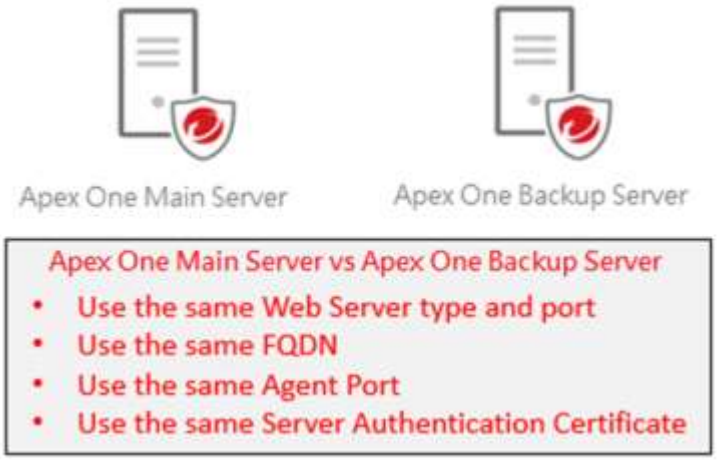
# Trend Micro Apex One™ and iServices

Disaster Recovery Guide

# Table of Contents

# Preparations for Apex One Server Backup

In order to effectively perform this guide, we recommend that you prepare the following setup for the Apex One backup server:



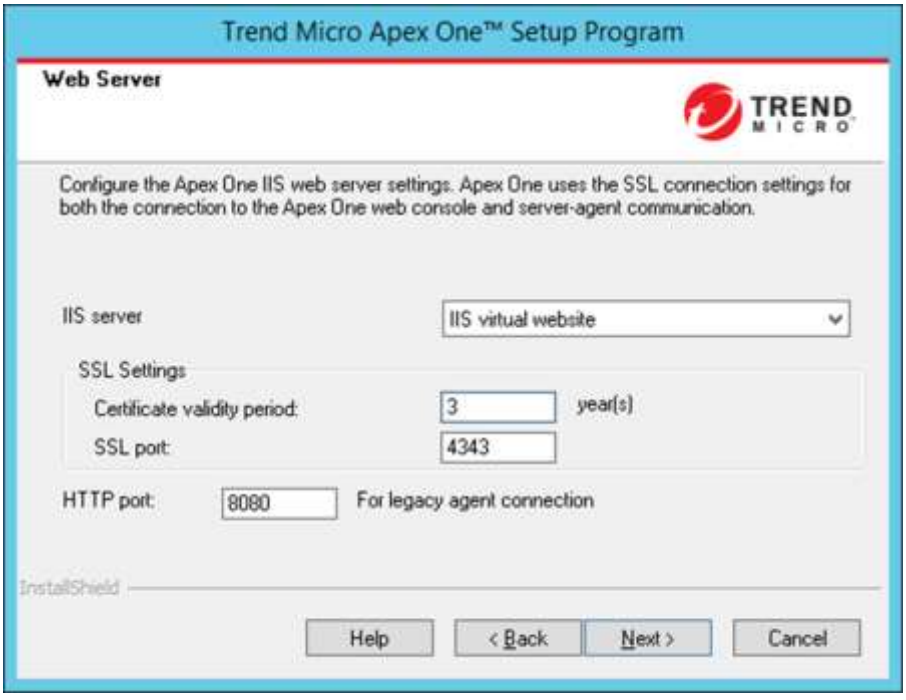

# Apex One Server Setup and Configuration

## Installation

When installing the Apex One backup server, there are steps that you need to check first.

