OfficeScan Client / Server Edition 10.5 Best Practice Guide

Alp Deveci
Jill Chua-Maceda
Jessie Prevost
Alwin Yu
US Core Team
# Table of contents

1. **Product Description** ................................................................. 3  
2. **Architecture** ............................................................................. 4  
   2.1. Installation .................................................................................. 4  
      2.1.1. Recommended Hardware ...................................................... 4  
      2.1.2. Software Requirements ...................................................... 6  
2.2. Operating System and Related Applications .............................. 8  
      2.2.1. Security Tuning ................................................................. 10  
3. **Sizing Summary** ......................................................................... 11  
   3.1. Smart Protection Server Layout (Standalone) ............................ 13  
      3.1.1. Load Balancing ................................................................. 14  
      3.1.2. Deployment Recommendations ........................................ 14  
   3.2. Integrated Smart Protection Server Best Practices ................... 16  
   3.3. Configuration ............................................................................. 17  
      3.3.1. Management Console ....................................................... 20  
      3.3.2. INI Configuration Files ..................................................... 38  
   3.4. Performance Tuning ................................................................. 39  
4. **Backup and Disaster Recovery** ................................................ 40  
   4.1. OfficeScan Server Database Files ............................................ 40  
   4.2. OfficeScan Server Configuration Files ..................................... 40  
   4.3. OfficeScan Client Configuration Settings .................................. 41  
5. **Behavior Monitoring** ............................................................... 42  
   5.1. Behavior Monitoring Overview ............................................... 42  
      5.1.1. Malware Behavior Blocking .............................................. 42  
      5.1.2. Event Monitoring ............................................................. 43  
      5.1.3. Enabling Behavior Monitoring ......................................... 46  
   5.2. Device Control Overview ......................................................... 46  
      5.2.1. Using Device Control ......................................................... 46  
      5.2.2. How Behavior Monitoring and Device Control Can Affect Performance .......................................................... 48  
      5.2.3. Deploying Behavior Monitoring and Device Control .......... 48  
   5.3. Alternative Ways to Prevent Performance Impact .................... 50  
      5.3.1. Disabling Features from the Web Console ......................... 51  
      5.3.2. Stopping the Service ......................................................... 51  
6. **Miscellaneous** ............................................................................ 51  
   6.1 Product Communication Ports .................................................. 51  
   6.3 Update Architecture and Network Usage .................................. 52  
      6.3.1. The Update Process .......................................................... 52  
      6.2.2. Network Usage (Bandwidth Consumption) ...................... 54  
   6.4 Virtual Desktop Infrastructure (VDI) ........................................ 55  
      6.4.1. Golden Image Preparation ................................................ 56  
      6.4.2. Install the VDI Support in OfficeScan server Plugin Manager 56  
   6.5 Recommended Installation Adjustments for Special Environments 58  
      6.5.1. Migration of Unsupported Platforms .................................. 58  
      6.5.2. Citrix Environment .......................................................... 59  
      6.5.2.1. Installation of OfficeScan Clients on Citrix Servers .......... 59  
      6.5.2.2. Citrix Known Issues ..................................................... 60  
      6.5.2.3. Citrix Exclusions .......................................................... 61  
      6.5.2.4. Citrix Firewall Port ...................................................... 62  
   6.5.3. Installation of OfficeScan Clients on Cisco Callmanager ...... 62  
   6.6. Recommended Scan-Exclusion List .......................................... 63
1. **Product Description**

There are four major components in an OfficeScan environment that need to be identified when architecting the deployment. Each component is briefly described below.

