Migration Guide for Trend Micro Apex One On-Premise

Overview

This document is intended to help aid partners/customers with information and steps to follow in order that the Trend Micro OfficeScan (OSCE) upgrade and migration process to Trend Micro Apex One On-premise is as painless as possible.

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.

On-premise vs. SaaS (Overview)

Comparison items	On-premise	SaaS
Server Location	On-premise	On the Cloud
EDR activity data Location	On-premise （Agent and Server side）	On the Cloud
EDR activity data Retention period	Up to about 3 months (2GB) (Agent Side)	30 days (default) / 90・180・365 days (need option license)
EDR supported OS	Windows/Mac	Windows/Mac/Linux
Offline Agents EDR	Primary analysis only	Detailed analysis is also possible
Connected Threat Defense	Between On-premise Products	Between SaaS Products
Sand Box	Use On-premise DD series （Other Products）	Cloud Sand box (option license)
VDI Option	Yes	No
DLP	YES (option license)	YES(default)
Reputation Query	SPS/SPN	SPN only
Manage Off-premise agent	Need Edge Relay Server	Off-premise agent can be connected to the server directly

On-premise vs SaaS. (Management Feature)

In the on-premise version, there are some differences in terms of operational and management functions compared to the SaaS version due to architectural changes.

Comparison items	On-premise	SaaS
Manage Agent settings	・Domain level settings from Apex One console ・Policy level setting from Central console	・Policy level setting from Central console
Server Patch Management	Need apply each patch by user manually	Automatically applied by monthly maintenance.
Component Rollback	Can be rolled back by user side operation.	Roll back by TM backend as needed
Administrator notification settings	・Email Notification by Apex One/Central Server (sent from specified SMTP server) ・Windows NT event/SNMP trap	・Email notification by Central server (sent from TM backend system)
Server/agent communication	Duplex Communication	Polling communication from agent
Collect Quarantined Files on the Server	Collect from Server directory in local	Collect by TM engineer in support case ・Specify a local quarantine folder and collect it directly

On-Premise vs Saas (Unchanging Feature)

Some of the features that are available in the SaaS version as well as the on-premises version.

Note: The following list shows just an example, and many other features are available as well

Comparison items	On-premise	SaaS
Agent functions	EPP/EDR	EPP/EDR (SaaS EDR is more enhanced)
Isolate Agents	✓	✓
Endpoint Location Setting	✓	✓
Update agent function	✓	✓
Component delivery control	✓	✓
Restore quarantined files	✓	✓
Add a login account	✓	✓
NAT environment	✓	✓
Syslog Transfer	✓	✓※1
Use ATTK	✓	✓※2
Deploy by Disk Image	✓	✓

※1. Need the SaaS server and Syslog server can be connected directly or using API.
※2. Remote delivery by TrendMicro ToolBox is not supported in SaaS.

Deployment Comparison

On-premise vs Saas (Pros & Cons)

Products	PROS	CONS
Apex One On-Premise	Full Coexist mode features	Higher initial cost in building or upgrading the infrastructure to host the Apex One, Apex Central, and Edge relay (hardware, software, electricity, rack space, etc.)
	Virtual desktop infrastructure (VDI) Support	Scalability is dependent on the customer's IT infrastructure
	More options for full sandbox integration	Patch management, Server maintenance, Backup strategy, and Disaster Recovery is dependent on customer's IT Security Management
	Unlimited* EDR log retention capability	
	Recommended for organizations preferring "on-premise only" and private cloud setup	
Apex One SaaS	Hosted in Azure	
	Lower setup cost as Apex One/Apex Central is hosted in the cloud	Downtime during backend maintenance is controlled by Trend Micro
	Reliable Apex One/Apex Central image provisioning, fast deployment and highly scalable	Not recommended for customers with very slow Internet or data transmission cap
	No maintenance overhead for Apex One/Apex Central Server	Trend Micro is responsible for the security and privacy of the hosted solution (Patching, OS hardening, VAPT, etc.)
	Suitable for new and existing Trend Micro customers supporting full and hybrid cloud setup	
	Cloud App Security Integration	

