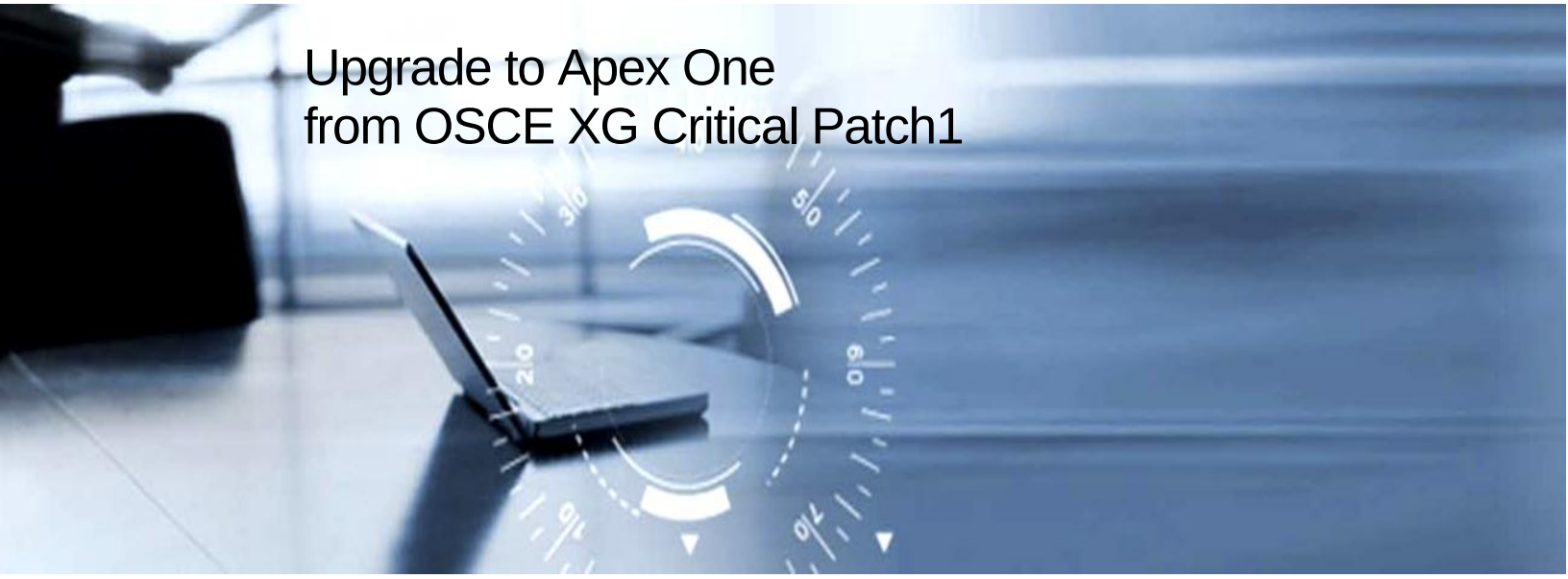
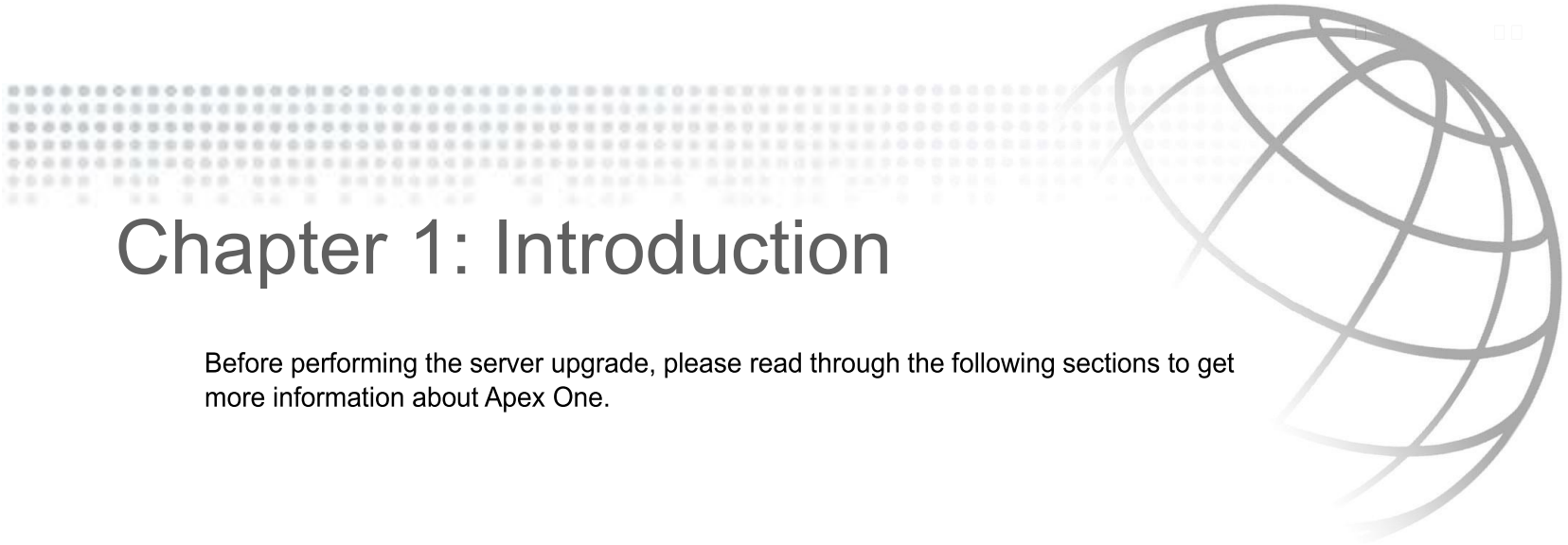
Trend Micro™
Apex One Version 2019



Anti-Spyware | Anti-Spam | Antivirus | Anti-Phishing | Content & URL Filtering

Released: October 2020

Contents



Chapter 1: Introduction

Before performing the server upgrade, please read through the following sections to get more information about Apex One.

1.1 > Upgrade Purpose

Upgrading to the most recent version will improve the functions and performance of the product. Apex One offers new features that provide protection from the latest threats and incorporates resolutions to requests from various customers.

NOTE Officially, the newest version of the product is named “Apex One”, which is named as OfficeScan (OSCE) formerly.

1.2 > What’s New

Apex One includes the following new features and enhancements:

Offline Predictive Machine Learning

Predictive Machine Learning has been upgraded to provide offline protection against portable executable files. The lightweight, offline model helps protect all endpoints against unknown threats when a functional Internet connection is unavailable.

Fileless Attack Protection

Security Agent policies provide increased real-time protection against the latest fileless attack methods through enhanced memory scanning for suspicious process behaviors. Security Agents can terminate suspicious processes before any damage can be done.

Secured HTTP communication (HTTPS)

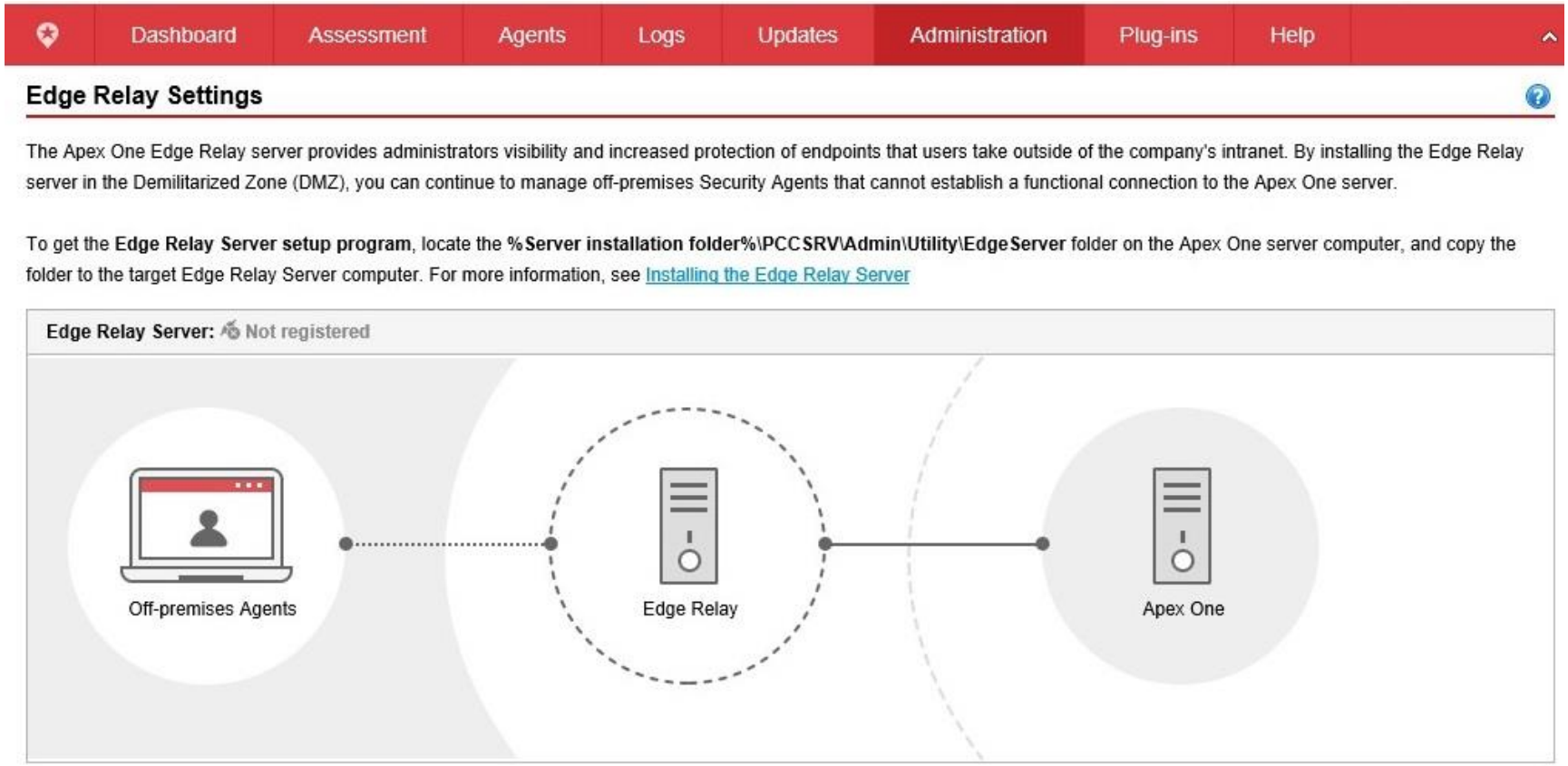
In Apex One version, the server and the agents communications are mandatorily using secured HTTP (HTTPS) method. In this version, there is no buffer to workaround using HTTP instead of HTTPS temporarily.
Trend Micro highly suggests to check the environment before upgrading OSCE product to Apex One, and make sure all platforms can support the same TLS version with the cipher suites.
For OS level TLS supporting information, please check below references:

- https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-
- https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

Off-premises Security Agent Protection

Enhanced Edge Relay Server support allows for increased communication between the Apex One server and off-premises Security Agents. Security Agents can receive updated policy settings from the Apex One server even when a direct connection to the server is unavailable.

Re-designed Edge Relay Server



- The re-designed Edge Relay uses IIS rewrite module as a reverse proxy to achieve communication between off premise agent and the Apex One server. It will redirect the polling request from the off-premise agent to its Apex One server.
- Off premise agents can communicate with their Apex One server through the Edge Relay, and work like SaaS agent.

- Upload the detection log.
- Sample submission.
- Configuration deployment.
- Update the hotfix.

