Trend Micro Apex One™ - 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 OfficeScan On-premise to Trend Micro Apex One On-Premise. 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 ONE ON-PREMISE

Description

Trend Micro Apex One™redefines endpoint security with its breadth of capabilities delivered as a single agent, with consistency across SaaS and on-premise deployments. This offers enhanced automated detection and response and actionable insights that maximize security for customers. It is built upon the XGen™ security techniques, which is a cross-generational blend of threat defense functionality that intelligently applies the right technology at the right time. The product includes the industry's most timely virtual patching capabilities powered by Trend Micro's Zero Day Initiative, along with a range of modern technologies to detect and block advanced attacks, including fileless threats.

Apex One™ offers an industry-leading breadth of capabilities from a single user agent. Apex One™ offers a powerful EDR with automated detection & response tools, simplifying deployment and eliminating silos. It also connects to Trend Micro's managed detection and response (MDR) service option that boosts in-house teams with threat hunting and alert monitoring.

As a rule of thumb, it is recommended to upgrade during off hours. Avoid upgrading during the system's peak usage times.

What's New	Release Date	Size (MB)
• Single, Integrated Security Agent • Endpoint Sensor Integration (iES) • Application Control Integration (iAC) • Vulnerability Protection Integration (iVP) • Offline Predictive Machine Learning • Fileless Attack Protection	18th March 2019	2452

• Cloud Sandbox Integration • Managed Detection and Response • Windows Server 2019 support		

Apex One System Requirement

I. Apex One Server

Overall Minimum Requirement

	Apex One	Apex One with Endpoint Sensor (iES)
CPU	• At least 1.86 GHz Intel™ Core™2 Duo • AMD™ 64 processor • Intel 64 processor	• At least 1.86 GHz Intel™ Core™2 Duo • AMD™ 64 processor • Intel 64 processor
RAM	• 3 GB or more	• 8 GB or more
Disk	• 12 GB or more	• 12.5 GB or more
SQL	Recommended to turn on SQL browser service	• SQL Server 2016 Standard SP1 or above • Must enable Full Text Search feature • SQL express is not supported

Software Specification

	Apex One	Apex One with Endpoint Sensor (iES)
OS	•Windows 2012 •Windows 2012 R2 •Windows 2016 •Windows 2019	Same with Apex One
SQL	SQL Server •2008 R2 Express •SP2 •2008 •2008 R2 •2012 •2014 •2016 •2016 Express SP1 •2017	•SQL Server 2016 Standard SP1 or above •Must enable Full Text Search feature •SQL express is not supported

Prerequisite for IES service

1. Cannot coexist with existing Redis server
2. Does not support upgrade and backward compatibility
3. Cannot coexist with old version of Trend Micro Endpoint Sensor (TMES)

II. Apex One Agent

Overall Minimum Requirement

	Apex One	Apex One with Endpoint Sensor (iES)
CPU	Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor	• Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	2 GB or more	2 GB or more
Disk	• 1.5 GB or more • 2 GB recommended	• 2 GB or more • 3 GB recommended

Software Specification

	Apex One	Apex One with Endpoint Sensor (iES)
OS	•Windows 7 SP1 •Windows 8.1 •Windows 10 •Windows 2008 R2 SP1 •Windows 2012 •Windows 2012 R2 •Windows 2016 •Windows 2019 •Embedded/server core/IOT..	•Windows 7 SP1 •Windows 8.1 •Windows 10

Change Request Summary

Summary Description	Upgrade OfficeScan XG to Apex One	
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
OfficeScan Key	AC will still work on Apex One but will only activate standard OfficeScan features. Please contact Trend Micro Sales to request for Apex One Full Feature Key.
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)
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 Vulnerability Protection (TMVP)	AC will work on Apex One to activate Vulnerability Protection Integration (iVP) feature but must be deployed via Apex Central.
Trend Micro Endpoint Sensor (TMVP)	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
Apex One While you have multiple upgrade methods to move to Apex One, it is highly recommended that you install a fresh Apex One server and move agents to the new server at a pace and schedule you decide upon. This gives you more control over your upgrade and limits possible risk factors. Prerequisites: • Supported OS • Supported Database • iVP service cannot be upgraded from TMVP Server. • iAC service cannot be upgraded from TMEAC Server. • iAC and iVP service shall be installed by Apex One Server Installer only • TMEAC and TMVP Server should be manually removed if users do not need it anymore prior to upgrade • If TMEAC or TMVP Agent exists, it will be uninstalled when Apex One security agent policies are pushed to these agents (with these features enabled). • Apex One agent should be installed and running properly before iAC and/or iVP security agent policy is deployed. • Apex One Server should register to Apex Central Server.