A. **OfficeScan Server** – Provides the OfficeScan management console and stores information in a local CodeBase® database. Standard http / https protocols are used for communication and to provide updates to managed clients. The three basic functions of an OfficeScan server are:
   a. Client configuration (Privileges and Policy settings)
   b. Provides program, scan engine, and virus pattern file updates
   c. Reporting, centralized logging and quarantine

B. **OfficeScan Client** – A host reporting to a particular OfficeScan server. An OfficeScan client can be configured to get update information from an OfficeScan server, an Update Agent, or directly from the internet (Trend Micro ActiveUpdate server). An OfficeScan client can also be configured to use Integrated Smart Protection Server or Stand Alone Smart Scan instead of conventional scan. This method minimizes the amount of pattern download by relying on cloud technology.

C. **Update Agent** – A regular OfficeScan client that is designated to replicate update information from an OfficeScan server for the purposes of distributing the update information to other OfficeScan clients. Any client can be configured as an Update Agent via the OfficeScan server management console. OfficeScan client IP address ranges are then assigned to get update information from specific update agents. Update agents can push component updates, setting updates, and program/hotfix updates to clients. Older version OfficeScan clients can receive program upgrades from OfficeScan 10.5 Update Agents as long as they report to the OfficeScan 10.5 Update Agents.

D. **Smart Protection Server** – The Smart Protection Server provides the file reputation and web reputation through a local cloud service by scanning files and sending URLs to a local web rating server when using web reputation protection when users opt to employ Smart Scan technology. There are two types of Smart Protection Server:

   a. **Integrated Smart Protection Server** – Installed as part of the OfficeScan server. Integrated Smart Protection Server is managed through OfficeScan management console.
   b. **Stand Alone Smart Protection Server** – Installed on a VMware or Hyper-V host.
2. Architecture

2.1. Installation

2.1.1. Recommended Hardware

Following sections show the recommended software and hardware specifications for an OfficeScan environment. For the full list of minimum system requirements, please refer to the Installation and Deployment Guide or OfficeScan Readme.

A. OfficeScan Server

The recommended hardware specification for an OfficeScan server managing 5000 client workstations is:

- Server with at least 2GHz dual processor with 2GB of RAM: 3,000 to 5,000 clients
- Server with at least 3GHz dual processor with 4GB of RAM: 5,000 to 8,000 clients

**Note:** Integrated Smart Protection Server not recommended for more than 3000 Smart Scan Clients. Stand Alone Smart Protection Server is recommended for more than 3000 clients.

B. Update Agent

The OfficeScan client with the best available resources at a particular site should be designated as an Update Agent. Since this client will be the one serving updates to the other clients in the remote office, this client must be reliable. This can be a domain controller on the site, a file server, print server or any type of server that is online all the time. This client should have an additional 700 MB of free disk space to store the engines and patterns, an additional 160 MB for programs/hot fix update and you also need an additional 20KB for every domain setting updates. Minimum requirements for Update Agents should follow the minimum hardware requirements of OfficeScan Clients.

C. OfficeScan Clients

The minimum/recommended hardware specifications for the OfficeScan client are:

**Windows XP/2003**

- 300MHz Intel Pentium processor or equivalent
- 256MB of RAM (512MB recommended)
- 350MB of available disk space

**Windows XP/2003 64-bit**

- Intel x64 processor, AMD x64 processor
- 256MB of RAM (512MB recommended)
- 350MB of available disk space

**Windows Vista**

- 1GHz Intel Pentium processor or equivalent
- 1GB of RAM (1.5GB of RAM recommended)
- 350MB of available disk space

**Windows Vista 64-bit**
- Intel x64 processor, AMD x64 processor
- 1GHz Intel Pentium processor or equivalent
- 1GB of RAM (1.5GB of RAM recommended)
- 350MB of available disk space

**Windows 7 32 bit**
- 1GHz Intel Pentium processor or equivalent (2GHz recommended)
- 1GB of RAM (2GB of RAM recommended)
- 350MB of available disk space

**Windows 7 64 bit**
- Intel x64 processor, AMD x64 processor
- Minimum 2GHz Intel Pentium processor or equivalent
- 1.5GB of RAM
- 350MB of available disk space

**Windows 2008**
- 1GHz Intel Pentium processor or equivalent (2GHz recommended)
- 512MB of RAM (2GB of RAM recommended)
- 350MB of available disk space