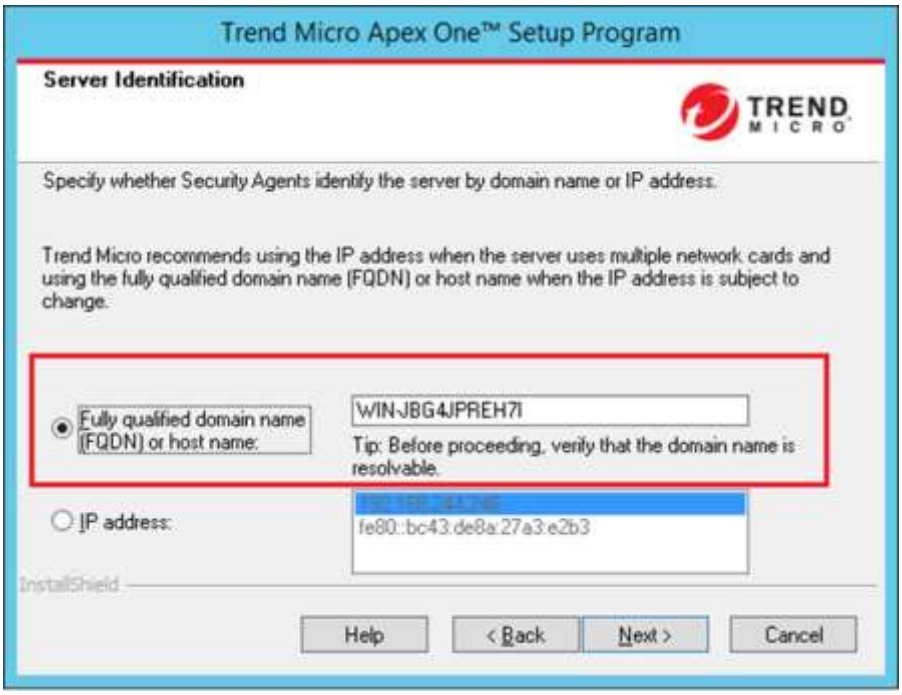
## Web Server

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



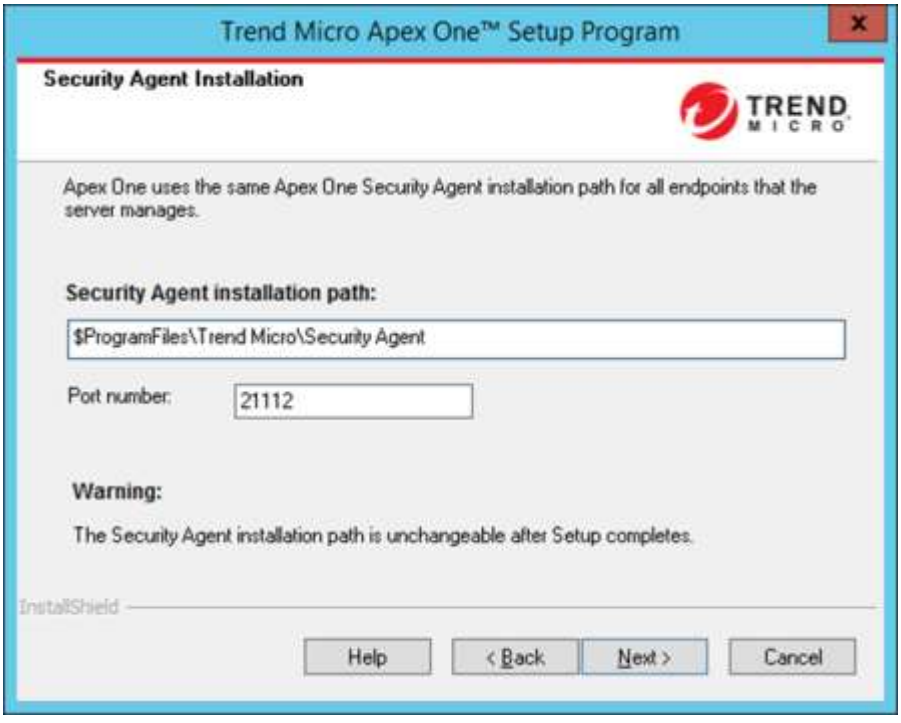
## Server Identification

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




## Agent Port

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

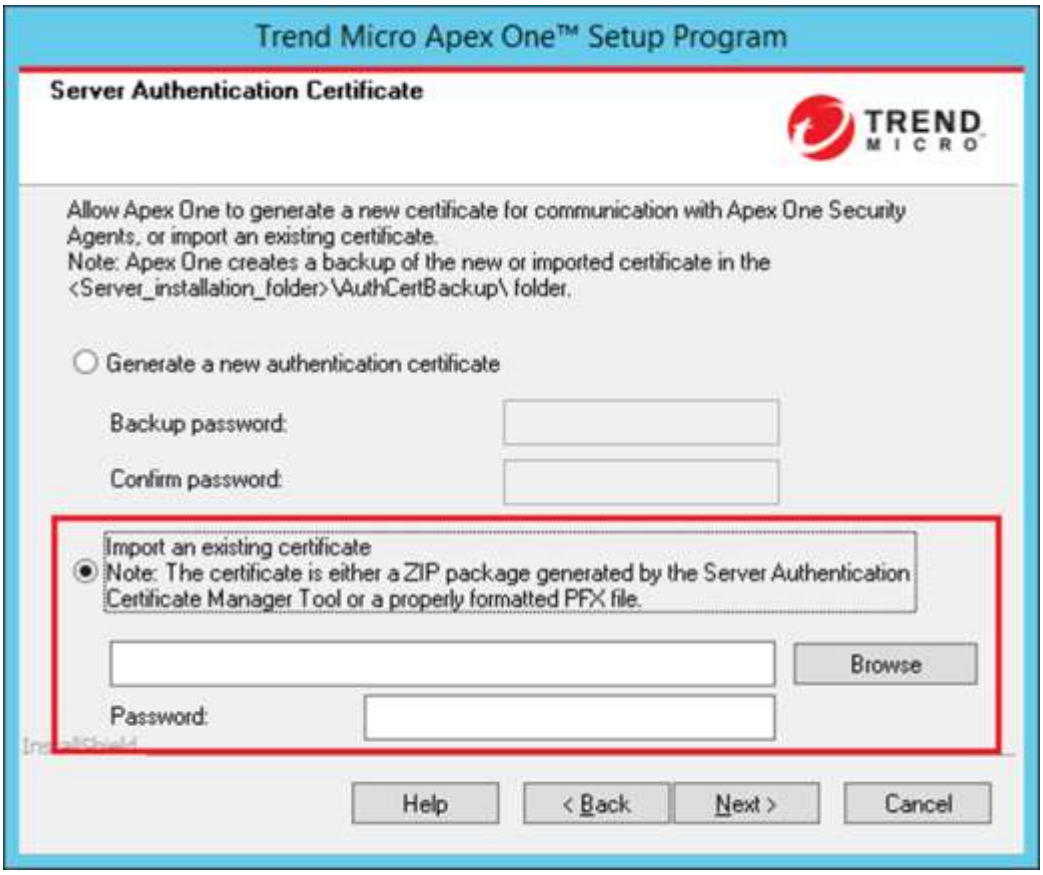


## Self Authentication Certificate

Please use the same Server Authentication Certificate. Select "Import an existing certificate" and use the original certificate file from the default Apex One server. The certificate file of the Apex One server can be found under following path:

<Server installation folder>\AuthCertBackup\OfficeScanAuth.dat

The file is in a ZIP format in Apex One. Please modify the file extension to .zip before importing the certificate.

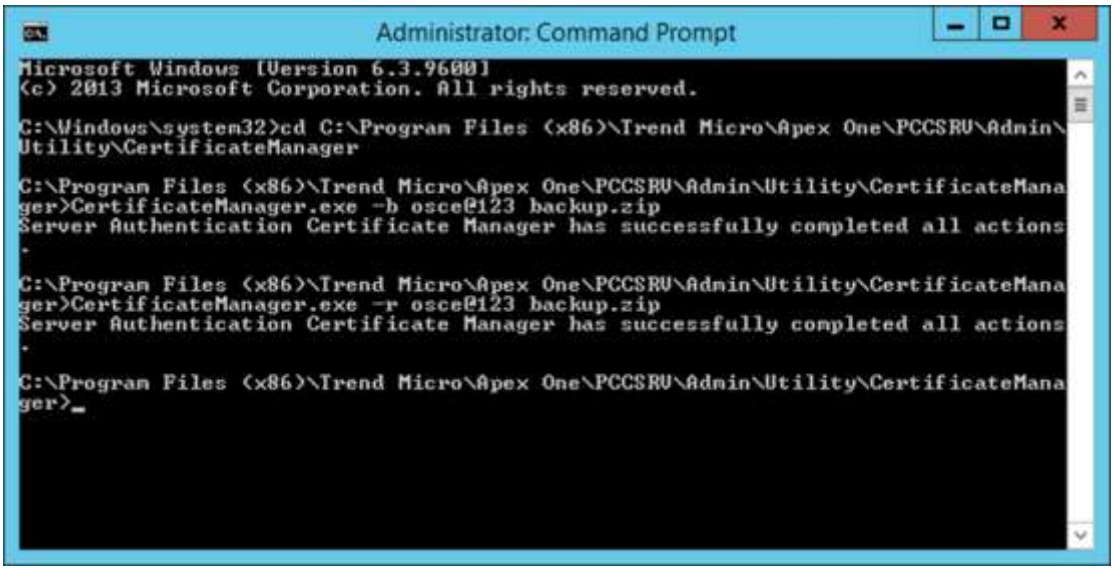



Certificate files can also be backed up by using the CertificateManager tool (under <Server installation folder>\PCCSRV\Admin\Utility\CertificateManager\). Please use the following command to back up the certificate:

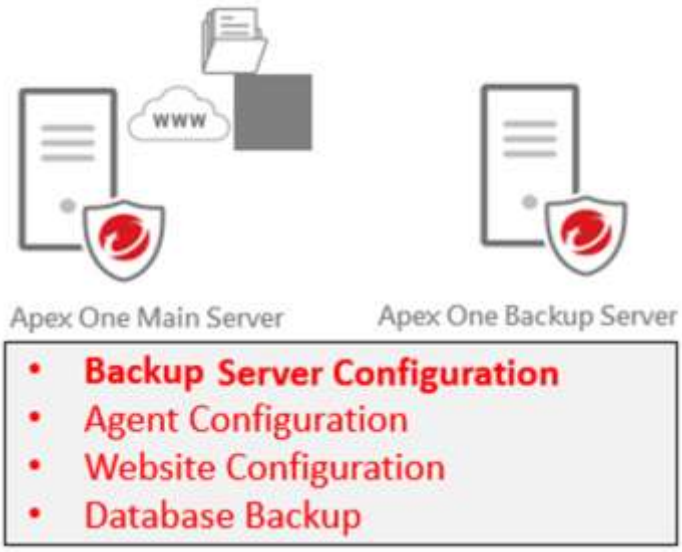
CertificateManager.exe -b [password] backup.zip

To restore the certificate from the backup certificate, please use the following command:

CertificateManager.exe -r [password] backup.zip


Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Progran Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\CertificateManager
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\CertificateManager>CertificateManager.exe -b osce@123 backup.zip
Server Authentication Certificate Manager has successfully completed all actions
.
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\CertificateManager>CertificateManager.exe -r osce@123 backup.zip
Server Authentication Certificate Manager has successfully completed all actions
.
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\CertificateManager>

# Apex One Server Configuration Backup



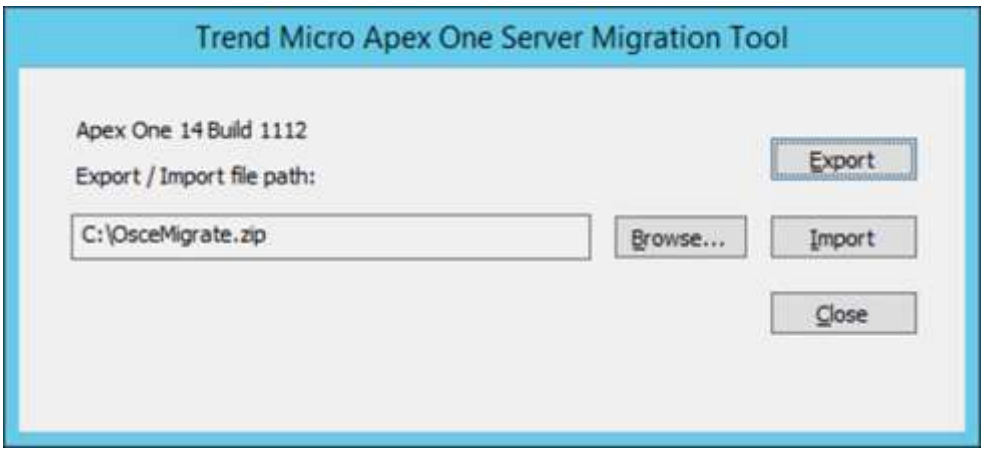

## Agent Configuration Backup

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

- Domain Structures
- The following settings 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
- Apex One Client Port (value of Client_LocalServer_Port in INI_CLIENT_SECTION of ofcscan.ini)

IMPORTANT The tool does not back up the client listings and endpoint setting.




To back up configurations for Global Agent Settings and Smart Protection, please follow the procedures below:

Copy the following files from the original Apex One server to the backup server:

- <Server installation folder>\PCCSRV\ofcscan.ini
- <Server installation folder>\PCCSRV\Private\ofcserver.ini

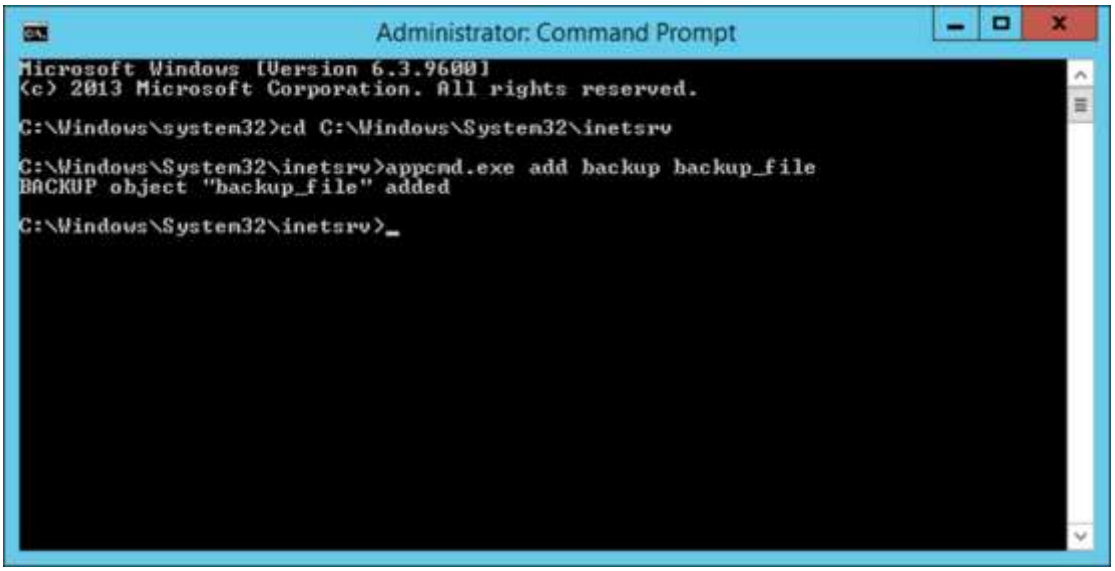
## Website Configuration Backup

Apex One uses IIS 7 or above as its web server. Follow the procedures below to back up the IIS configuration:

1. Open cmd.exe.
2. Navigate to %windir%\system32\inetsrv\.
3. Execute following command to back up the configuration:

   appcmd.exe add backup <backupname>

IIS configuration should be backed up under the %windir%\system32\inetsrv\backup\<backupname> folder.




