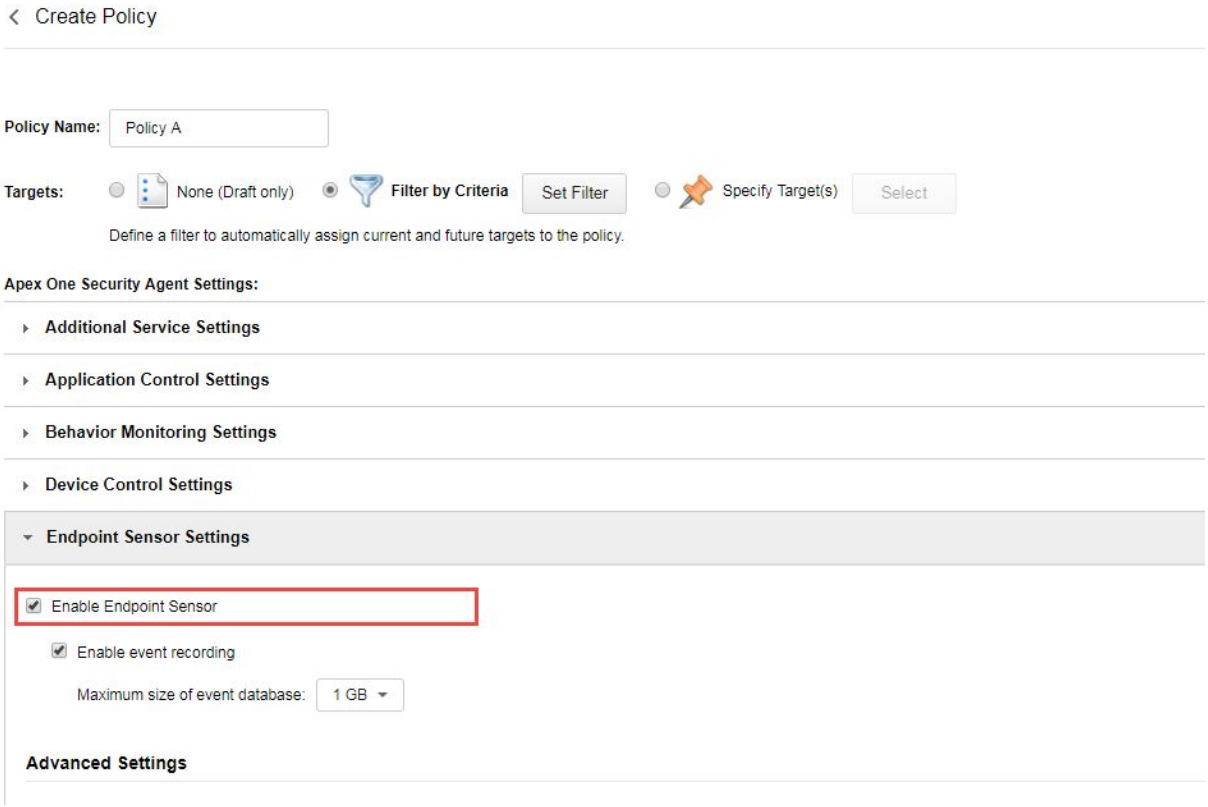
Enable Endpoint Sensor in Apex One security agent (Please skip this step if there is no Endpoint Sensor license Key)

1. Deploy Apex One Endpoint Sensor key or Trend Micro Endpoint Sensor license to managed Apex One server
    a. Go to Administration ➔ License Management ➔ Managed Products, click "Add and Deploy" and input the Endpoint Sensor AC Key

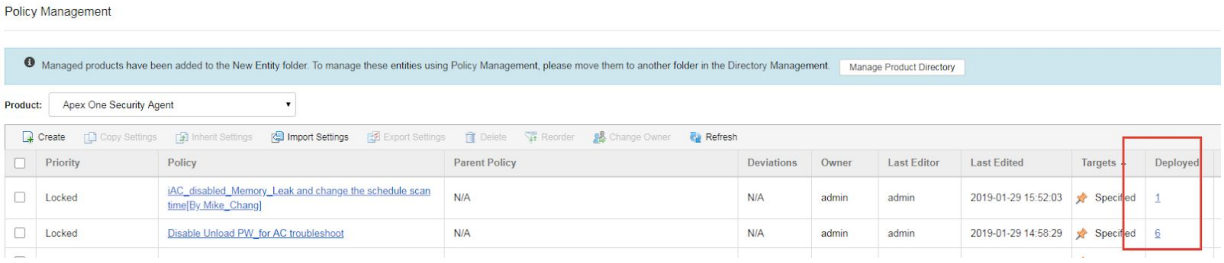


    b. Choose target Apex One server & Apex One (Mac) server to deploy the AC key
    c. Back to Managed Products page, and wait for few minutes until the product applied the license. (The activated products should greater than 0)

2. Go to Policy Management, choose products Apex One security agent, and create or edit policy to security agents with Endpoint Sensor enabled



3. Wait for a few minutes until policy status become deployed



Configure Endpoint Sensor server setting (Please ignore this step if there is no Endpoint Sensor license Key)

1. Go to Policy Management, choose products Apex One server, and create policy
2. Choose Target and configure the settings, then click Deploy

3. Wait for a while and check policy status becomes deployed

Backout Plan
Control Manager on Virtual Machine 1. Create VM snapshot of the Control Manager image before upgrading to Apex Central 2. Revert back to the VM snapshot if upgrade failed 3. Functional Verification of Backout plan Control Manager on Bare Metal (Bare Machine) 1. Backup Control Manager Database and files before upgrade 2. Perform Disaster Recovery Control Manager by reinstalling the previous TMCM version and restoring old files and database. 3. Functional Verification of Backout plan