Rebranded Console

The OfficeScan server and OfficeScan agent programs have been rebranded to the Apex One server and Security Agent respectively. The new Apex One server integrates with Apex Central (formerly Trend Micro Control Manager) to provide increased protection against security risks. The all-in-one Security Agent program continues to provide superior protection against malware and data loss but also allows you implement Application Control, Endpoint Sensor, and Vulnerability Protection policies without having to install and maintain multiple agent programs.

Support more browsers for the management web console

- Microsoft™ Internet Explorer™ 11
- Microsoft™ Edge™
- Google™ Chrome™

Apex One Server Platform

- Support new server OS platform: Windows Server 2019
- **Non-support** server OS platform: Windows server 2003, 2008, 2008R2.

Detailed information, please check section 1.3 below.

Apex One Security Agent Platform

- **Non-support** server OS platform: Windows server 2003, 2008.
- **Non-support** desktop OS platform: Windows XP, Vista, 8.

Detailed information, please check section 1.3 below.

Database

Codebase is not supported in Apex One version anymore. MS SQL is the supported database application in Apex One.

1.3 > System Requirements

Refer to the following document to read the system requirements:
https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_req.pdf

1.4 > Upgrade Considerations

Environment Requisition

Role	Version	Purpose
Current OSCE server	XG Critical Patch1 Build 1988 and later	Production OSCE Server
***** A New Server	XG Critical Patch1 Build 1988 and later (The same as the above)	Optional
***** SQL Server	Version 2016 SP1 and later	OSCE server database
***** Standalone Smart Protection Server	Version 3.3	Optional
***** Apex Central Server	Apex Central 2019 Build 3752 and later	Optional
SQL Native Client	SQL 2008 R2: 10.53.6560 and later SQL 2012 and later: 11.4.7001 and later	Support TLS1.2
Edge Relay	Version 2.0	Off-premise agents communicating with the management server

* **A New Server**: Prepared for Migrating OfficeScan server, including managed agents, configurations and logs from the current OfficeScan server to the new server. And the new server's OS platform should be Windows server 2012 and later. Please get more information from Chapter 2.

* **SQL Server:**

SQL server supported by Apex One WITHOUT Endpoint Sensor feature:

- SQL Express: 2008 R2 SP2 and later
- SQL Server: 2008 R2 and later

SQL server supported by Apex One WITH Endpoint Sensor feature:

- SQL Express: Not Support
- SQL Server:
  - 2016 SP1 with “Full-Text and Semantic Extractions for Search” installed
  - 2017 with “Full-Text and Semantic Extractions for Search” installed

* **Standalone Smart Protection Server (SPS):** If the current OSCE server has been configured any standalone SPS, the standalone SPS should be upgraded to version 3.3 before upgrading OSCE to Apex One. If the OSCE agent does not have network connection to Trend Micro global SPS server, it is also recommended to build a standalone smart protection server before upgrading.
Standalone SPS Installer Download Site:
https://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=5179&lang_loc=1

* **Apex Central Server:** If the current OSCE server has registered to a Control manager, please upgrade the control manager to Apex Central before upgrading OSCE to Apex One.
Apex One Installer Download Site:
https://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=5346&lang_loc=1

Upgrade Sequence

When multiple following Trend Micro products are installed in the environment, please follow the sequence to upgrade them one by one.

Sequence	Current Product	Upgrade To
1	Control manager	Apex Central 2019

2	Standalone SPS	Version 3.3
3	OfficeScan Server	Apex One Server Patch3 Build 8422 and later
4	Edge Relay	Version 2.0
5	OfficeScan Agent	Apex One Security Agent

OSCE Upgrade path

The following OSCE server versions can be upgraded to Apex One version:

- OSCE 11.0 SP1 Build 6675 and later
- OSCE XG GM Critical Patch1 1988 and later
- OSCE XG SP1 Build 5684 and later

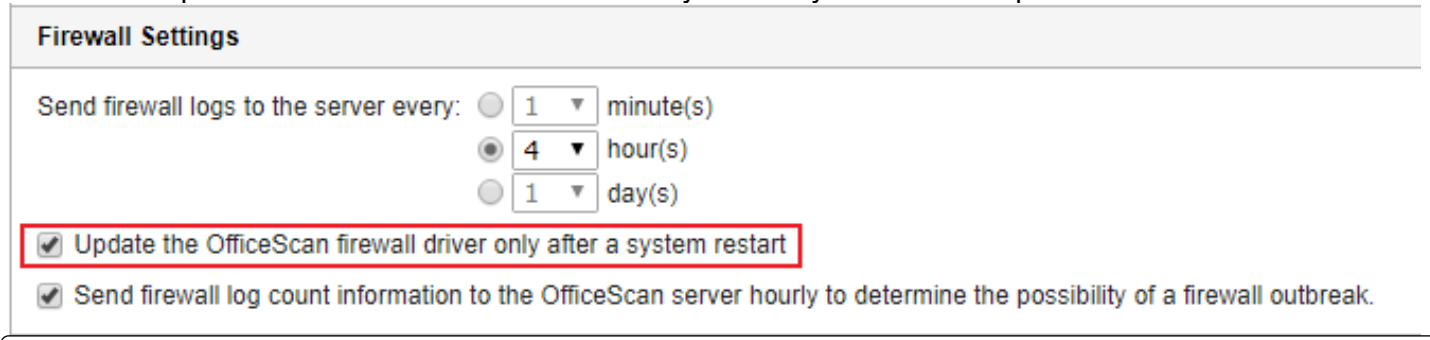
NOTE This document focuses on upgrading to Apex One from OSCE XG Critical Patch1. For more detailed information, please refer to the Apex One installation guide (Page 84):
https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf

Pre-configuration: Firewall driver update timing

When the Common Firewall Driver update starts, agents will be temporarily disconnected from the network. Users will not be notified before disconnection. To prevent the disconnection:

1. Logon the OSCE web management console.
2. Navigate to **Agents > Global Agent Settings**.
3. In the Security Settings tag, scroll down to the Firewall Settings section.

4. Enable the “Update the OfficeScan firewall driver only after a system restart” option.



NOTE This is a default setting. Trend Micro also suggests to keep enabled it.

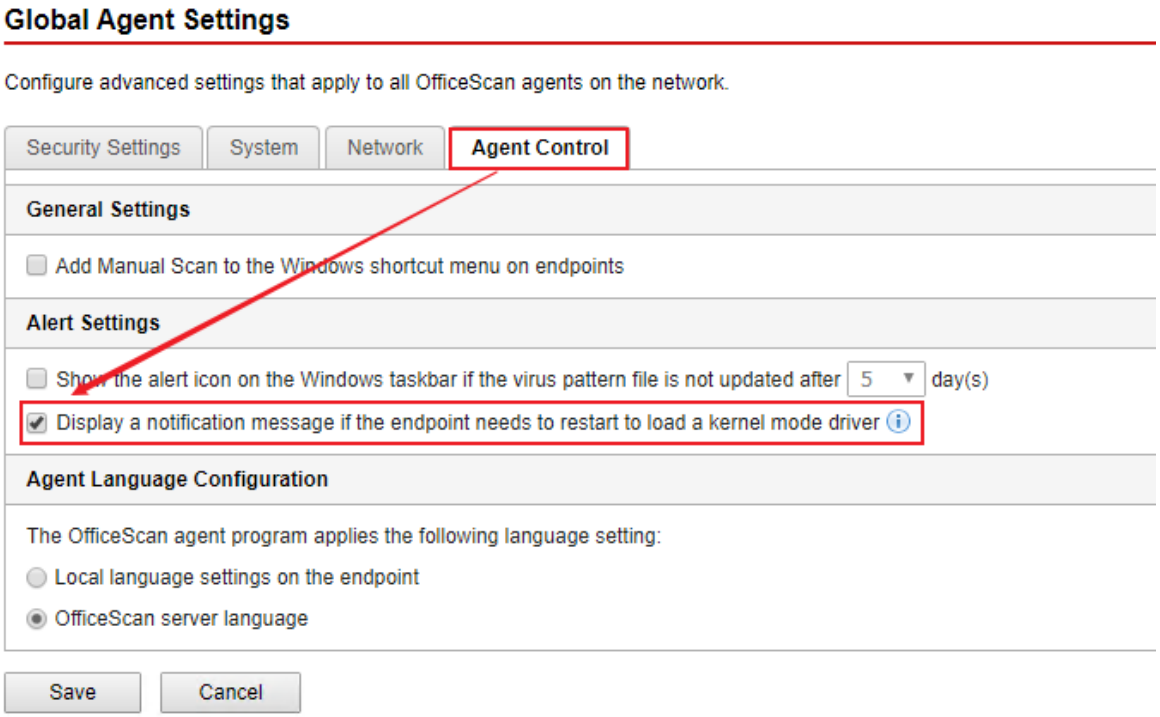
5. And click “Save” button
6. The agents will get it automatically.

Pre-configuration: System reboot requirement notification

There is a pop-up notification for the end-user if a restart is required. The option to display the restart notification message is enabled by default. If this was intentionally disabled, Trend Micro suggests to enable it. The procedures to enable this option:

1. Log in to the OSCE web management console.
2. Navigate to **Agents > Global Agent Settings**.
3. Go to the **Agent Control** tag

4. In **Alert Settings** blade, enable the "**Display a notification message if the endpoint needs to restart to load a kernel mode driver**" option.



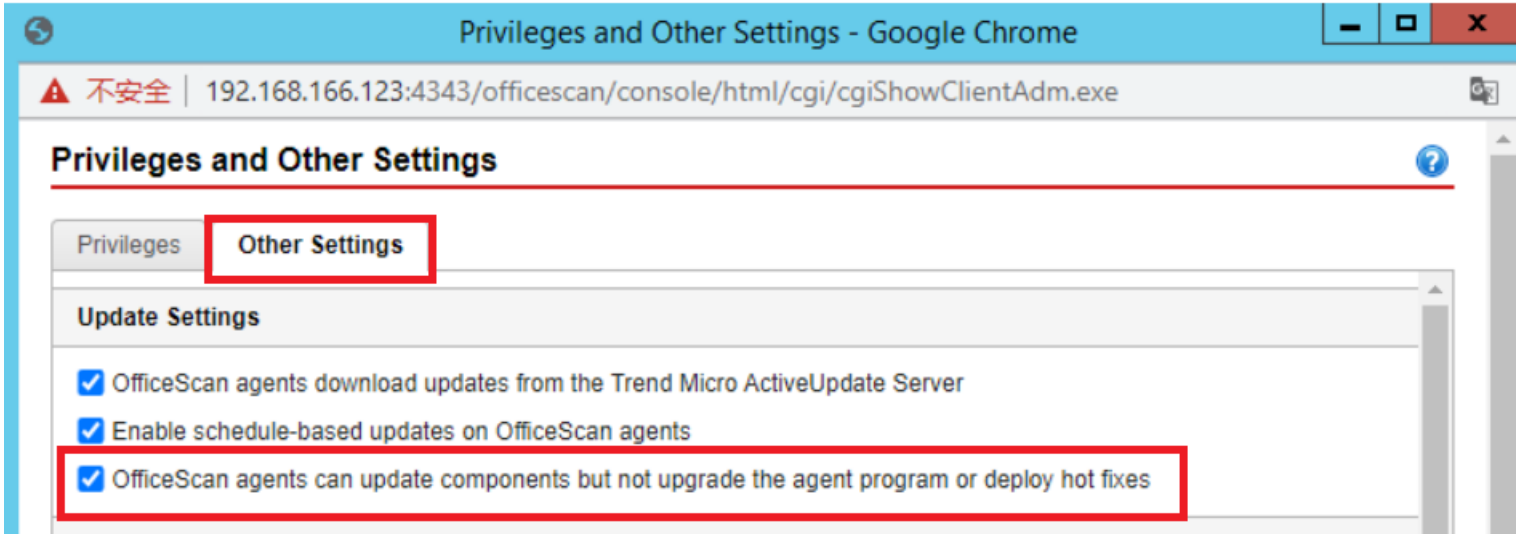
5. Save the change
6. The agent will get the configuration automatically

Pre-configuration: Component Update Setting

There is a setting indicating the OSCE agent update behavior which is located in: **Agents** > **Agent Management** > **Settings** > **Privileges and Other Settings** > **Other Settings**.