Deciding Which Upgrade Path to Follow

In-Place Upgrade	New Server Migration
The **in-place upgrade** allows you to upgrade your existing installation of OfficeScan to Apex One without removing the older version first. Also known as "on top" or "over the top" installation. This is the default upgrade method and the practical way to upgrade OfficeScan to Apex One but will require extensive planning. All components are upgraded to a newer version using the same configuration settings, ports, and policies as your previous installation.	The **new server migration** process requires you to install Apex One on a separate machine and then import the configuration settings, ports, and policies of your OfficeScan server. This upgrade path provides administrators with more control over your OfficeScan upgrade process and limits possible risk factors.
Requires extensive planning and due diligence prior to the upgrade.	Planning and due diligence are also required prior to the upgrade.
Best for customers with single OfficeScan server and a relatively small number of OfficeScan agents.	Best for customers with multiple OfficeScan servers and a large number of OfficeScan agents
Recommended for customers with budget constraints in terms of purchasing new hardware and software components.	Recommended for customers that can afford a new server instance
Best for customers with relatively lax downtime policy	Best for customers with strict downtime policy
Best for customers with the requirement to maintain or recycle existing infrastructure and resources.	Best for customers who are decommissioning the old or existing OSCE server machine in the near future.
Does NOT require purchasing a new physical box or provisioning a new VM	May require a new physical box or provisioned VM unless the customer has an available/spare server or VM instance.
May need to upgrade hardware and software components like the CPU, Memory, Disk Space, the OS, application, etc. including all required patches and service packs on the existing machine hosting the OSCE server to meet the Apex One system requirements.	It is assumed that the customer follows the Apex One system requirements in building or provisioning the target Apex One Server machine
	Apex One no longer supports the codebase database. Although the in-place upgrade is supported, it is recommended to set up a separate Apex One server and move existing agents to Apex One.

Pre-Upgrade Checklist

Item	Details	Remarks
Installation and Upgrade Guide	Apex One Installation and Upgrade Guide	The customer and the Trend Micro representative should review and agree with the installation and upgrade steps before proceeding with the actual upgrade process.
	Apex Central Installation and Upgrade Guide	
System Requirements	Apex One on-premises	The customer must meet all Apex One and Apex Central system requirements before proceeding with the upgrade.
	Apex Central on-premises	
Supported TMCM versions for Apex Central Upgrade	Control Manager 7.0 Patch 1	If the customer is using an older version, it is recommended that they upgrade to any of the listed TMCM versions prior to Apex Central upgrade or totally have a fresh Apex Central setup.
	Control Manager 7.0	
	Control Manager 6.0 Service Pack 3 Patch 3	
Supported OfficeScan versions for Apex One Upgrade	• OfficeScan XG Service Pack 1	If the customer is using an older version, it is recommended that they upgrade to any of the listed OfficeScan version prior to Apex One upgrade or totally have a fresh Apex One setup.
	• OfficeScan XG	
	• OfficeScan 11.0 Service Pack 1	
Compatible OS for Apex One Agents	• Windows 7 SP1	Trend Micro highly recommends applying all available patches and hotfixes on Windows machines before performing an upgrade.
	• Windows 8.1	
	• Windows 10	
	• Windows 2008 R2 SP1	
	• Windows 2012	
	• Windows 2012 R2	
	• Windows 2016	
	• Windows 2019	
Compatible OS for Apex Central	• Windows 2012	Windows 2012 requires updates KB2999226 and KB2975331 while Windows 2012 R2 requires KB2919442, KB2919355, and KB3000850 before installing or upgrading to the Apex Central server. Trend Micro highly recommends applying all available patches and hotfixes on the server before performing an upgrade.
	• Windows 2012 R2	
	• Windows 2016	
	• Windows 2019	
Supported Operating Systems to host Apex One Server	• Windows Server 2012	Windows 2012 R2 requires updates KB2919442 and KB2919355 before installing or upgrading to the Apex One server. Trend Micro highly recommends applying all available patches and hotfixes on the server before performing an upgrade.
	• Windows Server 2012 R2	
	• Windows Server 2016	
	• Windows Server 2019	

Item	Details	Remarks
Unsupported OS Apex One Agents	• Windows XP	Customers are recommended to keep their OfficeScan XG SP1 server to continue protecting and managing the following legacy Windows OS.
	• Windows 7	
	• Windows 8	
	• Windows Server 2003	
	• Windows Server 2008	
	• Windows MultiPoint Server 2010	
	• Windows MultiPoint Server 2011	

The knowledge base is available for this topic, please visit the link here.

Sizing Consideration

This section provides information on the number of supported agents depending on enabled features.

