Trend Micro Apex One™ and iProduct

Disaster Recovery Guide

Table of Contents

System Requirement

Please prepare at least three (3) Windows Server Platforms for installing the servers below:

- Standalone SQL server
- Apex One main server
- Apex One backup server

> Note: For Apex One Main server and Apex One Backup Server, please prepare two (2) identical Windows Server Platforms (i.e. two Windows Server 2016 platforms).

Preparation for Apex One Main Server

Since the option to export the Apex One Server Authentication Certificate is not allowed after **Apex One On-Premise Patch 3 Build 8378**, this guide must be prepared at the beginning of the Apex One Main Server installation.

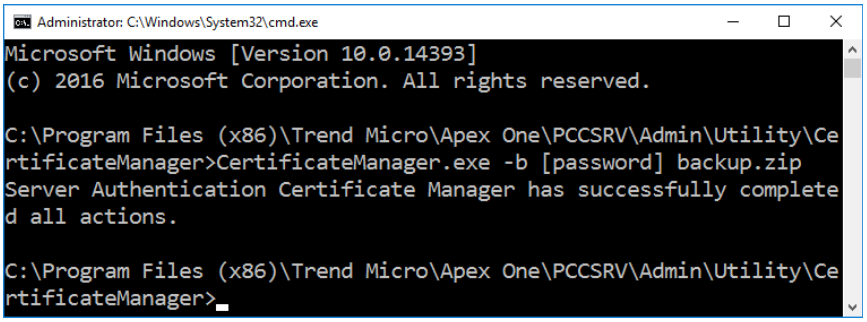
Install the Apex One GM Build (2012) and back up the certificate files.

a. After installing the Apex One Main Server (before applying Patch 3 Build 8378), back up the certificate file of Apex One server found under the following path:

<Server installation folder>\AuthCertBackup\OfficeScanAuth.dat

b. Certificate files can also be backed up using the Certificate Manager tool located on **<Server installation folder>\PCCSRV\Admin\Utility\CertificateManager\**. Please use following command to back up the certificate.

CertificateManager.exe -b [password] backup.zip



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\Ce
rtificateManager>CertificateManager.exe -b [password] backup.zip
Server Authentication Certificate Manager has successfully complete
d all actions.