In **Update Settings** blade, by default the highlighted drop list is selected "**All components (including hotfixes and the agent program)**", agents are able to update patterns, engines and program files from its update source.

To avoid high bandwidth consumption and high OSCE server workload, it is recommended to select ""Officescan agent can update components but not upgrade the agent program or deploy hot fixes" during the upgrading period.



NOTE The setting is also valid to offline agents registered on the OSCE server. When the offline agent becomes online, this setting is notified earlier than the upgrade program.

Security agent upgrade bandwidth

Below is the estimated upgraded bandwidth per agent. The real upgrading bandwidth will be impacted by many conditions like pattern version, enabled module, network stability, etc.

x86 platform:

- Without endpoint sensor feature enabled: 229.5MB
- With endpoint sensor feature enabled: 271.1MB

x64 platform:

- Without endpoint sensor feature enabled: 286.2MB
- With endpoint sensor feature enabled: 335.8MB

After the server upgrade has completed, change this setting back to "**All components (including hotfixes and the agent program)**" for a batch of agents (e.g. for a domain in the management console) or all agents.

Limitations

- If there are any agents running Login Script (AutoPcc.exe), the server cannot upgrade. Ensure that no agent is running Login Script before upgrading the server.
- If the server is performing any database-related task before upgrading, the server cannot upgrade. It is suggested that you check the status of the DbServer.exe process. For example, open Windows Task Manager and verify that the CPU usage for DbServer.exe is "00". If the CPU usage is higher, wait until usage is "00". This is a signal that database-related tasks have been completed. If you run an upgrade and encounter upgrade problems, it is possible that database files have been locked. In this case, stop the OfcService service or restart the server computer to unlock the files and then run another upgrade.
- Make sure that there is no mmc.exe process running in the Windows Task Manager.
- Make sure that there is no LogServer.exe process running in the Windows Task Manager, except when the debug log is required by the Trend Micro Support Team.

Server Backup (Recommended)

To avoid any unexpected problems that may occur during the upgrade process, it is recommended to back up the configuration information of the current OSCE server in advance.
This is to ensure that if any unfortunate situations occur, there is a way to restore the original state of the server by importing the backup data to the reinstalled/upgraded OSCE server.

Please refer to the following article for more information: https://success.trendmicro.com/solution/1039284

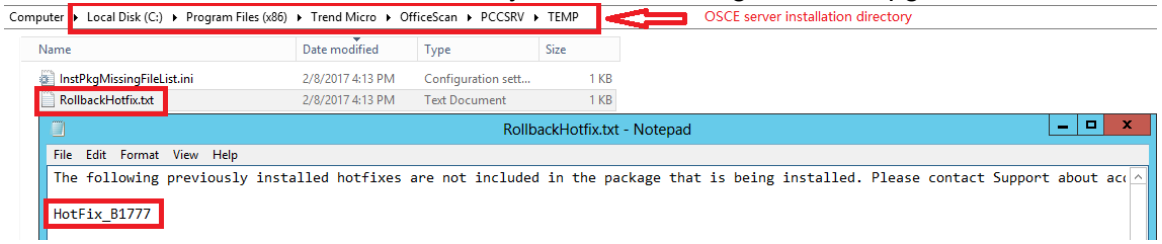
Intrusion Defense Firewall (IDF)

By default, there is no IDF Plug-in Service on the Plug-in Manager page of a freshly-installed Apex One server. The IDF has reached End-of-Support and IDF does not support Windows 10. Instead of IDF, Trend Micro highly recommends to use Trend Micro Vulnerability Protection (TMVP). For more information on TMVP, please refer to the TMVP installation guide.

1.5 > Hot Fix Deployment

It is suggested to check if there are any hot fixes missing after upgrading to the Apex One:

1. Logon the Apex One server.
2. Navigate to the Apex One server's installation directory.
3. Go to the TEMP folder and open RollbackHotfix.txt, if it exists.
4. Check the file to confirm if there are any hot fixes missing after the upgrade.



5. If there is any hot fix missed, please contact Trend Micro Technical Support for further supporting.

Important: The file may be older. Please make sure that the timestamp if not too far away from the upgrade date. The record will show something similar to the screenshot below.

1.6 > Firewall: IP, Port and Protocol

Destination Machine	Destination Port	Protocol	Purpose
Apex One Server	443, 4343	TCP, HTTPS	TLS communication
Apex One Server	80, 8080	TCP, HTTP	non-TLS communication. E.g. WRS of iSPS, legacy agent support
Apex One Server	445	TCP, Samba	Autopcc method installation
AD Server	389	TCP, LDAP	Integrate with Active directory
Standalone Smart Scan Server	80	TCP, HTTP	FRS HTTP mode
Standalone Smart Scan Server	5274	TCP, HTTP	WRS HTTP mode
Standalone Smart Scan Server	443	TCP, HTTPS	FRS HTTPS mode
Standalone Smart Scan Server	5275	TCP, HTTPS	WRS HTTPS mode

Standalone Smart Scan Server	4343	TCP, HTTPS	Standalone SPS web management console
Edge Relay Server	443	TCP, HTTPS	Off-premise agent connect to its server
Apex One security agent	21112	TCP, HTTPS	**Double confirm the value of "Client_LocalServer_Port" in ofcscan.ini**
Apex One security agent	135	TCP	Unreachable endpoints assessment
Apex Central	443	TCP, HTTPS	Control manager
SQL Server	1433	TCP	Apex One database
osce14-en-census.trendmicro.com	80, 443	TCP, HTTP, HTTPS	Trend Micro official Census server (Internet)
osce14bak-en-census.trendmicro.com	80, 443	TCP, HTTP, HTTPS	Trend Micro official Census redundancy server (Internet)
osce14-en.gfrbridge.trendmicro.com	80, 443	TCP, HTTP, HTTPS	Trend Micro official NFC server (Internet)
osce14.icrc.trendmicro.com	443	TCP, HTTPS	Trend Micro official FRS server (Internet)
osce14-0-en.url.trendmicro.com	80	TCP, HTTP	Trend Micro official WRS server (Internet)
osce14-p.activeupdate.trendmicro.com	443	TCP, HTTPS	Component update server: Patterns and engines (Internet)
docs.trendmicro.com	443	TCP, HTTPS	Trend Micro Official Online Help (Internet)
osce140-en-f.trx.trendmicro.com	443	TCP, HTTPS	Trend Micro Predictive Machine Learning Engine Rating Server for Static File (Internet)
osce140-en-b.trx.trendmicro.com	443	TCP, HTTPS	Trend Micro Predictive Machine Learning Engine Rating Server for Running Process (Internet)
osce14-ilspn30wr-p.activeupdate.trendmicro.com	443	TCP, HTTPS	Smart Scan server pattern update: WRS
osce14-ilspn30-p.activeupdate.trendmicro.com	443	TCP, HTTPS	Smart Scan server pattern update: FRS

Chapter 2: Upgrade Scenarios

This chapter contains an overview of the upgrade scenarios, as well as of the OSCE server with the plug-in service(s) installed. For detailed upgrade steps, please refer to the next chapter: Chapter 3.

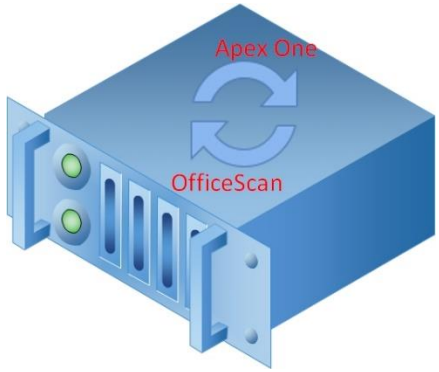
Generally, there are three (3) upgrade scenarios:

- Scenario 1: Upgrading the OSCE XG Critical Patch1 server directly
- Scenario 2: Migrating to a new OSCE XG Critical Patch1 server before upgrading to ApexOne
- Scenario 3: Replacing the OSCE XG Critical Patch1 server with a new ApexOne server

Here, “migrate” is defined as backend server transparent mode. This means that after the migration, the agent still considers that it is connected to the “same” server and that no settings have changed on the agent.

Additionally, “replace” is defined as backend server non-transparent mode. This means that after the replacement, some settings may require to be changed on the agent e.g. the OSCE server information (IP or Hostname/FQDN), update source, communication certificate, etc.

2.1 > Upgrading the OSCE XG Critical Patch1 server directly



This upgrade method is used when:

- The hardware meets the minimum system requirements. Please refer to System Requirements under Chapter 1.
- The Operating System (OS) is Windows Server 2012 or later.
- The OSCE server is offline during the upgrade.

Advantages

- This is an easy upgrade method.
- There are no additional costs required e.g. H/W purchase, network/topology setting, etc.
- This can be used if there is a plug-in service installed in the server.

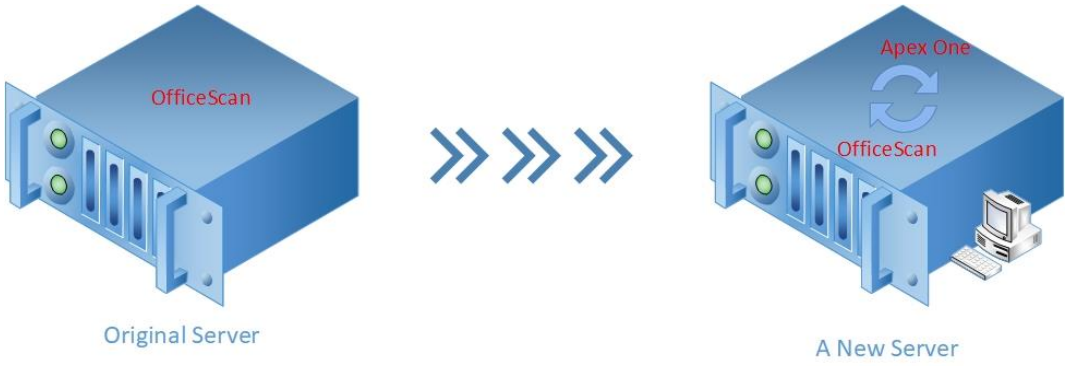
Disadvantages

- During the upgrade, the OSCE agents will not be able to connect to this OSCE server.
- If the OSCE agent is not allowed to connect to the internet, there will be no File Reputation Services (FRS) for the Smart Scan mode agent and Web Reputation Services (WRS) protection.

Recommendations

- Build a Standalone Trend Micro Smart Protection Server (TMSPS) before upgrading.
- To avoid any unexpected risk, please create a snapshot or backup of the current OSCE server before upgrading.

2.2 > Migrating to a new OSCE XG Critical Patch1 server before upgrading to ApexOne



In this method, there is a new server, which also has the same version and build of OSCE XG Critical Patch1 installed.

This upgrade method is used when:

- The OSCE server cannot be offline during the upgrade.
- The server hardware does not meet the system requirements. Please refer to System Requirements under Chapter 1.
- The server OS is Windows Server 2008 R2 or older, and it is inconvenient to upgrade to Server 2012 or a later version.

Advantages

- During the server upgrade period, the OSCE agent is still online.
- You can avoid any unexpected risk, because the original server is still working.
- Logs and system events can be kept.
- This provides a better support for the plug-in service e.g. iDLP, IDF (instead of TMVP), and TMSM.

