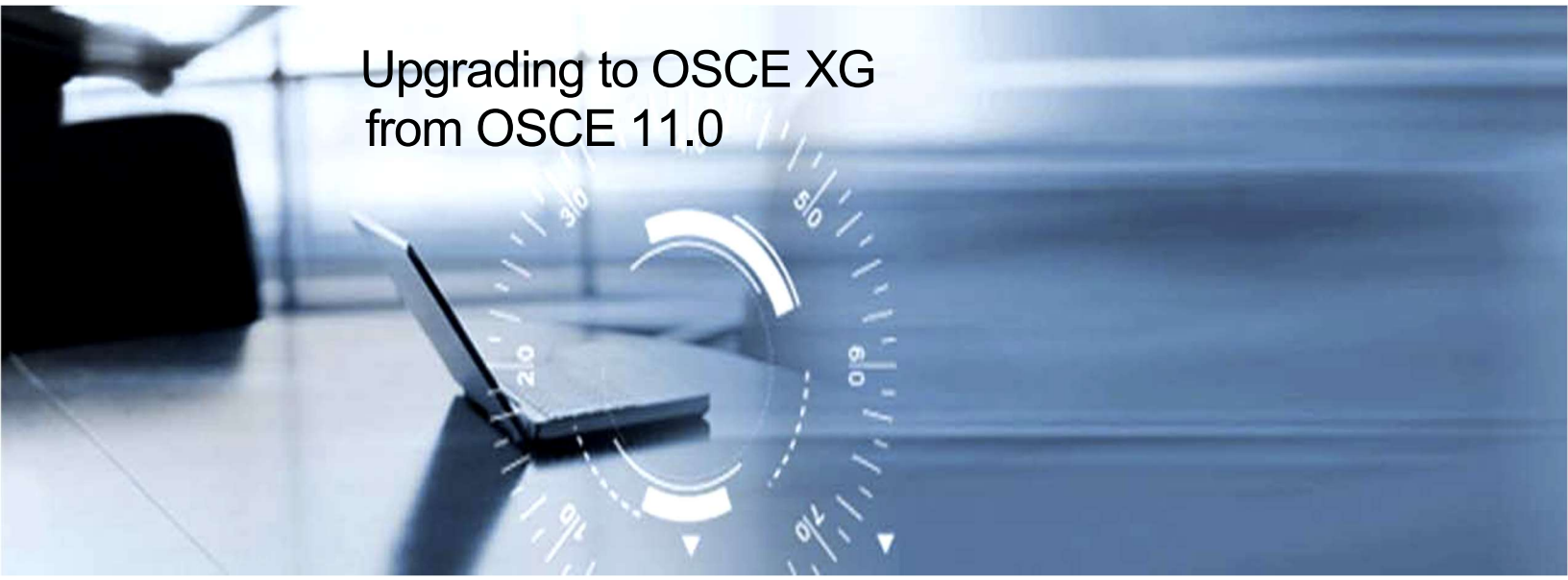
Trend Micro™ OfficeScan (OSCE) XG



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

Released: 8 February 2017

Contents

Chapter 1: Introduction 5
1.1 > Upgrade Purpose 6
1.2 > What's New 6
1.3 > System Requirements 8
1.4 > Hot Fix Deployment 8
1.5 > Upgrade Considerations 9

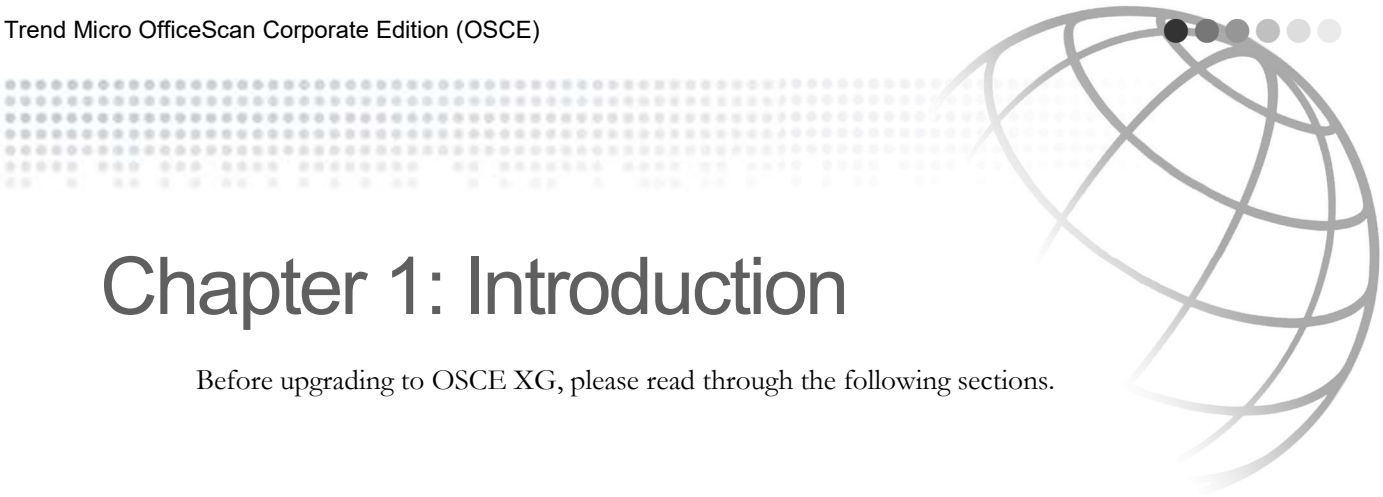
Chapter 2: Upgrade Scenarios 15
2.1 > Upgrading the server directly 16
2.2 > Migrating to a new OSCE XG server 16
2.3 > Migrating to a new OSCE 11.0 server before upgrading to OSCE XG 17
2.4 > Replacing an OSCE 11.0 server with a new OSCE XG server 19
2.5 > Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG 20

Chapter 3: Upgrade Processes 22
3.1 > Upgrading the server directly 23
3.2 > Migrating to a new OSCE XG server 40
3.3 > Migrating to a new OSCE 11.0 server before upgrading to OSCE XG 41
3.4 > Replacing an OSCE 11.0 server with a new OSCE XG server 43
3.5 > Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG 43

Chapter 4: Upgrade Verification 45
4.1 > Verifying if the OSCE server was upgraded properly 45
4.2 > Upgrading OSCE agents 46
4.3 > Verifying if the OSCE XG agent was properly upgraded 47

Chapter 5: Plug-in Service Migration 48

Chapter 6: Known Issue 50



Chapter 1: Introduction

Before upgrading to OSCE XG, please read through the following sections.

1.1 > Upgrade Purpose

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

1.2 > What's New

OfficeScan XG includes the following new features and enhancements:

Ransomware Protection enhancements

Your protection against ransomware attacks has been further enhanced to allow OSCE agents to recover files encrypted by ransomware threats, block processes associated with ransomware, and prevent compromised executable files from infecting your network.

Newly Encountered Program protection enhancement

To more easily maximize your ransomware protection security policy on individual agents, the newly encountered program detection feature has been moved to the Behavior Monitoring settings screen.

You can also customize the message that displays on agent endpoints after a user downloads and executes a newly encountered program.

Predictive Machine Learning

The Predictive Machine Learning engine can protect your network from new, previously unidentified, or unknown threats through advanced file feature analysis and heuristic process monitoring. Predictive Machine Learning can ascertain the probability that a threat exists in a file or process and the probable threat type, protecting you from zero-day attacks.

OfficeScan Edge Relay Server

The OSCE Edge Relay server provides you greater visibility and increased protection for endpoints that leave the local intranet by providing the following features:

- Suspicious Object list synchronization
- Sample submission
- Log submission
- Agent status information submission, such as current pattern and component versions

Suspicious File Sample Submission

To further enhance your integration with a Deep Discovery Virtual Analyzer, OSCE agents can now detect and send suspicious files that may contain previously unknown threats directly to the Virtual Analyzer for further analysis. After verifying that a threat exists, the Suspicious Object

lists are immediately updated and synchronized to all agents, preventing the threat from spreading across your network.

Dashboard UI enhancements

The Dashboard has been redesigned to provide better visibility of your network's protection status.

Control Manager integration enhancements

To prevent unauthorized communication between the Control Manager and OSCE servers, registration to the Control Manager server requires certificate authentication and policy management through the Control Manager server is managed using public-key encryption.

Anti-exploit protection

Real-time Scan allows you to detect and block threats using Common Vulnerabilities and Exposures (CVE) exploits.

Behavior Monitoring can also detect abnormal program behavior that is common to exploit attacks.

Suspicious Connections enhancement

You can now configure the Suspicious Connections feature to log or block network connections detected by the Global C&C IP list and malware network fingerprinting.

Firewall enhancements

The application filter of the OfficeScan Firewall now supports Windows 8 and later platforms.

You can grant OSCE agent users the privilege of configuring the firewall security level and exceptions list.

Independent mode

The previously named Roaming mode has been renamed as Independent mode.

Platform and browser support

This version of OSCE provides support for the following:

- Microsoft™ Windows™ Server 2016

This version of OSCE discontinues support of the Apache Web Server.

NOTE 🗎 Officially, the newest version of OSCE is named “OSCE XG”. Originally, it was “OSCE 12.0” and is still referred to as such.

1.3 > System Requirements

Refer to the following document to read the system requirements:

http://docs.trendmicro.com/all/ent/officescan/v12.0/en-us/osce_12.0_req.pdf

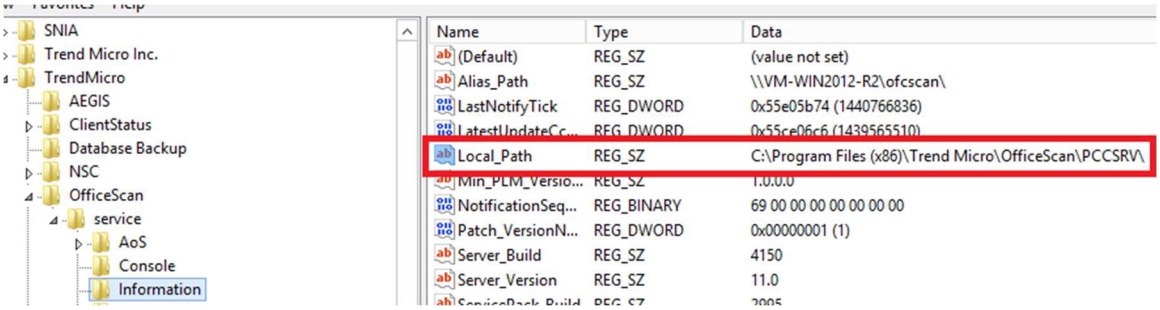
1.4 > Hot Fix Deployment

The following article contains a list of hot fixes included in OSCE XG:

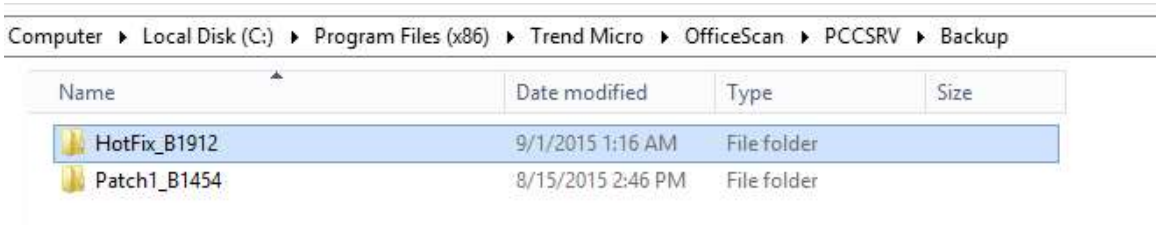
https://success.trendmicro.com/solution/1114882

We recommend that you check the current OSCE server's installed hotfix(es):

1. Log in to the OSCE server.
2. Open the registry and navigate to:
   a. For x86 platform:
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\Information@ Local_Path
   b. For x64 platform:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan\service\Information@ Local_Path
3. Get the value of "Local_Path" to find out where the OSCE server is installed, then navigate to the directory.



4. Go to the Backup folder and check the folders' names. For example:



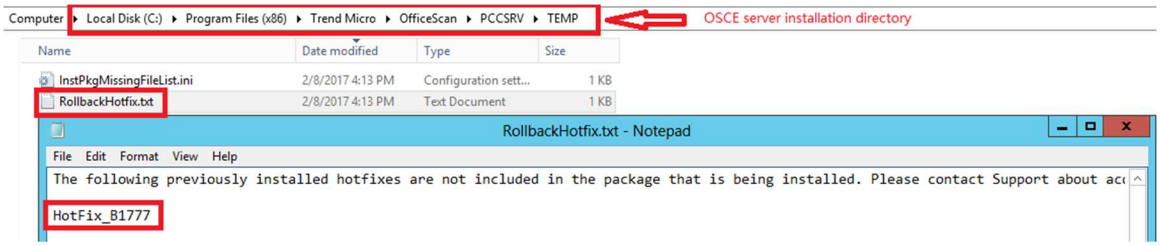
In this example, the OSCE server has only one hot fix installed: Hot Fix Build 1912.

5. Check "1912" in the link provided above:
   - If the hot fix is included in the list, then you can proceed because this means OSCE XG also has it.
   - If the hot fix is not included in the list, then contact Trend Micro Technical Support to help you apply the hot fix for XG before the upgrade.

It is suggested to check if there are any hot fixes missing after upgrading to OSCE XG:

1. Log in to the OSCE server.
2. Navigate to the OSCE server's installation directory.
3. Go to the TEMP folder and open RollbackHotfix.txt if it exists.
4. Check the file to see if there are any hot fixes missing after the upgrade.

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.



In this example, Hot Fix Build 1777 is missing.

5. If there are any missing hot fixes, please contact Trend Micro Technical Support so that they can apply the corresponding hot fix for the OSCE XG version if required. Deploy the hot fix after getting it from Trend Micro.

1.5 > Upgrade Considerations

Upgrade path

The following versions can be upgraded to OSCE XG:

- OSCE 10.6 SP3
- OSCE 11.0 or higher

NOTE 🗎 This document focuses on upgrading to OSCE XG from OSCE 11.0 or a higher version. For more detailed information, please refer to the OSCE XG installation guide (Page 18): http://docs.trendmicro.com/all/ent/officescan/v12.0/en-us/osce_12.0_iug.pdf.

Considerations

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. Log in to 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. Check if the "Update the OfficeScan firewall driver only after a system restart" option is enabled or not. We suggest that you enable it.

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, we suggest that you enable it.

To enable the option:

1. Log in to the OSCE web management console.
2. Navigate to **Agents** > **Global Agent Settings**.
3. Go to the Agent Control tag of the Alert Settings section.
4. Check if the "Display a notification message if the endpoint needs to restart to load a kernel mode driver" option is enabled or not.