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\Ce
rtificateManager>_
```

Preparation for Apex One Server Backup

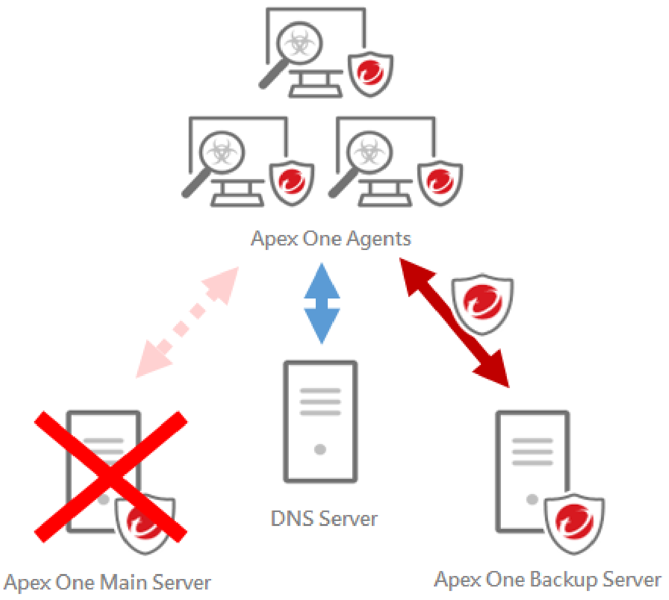
In order to effectively perform this guide, we recommend to prepare the following setup for Apex One Backup Server:

Apex One Main Server
Apex One Backup Server

Apex One Main Server vs Apex One Backup Server

- Use the same Web Server type and port
- Use the same FQDN
- Use the same Agent Port
- Use the same Server Authentication Certificate
- Use the same SQL Sever and Database

Offsite Backup Considerations



DNS

Since both main Apex One Server and Apex One Backup Server have to use the same FQDN, ensure all agents are available to connect to the correct Apex One Server by properly switching the DNS setting.

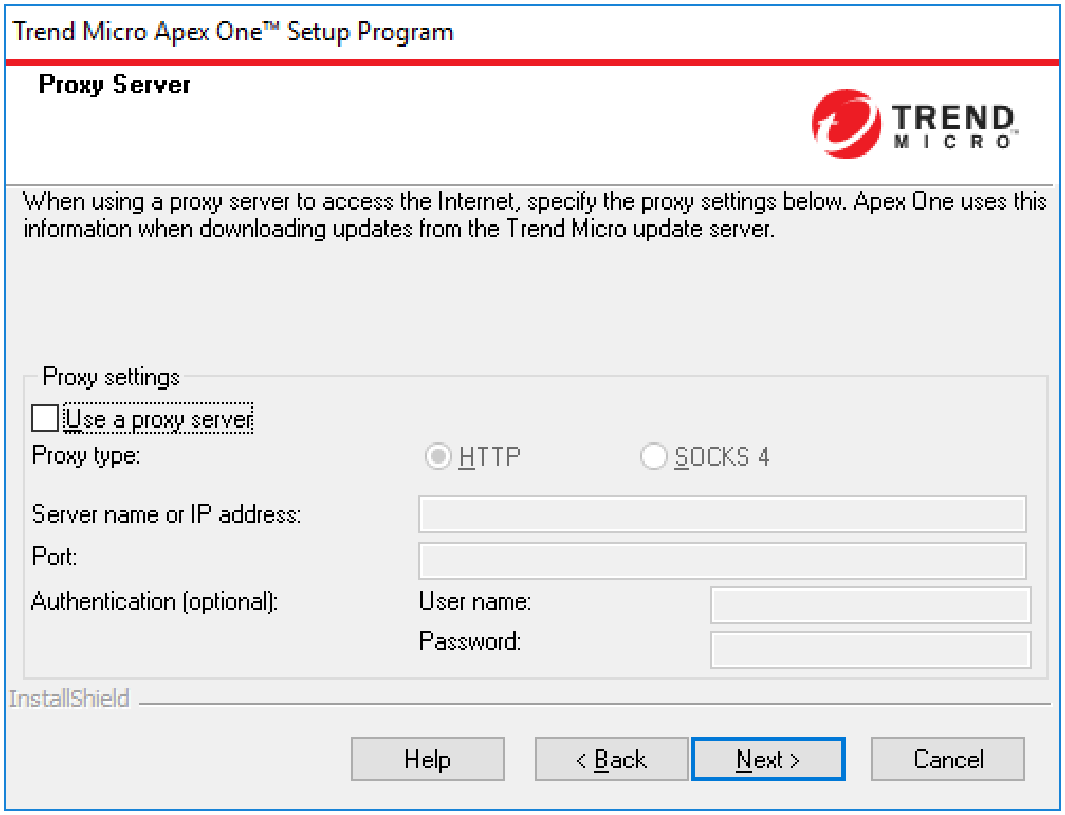
Apex One Server Setup and Configuration

Installation

In order to setup two (2) identical Apex One servers, please make sure the settings should be the same during installation.

Proxy Setting

Please use the same networking settings.



Trend Micro Apex One™ Setup Program

Proxy Server

When using a proxy server to access the Internet, specify the proxy settings below. Apex One uses this information when downloading updates from the Trend Micro update server.

Proxy settings

□ Use a proxy server

Proxy type: ● HTTP ○ SOCKS 4

Server name or IP address:

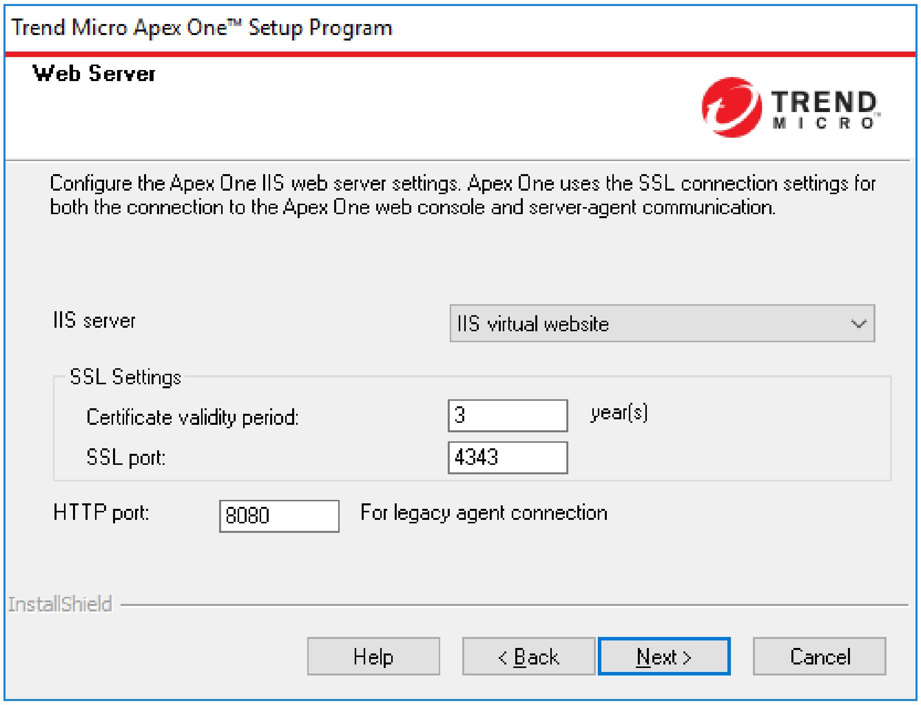
Port:

Authentication (optional): User name:

Password:

Web Server

The Apex One Backup Server has to use the same IIS server setting as default Apex One Server.



Trend Micro Apex One™ Setup Program

Web Server

Configure the Apex One IIS web server settings. Apex One uses the SSL connection settings for both the connection to the Apex One web console and server-agent communication.

IIS server: IIS virtual website

SSL Settings

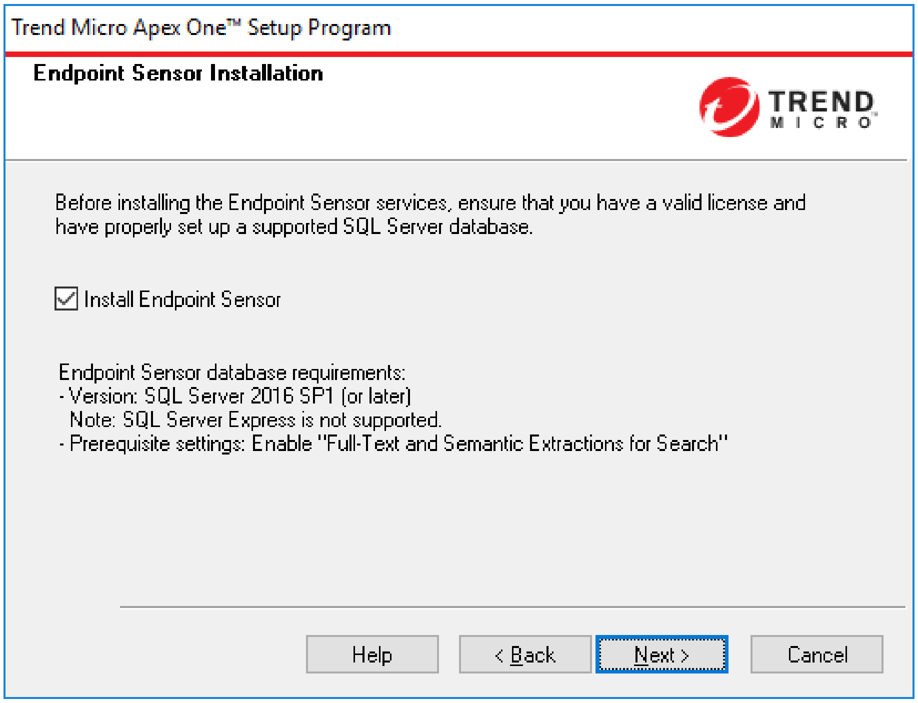
Certificate validity period: 3 year(s)

SSL port: 4343