The sizing data below is for reference only. It is possible for Apex One to manage more than the upper bound recommendation below if using higher spec machines. Customers can gradually increase the number of endpoints while observing the server performance data. The actual sizing limit can vary depending on product configurations and customer environment factors. For more info, visit this kb link.

APEX CENTRAL				
Overall Endpoint Count	**CPU**	**RAM**	**SQL**	**SQL Server Spec**
Up to 5,000	8 cores	12GB	Express/Standalone	N/A
Up to 20,000	8 cores	8GB	Standalone	8 cores, 12GB RAM
Up to 50,000	8 cores	8GB	Standalone	12 cores, 16GB RAM
Up to 200,000	12 cores	24GB	Standalone	24 cores, 80GB RAM (Enterprise SSD)

APEX ONE WITH PURE ANTI-MALWARE FUNCTION (NO INTEGRATED SERVICES)					
Endpoint Count	**CPU**	**RAM**	**SQL**	**SQL Server Spec**	**Smart Protection Server**
up to 5,000	4 cores	8GB	Express/Standalone	N/A	Integrated/Standalone
up to 20,000	8 cores	16GB	2016 Standalone	4 cores, 8GB RAM	Standalone
up to 50,000	12 cores	32GB	2016 Standalone	4 cores, 8GB RAM	Standalone

Note: *MS SQL Express has a 10GB maximum Database size and high load scenarios are not supported.*

APEX ONE WITHOUT ENABLING ENDPOINT SENSOR FEATURE					
Endpoint Count	**CPU**	**RAM**	**SQL**	**SQL Server Spec**	**Smart Protection Server**
up to 3,000	8 cores	8GB	Express/Standalone	N/A	Integrated/Standalone
up to 10,000	8 cores	32GB	2016 Standalone	4 cores, 8GB RAM	Standalone
up to 25,000	16 cores	64GB	2016 Standalone	4 cores, 8GB RAM	Standalone
25,000 and up	Multiple Apex One Servers are needed to distribute load. Apex Central can be used to manage multiple Apex One servers. Please refer to the Apex Central sizing data for more details.				

Note: *MS SQL Express has a 10GB maximum Database size and high load scenarios are not supported.*

APEX ONE WITH ENABLED ENDPOINT SENSOR FEATURE							
Endpoint Count	**CPU**	**RAM**	**Maximum Memory Allocation Setting**	**SQL**	**SQL Server Spec**	**Maximum Metadata Storage Setting**	**Smart Protection Server**
up to 3,000	8 cores	32GB	Recommended value: 20GB	2016 SP1 or higher (Standalone)	4 cores, 16GB RAM	Recommended value: 120GB per month	Standalone
Up to 10,000	16 cores	96GB	Recommended value: 48GB	2016 SP1 or higher (Standalone)	4 cores, 32GB RAM	Recommended value: 450GB per month	Standalone
10,000 and up	Multiple Apex One Servers are needed to distribute load. Apex Central can be used to manage multiple Apex One servers. Please refer to the Apex Central sizing data for more details.						

Note:

- ***Above estimates are for Apex One Security Agents running on Windows platform.***
- ***Maximum metadata storage and Maximum memory allocation settings are configured on the Apex Central console in Apex One Server policies. The default 4GB maximum memory allocation settings are recommended for up to 600 endpoint agents.***

SMART PROTECTION SERVER SIZING (HTTPS*)				
Endpoint Count	**vCPU**	**RAM**	**Disk**	**Hypervisor**
Up to 17,000	4 cores	4GB	55GB	ESXi 6.5
Up to 20,000				Xen 7.1
Up to 21,000				Hyper-V 2016

***Note*:** *Agents are configured to send queries with HTTPS.*

System Requirements

Apex One Server

	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

Apex One Agent

	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

Note: The information above for Apex One Server and Apex One Agent are all overall minimum system requirements.

Apex Central

For the Apex Central the minimum overall system requirement will depend on the Windows Server Operating system used. For more detailed information, please refer to this link.