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.
- Remote installation/upgrade will fail if the OSCE server's web server is using Apache. Please refer to Figure 1.4

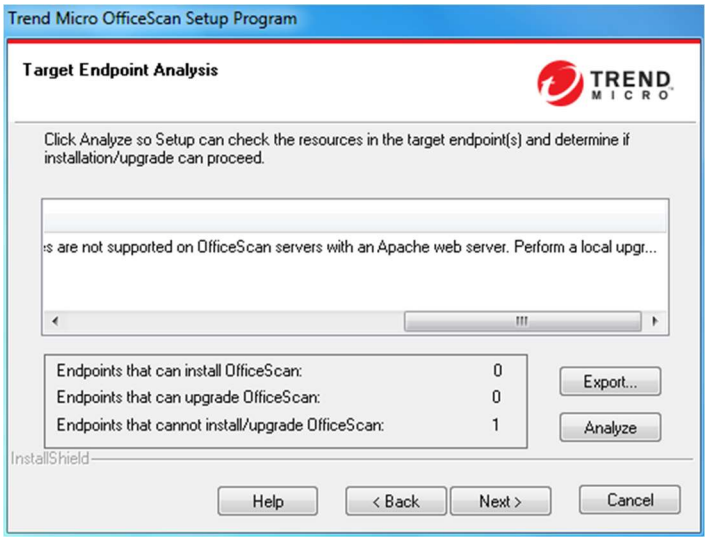


Figure 1.4: Request to perform local upgrade

- OSCE has a feature that verifies its own files by using the information that the digital signature of your OS has. A problem occurs when an invalid digital signature is found. The following messages may appear:
  - *This file was blocked because it does not have a valid digital signature that verifies its publisher.*
  - *An error occurred in copying <filename>.*
  - *At least one of downloaded files has invalid digital signature.*

  Please check the following article for more information:
  https://success.trendmicro.com/solution/1058226

Compatibility

- XG now supports Windows Server 2016
- XG supports Chrome when logging in to the web console
- XG no longer supports installation or upgrade of an OSCE server on Windows Server 2003 because OSCE XG uses PHP 7.0. Windows Server 2003 does not support PHP 7.0. Additionally, Windows Server 2003 already reached End-Of-Support (EOS) according to Microsoft (MS).
- XG web console no longer supports Internet Explorer (IE) 8, 9, and 10. It only supports IE 11 and Chrome.

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

Update Component Setting

If the "OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes" setting is enabled, agents are able to update components but not upgrade the agent program even though the OSCE server has been upgraded.

If the setting is disabled, the OSCE sever will immediately start deploying the upgraded program to the managed agents after upgrading.

Enabling or disabling the setting depends on the managed agent volume, server resources, and the bandwidth. Enable it if necessary.

To avoid bandwidth or OSCE server overload, Trend Micro recommends enabling the setting.

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.

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

Conventional mode:

x86 platform: 194MB

x64 platform: 233MB

Smart scan mode:

x86 platform: 152MB

x64 platform: 188MB

To enable the setting:

1. Log in to the web management console of the OSCE server.
2. Go to **Agents** > **Agent Management**.
3. Click the root domain (OSCE server).
4. Click **Settings** > **Privileges and Other Settings**.
5. In the Update Settings category under the Other Settings tab, enable the following option:

   "OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes"
6. Click **Apply to All Agents**.
7. Click **Close**.

Apache

OSCE XG no longer supports Apache Web Servers. When upgrading an OSCE server that uses Apache as a web server, the upgrade will automatically uninstall Apache and replace it with IIS.

Below is the web server upgrade process flow:

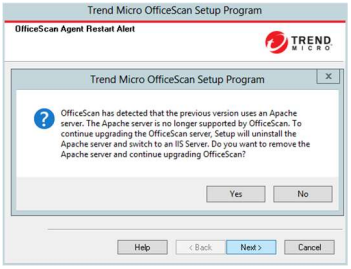
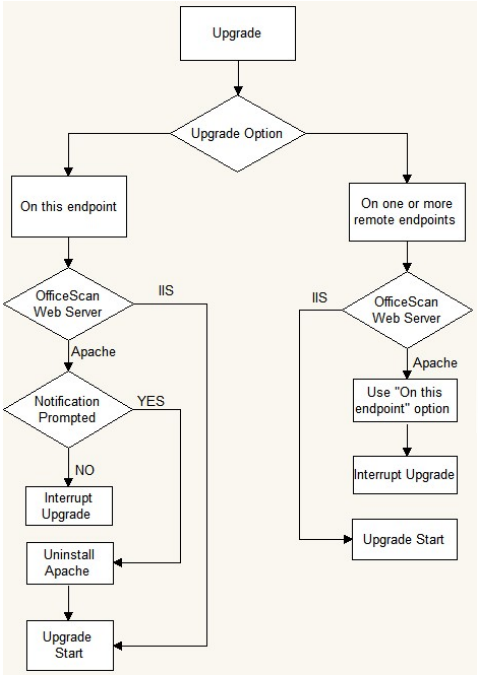


Figure 1.1: Notification prompt



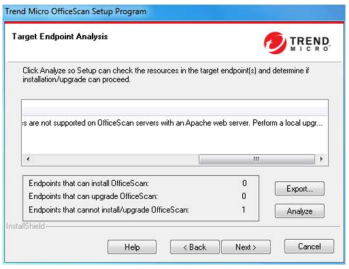


Figure 1.2: Remote installation failure

During the upgrade, setup will check whether the server is using IIS or Apache:

- If the OSCE server is using IIS, the default upgrade process will proceed.
- If the OSCE server is using Apache:
  - "On this endpoint" option: A prompted notification will either ask the administrator to continue the upgrade by removing Apache, or interrupt the upgrade. Please refer to Figure 1.1.
  - "On one or more remote endpoints" option: The upgrade process will tell the administrator to use "On this endpoint" method to upgrade. Please refer to Figure 1.2

Intrusion Defense Firewall (IDF)

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

During an upgrade to OSCE XG:

- If the IDF Plug-in Service is not installed on the OSCE server, there will still be an "Intrusion Defense Firewall" item on the Plug-in Manager page. However, you will not be able to install IDF because the installer has been removed from the Trend Micro Global ActiveUpdate server.
- If the IDF Plug-in Service is already installed, the plug-in service will not be affected and you will still be able to use it after the upgrade.

Control Manager (TMCM)

Upgrade TMCM to version 6.0 Service Pack 3 (SP3) before registering an OSCE XG server.

To prevent unauthorized communication between TMCM and OSCE servers, you must unregister the TMCM server from the OSCE web management console and re-register the connection to allow certification authorization to take effect after the upgrade. Below are the steps:

- On the TMCM server, obtain the certificate file from the TMCM server from <TMCM Installation folder>\Certificate\CA\TMCM_CA_Cert.pem>.
- On the OSCE server, import the TMCM server certificate. In the OSCE web management console, navigate to **Administration** > **Settings** > **Control Manager** and then click **Browse**. Locate the certificate that you copied from the TMCM server. (Figure 1.3)

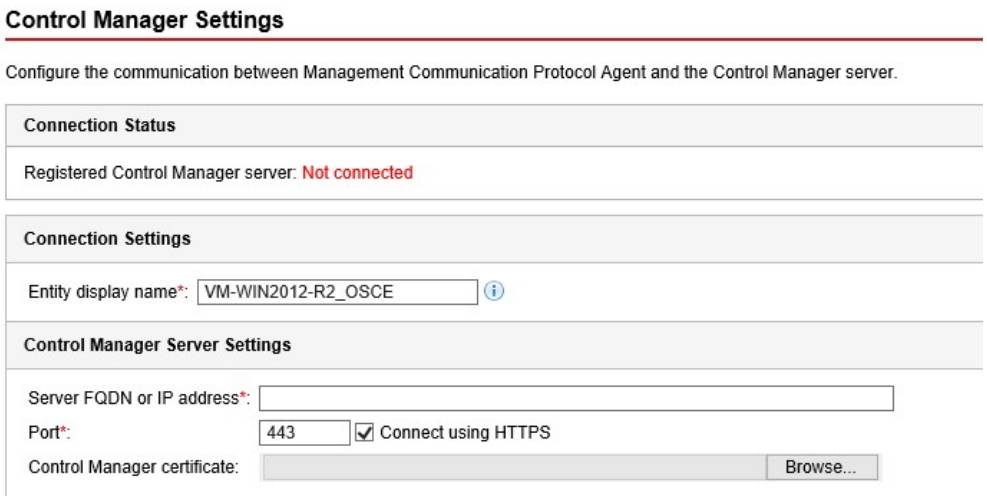


Figure 1.3: Import TMCM

Smart Protection Server (Standalone)

It is suggested that the customer upgrade Standalone Smart Protection Server (if present) to version 3.1 before upgrading OSCE to version XG because the Predictive Machine Learning feature only works with version 3.1.

Please refer to the following article for more detailed information:
https://success.trendmicro.com/solution/1116019

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 five (5) upgrade scenarios:

- Upgrading the OSCE 11.0 server directly
- Migrating to a new OSCE XG server
- Migrating to a new OSCE 11.0 server before upgrading to OSCE XG
- Replacing an OSCE 11.0 server with a new OSCE XG server
- Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG

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 are required 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 server directly

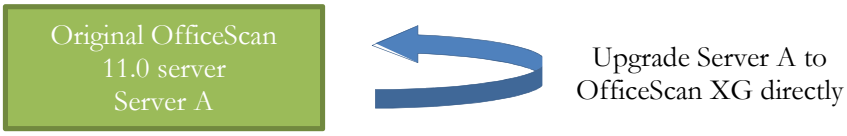


Figure 2.1: Upgrading the server directly

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 2008 or above.
- 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 the OSCE server.
- If the OSCE agent is not allowed to connect to the internet, there will be no File Reputation Services (FRS) and Web Reputation Services (WRS) protection for the Smart Scan mode agent.

Recommendations

- Build a Standalone Trend Micro Smart Protection Server (TMSPS) before upgrading. Below is the download URL for this free product: http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4974&lang_loc=1
- Create a snapshot or backup of the old OSCE server before upgrading to avoid any unexpected risk.

2.2 > Migrating to a new OSCE XG server

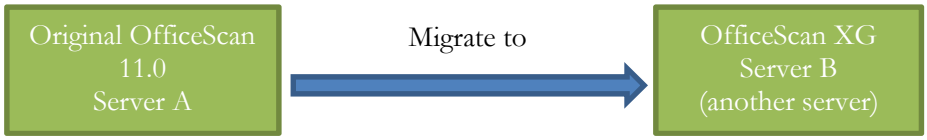


Figure 2.2: Migrating to a new OSCE XG server

In this method, there is a new Server B, which is a freshly-installed OSCE XG server. This upgrade method is used when:

- The OSCE server cannot be offline during the upgrade.
- The old server hardware does not meet the system requirements. Please refer to System Requirements under Chapter 1.
- The server OS is not compatible with XG e.g. the old server is running Windows Server 2003 and it is inconvenient to upgrade to Server 2008 or above.
- There is a need to install the OSCE server to a new server.
- No Plug-in Service e.g. IDF, Integrated Data Loss Prevention (iDLP), or Trend Micro Security for Mac (TMSM) is being used.

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.
- After Server B is ready, there is no agent information in the database.
- Logs e.g. virus/malware log, system events, etc. will be lost, so there is no way to check them and restore the quarantined files from the OSCE web management console.

Recommendations

- Do not restore the old database from Server A to Server B. There may be a schema mismatch risk.
- To avoid compatibility issues, do not use this method if a plug-in service is installed and used.
- The workaround for the quarantined files is to move the quarantined files from Server A to Server B. The default directory is: <OSCE Server installation folder>\PCCSRV\Virus\ Refer to this article if required: https://success.trendmicro.com/solution/1057903.

2.3 > Migrating to a new OSCE 11.0 server before upgrading to OSCE XG

Figure 2.3: Migrating to a new OSCE 11.0 server before upgrading to OSCE XG

In this method, there is a new Server B, which also has OSCE 11.0 installed. The version/build/hot fix and plug-in service(s) of Server B are the same as Server A.

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 2003 and it is inconvenient to upgrade to Server 2008 or a higher version.
- The customer needs to install the OSCE server on another server.

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 Server B is ready, the agent status may be incorrect for a while.
- The method is complex.
- You need to install the same version/build of the OSCE server on Server B like Server A first, before upgrading Server B to OSCE XG.
- 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 Server B because there is no resource anymore. It is suggested that the customer uses TMVP instead of IDF.

Suggestions

- If the customer has IDF on Server A and it is inconvenient to use TMVP instead of IDF, please upgrade the server directly.
- After Server B is online, please log in to the OSCE web management console to verify the agents' status. Go to **Web console** > **Agents** > **Connection Verification** and click **Verify Now**.

2.4 > Replacing an OSCE 11.0 server with a new OSCE XG server

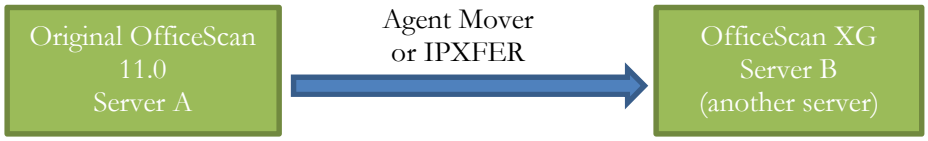


Figure 2.4: Replacing an OSCE 11.0 server with a new OSCE XG server

In this method, there is a new Server B, which is a freshly-installed OSCE XG server. This method is different with the aforementioned method introduced in section 2.2. In section 2.2, there is no need to change the agent's configurations. In this method, it is required to change the agent's configurations.

This upgrade method is used when:

- Multiple applications are used on the original OSCE server (Server A) and the customer wants to separate the OSCE server to another server (Server B).
- Server A and B are required to be online at the same time. This means Server A and B have different IP addresses and hostnames/FQDN.
- The original server's (Server A) hardware does not meet the system requirements. Please refer to System Requirements under Chapter 1. However, the customer still wants to keep Server A in LAN for other usage and will build a new server for OSCE.
- The server OS is not compatible with XG i.e. the old server is running Windows Server 2003 and it is inconvenient to upgrade to Server 2008 or above. However, the customer still wants to keep Server A in LAN for other usage and will build a new server for OSCE.
- 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, so there is no way to check them and restore the quarantined files from the OSCE web management console.
- IDF cannot be installed on Server B because there is no resource anymore. It is suggested that the customer uses TMVP instead of IDF.

Recommendations

- Do not restore the old database from Server A to Server B. There may be a schema mismatch risk.
- To avoid compatibility issues, do not use this method if iDLP is installed and used.
- The workaround for the quarantined files is to move the quarantined files from Server A to Server B. The default directory is: <OSCE Server installation folder>\PCCSRV\Virus\ Refer to this article if required: https://success.trendmicro.com/solution/1057903.

2.5 > Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG

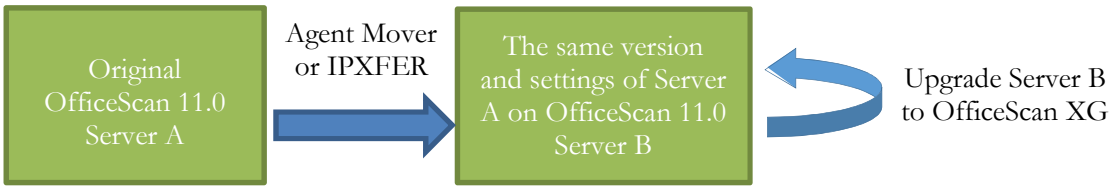


Figure 2.5: Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG

In this method, there is a new Server B, which also has OSCE 11.0 installed. The version/build/hot fix and plug-in service(s) of Server B are the same as Server A's. This method is different with the aforementioned method introduced in section 2.3. In section 2.3, there is no need to change the agent's configurations. In this method, it is required to change the agent's configurations.

This upgrade method is used when:

- Multiple applications are used on the original OSCE server (Server A) and the customer wants to separate the OSCE server to another server (Server B).
- Server A and B are required to be online at the same time. This means Server A and B have different IP addresses and hostnames/FQDN.
- The original server's (Server A) hardware does not meet the system requirements. Please refer to System Requirements under Chapter 1. However, the customer still wants to keep Server A in LAN for other usage and will build a new server for OSCE.
- The server OS is not compatible with XG i.e. the old server is running Windows Server 2003 and it is inconvenient to upgrade to Server 2008 or above. However, the customer still wants to keep Server A in LAN for other usage and will build a new server for OSCE.
- 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 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 iDLP.

Disadvantages

- You need to prepare more resource(s) e.g. H/W purchase, network/topology setting, etc.
- You need to install the same version/build of the OSCE server on Server B like Server A first, before upgrading Server B to OSCE XG.
- IDF cannot be installed on Server B because there is no resource anymore. It is suggested that the customer uses TMVP instead of IDF.