Disadvantages

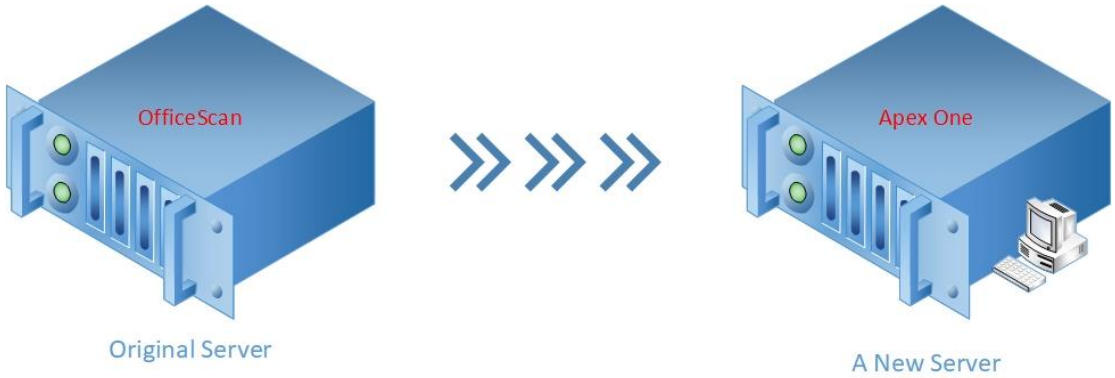
- You need to prepare more resource(s) e.g. H/W purchase, network/topology setting, etc.
- After the new server is ready, the agent status may be incorrect for a while.
- The procedure of this method is not as easy as previous method.
- You need to install the same version/build of the OSCE server on the new server before performing server upgrade.
- You need to move quarantined files from Server A to Server B manually. The default directory is: <OSCE Server installation folder>\PCCSRV\Virus\.
- IDF cannot be installed on the new because there is no resource anymore. It is suggested that the customer uses TMVP instead of IDF.

Suggestions

- After the new server is online, please log in to the Apex One web management console to verify the agents' status from **Agents** > **Connection Verification**, and click **Verify Now**.

- If the IDF PLS is used, please prepare TMVP in advance.

2.3 > Replacing the OSCE XG Critical Patch1 server with a new ApexOne server



In this method, there is a new server, which is a freshly-installed ApexOne server. In this method, it is required to change the agent's configurations.

This upgrade method is used when:

- Multiple applications are used on the current OSCE server. And the customer wants to separate the OSCE server to another server (The New Server).
- If both of the 2 servers are online at the same time, they need to have different IP addresses and hostnames.
- The original server's hardware or the operating system does not meet the system requirements. Please refer to System Requirements under Chapter 1. However, the customer still wants to keep the current server in the network for other usage.
- The network topology changed (i.e. IP section changed) and the customer is using an IP address for server-agent communication in the current OSCE environment.

Advantages

- During the server upgrade period, the OSCE agents are still online.
- Any unexpected risk can be avoided.

Disadvantages

- You need to prepare more resource(s) e.g. H/W purchase, network/topology setting, etc.
- Logs e.g. virus/malware log, system events, etc. will be lost.
- The quarantined files cannot be restored from the Apex One web management console. But here is a workaround to achieve it. Please refer to the KB: https://success.trendmicro.com/solution/1057903.

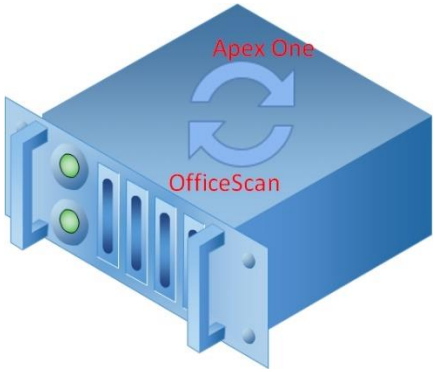
Recommendations

- Do not restore the old database from the current OSCE server to the new Apex One server. There will be a schema mismatched problem.
- To avoid compatibility issues, do not use this method if iDLP is installed and used.

Chapter 3: Upgrade Processes

This section provides more detailed information regarding the upgrading processes for each scenario mentioned in Chapter 2.

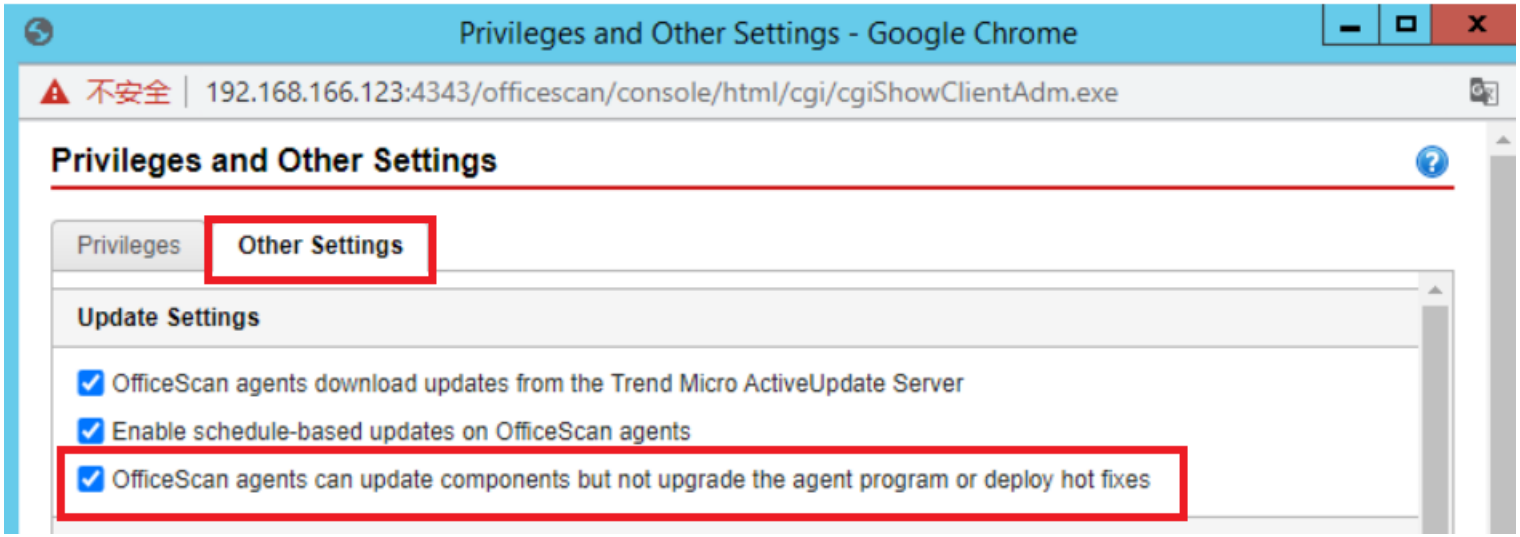
3.1 > Upgrading the server directly



Please follow the procedures to upgrade the server directly:

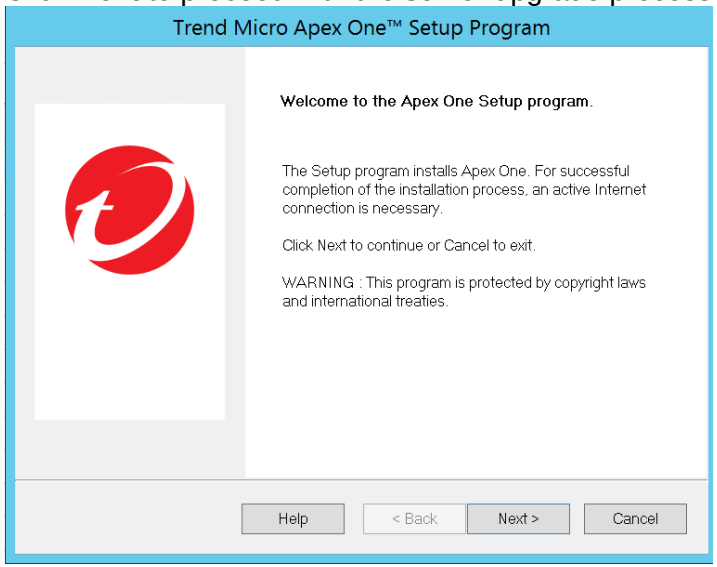
1. Download the installation package from the Trend Micro Official Site:
    - Apex One Installer: https://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=5347&lang_loc=1
    - Patch2 Upgrade package (Build 2146): https://files.trendmicro.com/products/Apex%20One/2020/apex_one_2019_win_en_patch2_b2146.exe
2. Do an image backup or snapshot for the current OSCE server (Recommended).
3. Build and configure a local TMSPS (Standalone), if there is no one configured.

4. Check the agents components update configuration, and make sure it has been set as “Officescan agent can update components but not upgrade the agent program or deploy hot fixes” from the root domain.



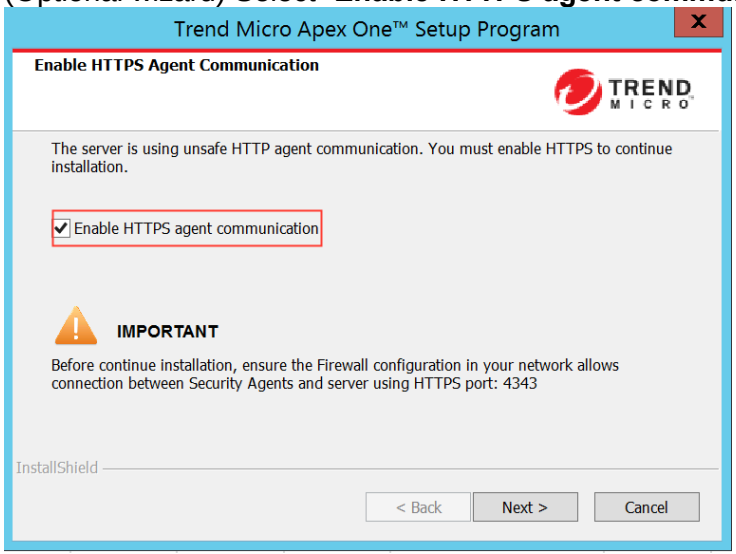
5. Run the installer to upgrade the OSCE server:

   - Click **Next** to proceed with the server upgrade processes



- Accept the **EULA** and click **Next**

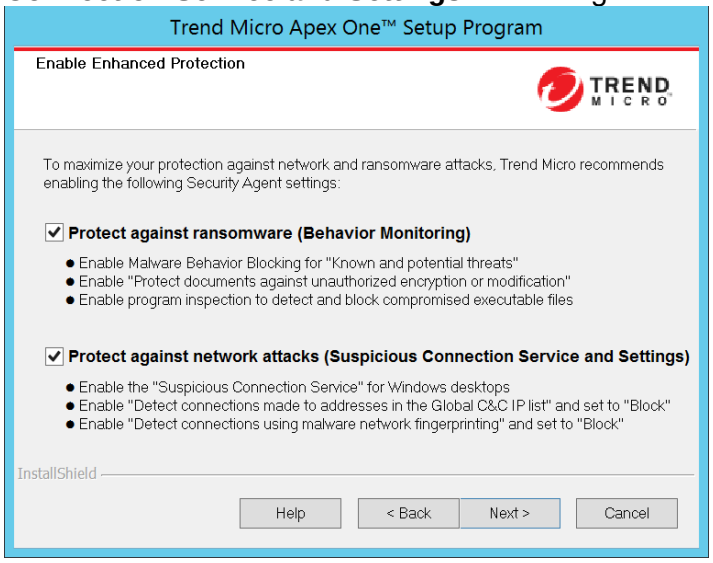
- (Optional wizard) Select “**Enable HTTPS agent communication”** and click **Next**



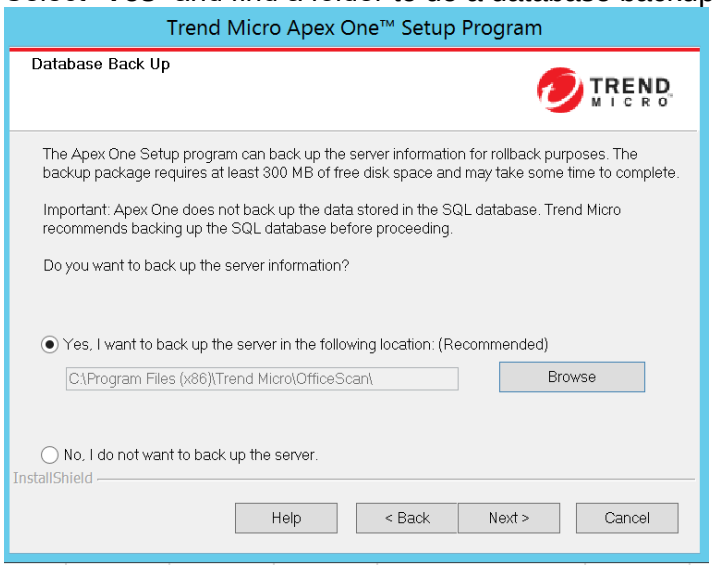
This wizard will pop-up while the OSCE agents use HTTPS protocol to communicate with the management server (OSCE server).