Apex One Security – Platform Difference

Apex One Features	Windows Servers	Windows Endpoints	Mac OS
Behavior Monitoring	✓	✓	✓
Predictive Machine Learning	✓	✓	✓
Data Loss Protection (DLP)	✓	✓	✗
Endpoint Sensor	✓	✓	✓
Application Control	✓	✓	✗
Vulnerability Protection	✓	✓	✗
Web Reputation Service	✓	✓	✓
Device Control	✓	✓	✓
Firewall	✓	✓	✗
Command and Control	✓	✓	✗

Apex One Endpoint Sensor – Platform Difference

Apex One Features		Windows Servers	Windows Endpoints	Mac OS
Active Data in Data Lake		✓	✓	✓
Historical Investigation		✓	✓	✓
Root Cause Analysis		✓	✓	✓
Attack Discovery Detection (ADE)		✓	✓	✗
Terminate Process		✓	✓	✗
Live Investigation	Disk IoC Scan	✓	✓	✗
	YARA Scan	✓	✓	✗
	Registry Scan	✓	✓	✗

Port and Protocol to Open

The below table enumerates the different ports and protocols used in OfficeScan/Apex One, which should be allowed to communicate via firewall or router. More information can be found on this link.

Source	Destination	Protocol	Ports
Apex Central	SQL Server	TCP	1433 / 1434
Apex Central	Apex One Servers	TCP	8080 / 4343
Apex Central	Deep Discovery Analyzer	TCP	443
Apex Central	Active Directory Controller	TCP	389 or 636
Apex Central	Syslog server	UDP	514
Apex Central	Mail Server	TCP	25
Apex Central	Apex Security Agents	TCP	Random 5-digit port number (generated during installation/customizable)
Apex Central	Internet	TCP	80/443

Source	Destination		Protocol	Ports
Apex One Servers	SQL Server		TCP	1433 / 1434
Apex One Servers	Apex Central		UDP	10323
Apex One Servers	Smart Protection Servers		TCP	80/443/5274
Apex One Servers	Active Directory Controller		TCP	389 or 636
Apex One Servers	Syslog server		UDP	514
Apex One Servers	Mail Server		TCP	25
Apex One Servers	Apex Security Agents		TCP	Random 5-digit port number (generated during installation/customizable)
Edge Relay Server	Apex One Servers		HTTPS	4343
Roaming Agents	Relay Server	External (Agent to Edge) Internal (Edge Server to Apex One Server	HTTPS	443
Apex One Agent	Apex One Server		HTTP/HTTPS	8080/4343
Update Agent	Security Agenrs		TCP	Random 5-digit port number (generated during installation/customizable)
Smart Protection Servers	Internet		TCP	80 / 443
SSPS	Apex One Server	File Reputation	HTTP/HTTPS	80/443
		Web Reputation	TCP/HTTPS	5274/4343
Administrators	Apex Central		TCP	8080 / 4343
Administrators	Apex One Servers		TCP	8080 / 4343

URLs to Be Allowed Through Firewall

Apex One On-Premise Environment

The Table below enumerates the URLs that should be allowed to pass through firewall. These are necessary for Apex One to work properly. More information can be found on this link.

ITEM	APEX ONE
TM AU	http://osce14-p.activeupdate.trendmicro.com/activeupdate
TM pre-opr	http://osce14-p.pre-opr-au.trendmicro.com/activeupdate
OSCE Plug-in AU	http://osce14-p.activeupdate.trendmicro.com/activeupdate
Integrated SPN FRS	http://osce14-ilspn30-p.activeupdate.trendmicro.com/activeupdate
Integrated SPS WRS	http://osce14-ilspn30wr-p.activeupdate.trendmicro.com/activeupdate
Standalone SPS FRS	http://slspn30-p.activeupdate.trendmicro.com/activeupdate/
Standalone SPS WRS	http://slspn30wr-p.activeupdate.trendmicro.com/activeupdate/
TrendX-File	http://osce140-de-f.trx.trendmicro.com/
	http://osce140-de-f.trx.trendmicro.com/
	osce140-es-f.trx.trendmicro.com
	osce140-fr-f.trx.trendmicro.com
	osce140-it-f.trx.trendmicro.com
	osce140-jp-f.trx.trendmicro.com
	osce140-kr-f.trx.trendmicro.com
	osce140-pl-f.trx.trendmicro.com
	osce140-ru-f.trx.trendmicro.com
	osce140-tc-f.trx.trendmicro.com