Recommendations

- If the customer has IDF on Server A and it is inconvenient to use TMVP instead of IDF, please upgrade the server directly.

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

There are two (2) options for upgrading the server directly:

- Upgrading the server by copying the installer on the server's local disk
- Upgrading the server remotely from another computer

To upgrade the server directly:

a. Download the installation package from the Trend Micro Official Site: http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4973&lang_loc=1

b. Do an image backup or snapshot before upgrading (Recommended).

c. Build a local TMSPS (Standalone).

d. If the customer is concerned with bandwidth consumption, please disable the following feature from OSCE web management console for root domain:

   - OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes

e. Run the installer to upgrade Server A:

   - For "On this endpoint":
     a. Click **Start** to proceed with the server upgrade processes.

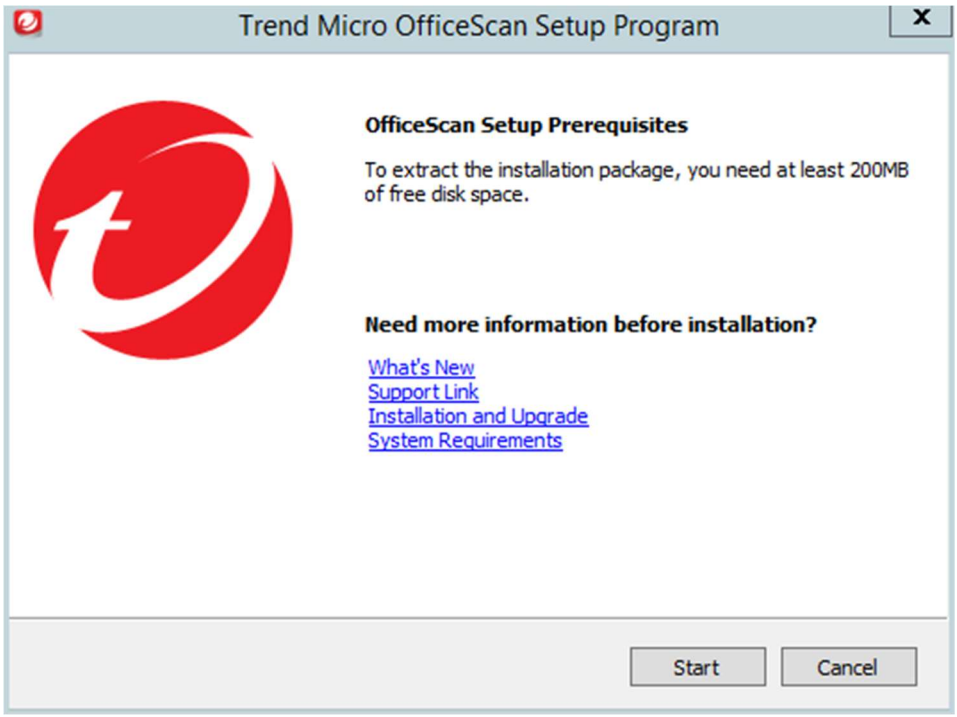


Figure 3.1: Start to upgrade OfficeScan server

b. Click the **Next** button.

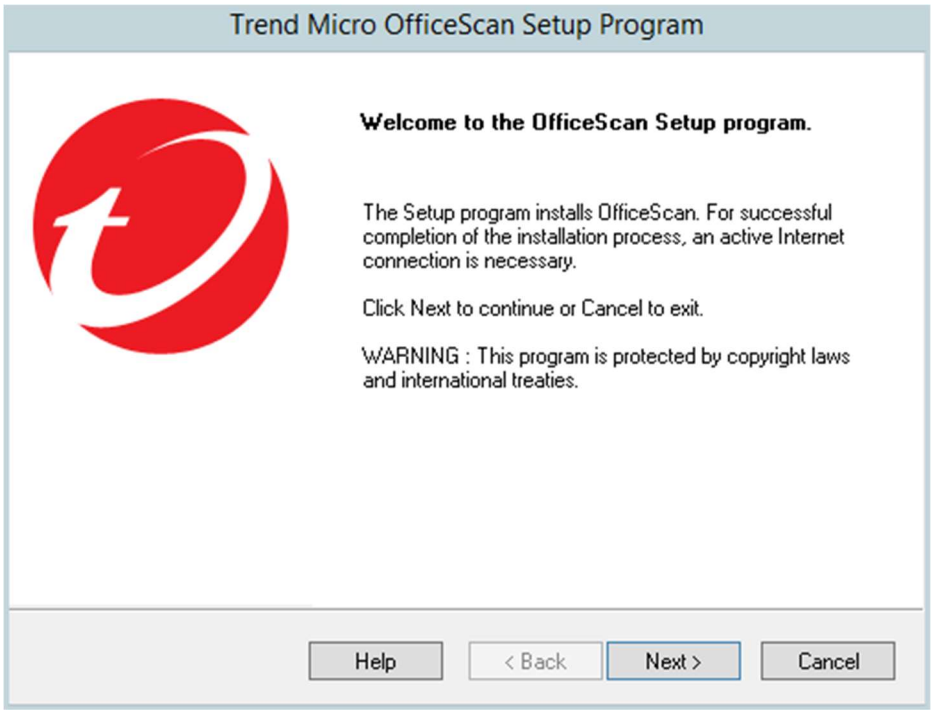


Figure 3.2: Welcome wizard

c. Agree with the EULA and click **Next**.

Figure 3.3: EULA

d. Choose "On this endpoint".

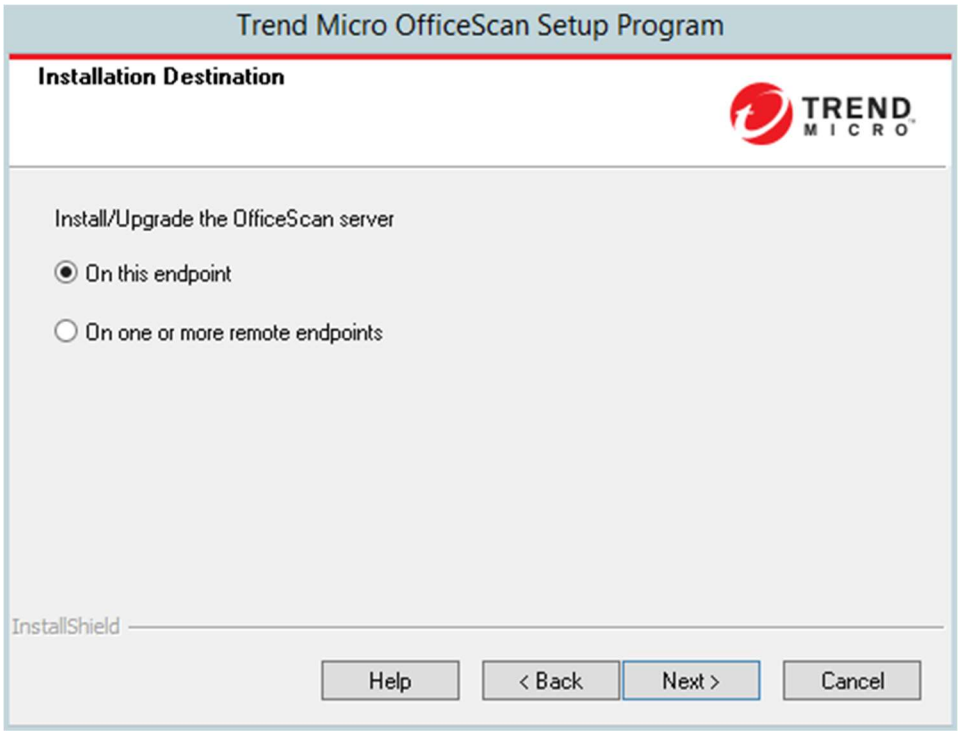


Figure 3.4: Use "On this endpoint" to upgrade

e. Choose "Scan the target endpoint".

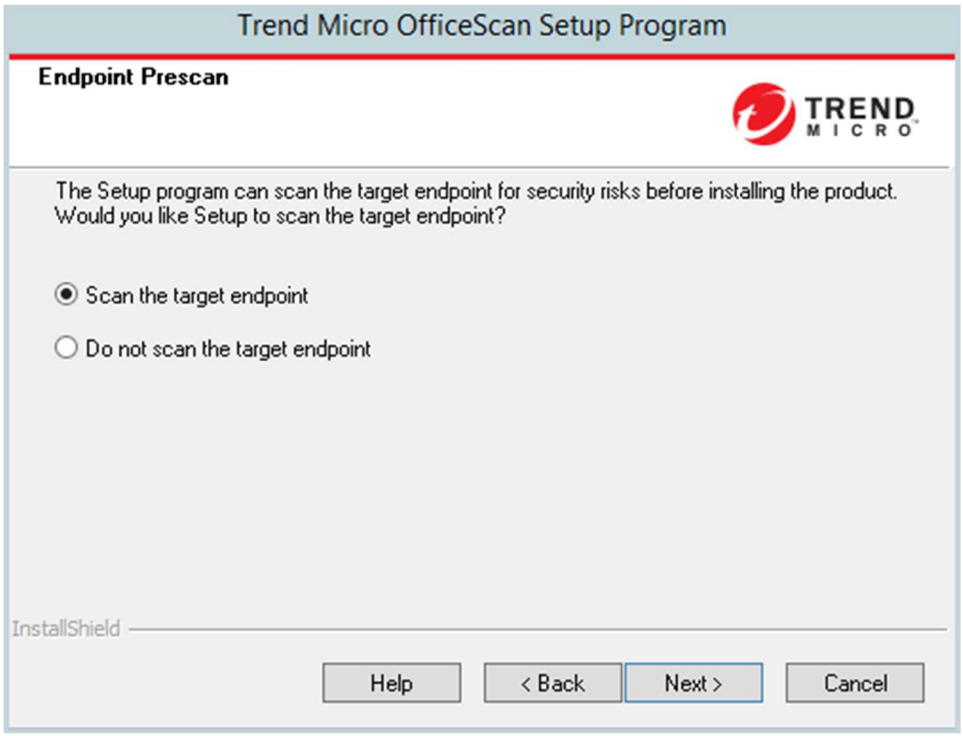


Figure 3.5: Do a pre-scan for current server

f. Wait until setup is done assessing the target server's environment.

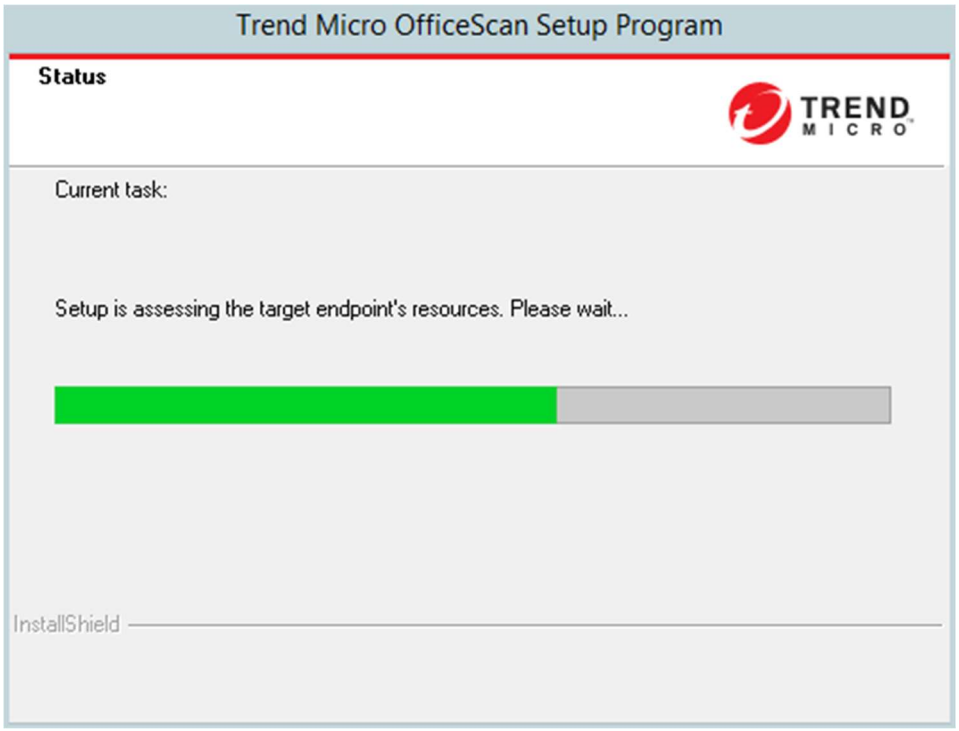


Figure 3.6: Checking current server's

g. Enable all of the features by clicking **Yes**.

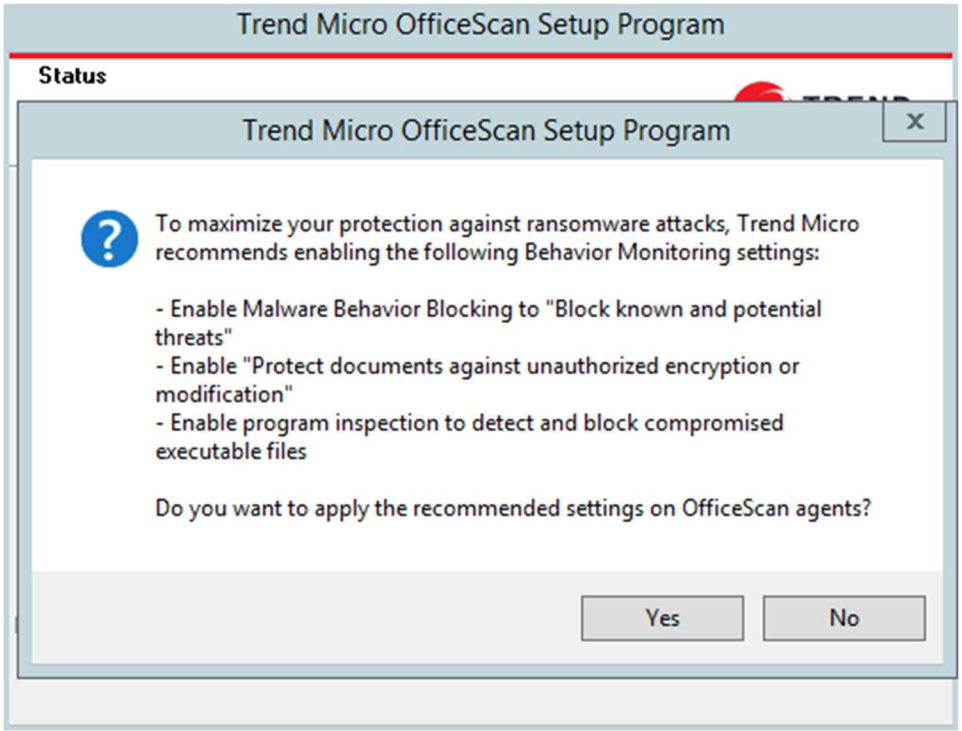


Figure 3.7: Protection settings recommendation

h. Click **Next**.