## Apex One Endpoint Sensor Configuration Backup

To back up the Endpoint Sensor configuration files, copy the following files from the original Apex One server to the backup server:

- <Server installation folder>\iServicesSrv\config.xml

  NOTE 🗎 If the Endpoint Sensor feature was installed in a database instance other than Apex One's.

- <Server installation folder>\iServicesSrv\iATAS\App_Data\ForensicCommandTable.tsv

  NOTE 🗎 If Apex Central is registered to Threat Investigation Center (Managed Detection and Response) and you would like to view previous tasks deployed.

## Apex One Application Control Configuration Backup

To back up the Application Control configuration files, copy the following files from the original Apex One server to the backup server:

- <Server installation folder>\iServicesSrv\iAC\config.xml

> NOTE If the Application Control feature was installed in a different database instance other than Apex One's.

## Apex One Vulnerability Protection Configuration Backup

To back up the following Vulnerability Protection configuration files, copy the following files from the original Apex One server to the backup server:

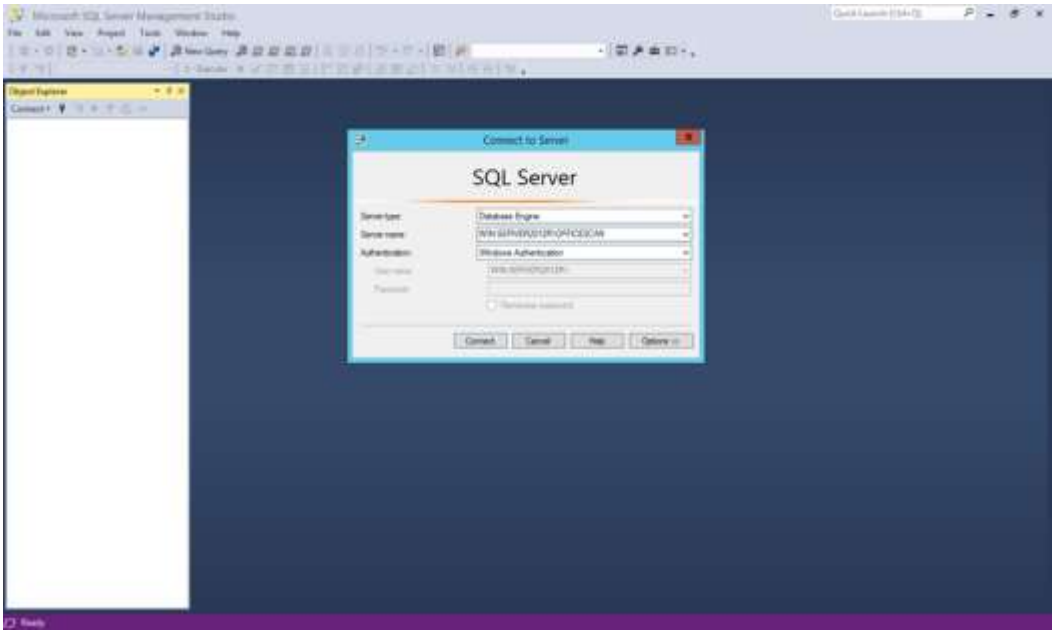
- <Server installation folder>\iServicesSrv\iVP\config.properties
- <Server installation folder>\iServicesSrv\iVP\Web\web.config

## Database Backup

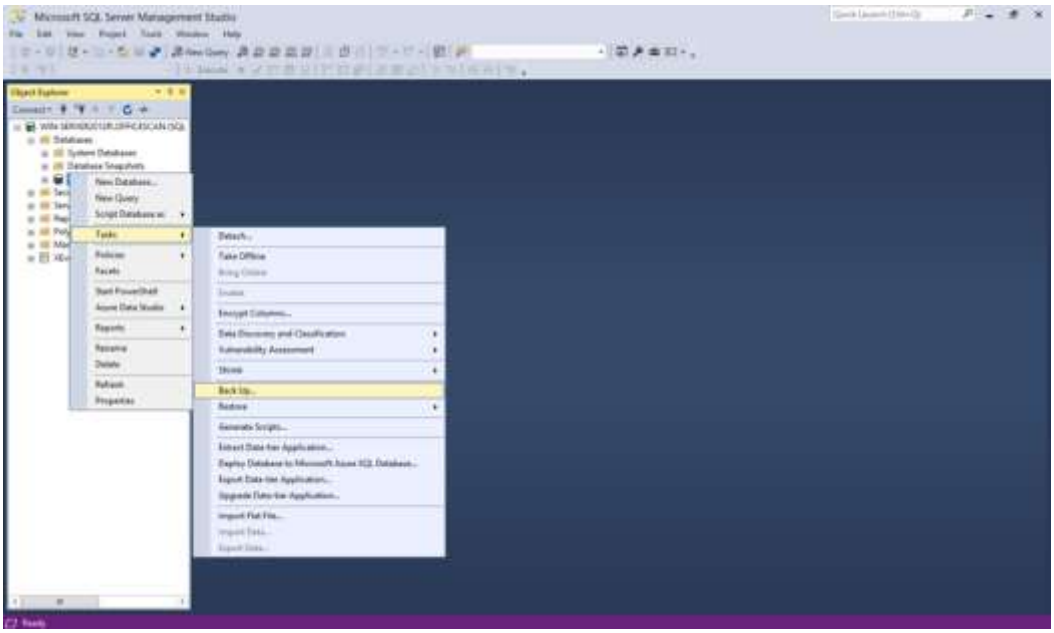
### SQL Server

The Apex One server uses the SQL server as database, so you have to use Microsoft SQL Server Management Studio (SSMS) to back up the database. Please follow the procedures below:

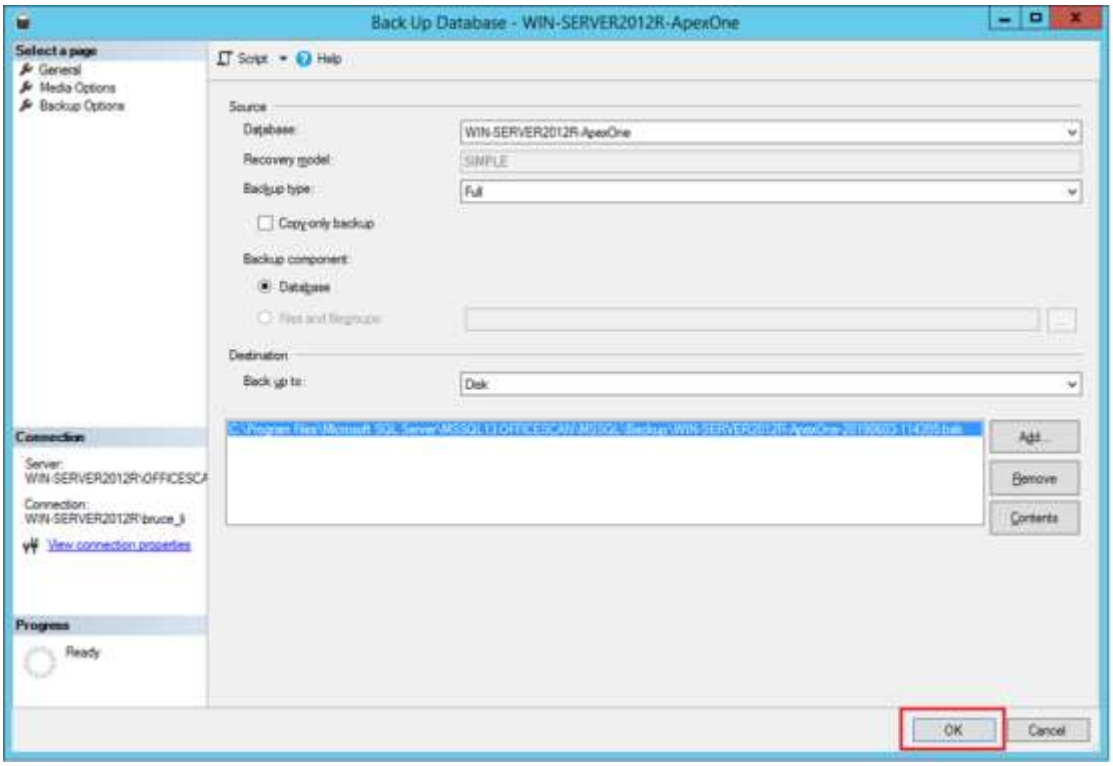
1. Stop the Apex One Master Service and Trend Micro Endpoint Sensor Service.
2. Connect to the SQL Server using SSMS.



3. Right-click the **Apex One database object** and select **Tasks** > **Backup**.



4. Configure the backup settings and click **OK** to start the progress. You may refer to the Microsoft SQL Server documentation to know the recommended settings.




5. Find the database backup in the backup folder that you set in the previous step.

6. Repeat Steps 3 to 5 again to back up Endpoint Sensor's database.
7. Restart the Apex One Master Service and Trend Micro Endpoint Sensor Service.

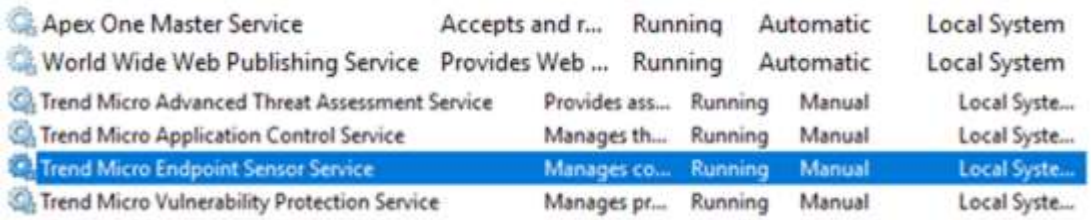
# Apex One Recovery from Backup


Apex One recovery includes Agent Configuration, Website Configuration, and Database recovery. Before recovering the Apex One server, please stop the following services:

- Apex One Master Service
- WWW Publishing Service

The following services should be stopped automatically after Apex One Master Service is stopped:

- Trend Micro Endpoint Service
- Trend Micro Application Control Service
- Trend Micro Advanced Threat Assessment Service
- Trend Micro Vulnerability Protection Service

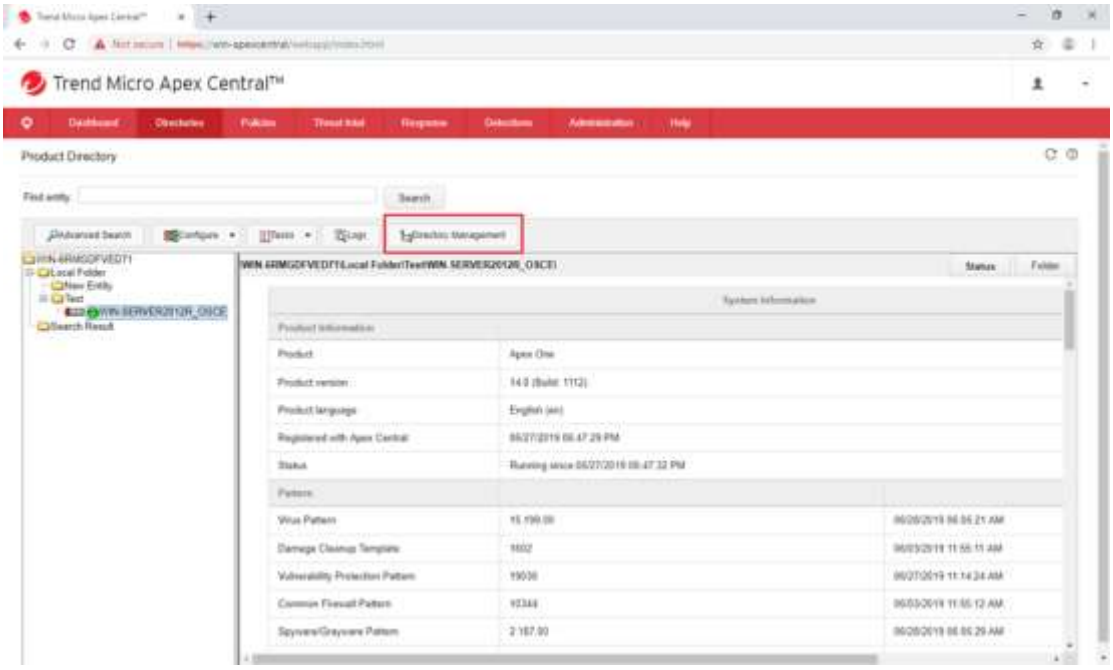



IMPORTANT You can only restore the Apex One server by using the same host name, FQDN, and installation path of the old or corrupted server.