HTTP port: 8080 For legacy agent connection

Install Endpoint Sensor

This disaster recovery guide supports installing iES or without installing iES. If the Endpoint Sensor will be installed, please install with the same Microsoft SQL instance as Apex One server.



Trend Micro Apex One™ Setup Program

Endpoint Sensor Installation

Before installing the Endpoint Sensor services, ensure that you have a valid license and have properly set up a supported SQL Server database.

☑ Install Endpoint Sensor

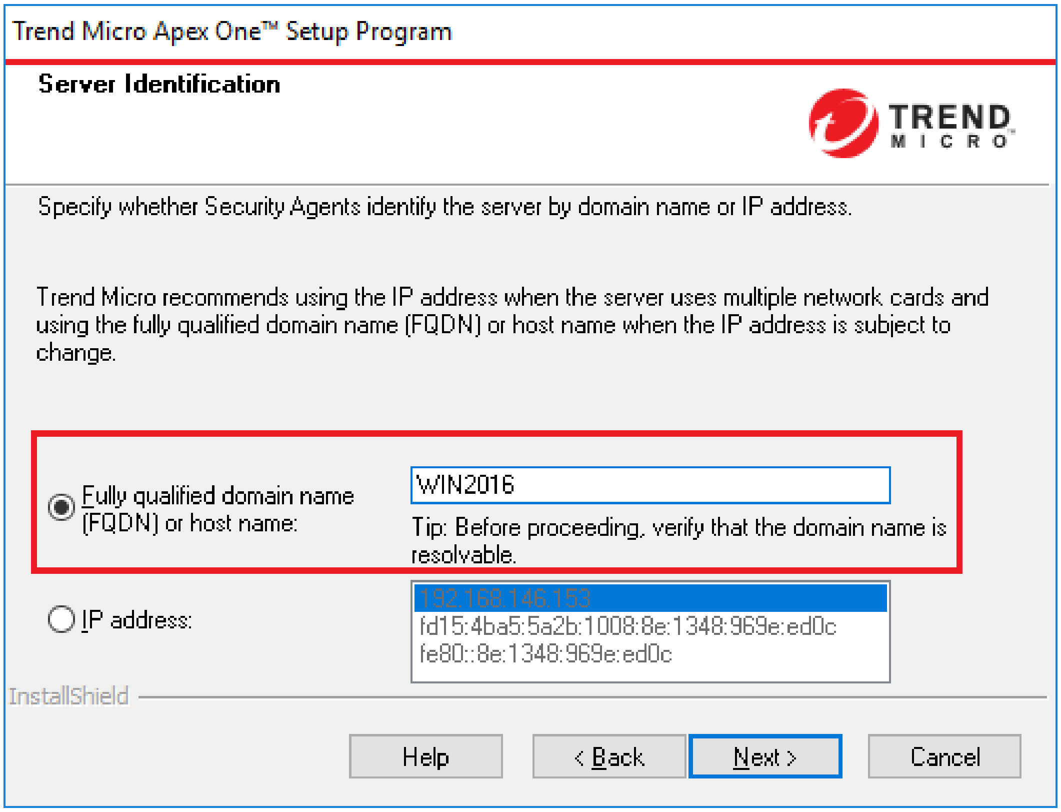
Endpoint Sensor database requirements:
- Version: SQL Server 2016 SP1 (or later)
  Note: SQL Server Express is not supported.
- Prerequisite settings: Enable "Full-Text and Semantic Extractions for Search"

Below are some notes to consider:

1. Please prepare another standalone SQL server if the iES needs to be installed on a different Microsoft SQL instance.
2. For installing the iES with different MSSQL instance, follow this article: Installing the Apex One Endpoint Sensor database and Apex One database in different MSSQL instances (KB 1122929). Please ensure that the Apex One Main Server and Backup Server set the same iES settings as well.

Server Identification

When setting the Server Identification, please make sure that both default server and backup server are using the same FQDN name.



Trend Micro Apex One™ Setup Program

Server Identification

Specify whether Security Agents identify the server by domain name or IP address.

Trend Micro recommends using the IP address when the server uses multiple network cards and using the fully qualified domain name (FQDN) or host name when the IP address is subject to change.

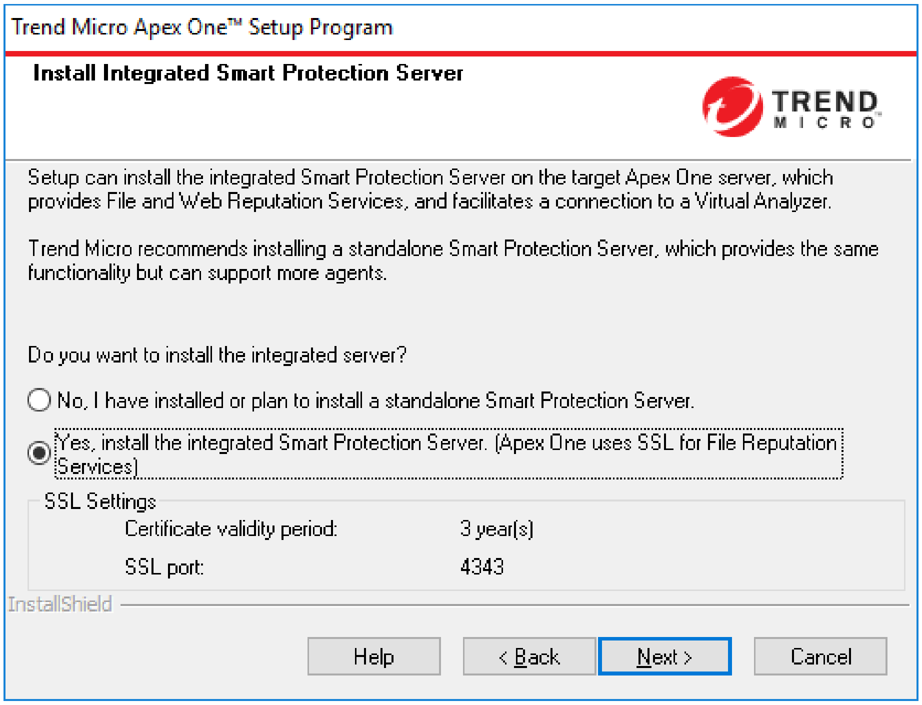
● Fully qualified domain name (FQDN) or host name: WIN2016

Tip: Before proceeding, verify that the domain name is resolvable.

○ IP address:
192.168.146.153
fd15:4ba5:5a2b:1008:8e:1348:969e:ed0c
fe80::8e:1348:969e:ed0c

Integrated Smart Protection Server