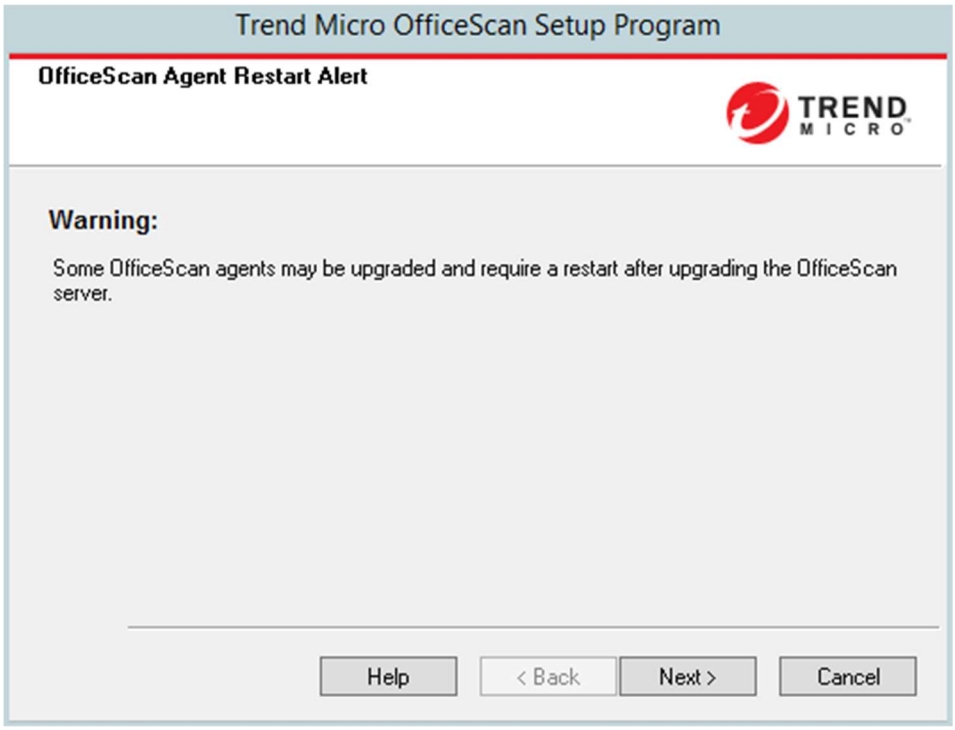


Figure 3.8: Upgrade warning information

i. Back up the current OSCE server, then click **Next**.

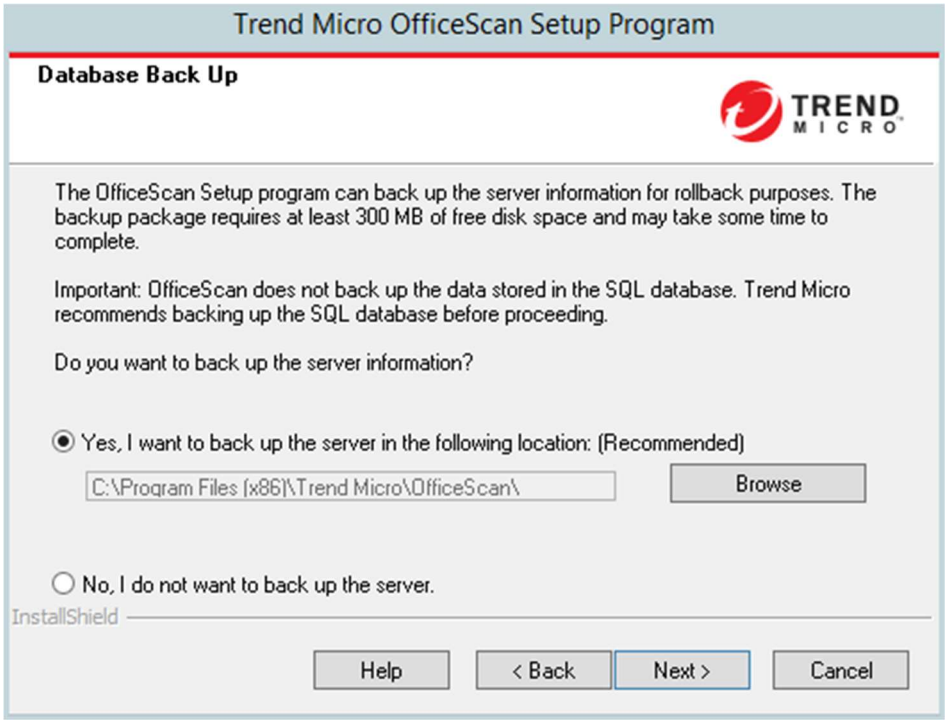


Figure 3.9: Backup server wizard

j. Click **Next** to start the upgrade. The upgrade should finish successfully.

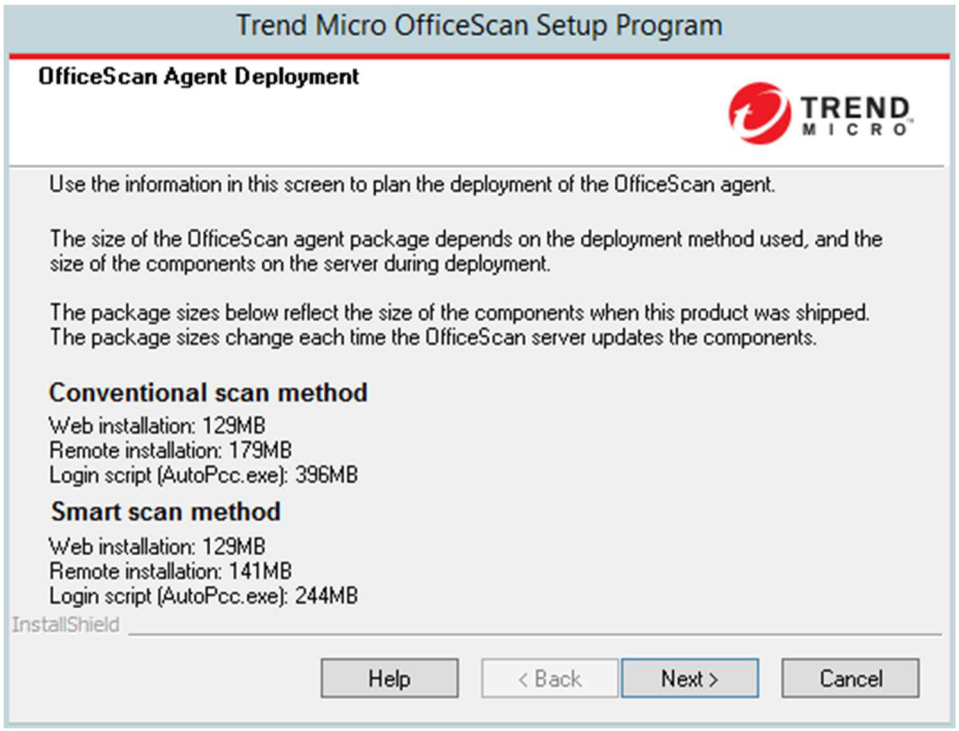


Figure 3.10: Agent deployment size information

k. Click **Finish**.

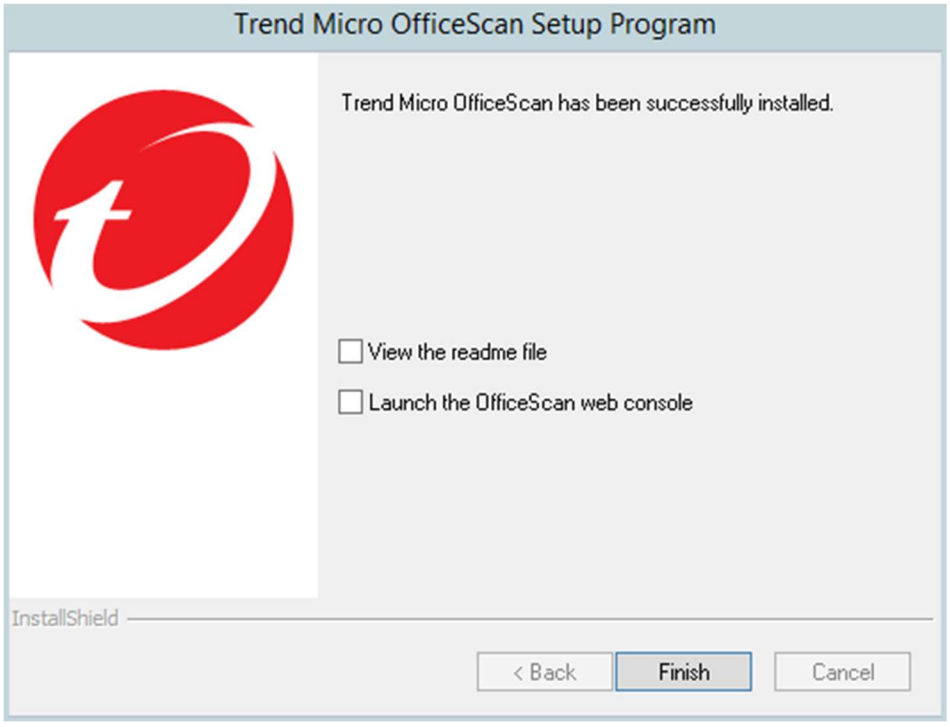


Figure 3.11: Upgrade completed successfully wizard

- For "On one or more remote endpoints":
  a. Click **Start** to proceed with the server upgrading processes.

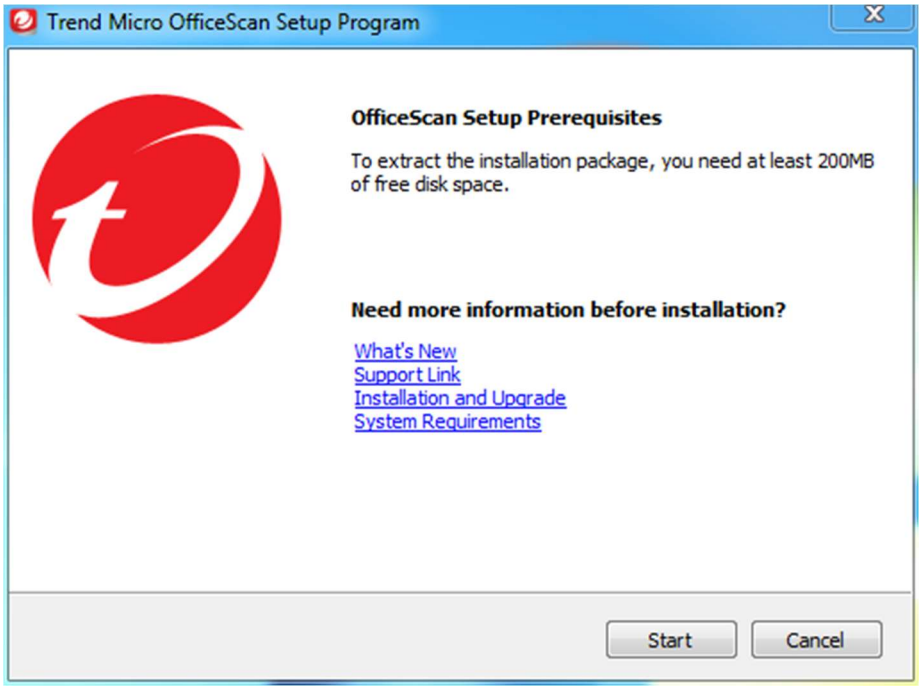


Figure 3.12: Start to upgrade OfficeScan server

  b. Choose "On one or more remote endpoints" and click **Next**.

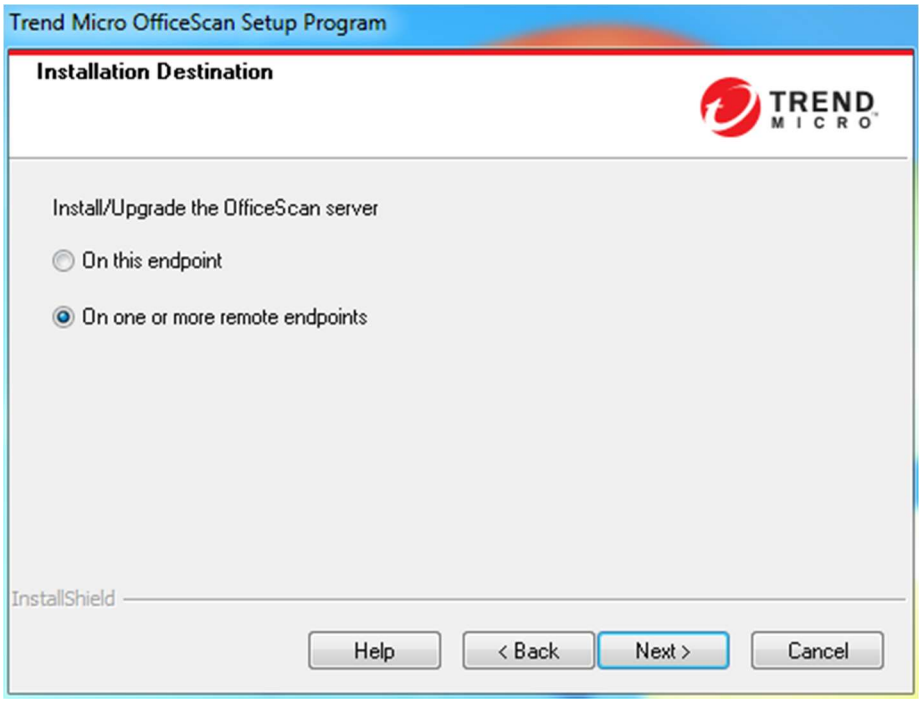


Figure 3.13: Use "On one or more remote endpoints" to upgrade OSCE

c. Choose "Scan the target endpoint" then click **Next**.

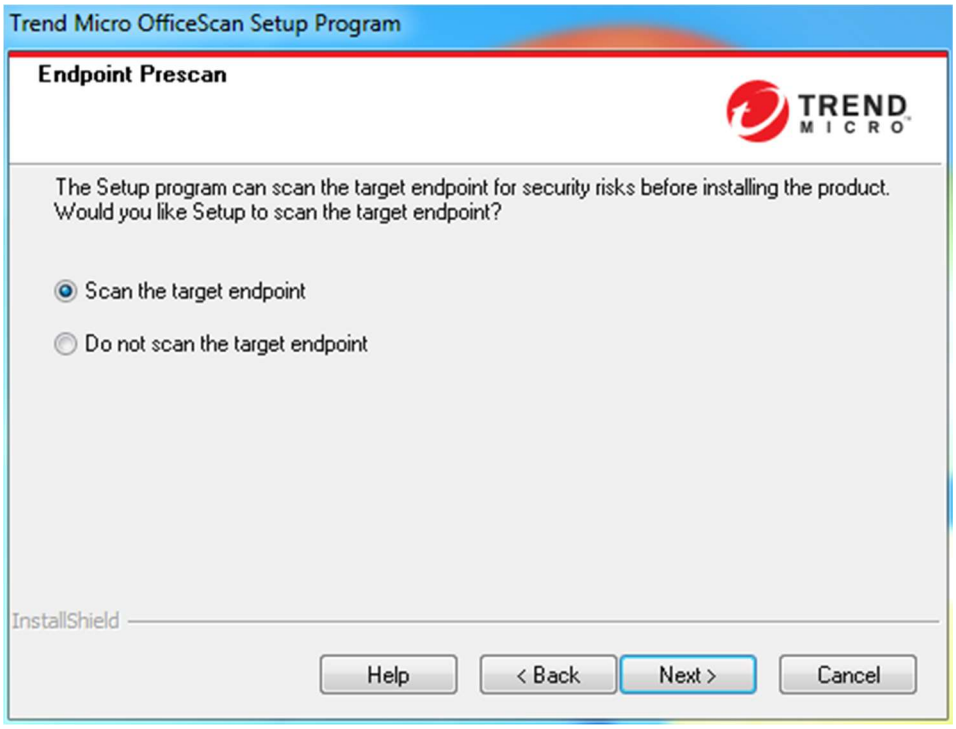


Figure 3.14: Do a pre-scan for current server

d. Confirm the remote OSCE server's installation directory and click **Next**.