**Windows 2008 64-bit**
- Intel x64 processor, AMD x64 processor
- 1.4GHz Intel Pentium processor or equivalent (2GHz recommended)
- 512MB of RAM (2GB of RAM recommended)
- 350MB of available disk space

**Windows 2008 R2 64-bit**
- 1.4GHz Intel Pentium processor or equivalent (2GHz recommended)
- 512MB of RAM (2GB of RAM recommended)
- 350MB of available disk space

**D. Integrated Smart Protection Server**
The minimum hardware specifications for Integrated Smart Protection Server are:
- Minimum 1.86 GHz Intel Core2Duo
- 1GB of RAM (2GB recommended)
- 3.2GB of available disk space

**E. Smart Protection Server (Standalone)**
The minimum hardware specifications for Standalone Smart Protection Server are:
- Dual 2.0 GHz Intel Core2Duo 64-bit processor supporting Intel Virtualization Technology or equivalent
- 1GB of RAM
• 20GB recommended for virtualization requirements if fewer than 1,000 endpoints. Add 15GB for every 1,000 endpoints.

**NOTE:** Trend Micro ™ Smart Protection Server automatically partitions the detected disk space as required

### 2.1.2. Software Requirements

#### A. OfficeScan Server

- Microsoft Windows Server 2003 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit/64-bit versions
- Microsoft Windows Server 2003 R2 (Standard, Enterprise, and Datacenter Editions) with Service Pack 2 or later, 32-bit/64-bit versions
- Microsoft Windows Storage Server 2003 (Basic, Standard, Enterprise, and Workgroup Editions) with Service Pack 2, 32-bit and 64-bit versions
- Microsoft Windows Storage Server 2003 R2 (Basic, Standard, Enterprise, and Workgroup Editions) with Service Pack 2, 32-bit and 64-bit versions
- Microsoft Windows Cluster Server 2003
- Microsoft Windows Server 2008 (Standard, Enterprise, Datacenter and Web Editions) with Service Pack 1 or 2, 32-bit and 64-bit versions
- Windows Server 2008 R2 (Standard, Enterprise, Datacenter and Web Editions), 64-bit version
- Windows Storage Server 2008 (Basic Edition), 32-bit and 64-bit versions
- Windows Storage Server 2008 (Standard, Enterprise, and Workgroup Editions), 64-bit version
- Microsoft Windows HPC Server 2008

**Note:** OfficeScan cannot be installed if Microsoft Windows 2008 runs on the Server Core environment.

OfficeScan supports server installation on guest Windows 2003/2008 operating systems hosted on the following virtualization applications:

- Microsoft Virtual Server 2005 R2 with Service Pack 1
- VMware ESX/ESXi Server 4 (Server Edition)
- VMware Server 2 (Server Edition)
- VMware Workstation and Workstation ACE Edition 7.0
- VMware vCenter™4
- Citrix™ XenServer™ 5.5
- Microsoft Windows Server 2008 64-bit Hyper-V™
- Microsoft Windows Server 2008 R2 64-bit Hyper-V
- Microsoft Hyper-V Server 2008 R2 64-bit