- Click **Next** to continue

- Select "**Protect against ransomware (Behavior Monitor)**" and "**Protect against network attacks (Suspicious Connection Service and Settings**" according to the environment, and click **Next**

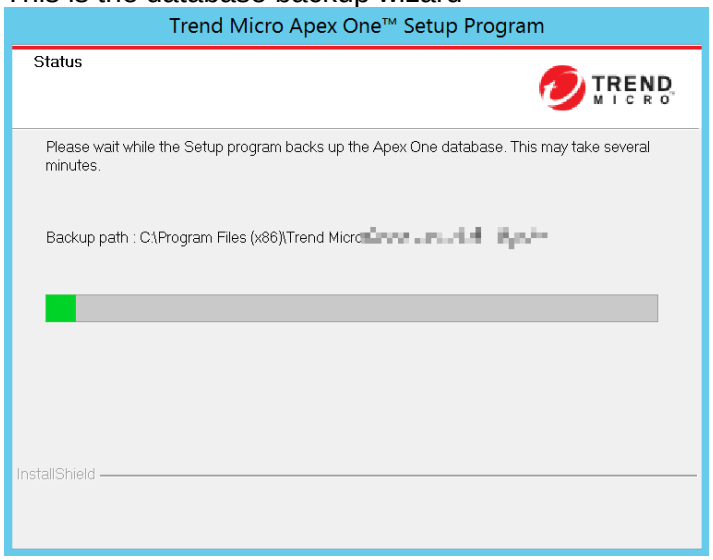


- Select “**Yes**” and find a folder to do a database backup, and click **Next**

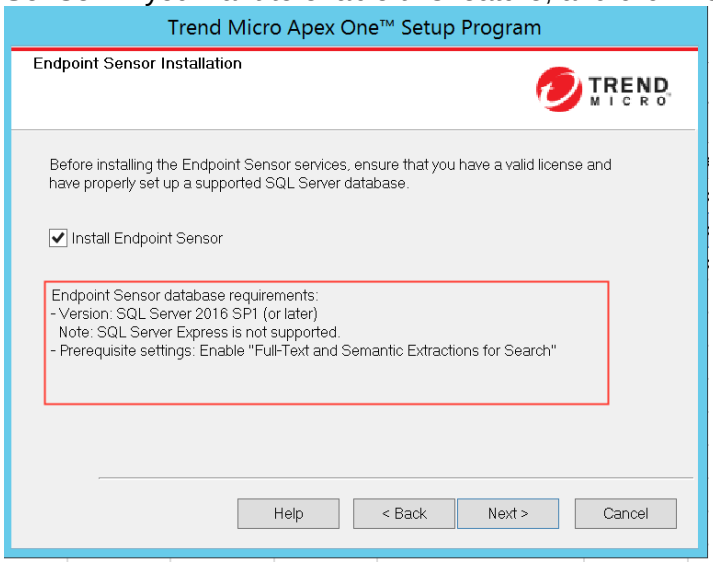


It highly recommends to perform a database backup.

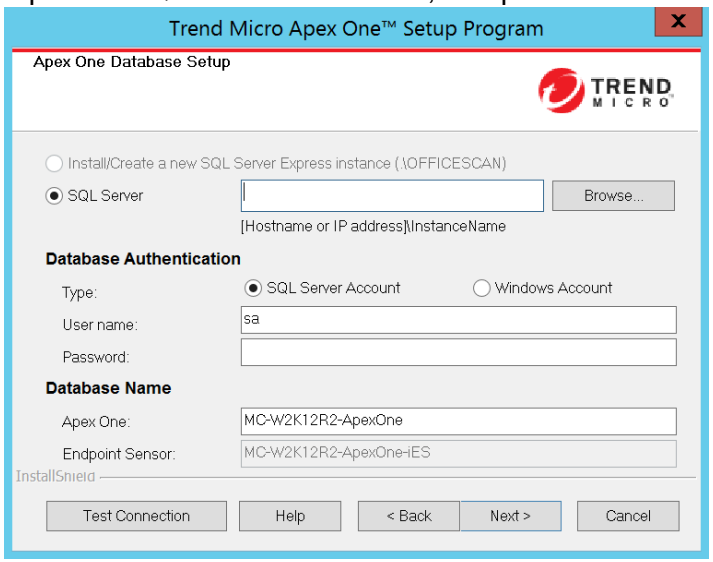
- This is the database backup wizard



- After the database backup finished. “**Endpoint Sensor Installation**” wizard will show here. Select “**Install Endpoint Sensor**” if you want to enable this feature, and click **Next**



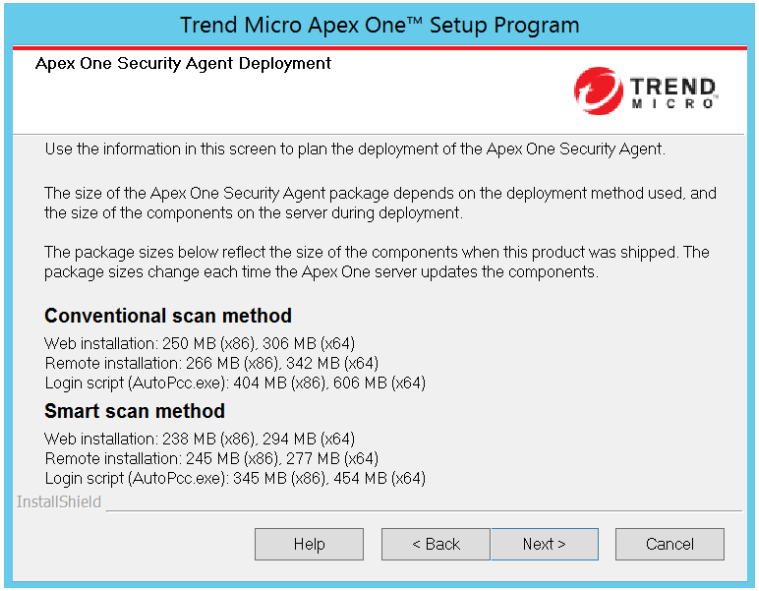
- Input the SQL server information, and provide the dedicate credential for OSCE server



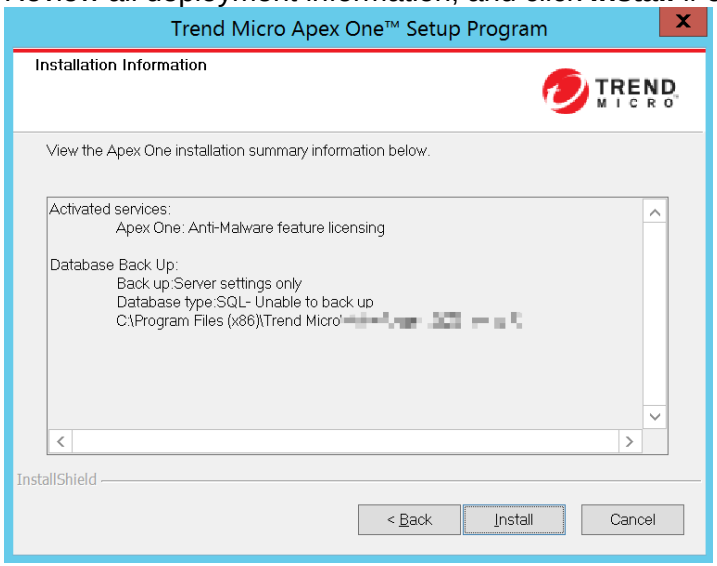
This wizard will show up ONLY when the OSCE server is using Codebase (HTTPDB) as its database application. If

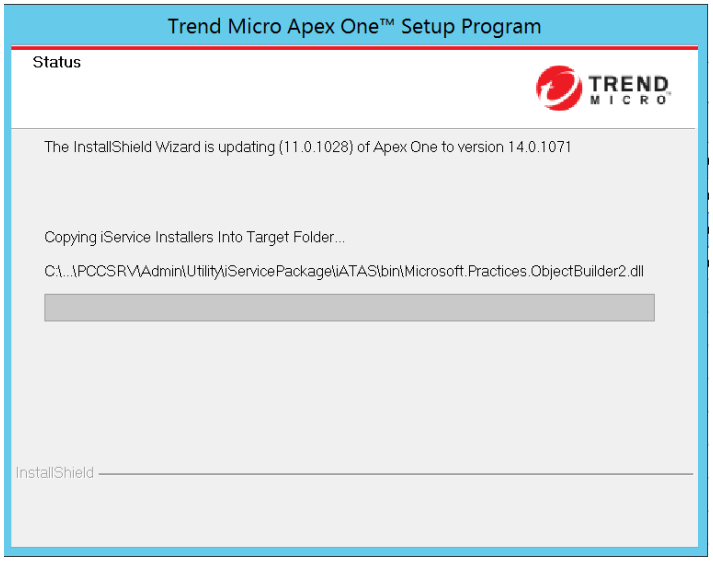
the OSCE server is already using SQL server as its database application, this wizard will be bypass by the installer. That means it will not show.

- This is the agent deployment information wizard. The main purpose is to clarify the deployment size per agent. Please click **Next** to continue

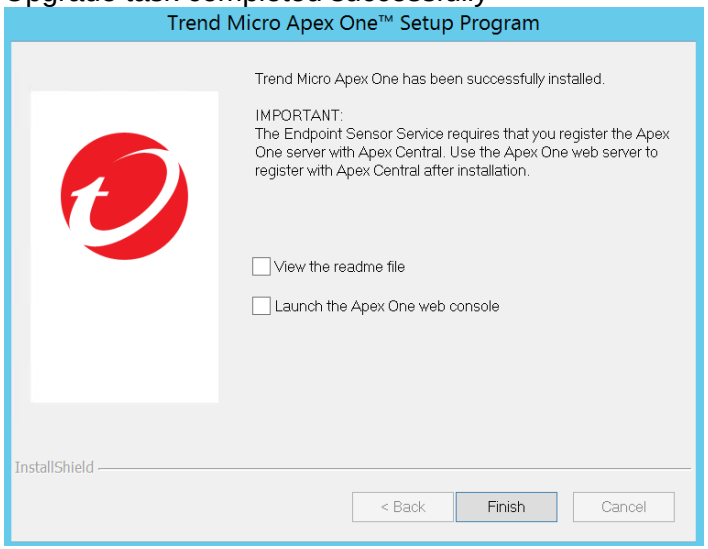


- Review all deployment information, and click **Install** if everything is confirmed



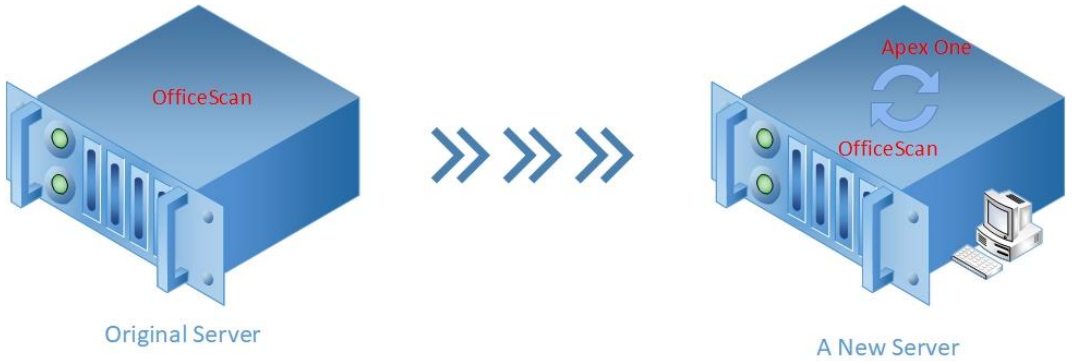


- Upgrade task completed successfully



- Trigger the update for the agents gradually according to the bandwidth.