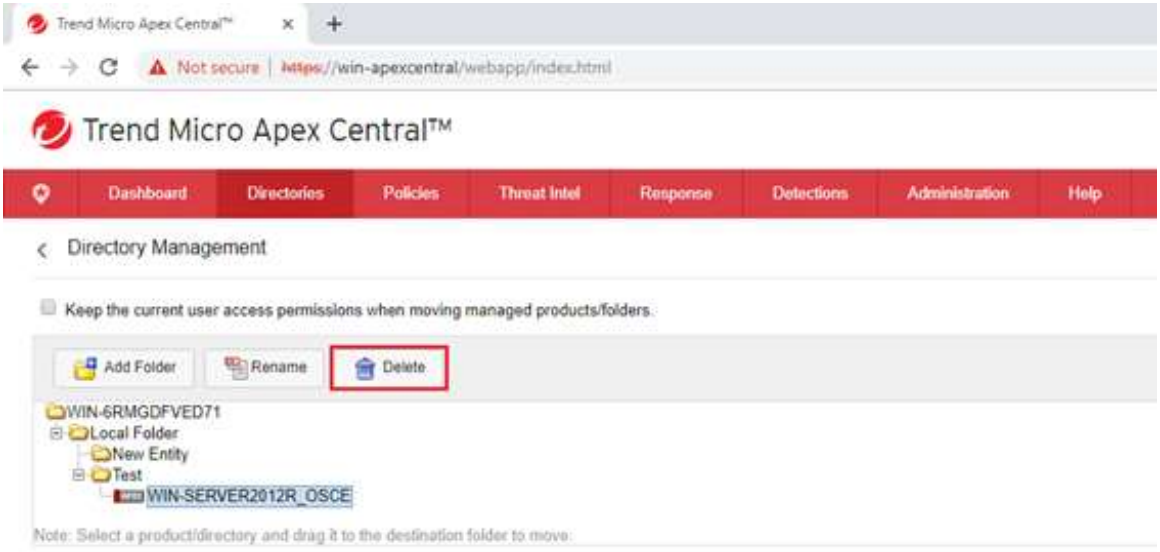
## Unregister from Apex Central

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 the **Apex Central console** > **Directories** > **Products**.
2. Click **Directory Management**.

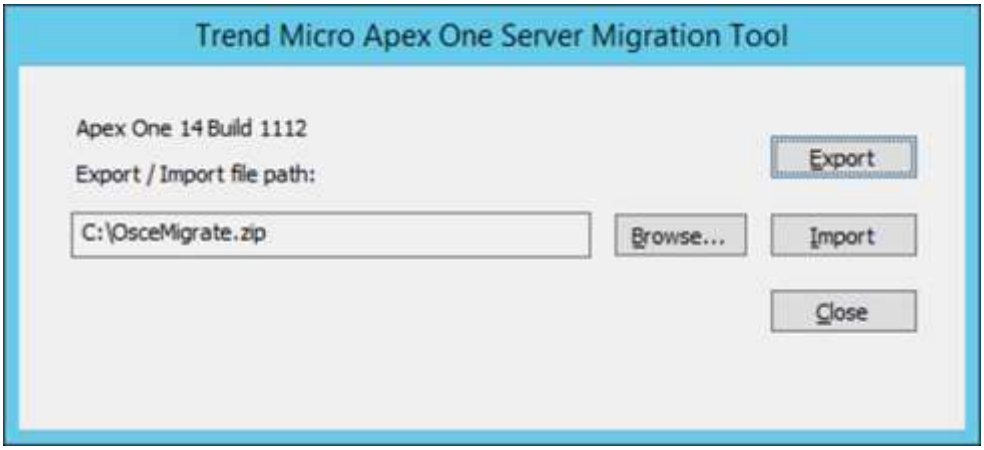



3. Select the server that you want to unregister and click **Delete** to unregister the original Apex One main server.



## Agent Configuration

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




For Global Agent Settings and Smart Protection, please replace following files with the backup files:

- <Server installation folder>\PCCSRV\ofcscan.ini
- <Server installation folder>\PCCSRV\Private\ofcserver.ini

## Website Configuration

To restore IIS configuration on the backup server, please follow the procedures below:

1. Copy the backup folder to the %windir%\system32\inetsrv\backup directory.
2. Go to the %windir%\system32\inetsrv\History directory.
3. Copy MetaBase_xxx_0000000000.xml and rename it to "MetaBase.xml".
4. Replace the above MetaBase.xml in the %windir%\system32\inetsrv\backup\<backupname> folder.
5. Execute the following command to restore the configuration:

   appcmd.exe restore backup <backupname>


6. Go to the %windir%\system32\inetsrv\config directory.
7. Open applicationHost.config by editor.
8. Make sure that there is no username and password in all anonymousAuthentication settings.

   For example:

   - No username and password:

     <anonymousAuthentication enabled="true"/>

   - With username and password:

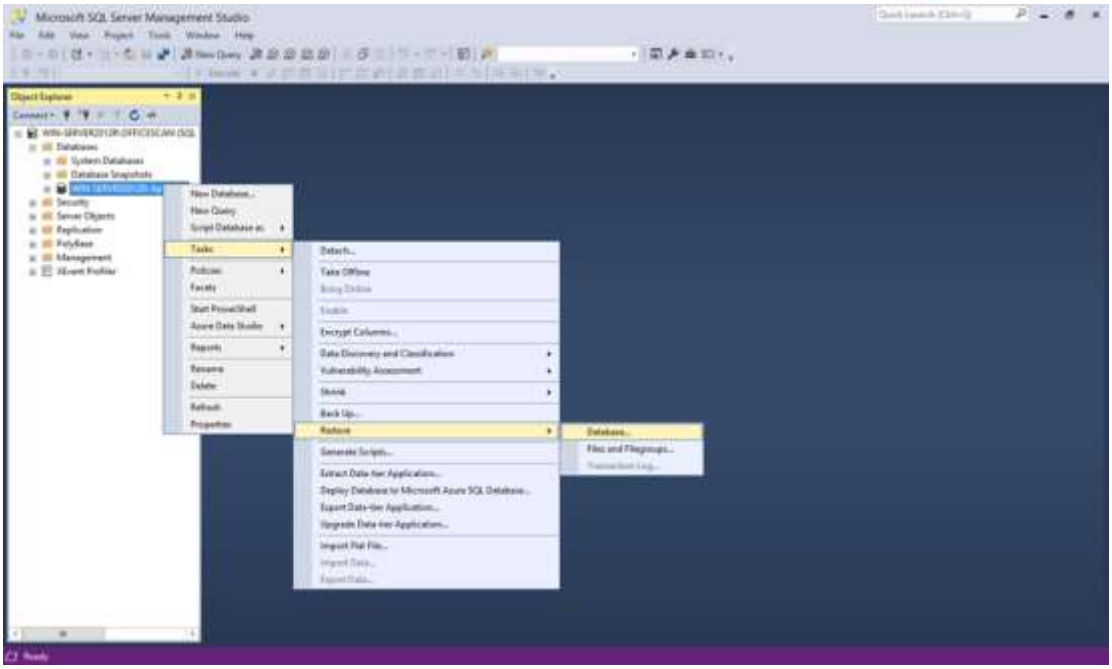
     <anonymousAuthentication enabled="true" userName="TestAccount" password="[enc:AesProvider:rTdmSub0OmMLAA5by46MWEl6CFKMwHNX5ogGe11jj74=:enc]" />

## Database Recovery

### SQL Server

To restore the SQL server database, please follow the procedures below:

1. Connect to the SQL Server using the Microsoft SQL Server Management Studio Tool.
2. Right-click on the **Apex One and Apex One Endpoint Sensor database object** and select "Tasks".
3. Click **Restore** > **Database**.



4. Configure the restoration settings:
    a. Select "Device" as the source.
    b. Choose the backup file as the source file.
    c. Select the source database.
    d. In the Backup Sets to Restore section, select the backup set from your backup file.
    e. Click **OK** to start the process.

## Apex One Endpoint Sensor Database Recovery

To restore the Endpoint Sensor settings (if it was installed in a separate DB instance), please replace following files with the backup file:

<Server installation folder>\iServicesSrv\iES\config.xml

## Setup Privilege

After recovering all configurations and database, please use svrsvcsetup.exe (under <Server installation folder>\PCCSRV\) to set up the privilege of the Apex One server. Execute the following command:

svrsvcsetup.exe -setprivilege

In the end, please start Apex One Master Service and WWW Publishing Service and make sure that the Apex One server is working properly

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

- Trend Micro Endpoint Sensor Service
- Trend Micro Application Control Service
- Trend Micro Advanced Threat Assessment Service
- Trend Micro Vulnerability Protection Service

## Apex One Endpoint Sensor Settings

To ensure Endpoint Sensor Advanced Threat Assessment Service is enabled successfully on the backup server, if Apex Central is registered to Threat Investigation Center (Managed Detection and Response):

1. Deploy the Endpoint Sensor Activation Code from Apex Central.
2. Unregister and/or register it back from the Managed Detection and Response page.
3. To view previous tasks from the Threat Investigation Center, replace <Server installation folder>\iServicesSrv\iATAS\App_Data\ForensicCommandTable.tsv in the backup server.
4. Restart the Trend Micro Advanced Threat Assessment Service.

## Apex One Application Control Setting

To restore the Application Control settings (if database was installed in a separate DB instance other than Apex One's), please replace following file with the backup file and restart Trend Micro Application Control Service:

<Server installation folder>\iServicesSrv\iAC\config.xml.

## Apex One Vulnerability Protection Settings

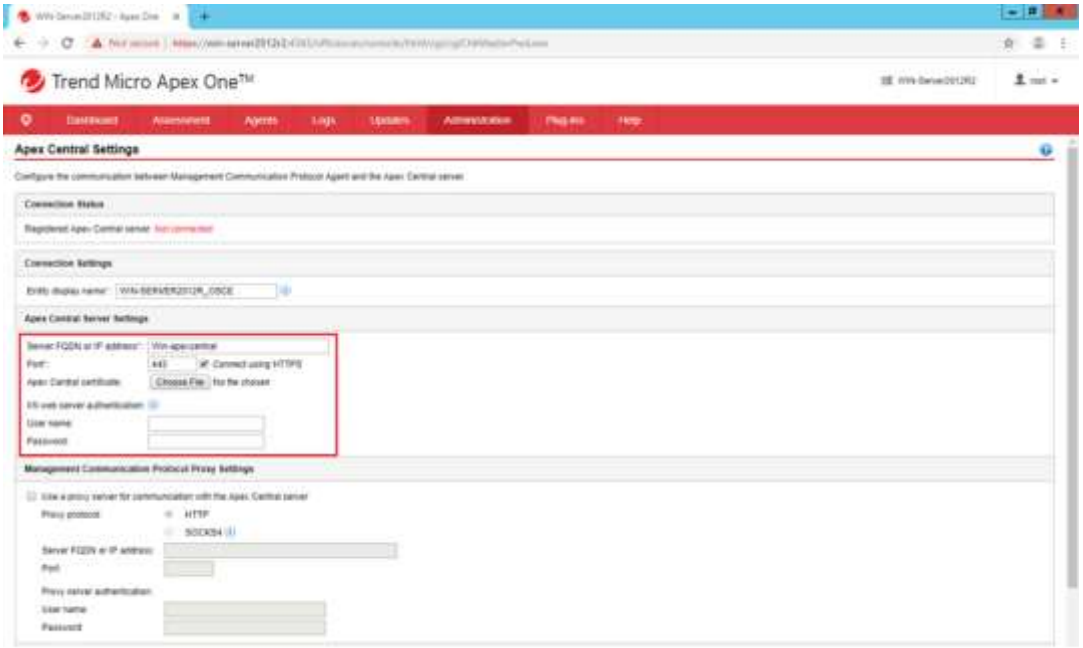
If Trend Micro Vulnerability Protection Service cannot start normally, follow the procedure below:

1. Replace the following with the backup files.
   - <Server installation folder>\iServicesSrv\iVP\config.properties
   - <Server installation folder>\iServicesSrv\iVP\Web\web.config
2. Restart the Trend Micro Vulnerability Protection Service.