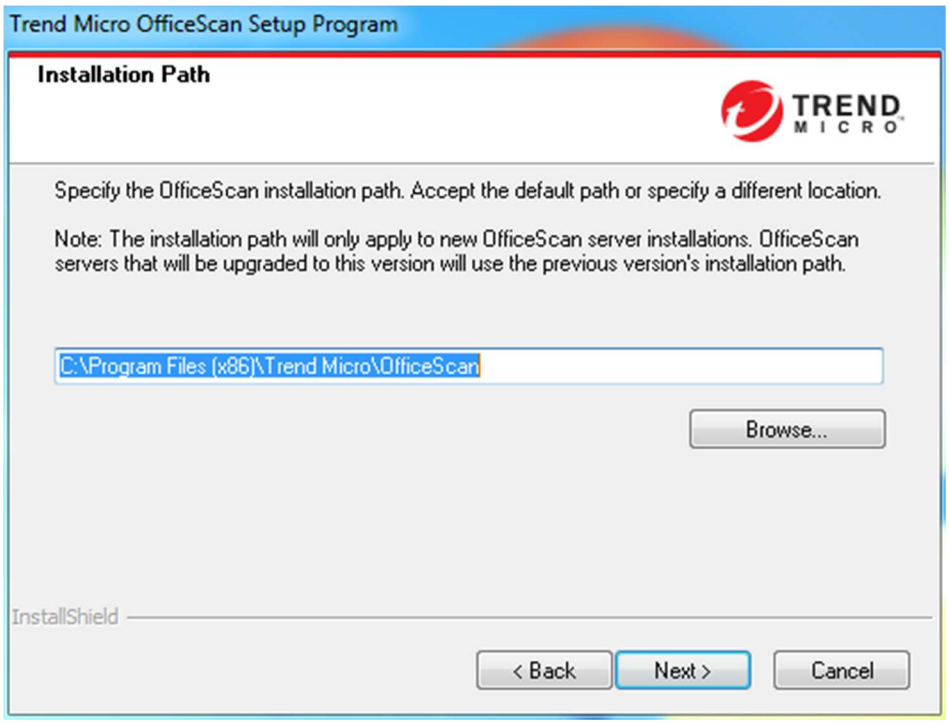


Figure 3.15: Remote OSCE server's installation directory

e. If there is a proxy, please check "Use a proxy server" and confirm the proxy's settings, then click **Next**. Otherwise, please ignore the proxy settings and just click **Next**.

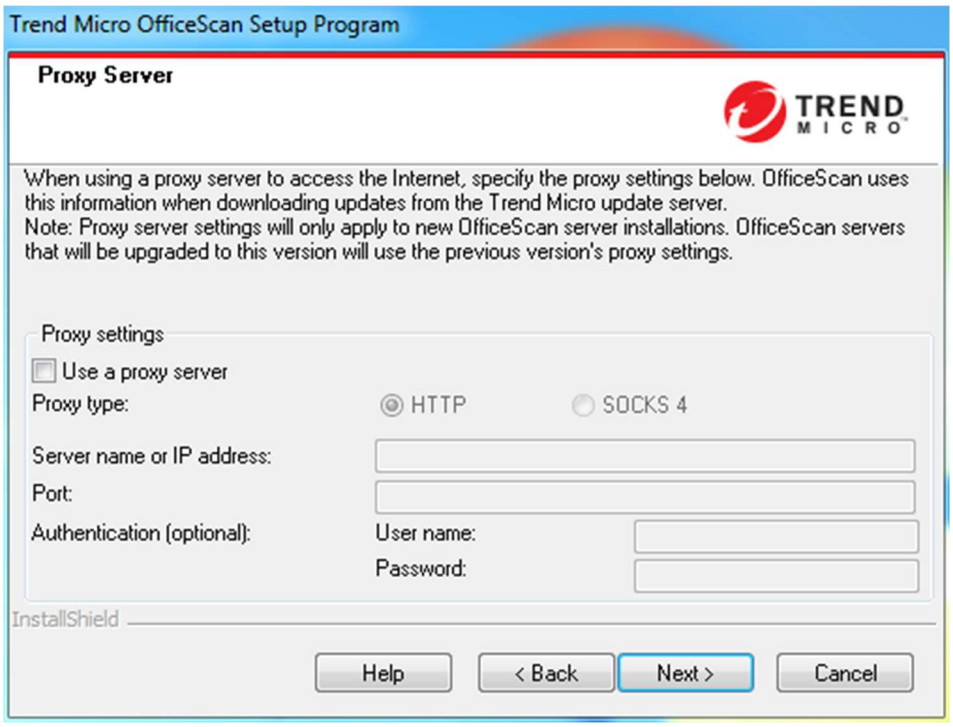


Figure 3.16: Proxy settings wizard

f. Confirm the config web server settings, then click **Next**.

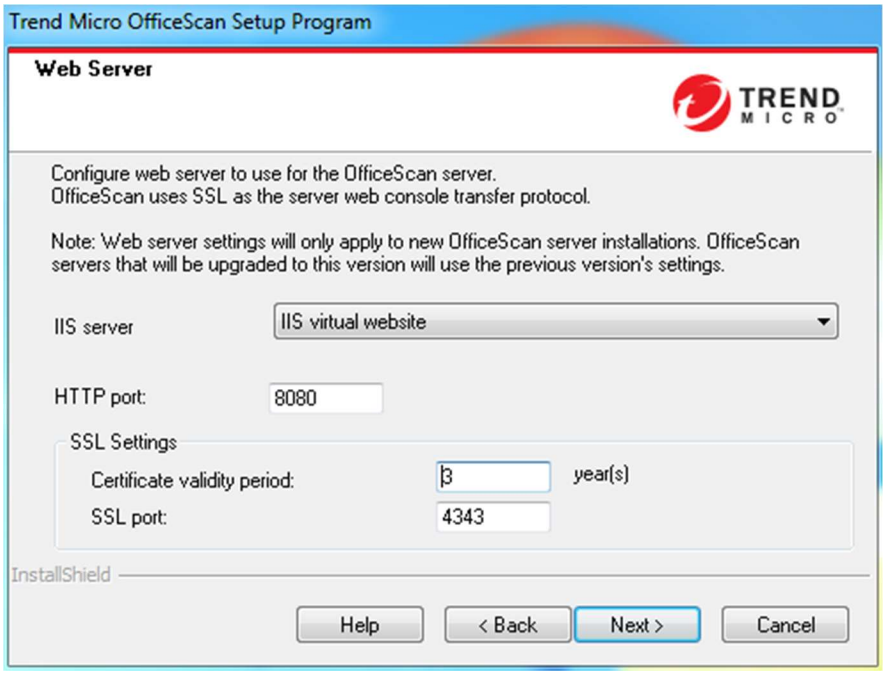


Figure 3.17: Web server settings

g. Depending on the environment, use FQDN or IP. In this example, IP address is checked. Click **Next**.

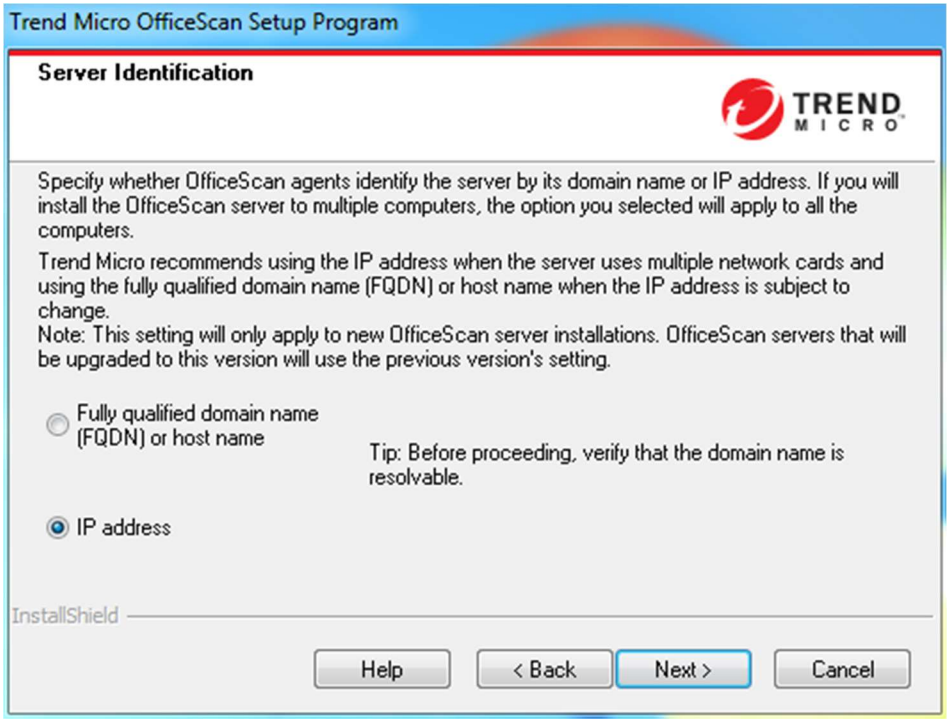


Figure 3.18: Server's identification method by OSCE agent

h. For the activation code (AC) verification, make sure that the AC is available. Remote upgrade requires verification of the AC. Local upgrade does not need to do it. Afte verifying, click **Next**.

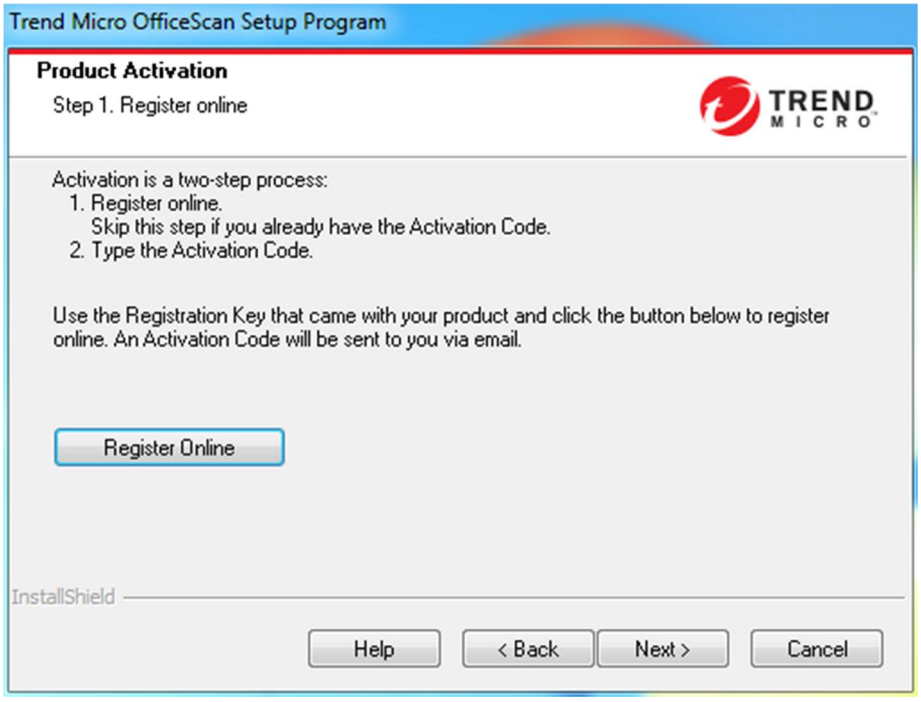


Figure 3.19: Activation code register wizard

i. Get the AC from the OSCE server intended to be upgraded and input it there, then click **Next**. Remote upgrade requires the input of the AC. Local upgrade does not need it.

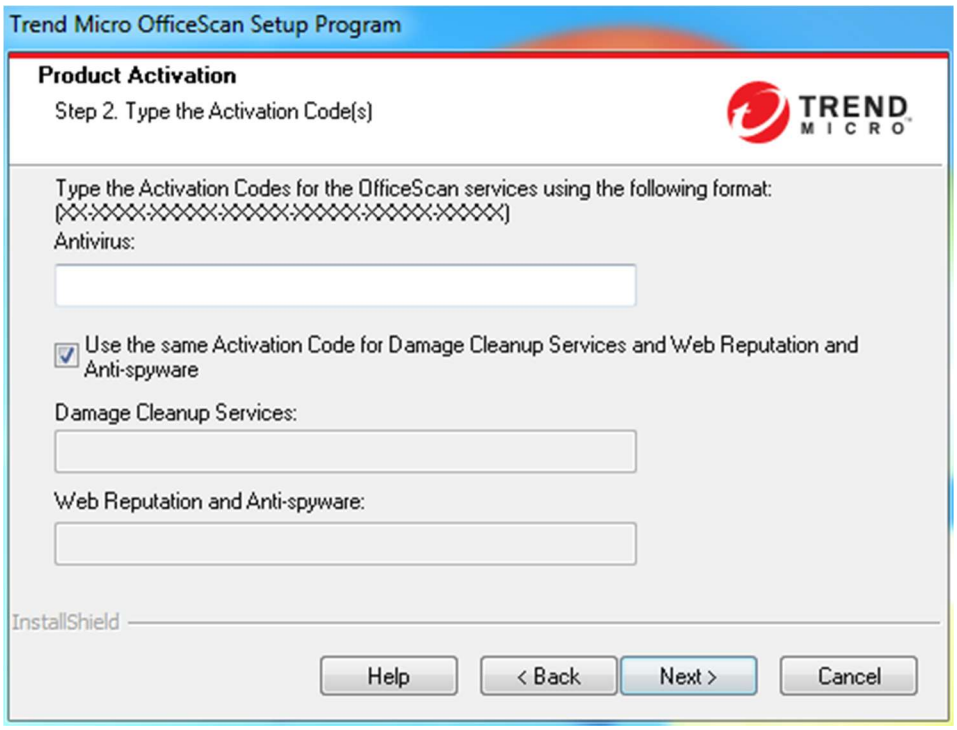


Figure 3.20: Activation code input wizard

j. Click **Next** to start the upgrade.