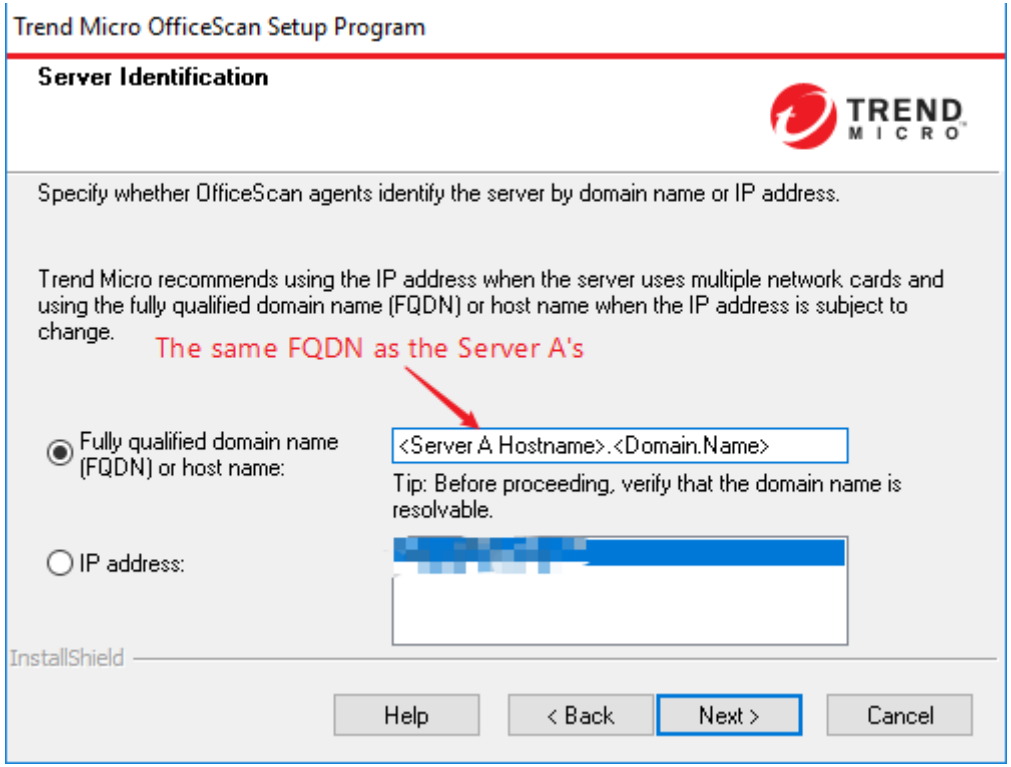
3.2 > Migrating to a new OSCE XG Critical Patch1 server before upgrading to Apex One



1. It is supposed the original server's name is "Server A".
2. Prepare a new server: It is supposed the name is "Server B".
3. Configure Server B according to Server A.
    - Scenario 1: If Server A is using the IP address (x.x.x.x) for OSCE agent-server communication.
        a. Put Server B in an isolated network other than Server A's.
        b. Assign the same IP address for Server B (x.x.x.x).
    - Scenario 2: If Server A is using FQDN for OSCE communication
        a. Put Server B in an isolated network other than Server A's.
        b. Set Server A's **HOSTNAME** for Server B to make sure they are using the same hostname. Server B is no need to assign the same IP Address as Server A's. Please don't join to the domain at this moment. Otherwise, Server A will be untrusted on the domain controller.
        c. Add a HOST file record on Server B. The record is:
        127.0.0.1 <Server B HostName>.<Domain.Name>

4. Do a fresh installation of OSCE XG Critical Patch1 on Server B. And then upgrade it to the same build number as Server A's.

   Attention: Please set the Server A's FQDN during the fresh installation.



5. After the same build OSCE XG server prepared on Server B:

   - Import the certificate from Server A to Server B. Refer to the following article: https://success.trendmicro.com/solution/1111610.
   - Run the tool as administrator [<OSCE Server folder>\PCCSRV\Admin\Utility\ServerMigrationTool] on Server A to export the settings.
   - Copy the exported zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.
   - Run the tool again on Server B to import the settings.

- Copy the whole folder of [<OSCE Server installation folder>\PCCSRV\Virus\] from the original OSCE server to the new Apex One Server [<Apex One Server installation folder>\PCCSRV\Virus\].
- Restore the database from Server A to Server B:
    - HTTPDB:
        i. Stop the OfcService service on Serve A.
        ii. Stop the OfcService service on Server B.
        iii. Copy [<OSCE Server Folder>\PCCSRV\HTTPDB] from Server A to overwrite the same location on Server B.
        iv. Start the OfcService service on Server B.
    - MS SQL Server: Refer to the KB https://success.trendmicro.com/solution/1113252.

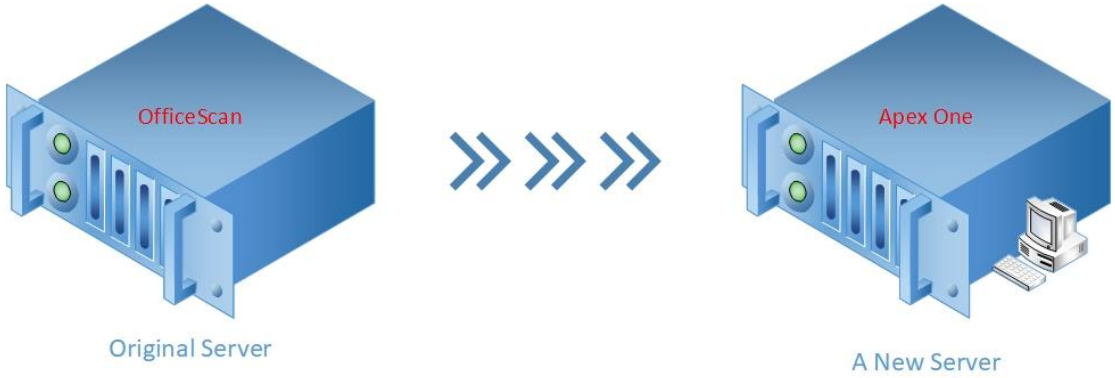
6. If any plug-in service is installed on Server A, please also install it on Server B.
    - For TMSM used on Server A: Please refer to the following article: https://success.trendmicro.com/solution/1055658.
    - For iDLP used on Server A:
        a. Overwrite [<OSCE Server Folder>\PCCSRV\Private\DLPForensicDataTracker.db] from Server A to server B in the same folder.
        b. Check the server's side settings on Server A by following the instructions in the following article: https://success.trendmicro.com/intkb/solution/1098469.
        c. If there is any customized parameter, copy it to Server B as well. If the EnableUserDefinedUploadFolder value is "1" on Server A, copy the whole folder set for UserDefinedUploadFolder to Server B in the same location.
        d. Compare ofcscan.ini on Server A and Server B:

```
UploadForensicDataEnable=x
UploadForensicDataSizeLimitInMb=xx
ForensicDataKeepDays=xxx
ForensicDataDelayUploadFrequenceInMinutes=x
```

e. Make sure Server B's settings are the same as Server A's.

7. After the settings restoration finishes on Server B, please upgrade Server B to XG Critical Patch1 build 1988
8. Then upgrade Server B to Apex One version. (Reference 3.1)
9. After upgrading Server B to Apex One version, please bring Server B online
    - Scenario 1:
        a. Bring Server A offline and move Server B into Server A's LAN, then immediately bring Server B online.
        b. Make sure that OSCE agents can reach Server B.
    - Scenario 2:
        a. Bring Server A offline.
        b. Register Server B to the domain where Server A is located in
        NOTE: After Server B registered, the Server A will be untrusted in the domain.
        c. Remove the HOST file's corresponding record which was added while installing Apex One product
        d. Move Server B to Server A's network if required. It is determined by the customer's network topology.
        e. Make sure that the OSCE agents can reach Server B.
10. Trigger the agents upgrade to Apex One as well.
11. Register Server B to a dedicated Apex Central, if required
12. Register Apex One Edge Relay Server to Server B, if required

3.3 > Replacing an OSCE XG Critical Patch1 server with a new Apex One server



1. It is supposed the original server's name is "Server A".
2. Prepare a new server: It is supposed the name is "Server B".
3. Do a fresh installation of Apex One on Server B
4. After the fresh installation finished
   - Rename the folder to [<OfficeScan Server Installation Folder>\PCCSRV\Admin\Utility\ServerMigrationTool] to [ServerMigrationTool_old] on Server A.
   - Copy the same folder from Server B to Server A. Put it in the same location.
   - Run this tool as Administrator on Server A to export the settings.
   - Copy the exported .zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.
   - Run the tool again on Server B to import the settings.
   - Move the agents from Server A to Server B and trigger update. There are two (2) methods to achieve it:
     - Method 1 via Agent Mover: https://success.trendmicro.com/solution/1056657
     - Method 2 via IPXFER: https://success.trendmicro.com/solution/0127004

5. Trigger the agents upgrade to Apex One as well.
6. Register Server B to a dedicated Apex Central, if required
7. Register Apex One Edge Relay Server to Server B, if required

Chapter 4: Upgrade Verification

In this chapter, it lists the information to verify an upgrading task completed successfully or not.