Please set the same iSPS setting for both Apex One servers.



Trend Micro Apex One™ Setup Program

Install Integrated Smart Protection Server

Setup can install the integrated Smart Protection Server on the target Apex One server, which provides File and Web Reputation Services, and facilitates a connection to a Virtual Analyzer.

Trend Micro recommends installing a standalone Smart Protection Server, which provides the same functionality but can support more agents.

Do you want to install the integrated server?

○ No, I have installed or plan to install a standalone Smart Protection Server.

● Yes, install the integrated Smart Protection Server. (Apex One uses SSL for File Reputation Services)

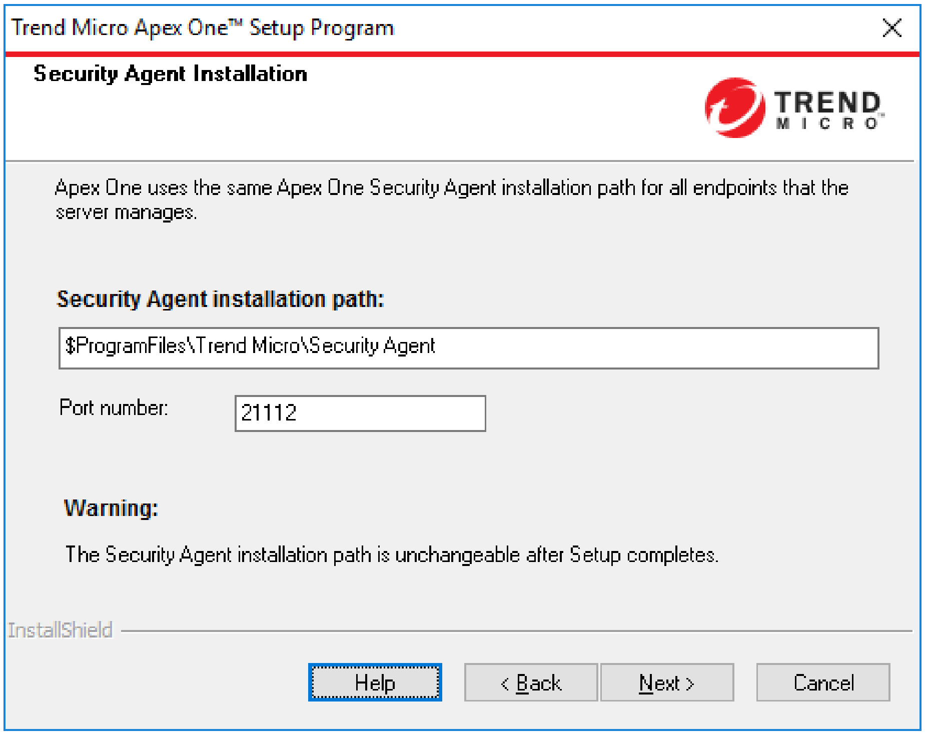
SSL Settings

Certificate validity period: 3 year(s)

SSL port: 4343

Agent Port

Please set the same agent port for both Apex One servers.



Trend Micro Apex One™ Setup Program

Security Agent Installation

Apex One uses the same Apex One Security Agent installation path for all endpoints that the server manages.

Security Agent installation path:

$ProgramFiles\Trend Micro\Security Agent

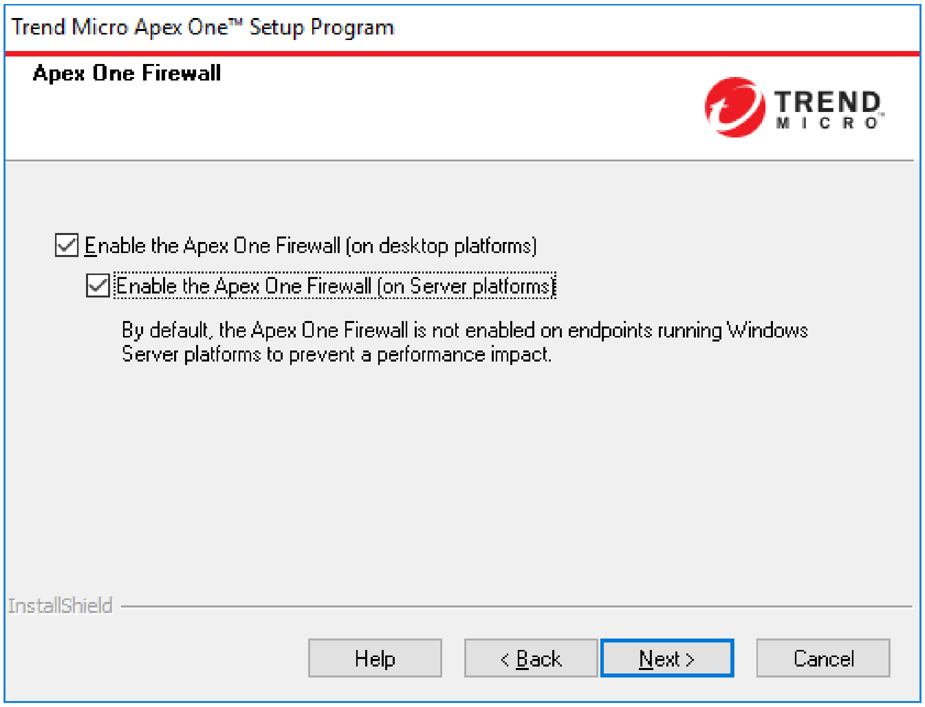
Port number: 21112

Warning:

The Security Agent installation path is unchangeable after Setup completes.

Firewall Setting

Please set the same firewall setting for both Apex One servers.



Trend Micro Apex One™ Setup Program

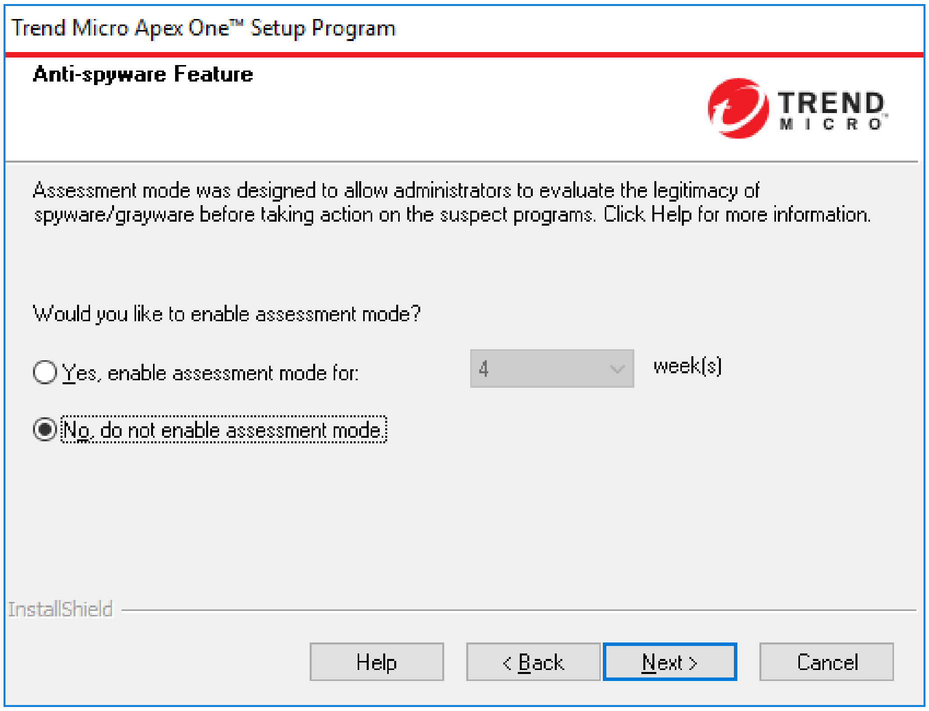
Apex One Firewall

☑ Enable the Apex One Firewall (on desktop platforms)

☑ Enable the Apex One Firewall (on Server platforms)

By default, the Apex One Firewall is not enabled on endpoints running Windows Server platforms to prevent a performance impact.

Assessment Mode



Trend Micro Apex One™ Setup Program

Anti-spyware Feature

Assessment mode was designed to allow administrators to evaluate the legitimacy of spyware/grayware before taking action on the suspect programs. Click Help for more information.

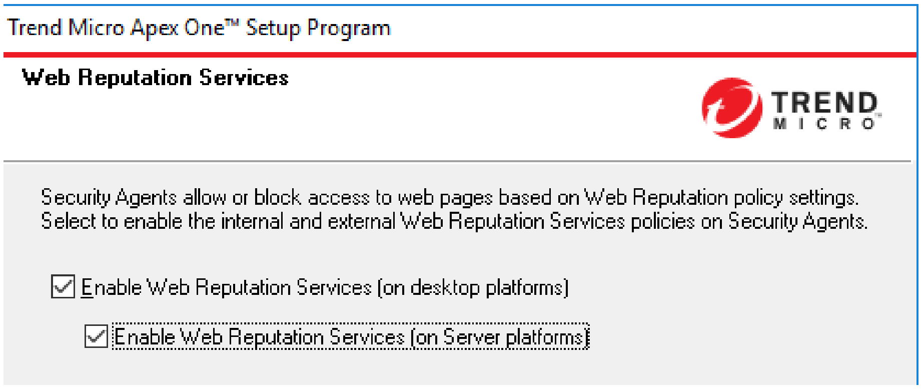