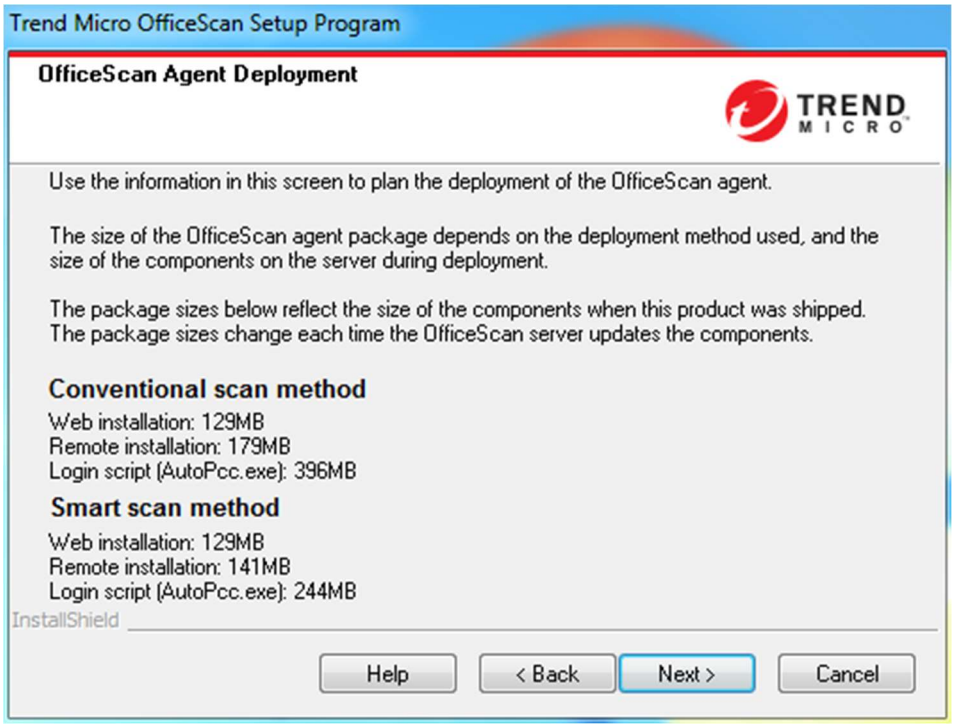


Figure 3.21: Agent deployment size information

k. Enable/Disable Integrated Smart Protection Server. Choose "Yes, install…" if there is no Standalone Smart Protection Server, then click **Next.**

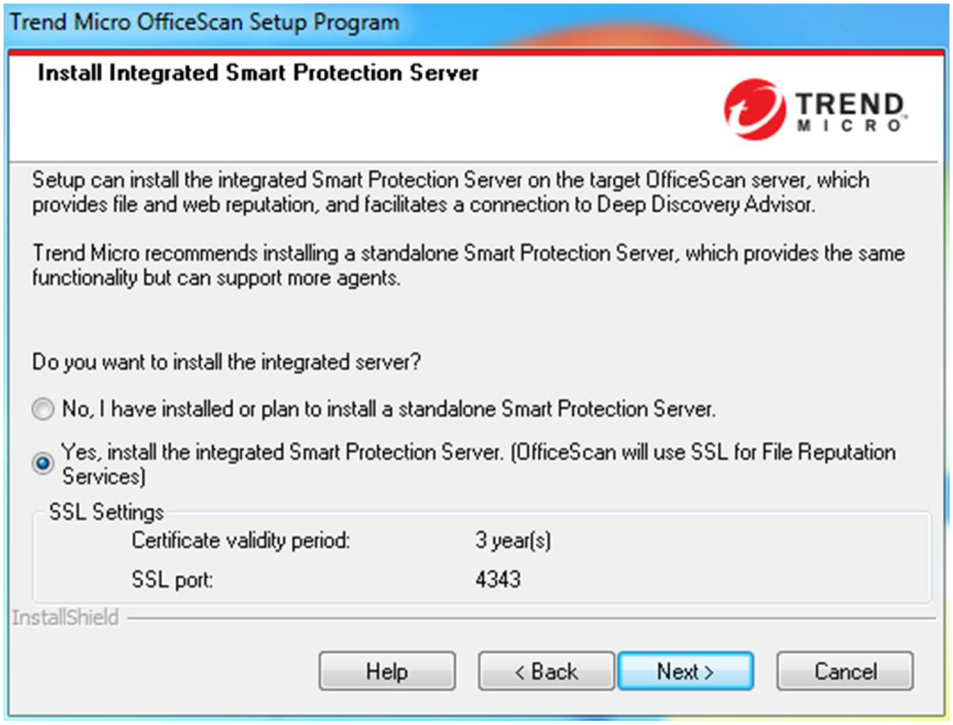


Figure 3.22: Integrated smart protection server

l. Add the OSCE server's IP address and click **Next**.

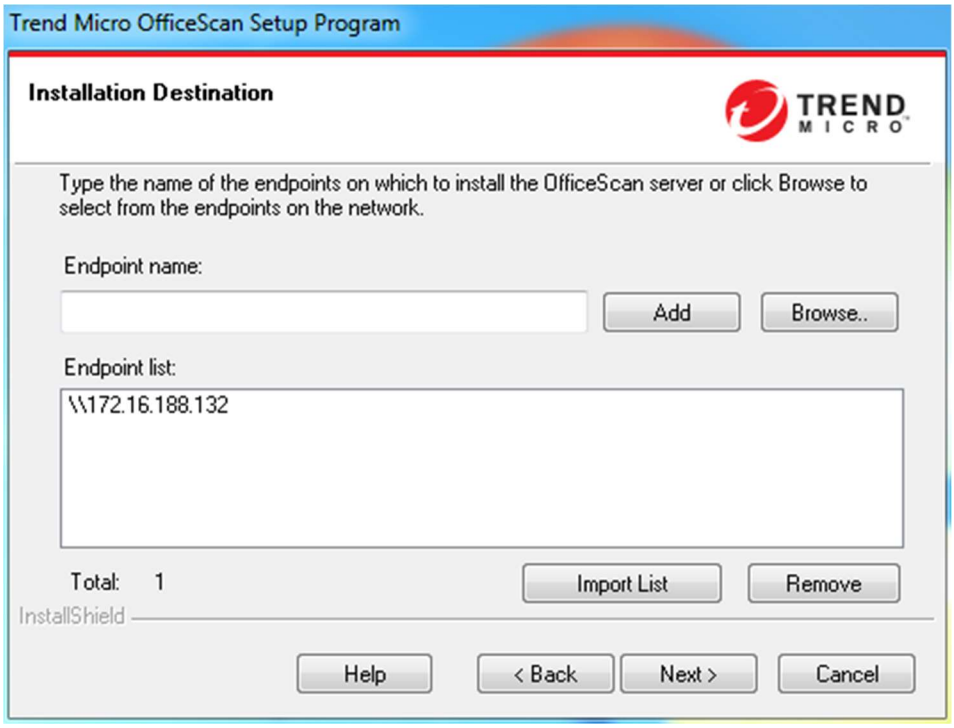


Figure 3.23: Remote OSCE server information

m. Click **Analyze** to verify the remote server's connection and status.

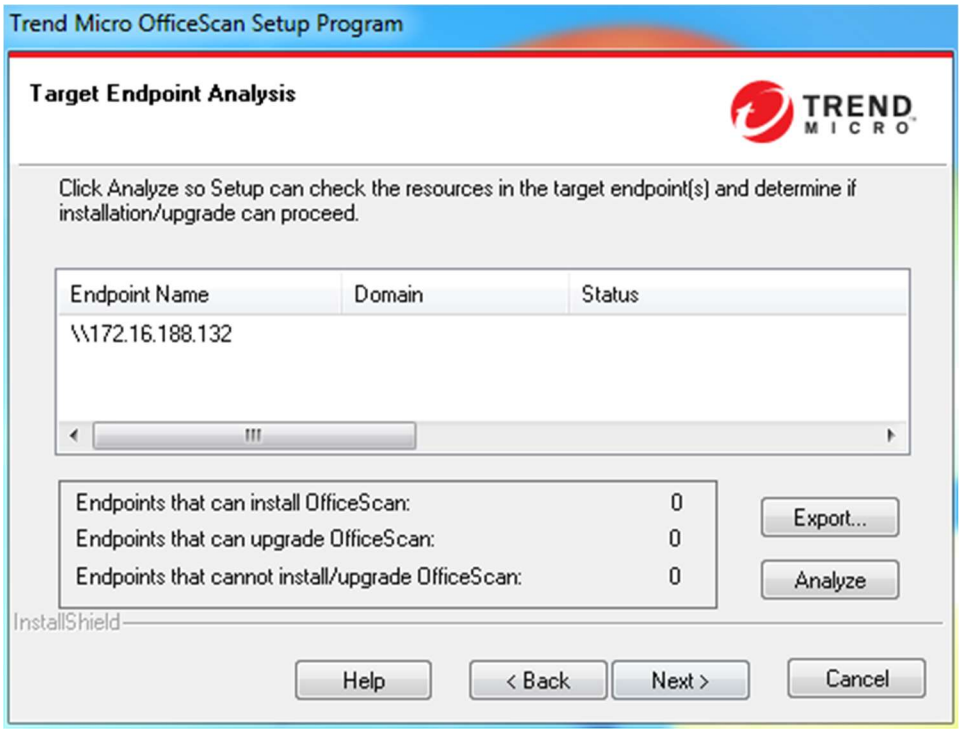


Figure 3.24: Remote OSCE server analysis

n. Input the credentials and click **OK** to start the remote server analysis.

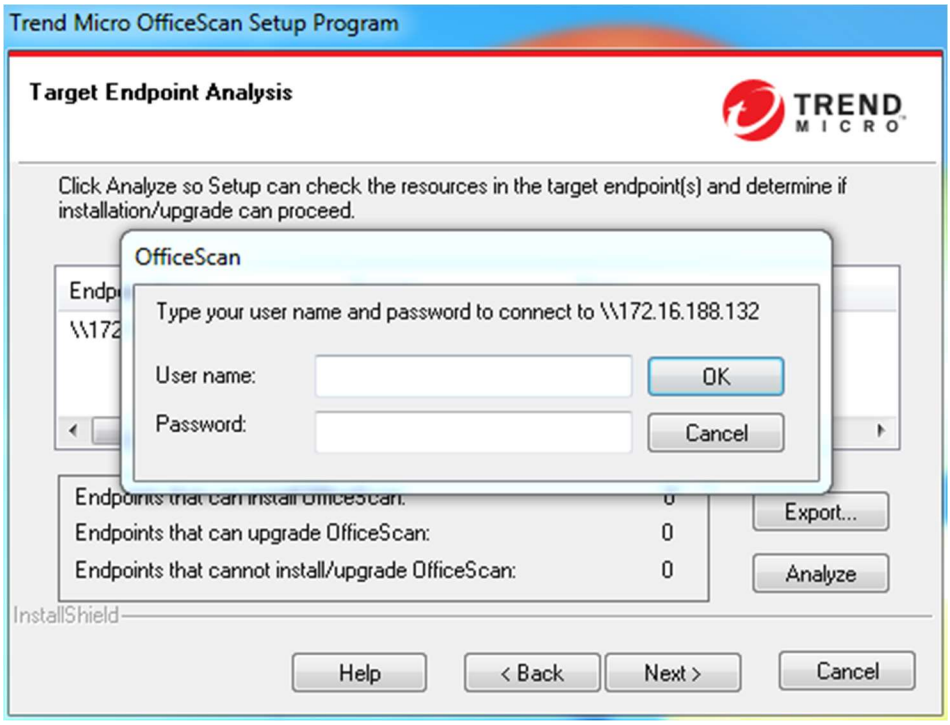


Figure 3.25: Remote OSCE server credential

To bypass Analyze, make sure that:

- The network to the OSCE server is stable and accessible from the computer.
- The firewall that was off under the "File and Printer Sharing" rules of the Windows Firewall was allowed in the OSCE server.
- The credentials used have Administrator permission on the OSCE server. If it is an AD account, make sure that the account is in the Domain Admins group. If the account is a local account, make sure that the account has Administrator permission on both the OSCE server and the computer. In this example, "Administrator" is used for testing.

o. Enable all of the features by clicking **Yes**.

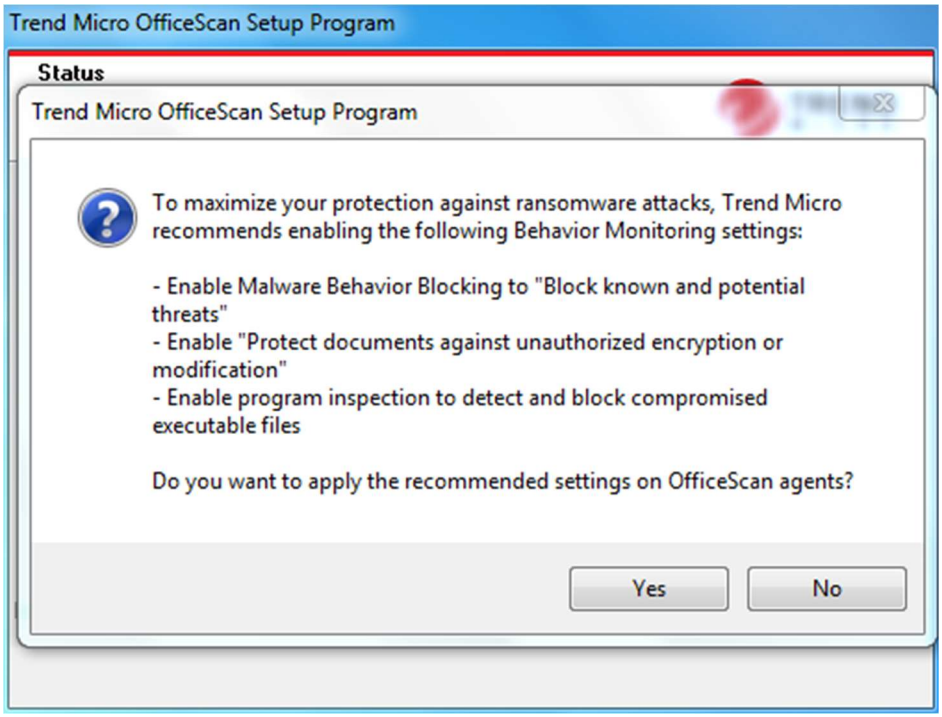


Figure 3.26: Protection settings recommendation

p. Wait until setup is done assessing the target server's environment.

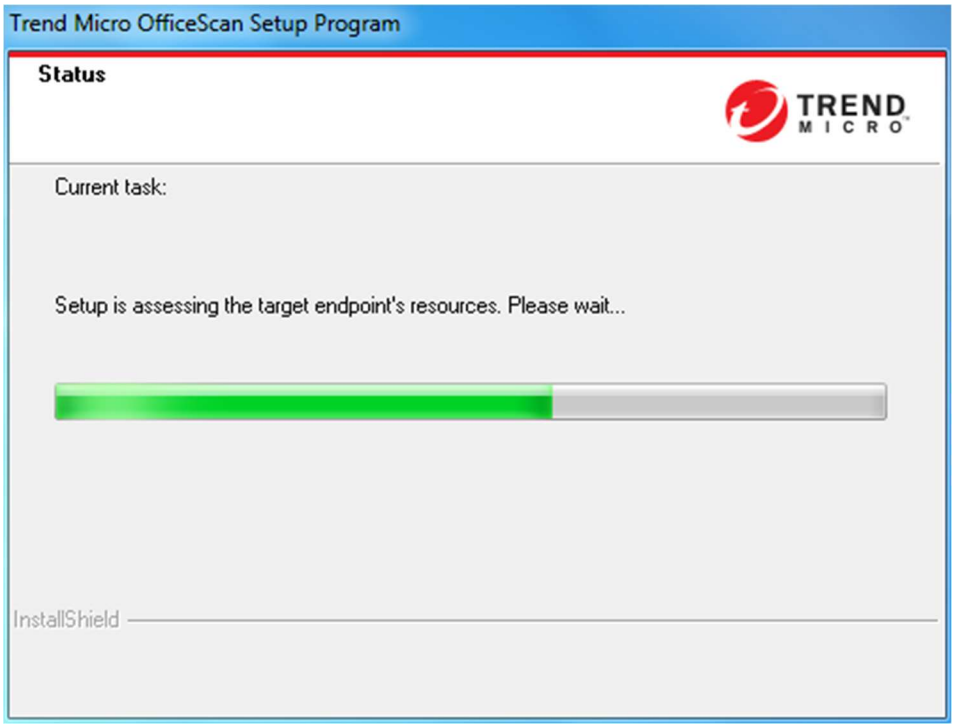


Figure 3.27: Checking remote server's environment for upgrading

q. Click **Next** if it shows "Passed. Proceed with upgrade." Otherwise, please check the network, account credentials, permission, and disk space where the OSCE server is installed.