#### B. OfficeScan Clients

- Microsoft Windows XP Professional with Service Pack 2 or later, 32-bit/64-bit versions
- Microsoft Windows XP Home with Service Pack 2 or later, 32-bit version
- Microsoft Windows Server 2003 (Standard, Enterprise, Datacenter, and Web Editions) with Service Pack 2 or later, 32-bit/64-bit version
• Microsoft Windows Server 2003 R2 (Standard, Enterprise, Datacenter) with Service Pack 2 or later, 32-bit/64-bit versions
• Microsoft Windows Storage Server 2003, 32-bit/64-bit versions
• Microsoft Windows Storage Server 2003 R2, 32-bit/64-bit versions
• Microsoft Windows Server 2008 (Standard, Enterprise, Datacenter, and Web Editions) with Service Pack 1 or 2, 32-bit/64-bit versions
• Windows Storage Server 2008 (Basic Edition), 32-bit and 64-bit versions
• Windows Storage Server 2008 (Standard, Enterprise, and Workgroup Editions), 64-bit version
• Microsoft Windows Server 2008 R2 (Standard, Enterprise, Datacenter, and Web Editions) 64-bit version
• Microsoft Windows HPC Server 2008
• Windows Vista™ (Business, Enterprise, Ultimate, Home Premium, Home Basic) with Service Pack 1 or 2
• Microsoft Windows 7 (Home Basic, Home Premium, Ultimate, Professional, Enterprise), 32-bit/64-bit versions

Note: OfficeScan cannot be installed if Windows 2008 runs on the Server Core environment

OfficeScan supports client installation on guest operating systems hosted on the following virtualization applications:
• Microsoft Virtual Server 2005 R2 with Service Pack 1
• VMware ESX/ESXi Server 4 (Server Edition)
• VMware Server 2 (Server Edition)
• VMware Workstation and Workstation ACE Edition 7.0
• VMware vCenter 4
• Citrix XenServer 5.5
• Microsoft Windows Server 2008 64-bit Hyper-V
• Microsoft Windows Server 2008 R2 64-bit Hyper-V
• Microsoft Hyper-V Server 2008 R2 64-bit

The administrator will not be able to remotely install OfficeScan client to Windows 7 x86 platforms without enabling the default administrator account. To resolve this issue:
• Enable the Remote Registry service on the Windows 7 machine. By default, Windows 7 machines disable this feature.
• Option A: Use the domain administrator account to remotely install OfficeScan 10.5 Service Pack 1 clients to Windows 7 computers.
• Option B: Use the default administrator account:
  1. Type the "net user administrator /active: yes" command from the command console to enable the default administrator account.
  2. Use the default administrator account to remotely install the OfficeScan client to the Windows 7 machine

C. Smart Protection Server (Standalone)
Smart Protection Server has the following VMware Support requirements:

- VMware ESX 3.0, 3.5 or 4.0
- VMware ESXi 3.5 Update 2 or 4.0
- VMware Server 2.0
- Windows 2008 R2 Hyper-V

**NOTE:** A purpose-built, hardened, and performance-tuned 64-bit Linux operating system is included with Trend Micro Smart Protection Server

The following requirements are recommended for Trend Micro Smart Protection Server as a Virtual Machine under Windows 2008 R2 Hyper-V, VMware Server 2.0, VMware ESX 3.0, 3.5, 4.0 or VMWare ESXi 3.5 Update 2, 4.0

- Create a new Virtual Machine with Red Hat Enterprise Linux 5 64-bit (Red Hat Enterprise Linux 4 64-bit for VMware ESX 3.0)
- Allocate this Virtual Machine with at least 1GB RAM and Dual 2.0 GHz CPU resources.
- Create a new Virtual Disk image which will be sufficient for your logging requirements.
- Allocate 1 physical network card for the virtual switch where Trend Micro Smart Protection Server is connected.

**Account**

Administrator or Domain Admin account to log-in to target hosts for installation.

**Ports**

- NetBIOS (445, 137,138,139) for NT Remote Install
- OfficeScan client port (defined during OfficeScan server installation and is saved under Ofcscan.ini Client_LocalServer_Port parameter).

**OfficeScan** virtual directory port as defined in Apache / IIS. This value needs to be consistent with what is defined in the OfficeScan management console [Administration | Connection Settings | port number].

**Bandwidth**

Approximately 50 MB (may vary depending on current virus pattern file size)

**Others**

Remote Registry service is enabled on target host.

System partition of the target host is administratively shared (C$).