Would you like to enable assessment mode?

○ Yes, enable assessment mode for: 4 week(s)

● No, do not enable assessment mode.

Web Reputation Services

Please set the same Web Reputation for both Apex One servers.



Trend Micro Apex One™ Setup Program

Web Reputation Services

Security Agents allow or block access to web pages based on Web Reputation policy settings. Select to enable the internal and external Web Reputation Services policies on Security Agents.

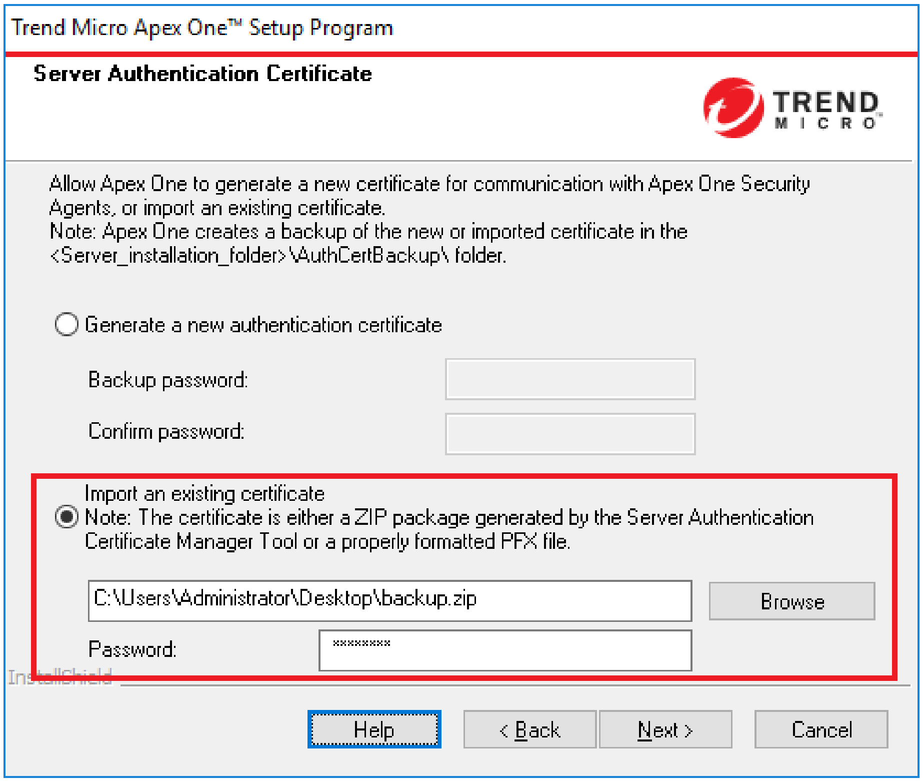
☑ Enable Web Reputation Services (on desktop platforms)

☑ Enable Web Reputation Services (on Server platforms)

Server Authentication Certificate

Please use the same Server Authentication Certificate. Select **Import an existing certificate** and use the original certificate file (OfficeScanAuth.dat) which is from default Apex One server. The file format of the certificate is zip in Apex One.

Please modify the file extension to .zip before importing the certificate or the zip file which was generated from the CertificateManager.exe tool.



Trend Micro Apex One™ Setup Program

Server Authentication Certificate

Allow Apex One to generate a new certificate for communication with Apex One Security Agents, or import an existing certificate.
Note: Apex One creates a backup of the new or imported certificate in the <Server_installation_folder>\AuthCertBackup\ folder.

○ Generate a new authentication certificate

Backup password:

Confirm password:

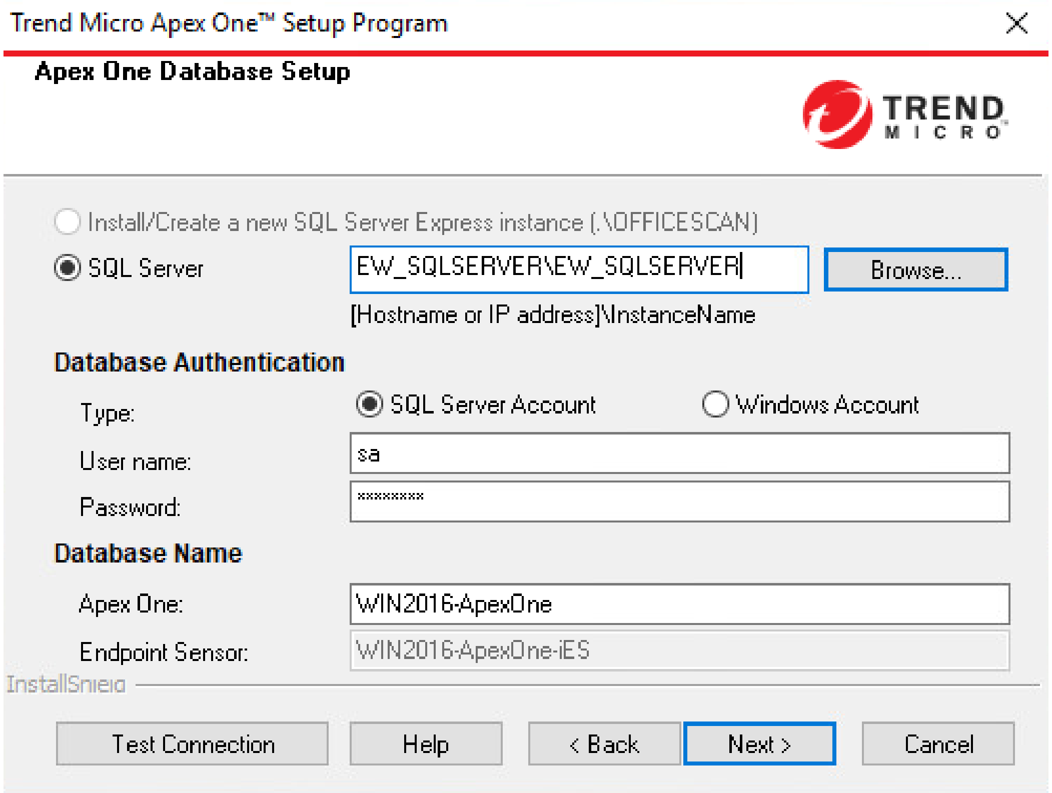
● Import an existing certificate
Note: The certificate is either a ZIP package generated by the Server Authentication Certificate Manager Tool or a properly formatted PFX file.

C:\Users\Administrator\Desktop\backup.zip

Password: *********

Connect to the same SQL server as Apex One Main Server

Install the Apex One Backup Server with the same SQL server and the same Database Name as Apex One Main server.



Trend Micro Apex One™ Setup Program