ITEM	APEX ONE
TrendX-Behavior	http://osce140-en-b.trx.trendmicro.com/
	osce140-de-b.trx.trendmicro.com
	osce140-es-b.trx.trendmicro.com
	osce140-fr-b.trx.trendmicro.com
	osce140-it-b.trx.trendmicro.com
	osce140-jp-b.trx.trendmicro.com
	osce140-kr-b.trx.trendmicro.com
	osce140-pl-b.trx.trendmicro.com
	osce140-ru-b.trx.trendmicro.com
	osce140-tc-b.trx.trendmicro.com
TrendX Co-exist mode	http://oscecmp140-de-f.trx.trendmicro.com/
	http://oscecmp140-en-f.trx.trendmicro.com/
	http://oscecmp140-es-f.trx.trendmicro.com/
	http://oscecmp140-fr-f.trx.trendmicro.com/
	http://oscecmp140-it-f.trx.trendmicro.com/
	http://oscecmp140-jp-f.trx.trendmicro.com/
	http://oscecmp140-kr-f.trx.trendmicro.com/
	http://oscecmp140-pl-f.trx.trendmicro.com/
	http://oscecmp140-ru-f.trx.trendmicro.com/
	http://oscecmp140-tc-f.trx.trendmicro.com/
Global Web Rating server	osce14-0-en.url.trendmicro.com
	http://osce14-0-jp.url.trendmicro.com/
	http://osce14-0-tc.url.trendmicro.com/
	http://osce14-0-de.url.trendmicro.com/
	http://osce14-0-fr.url.trendmicro.com/
	http://osce14-0-sp.url.trendmicro.com/
	http://osce14-0-ru.url.trendmicro.com/
	http://osce14-0-it.url.trendmicro.com/
	http://osce14-0-po.url.trendmicro.com/
	http://osce14-0-kr.url.trendmicro.com/
Global Smar Scan server	http://osce14.icrc.trendmicro.com/
	http://osce14-jp.icrc.trendmicro.com/
SPN feedback server	http://osce140-de.fbs25.trendmicro.com/
	http://osce140-en.fbs25.trendmicro.com/
	http://osce140-es.fbs25.trendmicro.com/
	http://osce140-fr.fbs25.trendmicro.com/
	http://osce140-jp.fbs25.trendmicro.com/
	http://osce140-pl.fbs25.trendmicro.com/
	http://osce140-it.fbs25.trendmicro.com/
	http://osce140-ru.fbs25.trendmicro.com/
	http://osce140-tc.fbs25.trendmicro.com/
	http://osce140-kr.fbs25.trendmicro.com/
Census server	http://osce14-en-census.trendmicro.com/
	http://osce14-de-census.trendmicro.com/
	http://osce14-fr-census.trendmicro.com/
	https://osce14-es-census.trendmicro.com
	http://osce14-it-census.trendmicro.com/
	http://osce14-pl-census.trendmicro.com/
	http://osce14-ru-census.trendmicro.com/
	https://osce14-jp-census.trendmicro.com
	http://osce14-kr-census.trendmicro.com/
	http://osce14-tc-census.trendmicro.com/

ITEM	APEX ONE
Census server backup	http://osce14bak-en-census.trendmicro.com/ http://osce14bak-de-census.trendmicro.com/ http://osce14bak-es-census.trendmicro.com/ http://osce14bak-fr-census.trendmicro.com/ http://osce14bak-it-census.trendmicro.com/ http://osce14bak-jp-census.trendmicro.com/ http://osce14bak-kr-census.trendmicro.com/ http://osce14bak-pl-census.trendmicro.com/ http://osce14bak-ru-census.trendmicro.com/ http://osce14bak-sc-census.trendmicro.com/ http://osce14bak-tc-census.trendmicro.com/
NFC Server	http://osce14-en.gfrbridge.trendmicro.com/ http://osce14-jp.gfrbridge.trendmicro.com/ http://osce14-tc.gfrbridge.trendmicro.com/ http://osce14-kr.gfrbridge.trendmicro.com/ http://osce14-de.gfrbridge.trendmicro.com/ http://osce14-fr.gfrbridge.trendmicro.com/ http://osce14-it.gfrbridge.trendmicro.com/ http://osce14-es.gfrbridge.trendmicro.com/ http://osce14-ru.gfrbridge.trendmicro.com/ http://osce14-po.gfrbridge.trendmicro.com/
License(PR) Server	http://licenseupdate.trendmicro.com/
PR Feedback Server	https://licenseupdate.trendmicro.com/fb/bifconnect.ashx
SPN Portal	http://www.smartprotectionnetwork.com/
Global URL Feedback Portal	http://reclassify.wrs.trendmicro.com/
Spyware Encyclopedia URL	http://about-threats.trendmicro.com/us/search.aspx?p=$SPYWARE_NAME$
Spyware Encyclopedia URL	http://about-threats.trendmicro.com/us/search.aspx?p=$SPYWARE_NAME$
Virus Encyclopedia URL	http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp

Apex Central On-Premise Environment

The table below shows the list of different URLs used by TMCM/Apex Central that should have “Allow” rule on the firewall. More information can be found on this link.