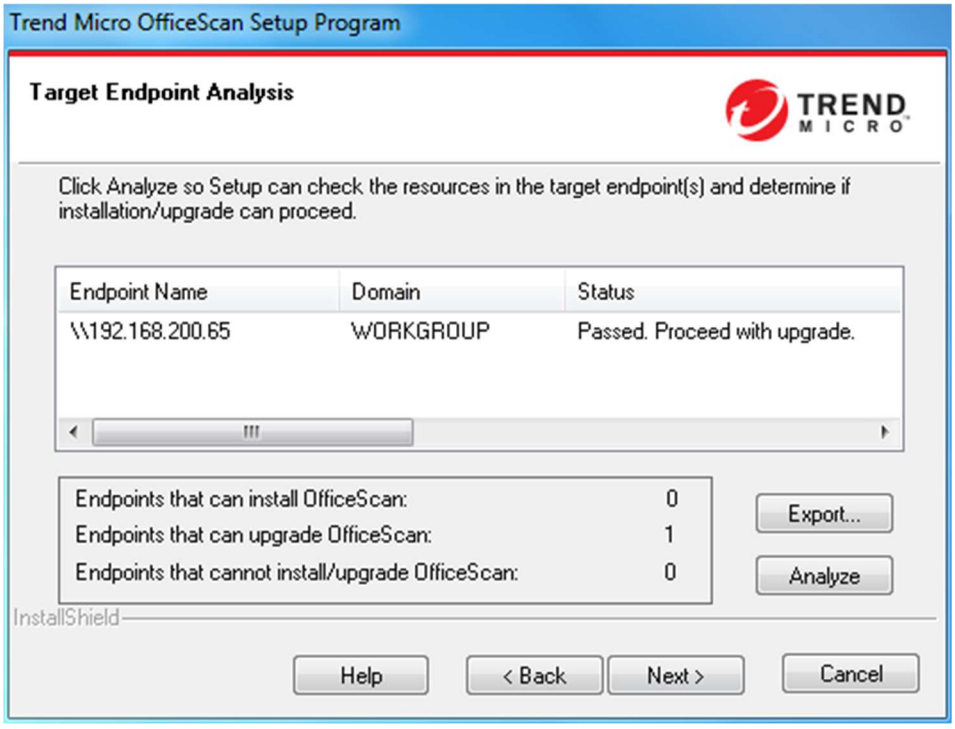


Figure 3.28: Checking remote server's environment passed

r. Click **Next**.

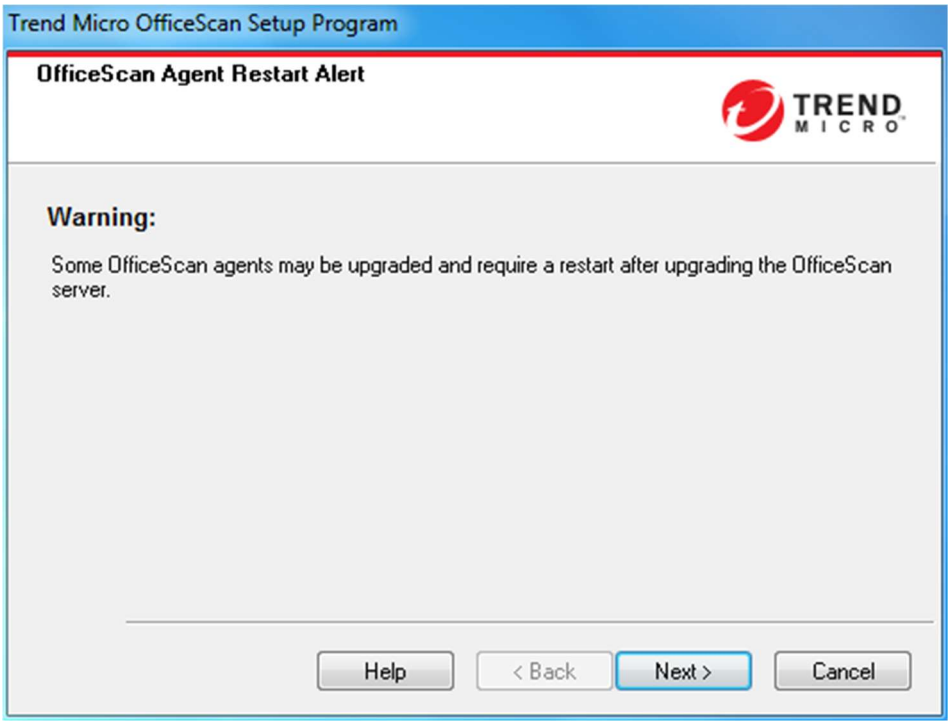


Figure 3.29: Upgrade warning information

s. Choose **Yes** to back up the remote server, then click **Next**.

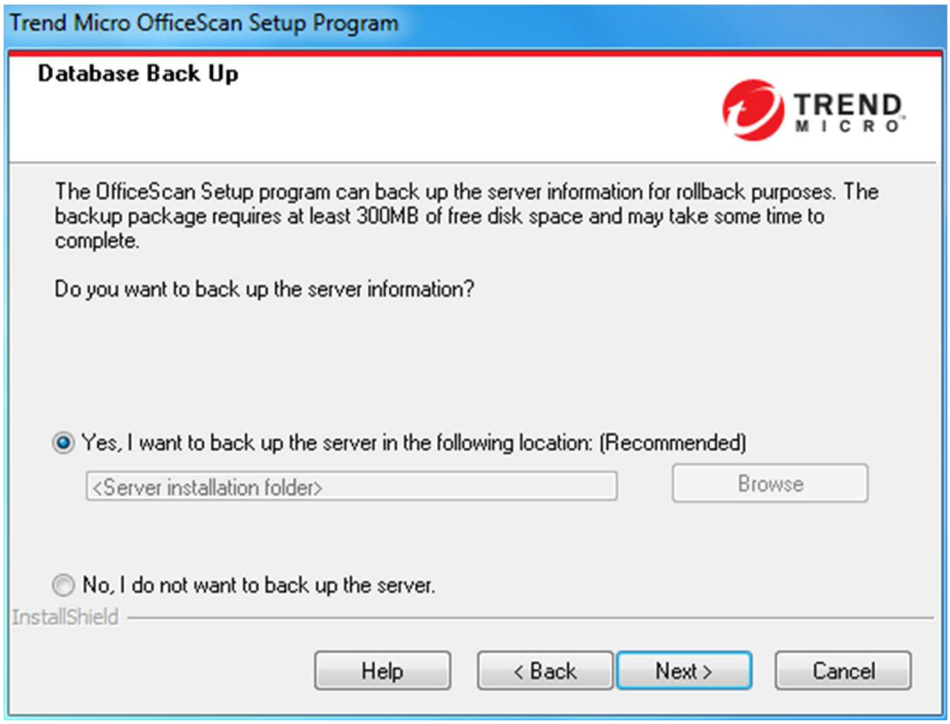


Figure 3.30: Backup server wizard

t. When the upgrade has started, wait for the process to finish.

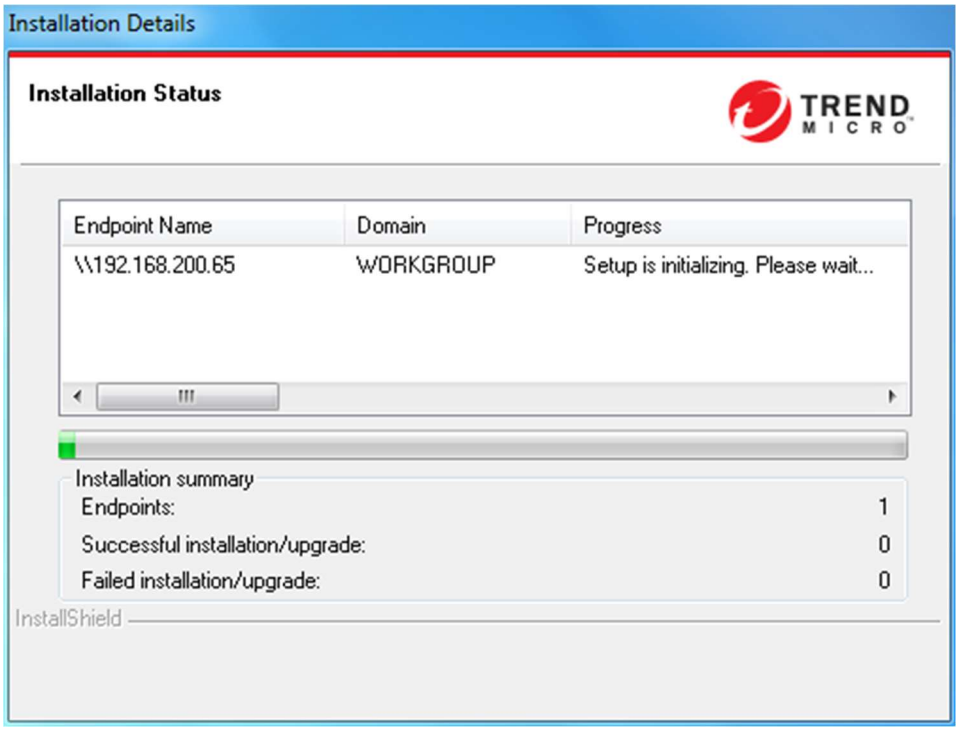


Figure 3.31: Upgrade proceeding

u. Click **OK** to exit the wizard.

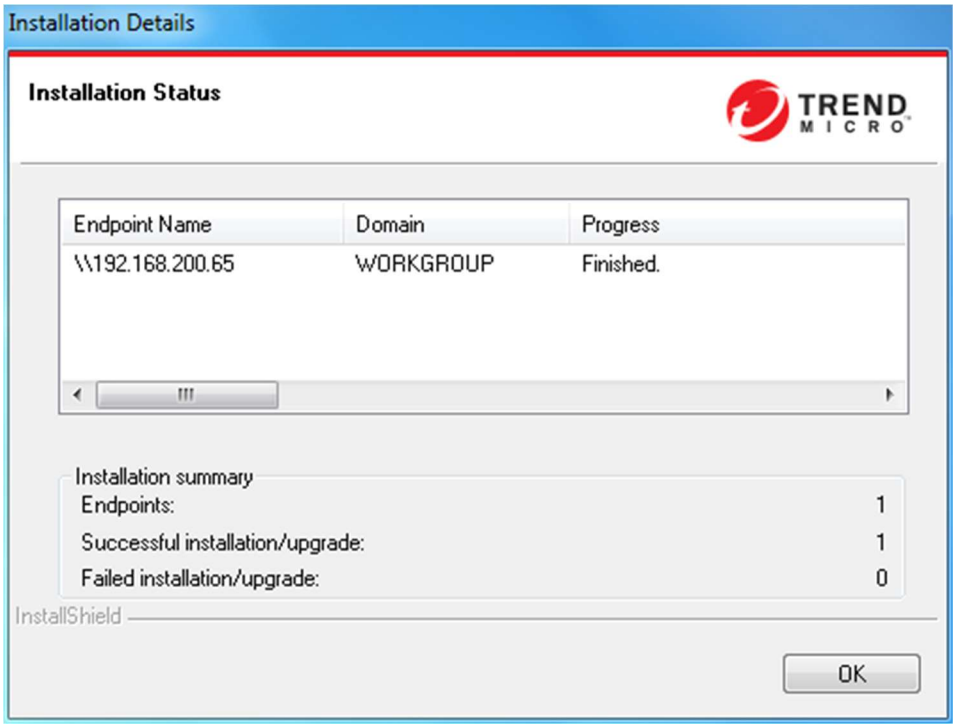


Figure 3.32: Upgrade finished

v. Trigger an update for the agent to upgrade to OSCE XG.

w. Before logging in to the OSCE XG web management console, clear the browser's cache.

3.2 > Migrating to a new OSCE XG server

1. Prepare another server: Server B.
2. Configure Server B according to Server A:
   - Scenario I: If Server A is using IP address (x.x.x.x) for OSCE communication:
     a. Put Server B in an isolated network other than Server A's.
     b. Set the same IP address for Server B (x.x.x.x).
   - Scenario II: If Server A is using FQDN for OSCE communication:
     a. Put Server B in another LAN/vLAN where Server A cannot reach Server B.
     b. Give it the same FQDN as Server A. The IP Address does not necessarily have to be the same as Server A's.
3. Do a fresh installation of OSCE XG on Server B.
4. After the fresh installation finishes:
   a. Import the certificate from Server A to Server B. Please refer to the following article: https://success.trendmicro.com/solution/1111610.
   b. Rename the folder to [<OfficeScan Server Installation Folder>\PCCSRV\Admin\Utility\ServerMigrationTool] to [ServerMigrationTool_old] on Server A.
   c. Copy the same folder from Server B to Server A. Put it in the same location.
   d. Run this tool as Administrator on Server A to export the settings.
   e. Copy the exported .zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.
   f. Run the tool again on Server B to import the settings.
5. After the settings are restored on Server B, bring it online:
   - For Scenario I:
     - Bring Server A offline, and then immediately bring Server B online.
   - For Scenario II:
     a. Update the DNS if Server B's IP is different from Server A.
     b. Bring Server A offline, then immediate bring Server B online if the IP address is the same.

6. If Server B's DB is empty, wait for the agent communicating and registering to the new OSCE server to finish. The OSCE agent will go back to Server B when the following events are triggered:
   - OSCE agent reloaded
   - Computer restarted
   - OSCE agent's IP address changed
7. Register the OSCE server to TMCM if the original server has or requires it.
8. Add a Standalone Smart Protection Server if the original server has or requires it.
9. Trigger an update for the agent to upgrade to OSCE XG.

Important: It is not suggested to use this method if IDF, DLP, or TMSM is being used. Please refer to section 3.1 or the following section 3.3 if the aforementioned are being used.

3.3 > Migrating to a new OSCE 11.0 server before upgrading to OSCE XG

This scenario is similar to the scenario introduced in the previous section 3.2:

1. Prepare another server: Server B.
2. Configure Server B according to Server A.
   - Scenario I: If Server A is using the IP address (x.x.x.x) for OSCE communication:
     a. Put Server B in an isolated network other than Server A's.
     b. Set the same IP address for Server B (x.x.x.x).
   - Scenario II: If Server A is using FQDN for OSCE communication:
     a. Put Server B in another LAN/vLAN where Server A cannot reach Server B.
     b. Give the same FQDN as Server A. It is not required that the IP Address be the same as Server A's.
3. Do a fresh installation of OSCE 11.0, which is the same as Server A, on Server B.
4. After the fresh installation finishes:
   a. Import the certificate from Server A to Server B. Refer to the following article: https://success.trendmicro.com/solution/1111610.
   b. Run the tool as administrator [<OSCE Server folder>\PCCSRV\Admin\Utility\ServerMigrationTool] on Server A to export the settings.
   c. Copy the exported zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.
   d. Run the tool again on Server B to import the settings.
   e. Restore the database from Server A to Server B:

- HTTPDB:
  i. Stop the OfcService service on Server 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: Refer to https://success.trendmicro.com/solution/1113252.

- If any plug-in service is installed on Server A, install it on Server B as well.
  - For IDF used on Server A: Deactivate the IDF agent and use TMVP instead.
  - For TMSM used on Server A: Please refer to the following article: https://success.trendmicro.com/solution/1055658.
  - For iDLP used on Server A:
    i. Overwrite [<OSCE Server Folder>\PCCSRV\Private\DLPForensicDataTracker.db] from Server A to server B in the same folder.
    ii. Check the server's side settings on Server A by following the instructions in the following article: http://intkb.trendmicro.com/solution/en-us/1098469.aspx. 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.
    iii. Compare ofcscan.ini on Server A and Server B:

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

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

5. After the settings restoration finishes on Server B, upgrade Server B to OSCE XG.
6. After upgrading Server B to OSCE XG, please bring Server B online.

- For Scenario I:
  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.
- For Scenario II:
  a. Update the DNS if Server B's IP is different from Server A's.
  b. Bring Server A offline.
  c. Move Server B to Server A's LAN if required. It is determined by the customer's network environment's design.

d. Make sure that the OSCE agents can reach Server B.

7. Trigger an update for agents to upgrade to OSCE XG.

3.4 > Replacing an OSCE 11.0 server with a new OSCE XG server

1. Prepare another server: Server B.
2. Do a fresh installation of OSCE XG on Server B.
3. After the fresh installation finishes:
   a. Rename the folder to [<OfficeScan Server Installation Folder>\PCCSRV\Admin\Utility\ServerMigrationTool] to [ServerMigrationTool_old] on Server A.
   b. Copy the same folder from Server B to Server A. Put it in the same location.
   c. Run this tool as Administrator on Server A to export the settings.
   d. Copy the exported .zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.
   e. Run the tool again on Server B to import the settings.
4. Move the agents from Server A to Server B. 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. Register the OSCE server to TMCM if the original server has or requires it.
6. Add a Standalone Smart Protection Server if the original server has or requires it.