4.1 > Verifying The Upgraded Apex One Server

1. Installed services

Name	Process	Machine	Startup Type	Status	Requirement
World Wide Web Publishing Service	W3wp.exe	Apex One Server	Automatic	Running	IIS installed
Apex One Master Service	Ofcservice.exe	Apex One Server	Automatic	Running	Master service. Very important.
Apex One Active Directory Integration Service	osceintegrationservice.exe	Apex One Server	Manual	Running	
Apex One Plug-in Manager	OfcAoSMgr.exe	Apex One Server	Automatic	Running	
Apex One Deep Discovery Service	OfcDdaSvr.exe	Apex One Server	Manual	Running	
Apex One Log Receiver Service	OfcLogReceiverSvc.exe	Apex One Server	Manual	Running	
Apex One Apex Central Agent	OfcCMAgent.exe	Apex One Server	Automatic	<Depends>	Running while Apex One server registered to an Apex Central Server
Trend Micro Advanced Threat Assessment Service	ATAS_Service.exe	Apex One Server	Manual	Running	Endpoint sensor feature installed
Trend Micro Endpoint Sensor Service	TrendMicroEndpointSensorService.exe	Apex One Server	Manual	Running	Endpoint sensor feature installed
Redis	redis-server.exe	Apex One Server	Automatic	Running	Endpoint sensor feature installed
Trend Micro Application Control Service	TMiACSvc.exe	Apex One Server	Manual	Running	
Trend Micro Vulnerability Protection Service	iVPServer.exe	Apex One Server	Manual	Running	
Trend Micro Smart Protection Query Handler	SRService.exe	Apex One Server	Manual	Running	
Trend Micro Smart Protection Server	iCRCService.exe	Apex One Server	Manual	Running	iSPS installed and FRS enabled
Trend Micro Local Web Classification Server	LWCSService.exe	Apex One Server	Manual	Running	iSPS installed and FRS enabled
SQL Server (<Instance Name>)	sqlservr.exe	SQL Server	Automatic	Running	
SQL Full-text Filter Daemon Launcher ((<Instance Name>)	fdlauncher.exe	SQL Server	Manual	Running	Endpoint sensor feature installed

2. Important processes:

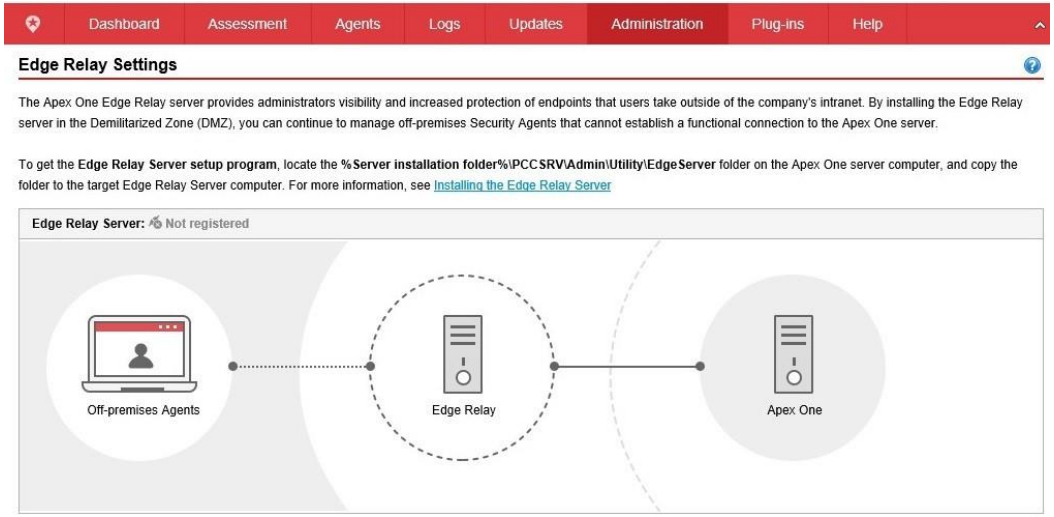
Name	Status	Purpose	Requirement
DBServer.exe	Running	Touch database	
Ofchotfix.exe	By request	Packet program files	
Verconn.exe	By request	Check agent status	
Php-cgi.exe	Running	Handle web request	Locate in PCCSRV\PLM\PHP folder

3. Confirm that the registry keys below exist:
   [**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan**]
4. Confirm that the Apex One web management console can be logged into using the default user name: root.

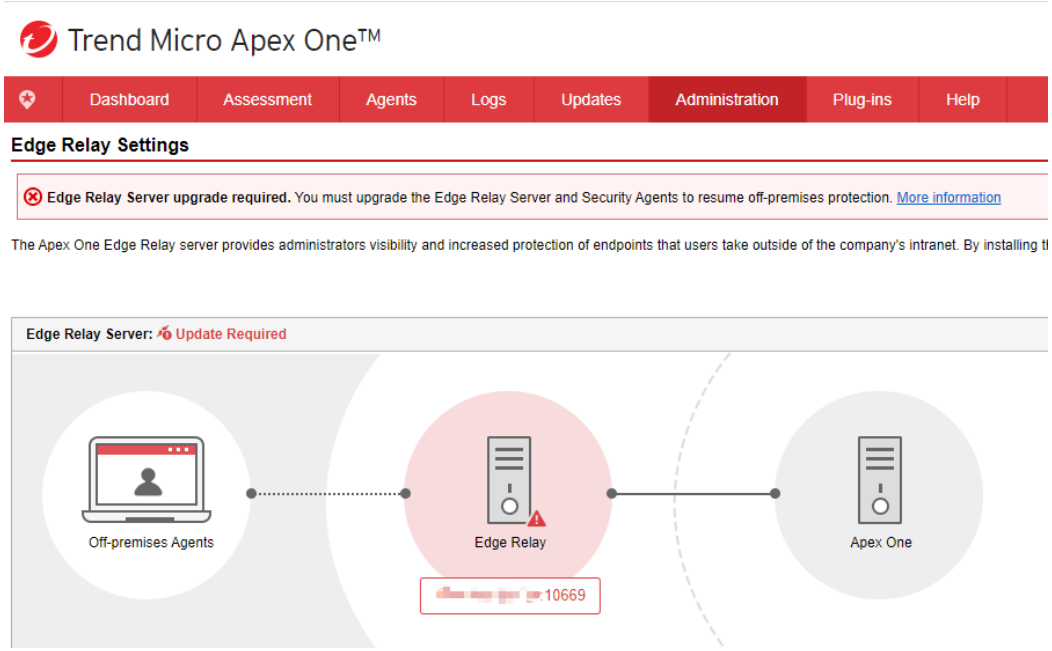
4.2 > Upgrade the Edge Relay server

Before performing edge relay server upgrade action, please check the edge relay server status in Apex One management console.

- Not Registered to an edge relay:



- Registered to an edge relay in XG version:



If the OSCE server has registered to an edge relay server, it is required to upgrade the edge relay server to version 2.0.

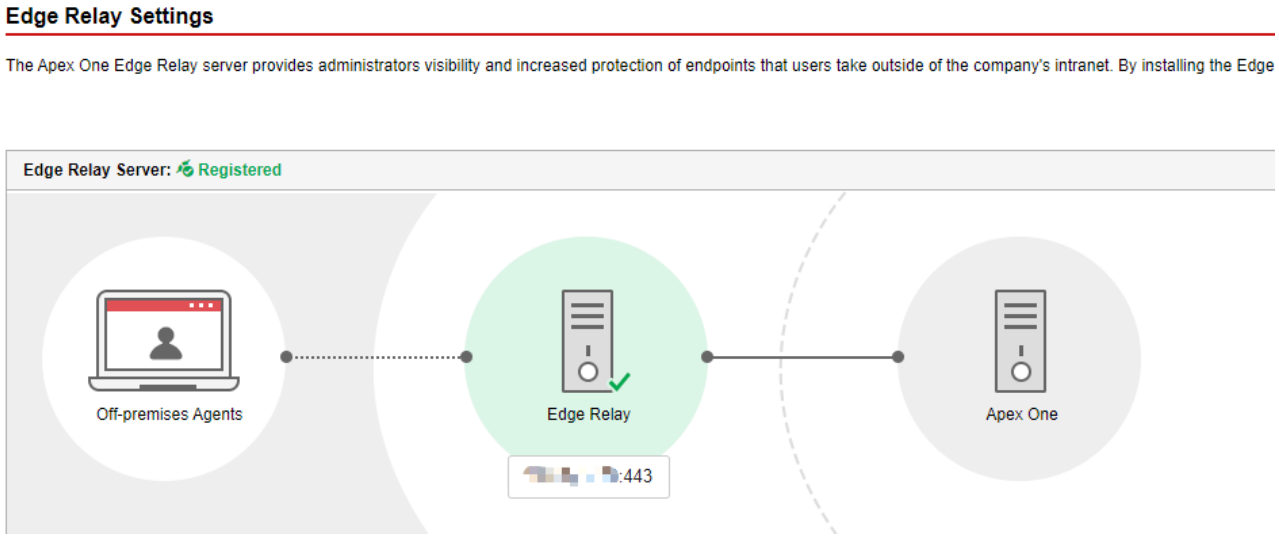
To do this:

1. Login the Apex One server
2. Navigate to the directory: [<…>\Trend Micro\Apex One\PCCSRV\Admin\Utility\EdgeServer\]
3. Copy the whole “EdgeServer” folder to the Edge Relay server
4. Execute “EdgeServer\setup.exe” to directly upgrade the edge relay server
5. After the installation completed, please run cmd.exe as administrator. Then execute the prompt to register the version 2.0 edge relay server to the Apex One server:
   <…>\Trend Micro\OfficeScan Edge Relay\OfcEdgeSvc**ofcedgecfg.exe --cmd reg --server <Apex One Server> --port**

<Apex One Server SSL Port> --pwd <The password of ROOT for Apex One management console login>

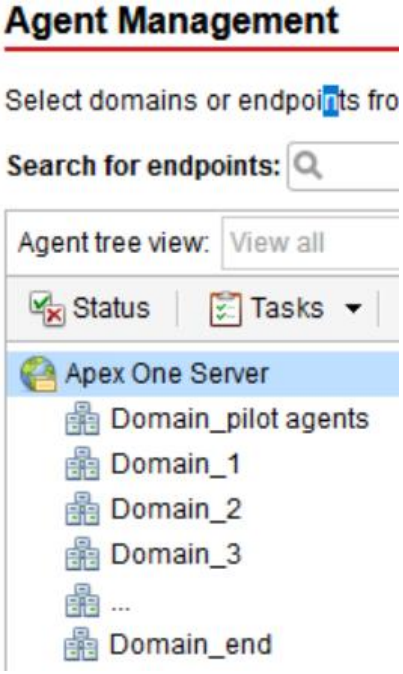
```
C:\Program Files\Trend Micro\OfficeScan Edge Relay\OfcEdgeSvc>ofcedgecfg.exe --c
md reg --server [redacted]  --port 4343 --pwd [redacted]
Command executes successfully

C:\Program Files\Trend Micro\OfficeScan Edge Relay\OfcEdgeSvc>
```

6. Confirm the edge relay registered in Apex One web management console:



4.3 > Upgrade the managed agents

It is recommended to upgrade some pilot agents, and monitor them for some days (depend on the requirement). Confirmed that the upgraded agents are working well, then upgrade the rest of the them.



In this example, put the pilot agents into “Domain_pilot agents” domain. And upgrade the agents in this domain.

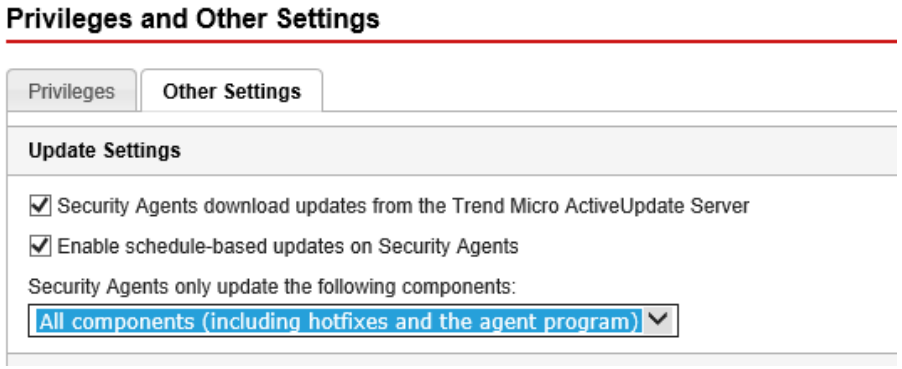
After the upgraded pilot agents confirmed running well, then upgrade the rest agents domain by domain:
Upgrade agents located in Domain_1, then upgrade agents located in Domain_2 etc. Till the last domain “Domain_end” has been performed upgrade action.

Please check following detailed steps to achieve it.

To do this:

1. Log in to the web management console.
2. Go to **Agents** > **Agent Management**
3. Put some pilot agents into “Domain_pilot agents”
4. On the agent tree, click on the “Domain_pilot agents”. Then navigate to **Settings** > **Privileges and Other Settings**

5. In **Update Settings** blade, choose "**All components (including hotfixes and the agent program)**" from the drop down list



6. **Save** the change
7. Wait for all of the pilot agents upgraded
8. Monitor them for some days
9. Confirmed that the new Apex One agent program is working well.
10. Upgrade the rest of the agents by repeat step 4 to step 6 for each domain.