ITEM	APEX CENTRAL
AU Source	https://apexcentral80-p.activeupdate.trendmicro.com/activeupdate https://cm60-lspn30-p.activeupdate.trendmicro.com https://cm55-lspn25wr-p.activeupdate.trendmicro.com https://avclientxml.trendmicro.com
License / BIF	https://licenseupdate.trendmicro.com
SPN / FeedBack	https://tmcm55-en.fbs10.trendmicro.com https://wtc.trendmicro.com
Cloud Service Integration	https://sco-nabu.trendmicro.com https://login.trendmicro.com/ http://status.saas.trendmicro.com http://status2.saas.trendmicro.com
OLH	http://docs.trendmicro.com/
Support Link	https://success.trendmicro.com/
Threat Connection	https://tmcm6-threatconnect.trendmicro.com/
SandBox as a Service	https://*.ddcloud.trendmicro.com
Policy WCU (TMSM)	http://sitesafety.trendmicro.com/ http://reclassify.wrs.trendmicro.com/
IG Server (User/Endpoint Directory - General Information)	https://tmcm60-spn.trendmicro.com

ITEM	APEX CENTRAL
CLP	https://clp.trendmicro.com
	https://olr.trendmicro.com
Endpoint Sensor	ies3-0.url.trendmicro.com
Endpoint Sensor (File Census)	ies300-en-census.trendmicro.com https://threatconnect.trendmicro.com
Endpoint Sensor	https://www.virustotal.com

Backup And Disaster Recovery

- Backup Server Configuration
- Agent Configuration
- Website Configuration
- Database backup

The following knowledge base article can guide you on how you can perform backup prior to do migration/upgrade to Apex One and Apex central Server.

- Files to backup before Upgrading, migrating, or uninstalling the OfficeScan Server
- Reinstalling Control Manager (TMCM)/ Apex Central 2019 on a different machine using the same SQL server.
- Trend Micro Apex One and iServices Disaster Recovery Guide

OfficeScan 11 Service Pack 1 to Apex One On-Premise

New Server Upgrade (RECOMMENDED)

Phase I: Install Apex One Server

1. Download Apex One Installer file from this link.
2. Download Apex One Installation and Upgrade Guide in PDF form from this link.
3. Can also watch Installation video from this Youtube link.

Phase II: **Install Apex Central Server**

1. Download Apex Central Installer file from this link
2. Download Apex Central Installation and Upgrade Guide in PDF form from this link
3. Can also watch Installation video from this Youtube link

Phase III: **Export/Import Policy Settings**

1. Export your OfficeScan policies using the Apex One Settings Export Tool procedure from the kb link.
2. Import the appropriate exported policy packages to Apex One and Apex Central respectively.
3. A Youtube video is also available.

The default names of the export packages are:

- *ApexOne_Agent_DLP_Policies.zip (used to import DLP policy settings into Apex Central)*
- *ApexOne_Agent_Policies.zip (used to import all other Security Agent policy settings into Apex Central)*
- *Server_Settings_Migration.zip (used to import all Security Agent policy settings and OfficeScan server settings to another Apex One server)*

Phase IV: **Move your Agents to the new Apex One Server**

1. Disable Automatic Apex One Agent Upgrade to ALL Policies in Apex Central
2. Move the OfficeScan endpoints from OfficeScan 11 Console to Apex One Server.

Move endpoints to APEX One by batches. Like a group of 300 endpoints at a given time. Best to migrate all Update Agents first.