In-place Upgrade of OSCE XG to Apex One

1. Download the Apex One installation package
2. Check the Prerequisite
3. Uninstall TMEAC, TMVP or TMES server running on the same machine
4. Double-click the installer on the OSCE XG server to start the upgrade process
5. Follow the installation procedure
6. Once installation is finished, the services will be restarted.
7. Functional verification of test plan

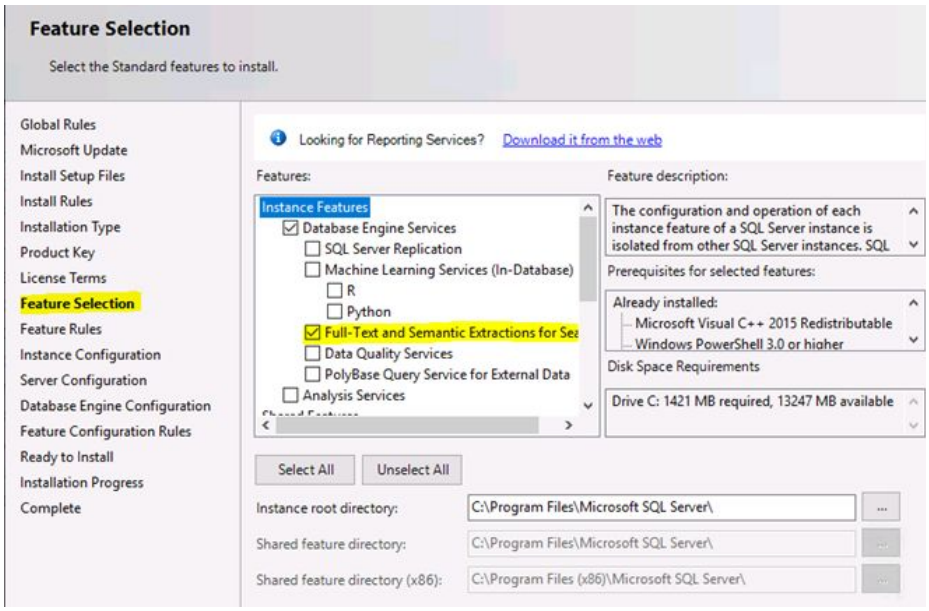
Apex One with Endpoint Sensor (iES)

Prerequisites:

- Supported OS
- Supported Database
- iES service cannot be upgraded from TMES Server.
- iVP service cannot be upgraded from TMVP Server.
- iAC service cannot be upgraded from TMEAC Server.
- iAC, iVP and iES service shall be installed by Apex One Server Installer only
- TMEAC, TMVP and TMES Server should be manually removed if users do not need it anymore prior to upgrade
- If TMEAC, TMVP or TMES Agent exists, it will be uninstalled when Apex One security agent policies are pushed to these agents (with these features enabled).
- Apex One agent should be installed and running properly before iAC, iVP and/or iES security agent policy is deployed.
- Apex One installer will check if the server has existing and running Redis service. If yes, Apex One installer will ask user to remove the existing Redis or advise user to install iES in another server because iES will install a dedicated Redis service which cannot coexist with another Redis service.
- Apex One Server should register to Apex Central Server.

In-place Upgrade of OSCE XG to Apex One

1. Download the Apex One installation package
2. Check the Prerequisite
3. Uninstall TMES server running on the same machine
4. Follow SQL practice to upgrade existing DB to MS SQL 2016 SP1 std or above (SQL express is not supported.) Must turn on “Full text search” feature in advance.



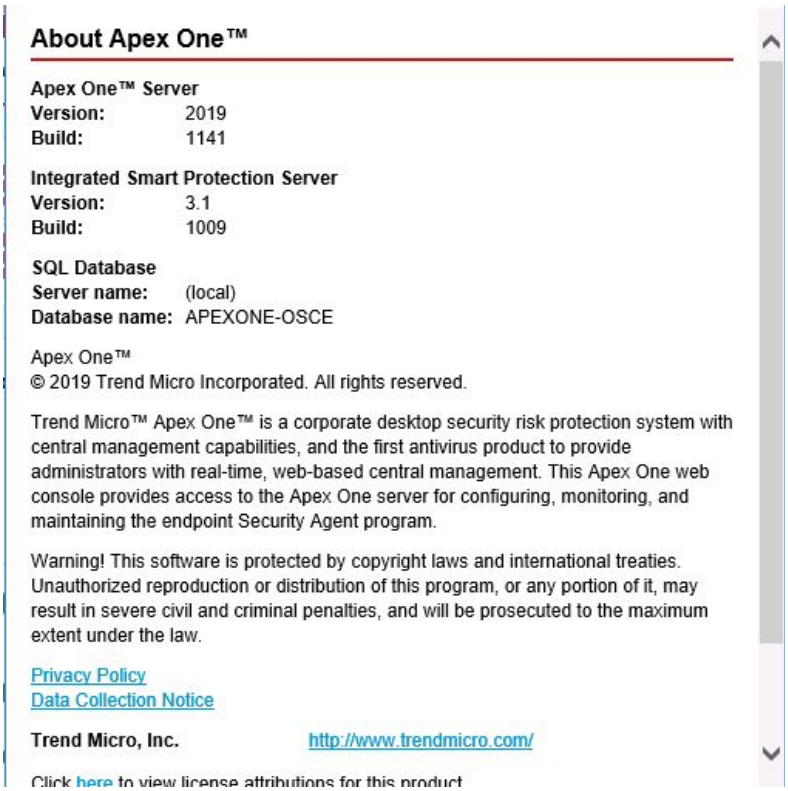
5. Once iES supported DB is ready, proceed with OSCE XG upgrade
6. Double-click the installer on the OSCE XG server to start the upgrade process
7. Follow the installation procedure
8. Once installation is finished, the services will be restarted.
9. Functional verification of test plan