Important: It is not suggested to use this method if iDLP is being used. Please refer to section 3.1 or 3.3 or the following section 3.5 if the aforementioned are being used.

3.5 > Replacing an OSCE 11.0 server with another OSCE 11.0 server before upgrading to OSCE XG

This scenario is similar to the scenario introduced in the previous section 3.4:

1. Prepare another server: Server B.
2. Do a fresh installation of OSCE 11.0, which is the same as Server A, on Server B.
3. After the fresh installation finishes:
   a. Run the tool as administrator [<OSCE Server folder>\PCCSRV\Admin\Utility\ServerMigrationTool] on Server A to export the settings.

b. Copy the exported zip file (i.e. C:\OsceMigrate.zip) to Server B and put it in the same location as Server A.

c. Run the tool again on Server B to import the settings.

d. Restore the database from Server A to Server B:

   - HTTPDB:

     v. Stop the OfcService service on Server A.

     vi. Stop the OfcService service on Server B.

     vii. Copy [<OSCE Server Folder>\PCCSRV\HTTPDB] from Server A to overwrite the same location on Server B.

     viii. Start the OfcService service on Server B.

   - MS SQL: Refer to https://success.trendmicro.com/solution/1113252.

4. After the database restored on Server B. Please login OSCE web management console. And navigate to **Agents** > **Agent Management**.

5. Remove all the agents shown in the agent tree. Here, the agents shown in the agent tree are the agents from Server A. This step is very important if iDLP is required to do restore on Server B.

6. Restore quarantined files from Server A to Server B manually. The default directory is: <OSCE Server installation folder>\PCCSRV\Virus\

7. Restore PLS if required. Please refer to Chapter 4 for more information.

8. Move the agents from Server A to Server B. 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

9. After the settings and agents restoration is finished on Server B, upgrade Server B to OSCE XG.

10. Register the OSCE server to TMCM if the original server has or requires it.

11. Add a Standalone Smart Protection Server if the original server has or requires it.

Chapter 4: Upgrade Verification

4.1 > Verifying if the OSCE server was upgraded properly

1. Confirm that the following services have the status "Running":
   - IIS Admin Service
   - World Wide Web Publishing Service
   - OfficeScan Master Service
   - OfficeScan Plug-in Manager
   - OfficeScan Active Directory Integration Service
   - OfficeScan Deep Discovery Service
   - OfficeScan Log Receiver Service
   - OfficeScan Control Manager Agent (This should be running if the OSCE server has been registered to TMCM.)
   - Trend Micro Smart Scan Server (This should be running if Integrated Smart Scan Server has been installed and enabled.)
   - Trend Micro Local Web Classification Server (This should be running if Integrated Smart Scan Server has been installed and Web Reputation Services has been enabled.)
   - Trend Micro Smart Protection Query Handler (This should be running if Integrated Smart Scan Server has been installed and both File Reputation Services and Web Reputation Services have been enabled.)

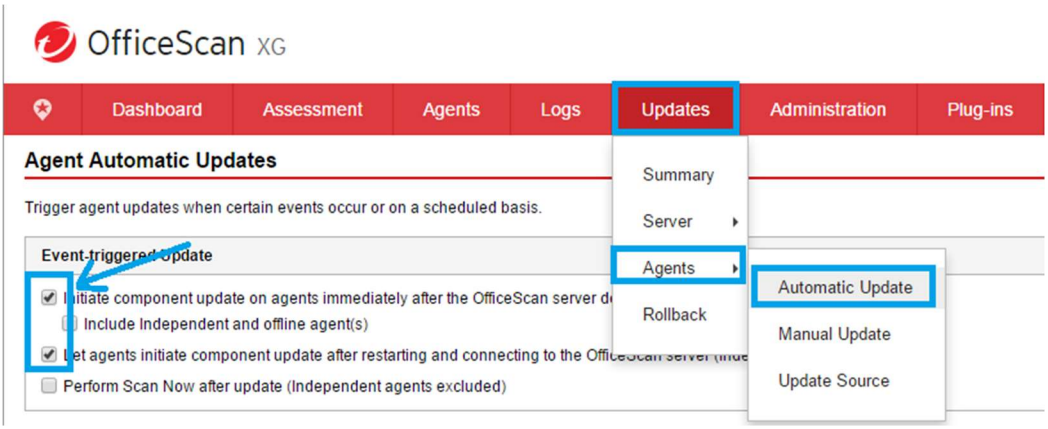
   If a service is not running, please try to start it manually. If any one of them fails to start, please contact Trend Micro Technical Support.
2. Confirm that the following processes are running in the Windows Task Manager:
   - DBServer.exe
   - fcgiOfcDda.exe
3. Confirm that the registry keys below exist:
   - 32-bit platform: [HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan]
   - 64-bit platform: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan]
4. Confirm that the OSCE web management console can be logged into using the default user name: root.

4.2 > Upgrading OSCE agents

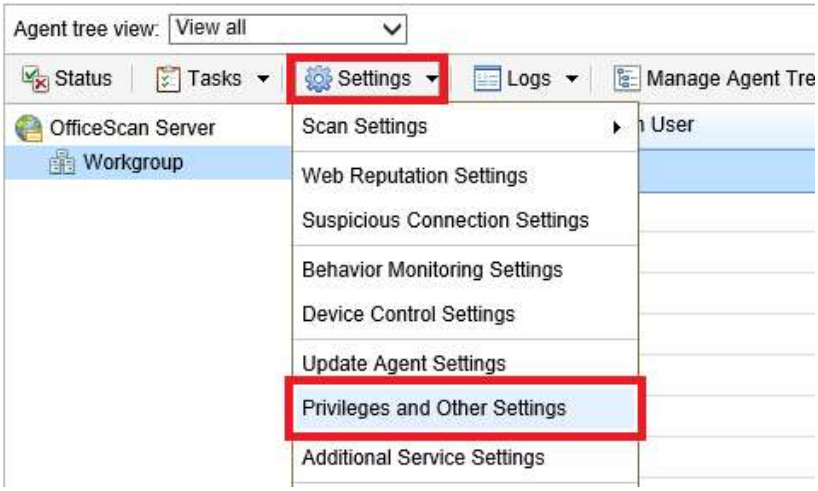
It is recommended that you upgrade the agents by parts, like upgrading serially for each domain, in order to avert huge network bandwidth consumption, high server workload, and any other unexpected issues. After confirming the upgraded agents do not have any problems, upgrade the rest of the agents.

To do this:

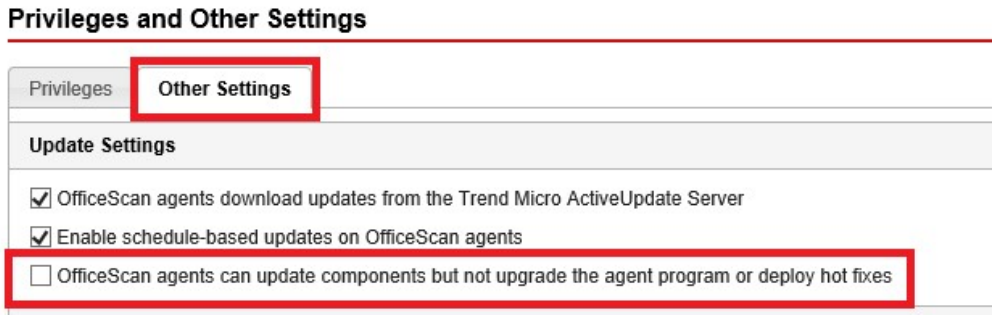
1. Log in to the web management console.
2. Go to **Updates** > **Agents** > **Automatic Update** and make sure that the following options are enabled:
   - "Initiate component update on agents immediately after the OfficeScan server downloads a new component"
   - "Let agents initiate component update after restarting and connecting to the OfficeScan server (roaming agents excluded)"



3. Go to **Agents** > **Agent Management**.
4. On the agent tree, select the agent or domain to be upgraded, then go to **Settings** > **Privileges and Other Settings**.



5. In Update Settings category under the Other Settings tab, make sure following option is unchecked: "OfficeScan agents can update components but not upgrade the agent program or deploy hot fixes".



6. Click **Save**.

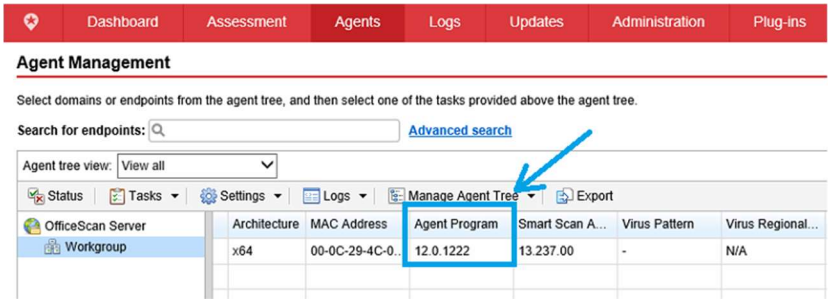
- After the above option has been unchecked, upgrading the targeted agent will start immediately after the agent initiates the component update.
- After the upgrade is complete, confirm that there are no further issues, then repeat steps 3 to 6 serially for all of the agents.

NOTE 🗎 All of the agents connected to the OSCE server will be upgraded. However, the agents that cannot receive notifications from the OSCE server, such as those behind a NAT environment, will NOT be upgraded. Those agents will be upgraded according to the start time of a scheduled-based update, so it will take some time before it starts upgrading.

A client package (EXE or MSI) can also be used to upgrade the agent.

4.3 > Verifying if the OSCE XG agent was properly upgraded

1. Log in to the OSCE XG server's web management console.
2. Go to **Agents** > **Agent Management**.
3. Select the upgraded agent on the agent tree and check if the "Agent Program" is 12.0.1222.



NOTE 🗎 In this example, the OSCE agent's version is 12.0.1222. Your OSCE agent's version may be higher than this.

Chapter 5: Plug-in Service Migration

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

IDF

For IDF used on the original server, deactivate the IDF agent and use TMVP instead.

TMSM

For TMSM used on the original server, please refer to the following article: https://success.trendmicro.com/solution/1055658.

iDLP

For iDLP used on the original server:

1. Install iDLP PLS on the new server, and then activate it.
2. Make sure the OfficeScan Master Service has been stopped.
3. Run ServerMigrationTool as Administrator [<OSCE Server folder>\PCCSRV\Admin\Utility\ServerMigrationTool] on the original 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 new 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 original server:

   <OSCE Server folder>\PCCSRV\Private\DLPForensicDataTracker.db

   Forensic folder: Please confirm the folder's location from <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

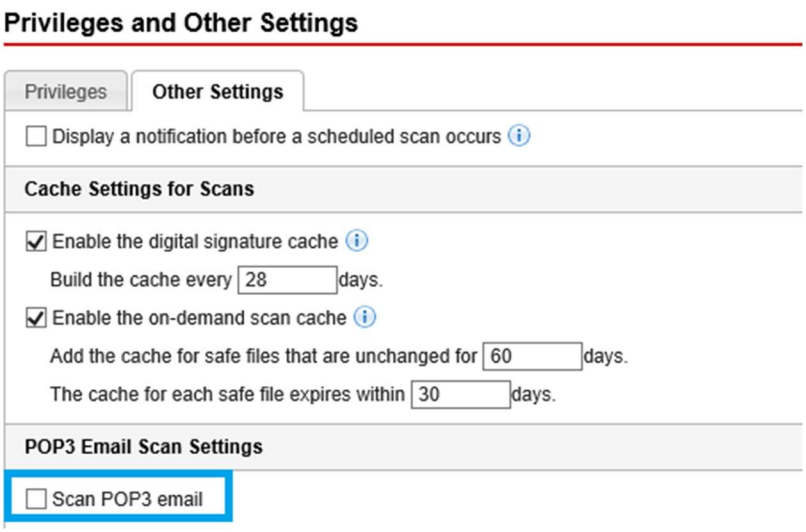
- When there is an Apache 2.2 service running on the OSCE server while upgrading to OfficeScan XG, the installer will stop the Apache 2.2 service. However, there is no impact to other version of Apache (e.g. Apache 2.4). The workaround is to manually start up Apache 2.2 after the upgrade has finished.

NOTE There is no impact on other version of the Apache service e.g. Apache 2.4.

Please clear the browser cache before logging in to the XG version's web management console.

- After upgrading to OSCE XG, the sender or the body of a received email may be missing on an agent computer that enabled POP3 Email Scan. The workaround is to disable POP3 Email Scan Setting for that agent:

  1. Log in to the OSCE web management console.
  2. Go to **Agents** > **Agent Management.**
  3. Select the problematic agent from the agent tree.
  4. Click **Settings** > **Privileges and Other Settings** > **Other Settings** tag.
  5. Uncheck "Scan POP3 email".



NOTE After this setting is disabled, the Real-Time Scan will be triggered while a file I/O occurs (e.g. opening an email or attached file), so there is no risk concern when disabling the "Scan POP3 email" feature.

- When upgrading by moving an agent to an OSCE XG server, the Common Firewall Pattern version may be "N/A". To resolve the issues:

  1. Stop the Cryptographic Services from the Microsoft Management Console.
  2. Navigate to C:\Windows\system32 and rename the "catroot2" folder to "oldcatroot2".

3. Start the Cryptographic Services.
4. Open a command prompt (cmd.exe) and run the following commands:
   - regsvr32 wintrust.dll
   - regsvr32 netcfgx.dll
5. Restart the endpoint.

- To perform agent web installation on endpoints with a 64-bit processor architecture, you must use the 32-bit version of Internet Explorer. The 64-bit version of Internet Explorer is not supported.
- The upgrade may fail if you are using an MSI package to upgrade an OSCE agent that was originally installed also using an MSI package. As a workaround:
  1. Ensure that the new MSI package has the same file name as the original package. If you do not know the file name of the original MSI package, check the following registry key: HKEY_CLASSES_ROOT\Installer\Products\F4D73DF48B1EA594592F1CD021C5A1C9\SourceList\PackageName.
  2. Install the new MSI package. Use Command Prompt to execute the package with the parameter "/fvo". For example, msiexec /fvo c:\temp\package.msi.
- There may be some applications that depend on the Microsoft driver HTTP.sys. If HTTP.sys driver fails to be stopped, the upgrading may be also fail.

  To avoid this issue:
  1. Stop the OfficeScan Master Service and make sure ofcservice.exe does not appear in the Task Manager Console. Server platform: Windows 2008 or Windows Server 2008 R2.
  2. Open cmd.exe using “Run as administrator”.
  3. Execute the following command net stop http. The following services will be shown:
     - Windows Remote Management
     - World Wide Web Publishing Service
     - Print Spooler
     - IIS Admin Service

NOTE There may be more services shown depending on the environment. All of them need to be restarted later after the OSCE upgrade finishes, so please take note of them.

  4. If the HTTP.sys driver fails to be stopped, it means that another application is using the driver. Manually stop the corresponding application:

```
The HTTP Service service is stopping.....
The HTTP Service service could not be stopped.
```

  5. Press “y” to continue.
  6. Upgrade the OSCE server.

7. Run Command Prompt as administrator and execute the following command: net start http.
8. Start the services stopped in step 3.

- When the Web Server (IIS or Apache) is being used by other applications, it may fail to be stopped, which causes the upgrade to fail. To prevent this, check if the Web Server (IIS or Apache) services can be restarted:
  1. Open the Windows Service Management Console (services.msc).
  2. Restart the service below from the console:
     - When using Apache: Apache2.2
     - When using IIS: World Wide Web Publishing Service

NOTE 🗎 For other applications that may be using the Web Server, please take action if it takes no effect.