Apex One Database Setup

○ Install/Create a new SQL Server Express instance (.\OFFICESCAN)

● SQL Server: EW_SQLSERVER\EW_SQLSERVER

[Hostname or IP address]\InstanceName

Database Authentication

Type: ● SQL Server Account ○ Windows Account

User name: sa

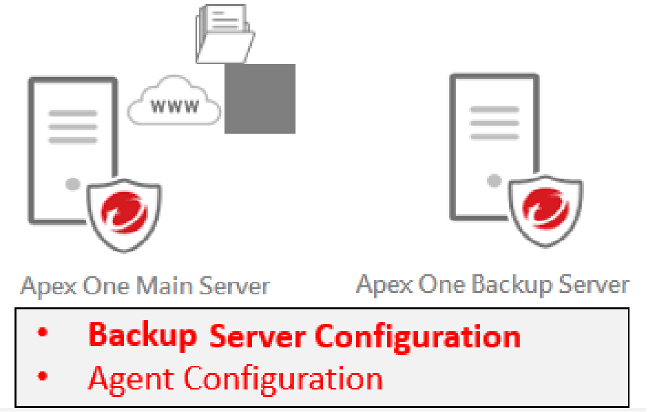
Password: *********

Database Name

Apex One: WIN2016-ApexOne

Endpoint Sensor: WIN2016-ApexOne-iES

Backup Apex One Server Configuration



- **Backup Server Configuration**
- Agent Configuration

Agent Configuration Backup

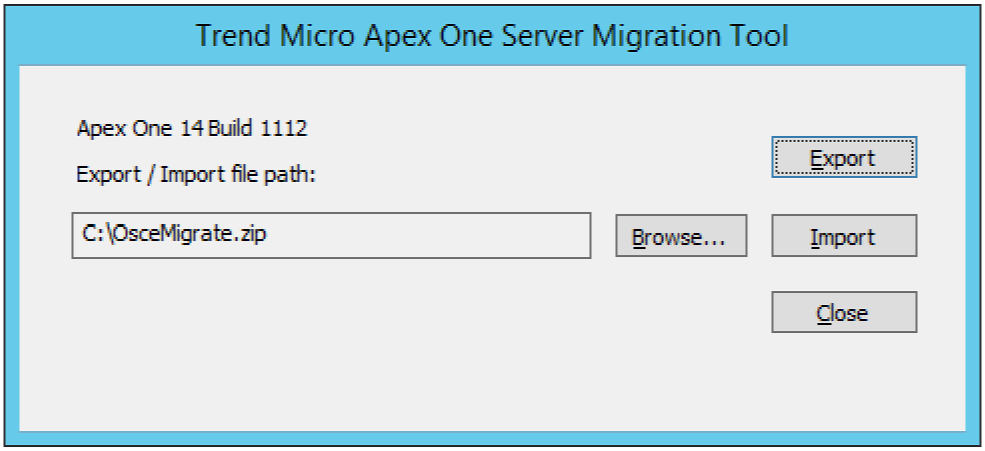
To back up the configuration, please use Server Migration Tool located under <Server installation folder>\PCCSRV\Admin\Utility\ServerMigrationTool. This tool can export and import the following Apex One settings:

- Domain structures
- Settings that will be backed up at both root and domain levels:
  - Scan configurations for all scan types (Manual, Real-time, Scheduled, Scan Now)
  - Web reputation configurations
  - Approved URL list
  - Behavior Monitoring settings
  - Device Control settings
  - Digital Asset Control settings
  - Privileges and other settings
  - Additional service settings
  - Spyware/Grayware approved list
  - Suspicious connection setting
- Endpoint (Computer) location
- Firewall policies and profiles
- Connection Verification (Scheduled Verification settings)
- Smart Protection sources
- Server update schedule

- Client update source and schedule
- Logs (Log Maintenance)
- Notifications
- Administration
  - Proxy settings
  - Inactive Agent
  - Quarantine Manager
  - Web Console Settings

Trend Micro Apex One Server Migration Tool

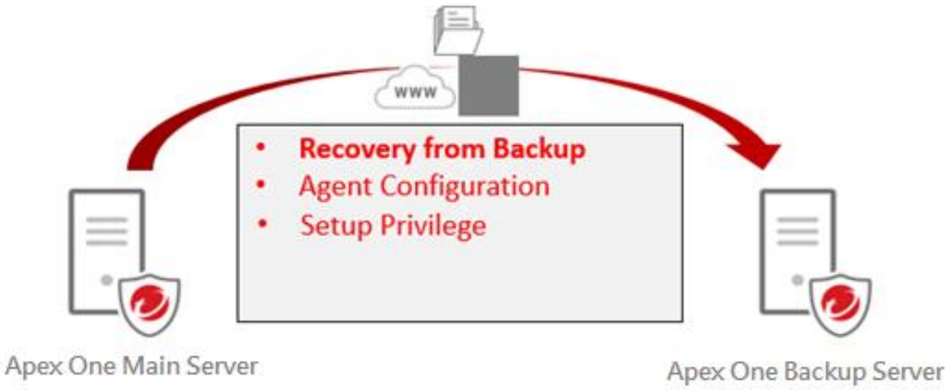
Input the Export/Import file path and select **Export**, and a zip file will be generated.


Trend Micro Apex One Server Migration Tool

Apex One 14 Build 1112

Export / Import file path: C:\OsceMigrate.zip

Apex One Recovery from Backup

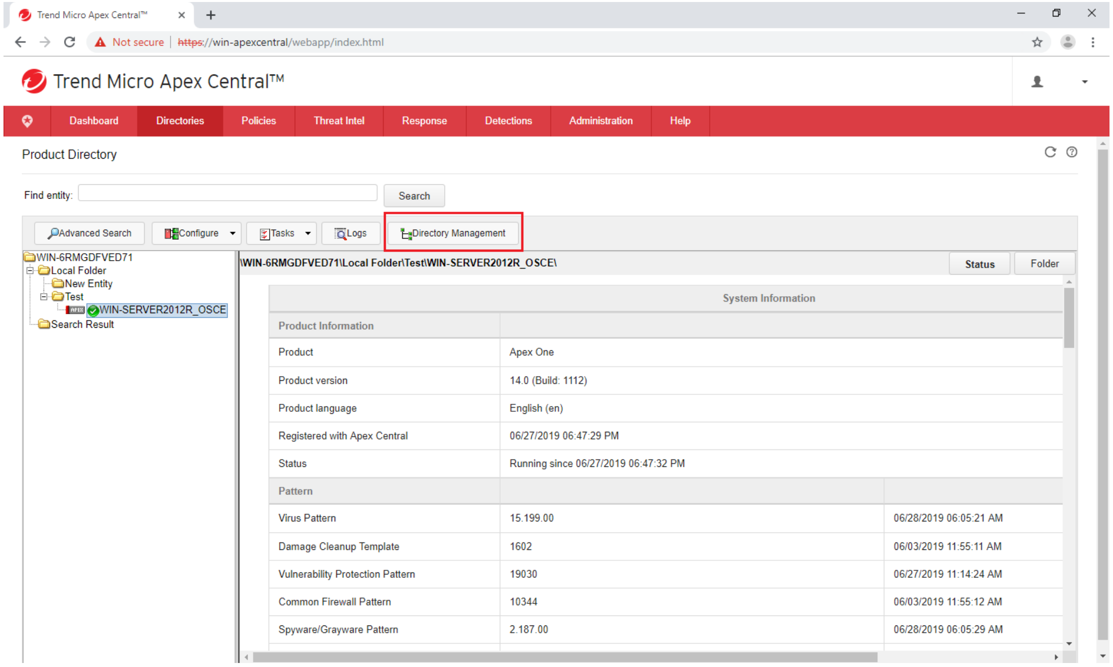