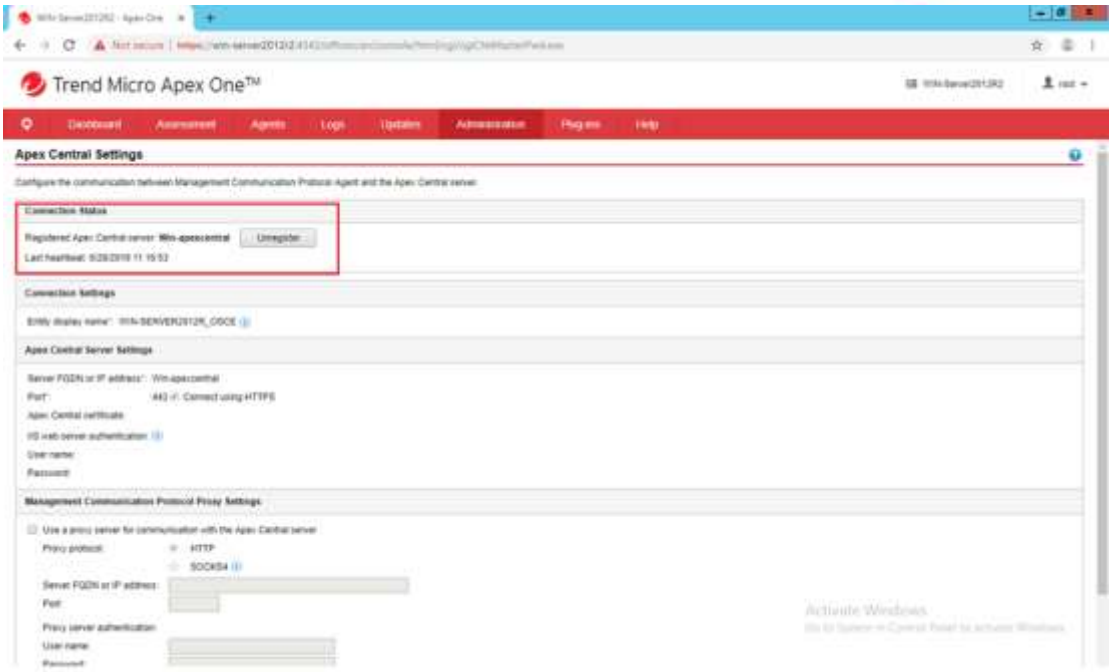
## Register to Apex Central

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

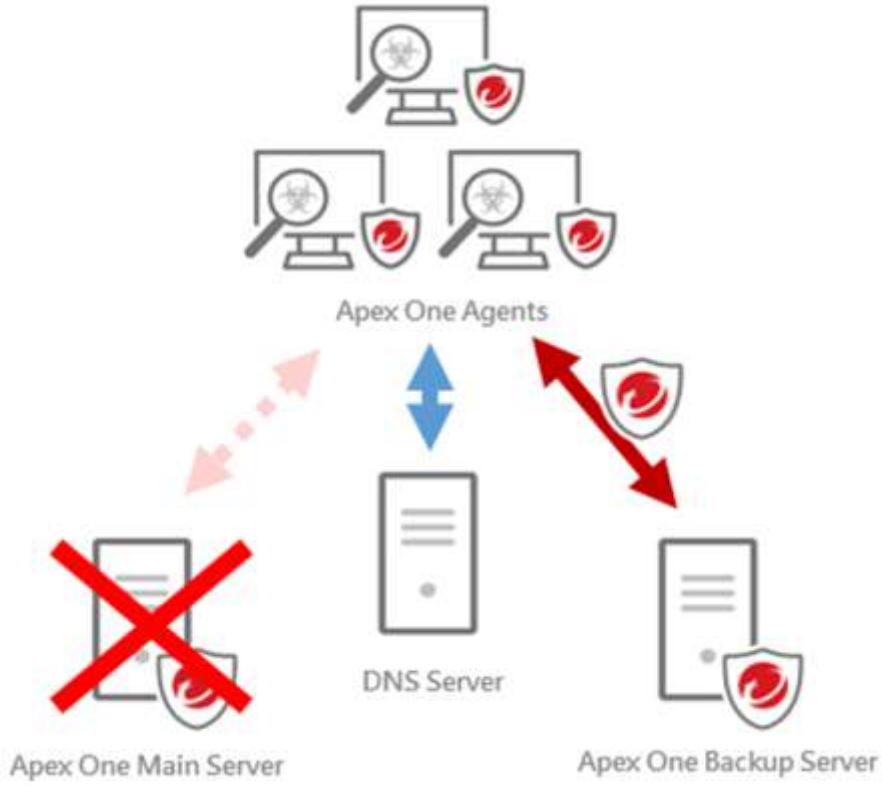
1. Go to the **Trend Micro Apex One console** > **Administrator** > **Settings** > **Apex Central**.
2. Fill in the information of Apex Central under the Apex Central Server Settings.




3. Click **Test Connection** at the bottom to verify the connection between the Apex One server and Apex Central to make sure that the connection works.
4. Click **Register** to register to Apex Central
5. Check the Connection Status section as shown in the following image to make sure the Apex One server has registered to the Apex Central server.


Trend Micro Apex One™
Dashboard
Assessment
Agents
Logs
Updates
Administration
Plug-ins
Help
Apex Central Settings
Configure the communication between Management Communication Protocol Agent and the Apex Central server.
Connection Status
Unregister
Connection Settings
Apex Central Server Settings
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:
Activate Windows

# Offsite Backup Consideration




## DNS

Since both the main Apex One server and Apex One backup server have to use the same FQDN, please make sure all agents are available to connect to the correct Apex One server by switching the DNS setting properly.

# Agent Protection When Apex One Server is Down

When the Apex One Server is down, the Apex One agent's location will display "External". This means that it cannot connect to the Apex One server. Even in this condition, the Apex One agent still has the following protection features:


All Protection features work even when the 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 |

| Feature | Functional |
|---|---|
| Real-Time Scan | Yes |
| Smart Scan | Yes |
| Suspicious Connection Service | Yes |
| Vulnerability Protection | Yes |
| Web Reputation | Yes |

Table 1: Protection Features