Different methods to move agents to Apex One

- Move Agent function via OfficeScan console.
- Using the IPXfer Utility as explained in this KB article
- via CUT tool as explained in this KB article

3. Open the Apex One management console and check whether the moved OfficeScan agents are now reporting to the new server
4. Deploy Policy to target endpoints
5. Confirm that the policy is applied to the target endpoints
6. Monitor the Apex One logs from Apex Central Console
7. Check the Apex One management console shows all the endpoints

PHASE V: Use the Agent Migration Tool to migrate entities from TMCM to Apex Central

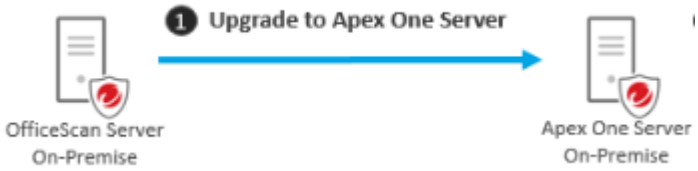
1. Use the Agent Migration Tool to migrate entities from TMCM to Apex Central as described in this link.

The Agent Migration Tool only supports migrating managed products and managed product logs. The Agent Migration Tool does not support migrating reports or the Product Directory structure from the previous server.

PHASE VI (*optional*): **Decommission the OfficeScan Server and Control**

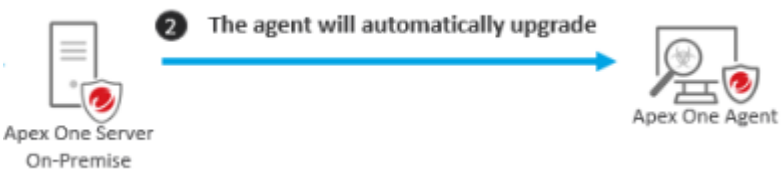
In-place Upgrade

Phase I: Upgrade Server to Apex One



1. Check if Officescan 11 is currently on SP1
2. Make sure that the Agents are not allowed to do auto-upgrade. How?
3. Download Apex One Installer file from this link.
4. Download Apex One Installation and Upgrade Guide from this link.

Phase II: Upgrade Officescan Agent 11 SP1 to Apex One Security Agent

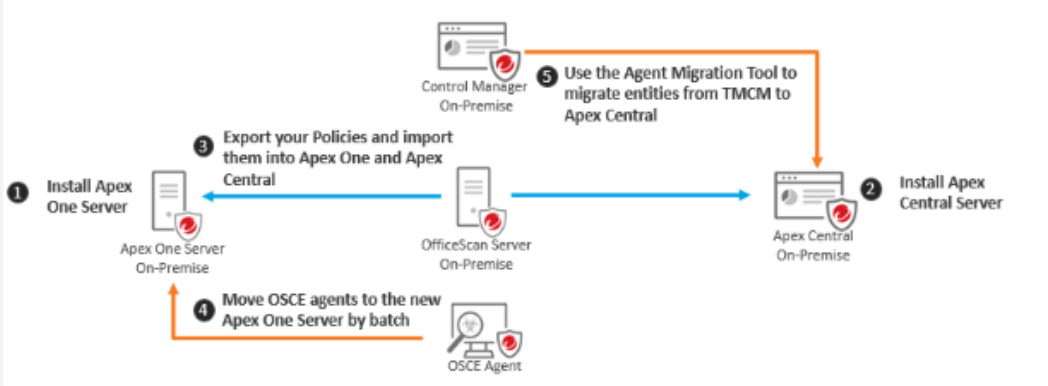


1. Make sure to have a list of sub-group with priority listing
2. Then upgrade sub group by Batch. How?

OfficeScan XG to Apex One On-Premise

New Server Upgrade (RECOMMENDED)

The Customer wants to upgrade their existing OfficeScan XG and TMCM 7.0 environment to Apex One and Apex Central.



PHASE 1: Install Apex One Server

Download the Apex One Installation and Upgrade guide from this link.
A Youtube video is also available.

PHASE 2: **Install Apex Central**

Download the Apex Central Installation and Upgrade guide from this link. A Youtube video is also available.

PHASE 3: **Export your OfficeScan policies and import them to Apex One and Apex Central**

Export your OfficeScan policies Using the Apex One Settings Export Tool procedure from the online help center page. Import the appropriate exported policy packages to Apex One and Apex Central respectively. A Youtube video is also available.

The default names of the export packages are:

- *ApexOne_Agent_DLP_Policies.zip (used to import DLP policy settings into Apex Central)*
- *ApexOne_Agent_Policies.zip (used to import all other Security Agent policy settings into Apex Central)*
- *Server_Settings_Migration.zip (used to import all Security Agent policy settings and OfficeScan server settings to another Apex One server)*

PHASE 4: Move your Agents to the new Apex One Server

1. Disable Automatic Apex One Agent Upgrade to ALL Policies in Apex Central

2. Move the OfficeScan endpoints from OfficeScan Console to Apex One Server. Move endpoints to APEX One by batches. Like a group of 300 endpoints at a given time. Best to migrate all Update Agents first.