Apex One recovery includes **Agent Configuration**. Before recovering the Apex One server, please follow the steps below.

Unregister from Apex Central

If the Apex One main server has registered to Apex Central, please follow the instructions below to unregister Apex One server from Apex Central:

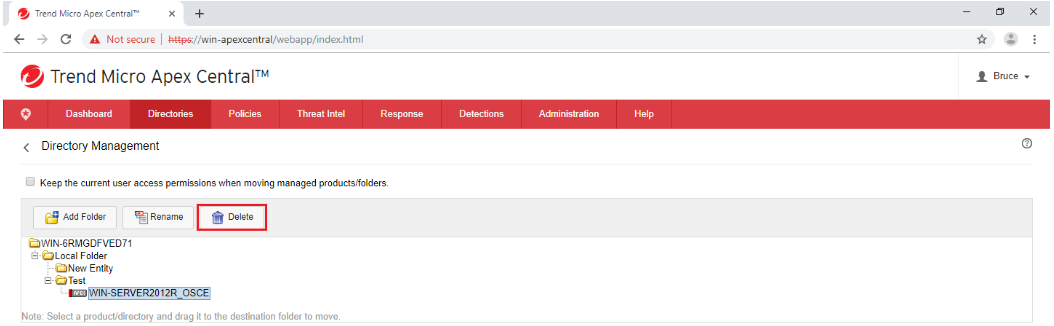
1. Go to Apex Central console > **Directories** > **Products**.
2. Click on **Directory Management**.



\WIN-6RMGDFVED71\Local Folder\Test\WIN-SERVER2012R_OSCE\

System Information		
Product Information		
Product	Apex One	
Product version	14.0 (Build: 1112)	
Product language	English (en)	
Registered with Apex Central	06/27/2019 06:47:29 PM	
Status	Running since 06/27/2019 06:47:32 PM	
Pattern		
Virus Pattern	15.199.00	06/28/2019 06:05:21 AM
Damage Cleanup Template	1602	06/03/2019 11:55:11 AM
Vulnerability Protection Pattern	19030	06/27/2019 11:14:24 AM
Common Firewall Pattern	10344	06/03/2019 11:55:12 AM
Spyware/Grayware Pattern	2.187.00	06/28/2019 06:05:29 AM

3. Select the server you want to unregister and click **Delete** to unregister the original Apex One main server.



Directory Management

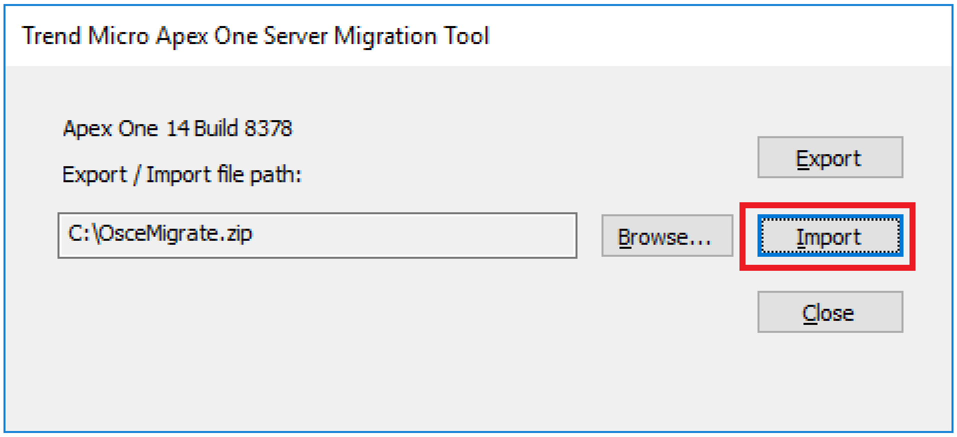
□ Keep the current user access permissions when moving managed products/folders.

WIN-6RMGDFVED71
Local Folder
New Entity
Test
WIN-SERVER2012R_OSCE

Note: Select a product/directory and drag it to the destination folder to move.

Agent Configuration

To restore the configuration, please use the Server Migration Tool located under <Server installation folder>\PCCSRV\Admin\Utility\ServerMigrationTool to import the backup zip file which was generated in the previous chapter.



Trend Micro Apex One Server Migration Tool

Apex One 14 Build 8378

Export / Import file path: C:\OsceMigrate.zip

Setup Privilege

After recovering all configurations, please use **svrsvcsetup.exe** located under <Server installation folder>\PCCSRV\ to setup the privilege of Apex One server. Execute the following command:

```
svrsvcsetup.exe -setprivilege
```

Note: Please run the command if you have set up any folder/file permission on Apex One Main Server.

In the end, please restart **Apex One Master Service** and make sure Apex One server is working properly.

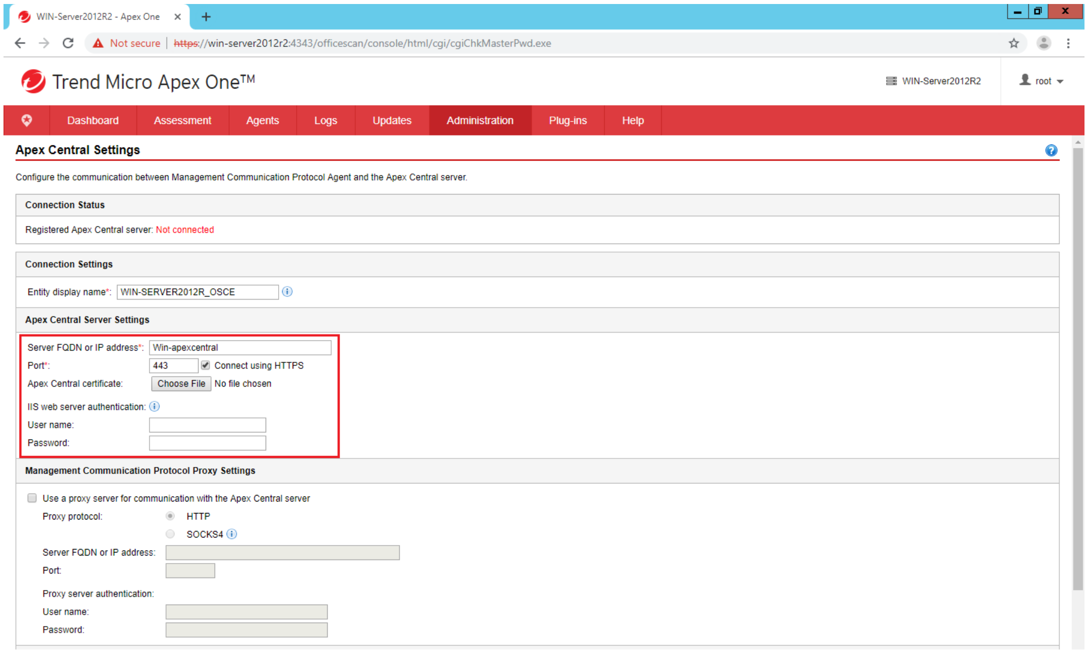
The following services will be started by Apex One Master Service automatically, check the service status after a few minutes:

- Trend Micro Endpoint Sensor Service (if the iES is installed)
- Trend Micro Advanced Threat Assessment Service
- Trend Micro Application Control Service
- Trend Micro Vulnerability Protection

Register to Apex Central

If the Apex One main server has registered to Apex Central, please follow the instructions below to register Apex One server to Apex Central instead:

1. Go to Trend Micro Apex One console > **Administrator** > **Settings** > **Apex Central.**
2. Fill in the information of Apex Central under Apex Central Server Settings.



Apex Central Settings

Configure the communication between Management Communication Protocol Agent and the Apex Central server.

Connection Status

Registered Apex Central server: Not connected

Connection Settings

Entity display name*: WIN-SERVER2012R_OSCE

Apex Central Server Settings

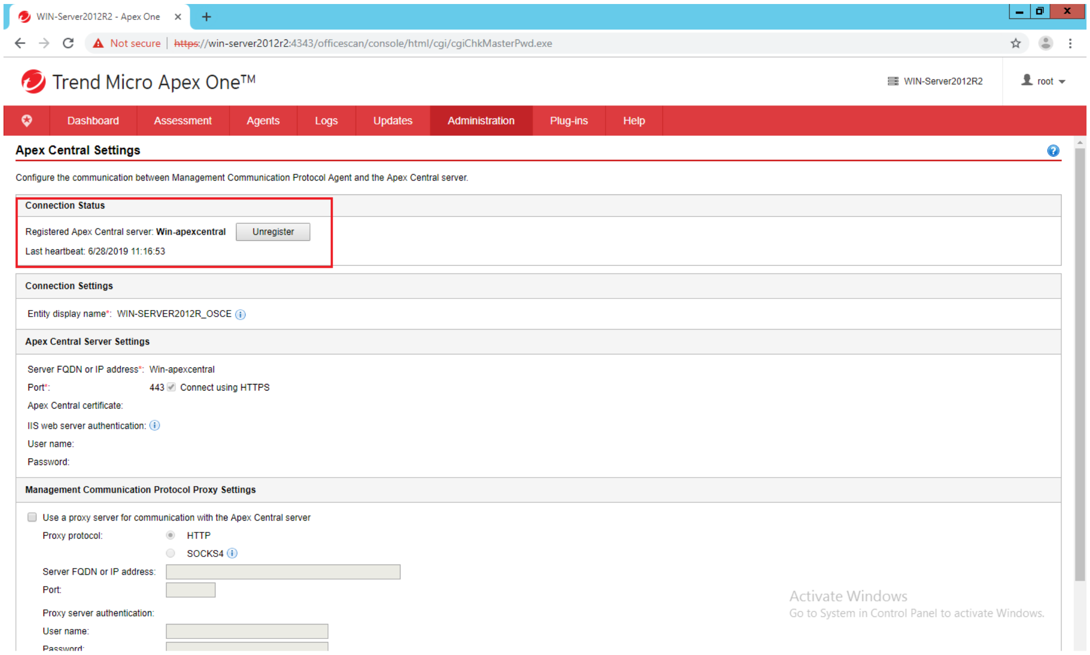
Server FQDN or IP address*: Win-apexcentral
Port*: 443 ☑ Connect using HTTPS
Apex Central certificate: Choose File No file chosen
IIS web server authentication:
User name:
Password:

Management Communication Protocol Proxy Settings

□ Use a proxy server for communication with the Apex Central server
Proxy protocol: ● HTTP ○ SOCKS4
Server FQDN or IP address:
Port:
Proxy server authentication:
User name:
Password:

3. Click **Test Connection** at the bottom to verify the connection between Apex One server and Apex Central to make sure the connection is work.
4. Click **Register** to register to Apex Central.

5. Check the **Connection Status** section and make sure the Apex One server has registered to the Apex Central server.


WIN-Server2012R2 - Apex One
Not secure
https://win-server2012r2:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe
Trend Micro Apex One™
WIN-Server2012R2
root
Dashboard
Assessment
Agents
Logs
Updates
Administration
Plug-ins
Help
Unregister
Activate Windows
Go to System in Control Panel to activate Windows.

Apex Central Settings

Configure the communication between Management Communication Protocol Agent and the Apex Central server.

Connection Status

Registered Apex Central server: **Win-apexcentral**

Last heartbeat: 6/28/2019 11:16:53

Connection Settings

Entity display name*: WIN-SERVER2012R_OSCE

Apex Central Server Settings

Server FQDN or IP address*: Win-apexcentral

Port*: 443 ☑ Connect using HTTPS

Apex Central certificate:

IIS web server authentication:

User name:

Password:

Management Communication Protocol Proxy Settings

☐ Use a proxy server for communication with the Apex Central server

Proxy protocol: ● HTTP ○ SOCKS4

Server FQDN or IP address:

Port:

Proxy server authentication:

User name:

Password:

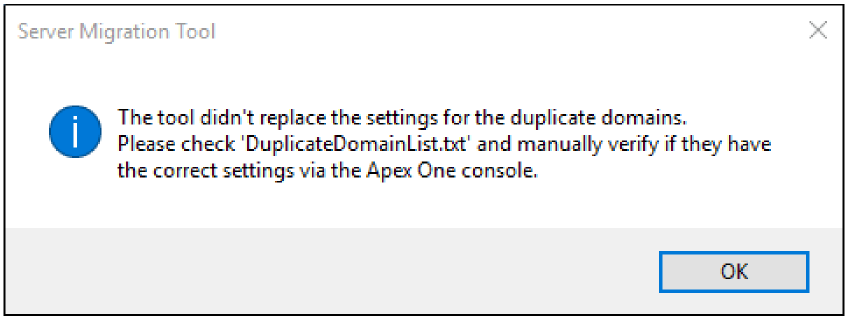
Agent will unload and reload after connecting to the Apex One Backup Server in order to renew some information from the backup server.

Switch Back to the Apex One Main Server

If the main server is back to normal, the agent can be switched from backup server by the same steps.

> Note: As the current spec of Server Migration Tool. A dialogue will pop up when importing the settings to the main server if there is any duplicate domain existing in Agent Management.

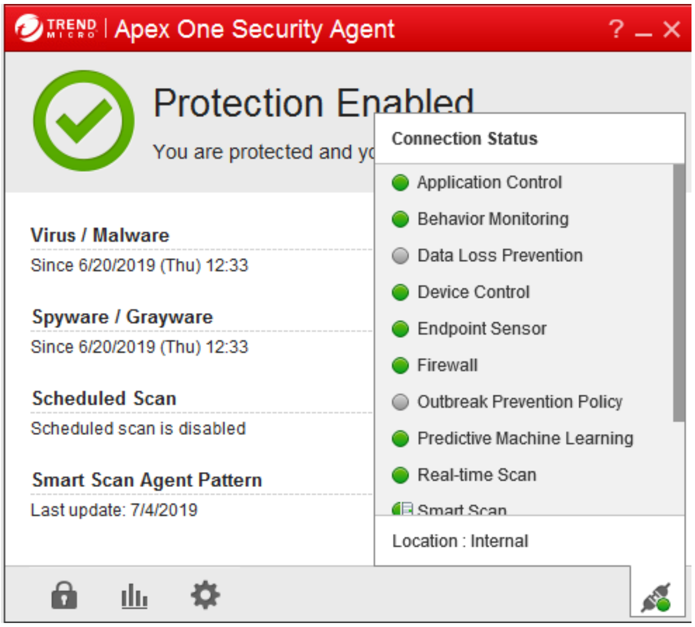
Only the added or new domain will be imported.



The tool didn't replace the settings for the duplicate domains.
Please check 'DuplicateDomainList.txt' and manually verify if they have the correct settings via the Apex One console.

Agent’s protection when Apex One Server is down

When Apex One Server is down, Apex One Agent’s location will show “*External*” which means that it cannot connect to the Apex One server. Even on this condition, Apex One agent still have the following protection features.



Protection Enabled

You are protected and yo

Virus / Malware
Since 6/20/2019 (Thu) 12:33

Spyware / Grayware
Since 6/20/2019 (Thu) 12:33

Scheduled Scan
Scheduled scan is disabled

Smart Scan Agent Pattern
Last update: 7/4/2019

Connection Status

- ● Application Control
- ● Behavior Monitoring
- ○ Data Loss Prevention
- ● Device Control
- ● Endpoint Sensor
- ● Firewall
- ○ Outbreak Prevention Policy
- ● Predictive Machine Learning
- ● Real-time Scan
- Smart Scan

Location : Internal

All Protection features are working even when Apex One Server is down. Please see the table below:

Feature	Functional
Application Control	Yes
Behavior Monitoring	Yes
Data Loss Prevention	Yes
Device Control	Yes
Endpoint Sensor	Yes
Firewall	Yes
Outbreak Prevention	Yes

Predictive Machine Learning	Yes
Real-Time Scan	Yes
Smart Scan	Yes
Suspicious Connection Service	Yes
Vulnerability Protection	Yes
Web Reputation	Yes

Securing Your Connected World

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value- added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our web site at www.trendmicro.com.