Test Plan

Apex One Server side:

1. Check the following Apex One server services:
    a. Apex One Master Service
    b. Apex One Plug-in Manager
    c. Apex OneActive Directory Service
    d. Apex One Log Receiver Service
    e. Apex One Deep Discovery Service
    f. Apex One database process

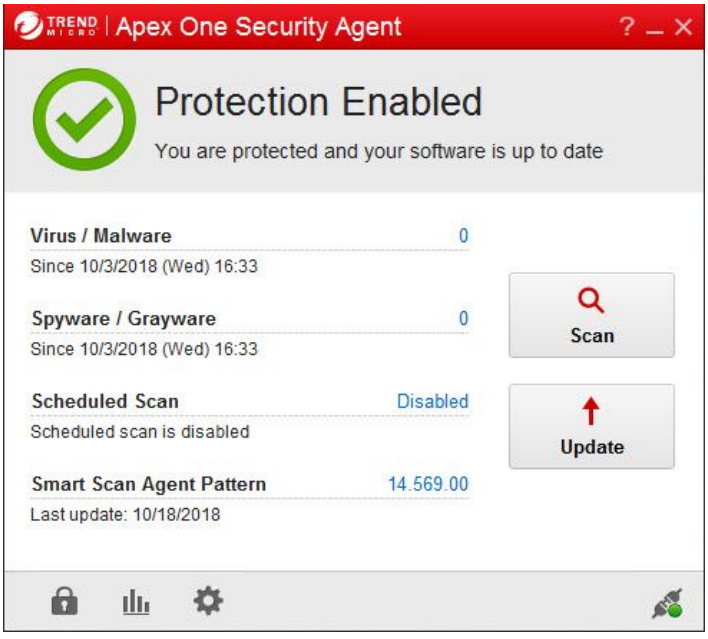
2. Apex One console can be accessed without issue
3. Apex One version 2019 is showing in the Help > About console page



4. All agents are showing in the console

Apex One Agent side:

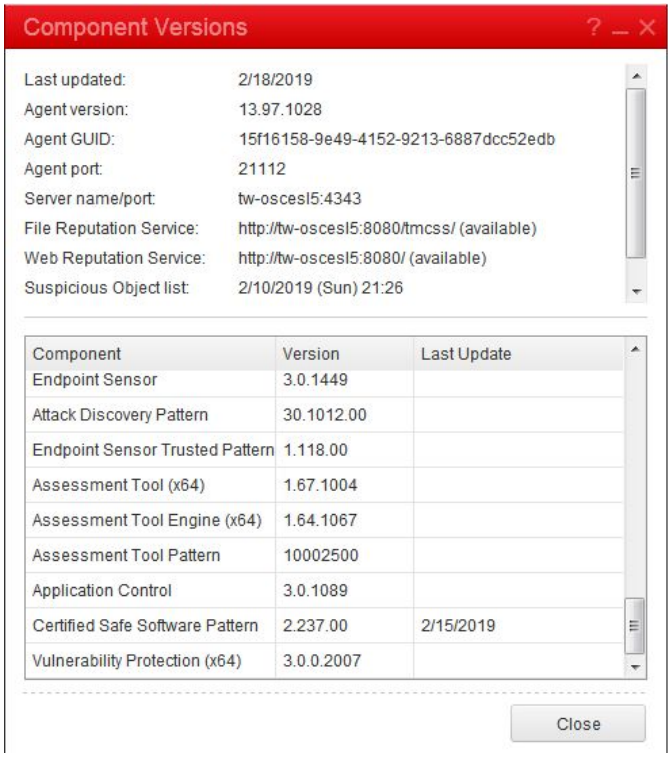
- Check Apex One Security Agent status



- The following services are present and running:
  - Apex One Common Client Solution Framework Service

- Apex One NT Firewall
- Apex One NT Listener
- Apex One NT RealTimeScan
- Trend Micro Unauthorized Change Prevention Service
- Trend Micro Apex One Data Protection Service

- Check agent version from Component versions of Apex One



- Check service if enabled (green) via Apex One Security Agent

Backout Plan
OfficeScan XG on Virtual Machine ● Create VM snapshot of the OfficeScan XG image before upgrading to Apex One ● Revert back to the VM snapshot if upgrade failed ● Functional Verification of Backout plan OfficeScan XG on Bare Metal (Bare Machine) ● Backup OfficeScan XG database and files before upgrade ● Perform Disaster Recovery for OfficeScan XG by reinstalling the previous OSCE version and restoring old files and database. ● Functional Verification of Backout plan