   Different methods to move agents to Apex One

   - Move Agent function via OfficeScan console.
   - Using the IPXfer Utility as explained in this KB article
   - via CUT tool as explained in this KB article

3. Open the Apex One management console and check whether the moved OfficeScan agents are now reporting to the new server
4. Deploy Policy to target endpoints
5. Confirm that the policy is applied to the target endpoints
6. Monitor the Apex One logs from Apex Central Console
7. Check the Apex One management console shows all the endpoints

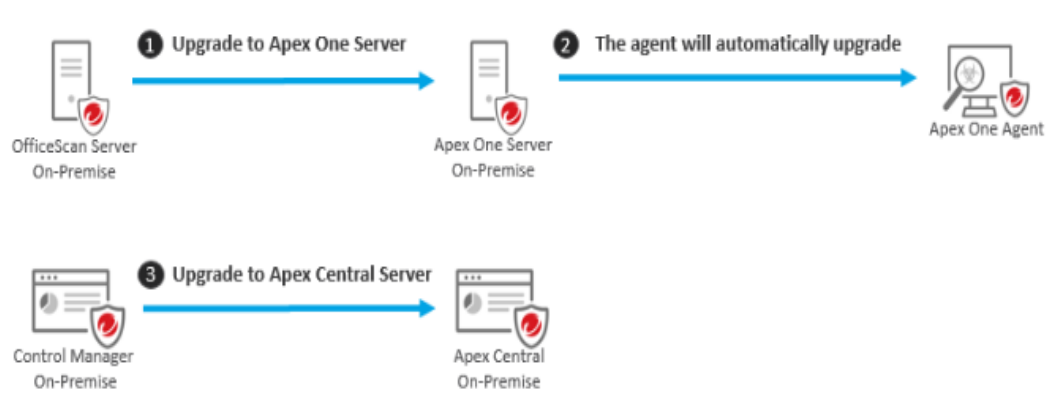
PHASE 5: Use the Agent Migration Tool to migrate entities from TMCM to Apex Central

Use the Agent Migration Tool to migrate entities from TMCM to Apex Central as described in this online help center link.
The Agent Migration Tool only supports migrating managed products and managed product logs. The Agent Migration Tool does not support migrating reports or the
Product Directory structure from the previous server.

PHASE 6 (optional): Decommission the OfficeScan Server and Control Manager

In-place Upgrade

Scenario 1: The Customer wants to upgrade their existing OfficeScan XG and TMCM 7.0 environment to Apex One and Apex Central.



PHASE 1: Upgrade to Apex One Server

1. Download the Apex One Installation and Upgrade guide from this link.

2. The administrator can defer the OfficeScan agent upgrade to Apex One by following KB 1113015

PHASE 2: Upgrade to Apex Central Server

Download the Apex Central Installation and Upgrade guide from this link.

Scenario 2: The Customer wants to upgrade their existing OfficeScan XG environment to Apex One and enable Apex Central for centralized management and advanced features.

PHASE 1: Upgrade to Apex One Server

1. Download the Apex One Installation and Upgrade guide from this link.
2. The administrator can defer the OfficeScan agent upgrade to Apex One by following KB 1113015

PHASE 2: Install Apex Central Server

Download the Apex Central Installation and Upgrade guide from this link.

PHASE 3: **Register Apex One to Apex Central**

Refer to Registering Apex One to Apex Central Online Help Center link.
A Youtube video is also available.

We use the following abbreviations in this document.

Product/Function Name	Abbreviation
Trend Micro Apex Central	Apex Central
Trend Micro Apex One	Apex One
Trend Micro Apex One as a Service	Apex One SaaS
Trend Micro Control Manager	TMCM
Office Scan Corporate Edition	OSCE
Smart Protection Server	SPS
Smart Protection Network	SPN
Endpoint Protection Platform	EPP
Endpoint Detection and Response	EDR

Documents Control:

Revision	Date	Author	Description
0.5	7/13/2020	Rowena Bautista	Initial Draft
1.0	7/27/2020	Rowena Bautista	1st Release
1.5	9/16/2020	Rowena Bautista	Modified Release