> **NOTE** All of the agents connected to the Apex One server will be upgraded. However, for the agents that cannot receive notifications from the Apex One server, such as those behind a NAT environment, will NOT be upgraded immediately. Those agents will be upgraded according to the start time of a schedule-based update, so it will take some time before it starts upgrading. A client package (EXE or MSI) can also achieve it.

Chapter 5: Plug-in Service Migration

This section shows how to handle the installed plug-in service(s) during Apex One server migration/replacement.

5.1 > TMSM

For TMSM used on the original server, currently there is no equivalent utility for the TMSM client migration. The administrator has to uninstall/reinstall the TMSM client to transfer it to another server.
Please refer to the following article:
https://success.trendmicro.com/solution/1055658

5.2 > iDLP

For iDLP used on the original server:

1. Install iDLP PLS on the new server, and then activate it.
2. Make sure the Apex One Master Service has been stopped.
3. Run ServerMigrationTool as Administrator [<Apex One Server folder>\PCCSRV\Admin\Utility\ServerMigrationTool] on the original OSCE server to export settings. (Please ignore this step if it has been done during this migration or replacement.)
4. Copy the exported zip file (i.e. C:\OsceMigrate.zip) to the new server and put it in the same location as the original server. (Please ignore this step if it has been done during this migration or replacement.)
5. Run the tool again on the Apex One server to import settings. (Please ignore this step if it has been done during this migration or replacement.)
6. Back up the database on the original server and restore it on the new server. (Please ignore this step if it has been done during this migration or replacement.)
7. Back up the following data on the OSCE server:
    - <OSCE Server folder>\PCCSRV\Private\DLPForensicDataTracker.db
    - Forensic folder

    This folder's information is saved in <OSCE Server folder>\PCCSRV\Private\ofcserver.ini.

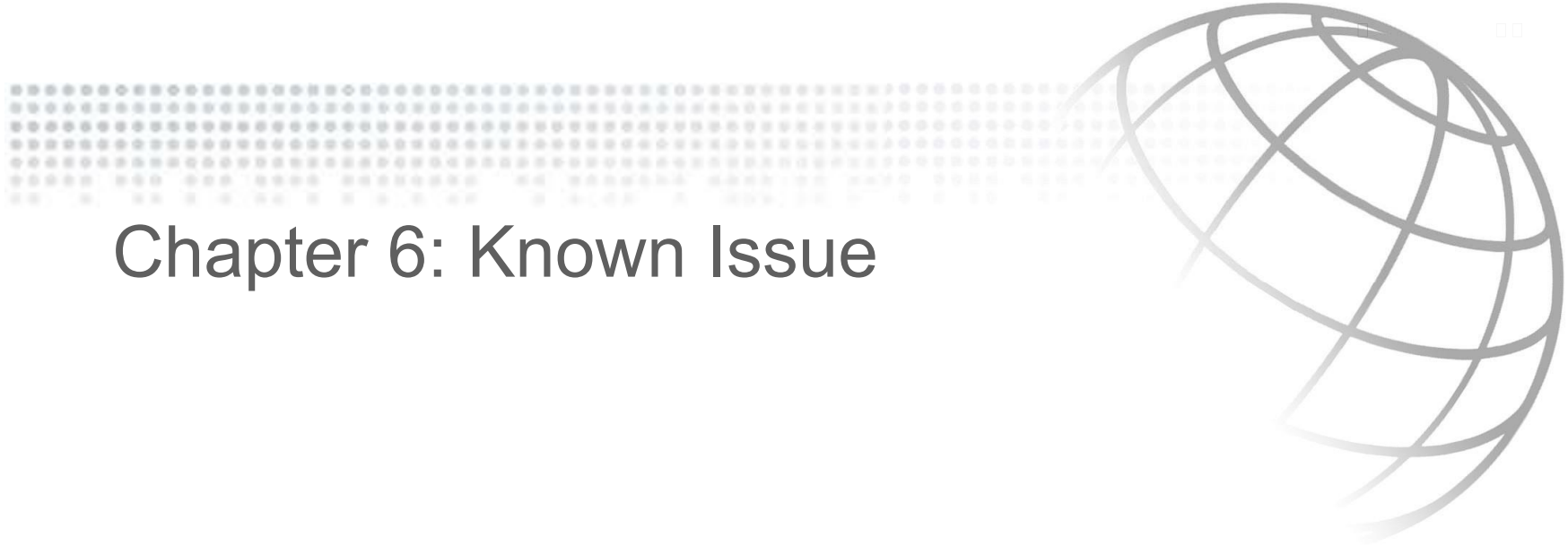
    [INI_IDLP_SECTION]
    EnableUserDefinedUploadFolder = <value>
    UserDefinedUploadFolder = <value or NULL>

- If the value of EnableUserDefinedUploadFolder is “0”, it is a default value. The folder’s location by default is <OSCE Server folder>\PCCSRV\Private\DLPForensicData.
- If the value of EnableUserDefinedUploadFolder is “1”, the folder’s location should be set after “UserDefinedUploadFolder =”.

8. Restore and overwrite DLPForensicDataTracker.db and the forensic folder from the original server to the new server in the same locations.
9. Compare the following part in the ofcscan.ini of both servers to make sure there are no changes on both of the servers:

```
UploadForensicDataEnable=x
UploadForensicDataSizeLimitInMb=xx
ForensicDataKeepDays=xxx
ForensicDataDelayUploadFrequenceInMinutes=xxxx
```

10. Verify iDLP’s rules, settings, and logs on the new server.



Chapter 6: Known Issue

6.1 > Other Update Source (OUS)

Issue description:

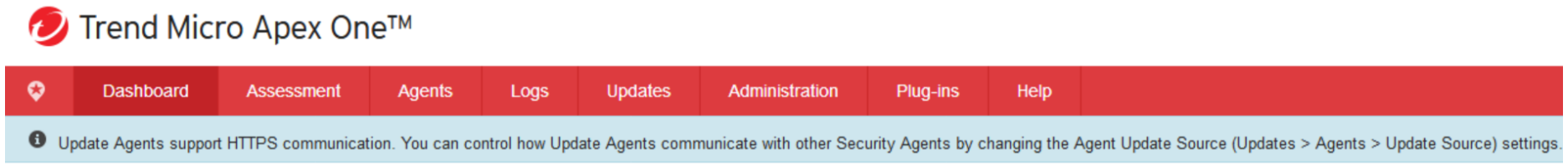
Some agent may fail to get update from its dedicated update source.

Reason:

Since Apex One version, the communication protocol between agent-server and agent-OUS is HTTPS mandatorily. There is no workaround to set it back to HTTP mode.

Suggestion to resolve the issue:

So, after the sever has been upgraded to Apex One, please login the web management console, and pay attention the dashboard's banner.



If the banner shows, please update the HTTP OUS to HTTPS mode from **Updates** > **Agents** > **Update Source.**

If the OUS is promoted from a security agent, please make sure it has been upgraded to Apex One version.

6.2 > Edge Relay

Issue description:

The Apex One server and security agent cannot get the expected information from the registered edge relay server.

Reason:

In Apex One version, the edge relay server has been re-designed. Officially, this version's edge relay is called version 2 (v2). The previous edge relay server is version 1 (v1).

Edge relay v2 is working as a reverse proxy. It is totally different from v1.

Suggestion to resolve the issue:

Please refer to Chapter 4 section 2 (4.2) to upgrade the old edge relay server to version 2.

6.3 > Apex One Version

Issue description:

The apex one agent may encounter looping upgrade problem, while the Apex One server was upgraded from OSCE 11.0 or XG version.

Reason:

Following files are not used in Apex One any more. When the OSCE agents are trying to upgrade to Apex One version, it will still try to download following files. But those files are non-existing on the update source, so it will fail to download them. Then the upgrade procedure will be rollback, and then looping upgrade issue happens.

- /officescan/hotfix_pccnt/COMMON/Microsoft.VC80.CRT.manifest
- /officescan/hotfix_pccnt/COMMON/msvcm80.dll
- /officescan/hotfix_pccnt/COMMON/msvcp80.dll
- /officescan/hotfix_pccnt/COMMON/msvcr80.dll

Suggestion to resolve the issue:

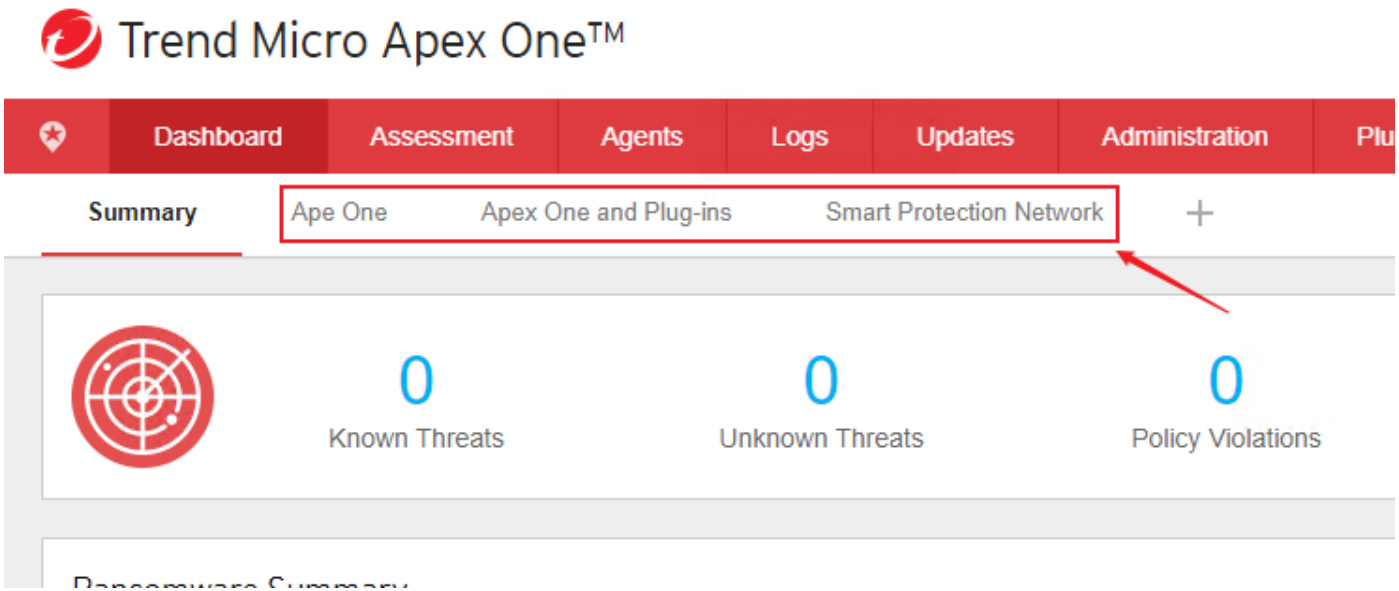
While upgrading OSCE server to Apex One version, please continue to upgrade to Apex One Patch2 Build 2146.

6.4 > Dashboard

Issue description:

Upgrade the server to Apex One, there may be other 3 pages in **Dashboard** in the management console expect “**Summary**”. These pages are “**Apex One**”, “**Apex One and Plug-ins**”, “**Smart Protection Network**”. These 3 pages will not show in the

management console while performing an Apex One server fresh installation.



Reason:

Those 3 legacy pages are not used any more in Apex One version. This known issue may be encountered when the Apex One server was upgraded from a previous version.

Suggestion to resolve the issue:

1. Login in this upgraded Apex One Server
2. Backup the file: <..\PCCSRV\Web_OSCE\Web_console\HTML\widget\repository\db\sqlite\tmwf.db>
3. Copy the same file from a fresh installed Apex One server to the upgraded Apex One server.
4. Overwrite it, and reload the management console