Windows XP Simple File Sharing must be disabled on the client machines. SFS is a Microsoft feature that forces all network connections to login as Guest even if alternate credentials are provided. When SFS is enabled, OSCE can't login to the machine using the credentials specified, so the installation fails. SFS can be disabled via GPO or a registry hack. It can be disabled in the target machines individually under [My Computer | Tools | Folder Options | View | Use Simple File Sharing (Recommended)] option.

### 2.2. Operating System and Related Applications

#### A. TCP Stack

The OfficeScan server may receive and establish multiple HTTP sessions to communicate with its clients. The TCP properties of Windows can be modified to prevent delays and slowdowns caused by TCP time-wait accumulation and port exhaustion. Add or modify the following registry keys as recommended to improve TCP performance.

**MaxUserPort**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort  
Data type: REG_DWORD  
Default value: 5000  
Range: 5,000–65,534 (port number)  
Purpose: Determines the highest port number TCP can assign when an application requests an available user port from the system.  
Trend Recommendation: 65,534

**TcpTimedWaitDelay**  
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay  
Data type: REG_DWORD  
Default value: 0xF0 (240 seconds = 4 minutes)  
Range: 0x1E 0x12C (30–300 seconds)  
Purpose: This determines the time that must elapse before TCP can release a closed connection and reuse its resources.  
Trend Recommendation: 30

**NOTE:** These changes will require a reboot.

**B. Microsoft IIS / Apache Web Server**

The OfficeScan server uses either Apache or Windows IIS to communicate with its clients. The application’s CGI timeout can be increased to allow more time for the server and client to communicate with each other. The *Remote Install* deployment method is dependent on this timeout as well. Copy process for the installation files over a slow link may cause installation failures.

**Microsoft IIS**

To modify IIS CGI settings, download and install *MetaEdit* or *Metabase Explorer* depending on the version of IIS in use.

1. Download and install a copy of *MetaEdit* for IIS 4 and 5 from Microsoft’s Support page  
   [http://support.microsoft.com/kb/301386](http://support.microsoft.com/kb/301386)  
   For IIS 6, download Metabase Explorer from  

2. Install MetaEdit / Metabase Explorer.

3. After installation, open [Start | All Programs | Administrative Tools | MetaEdit <version number>]  
   Or  
   [Start | All Programs | IIS Resources | Metabase Explorer | Metabase Explorer]

4. In the MetaEdit or Metabase Explorer console, Locate the key [LM | W3SVC | 6033]. This corresponds to the CGITimeout key.

5. Double-click 6033 key to edit its properties. Set data parameter to 3600. Click OK to save changes.

   For Microsoft IIS 7 on Windows 2008:

1. Download and install the Microsoft Administration Pack for IIS 7.0
http://www.iis.net/downloads/default.aspx?tabid=34&g=6&i=1682

Or use the default IIS Manager that comes with IIS 7.0

2. Open IIS Manager
3. Select the Server in the Connections Tree View, then select the OfficeScan site
4. In Features view, double-click CGI
5. Type the appropriate time-out value in Timeout (hh:mm:ss) text box, 00:60:00, press ENTER, and click Apply.

**Apache**

Follow the procedure below to modify Apache’s CGI timeout:

1. Open `<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\apache2\conf\httpd.conf` configuration file.
2. Set Timeout 300 to Timeout 600.
3. Restart the Apache service.

*Note: The definition of the Apache timeout is different from the IIS CGI timeout. With IIS, a CGI timeout of 300 seconds means that the CGI (e.g. cgiremoteinstall) must finish within 300 seconds or the session is timed out. In Apache, the timeout parameter of 300 seconds means that if there is "no action" (or no next action) for 300 seconds, the session is timed out.*

### 2.2.1. Security Tuning

The following are recommended permission settings to the OfficeScan folders and files. These are already set as default during installation:

<table>
<thead>
<tr>
<th>Directory/User</th>
<th>Administrator</th>
<th>Everyone</th>
<th>User</th>
<th>System User</th>
<th>Network Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>\PCCSRV</td>
<td>Full control</td>
<td>RX</td>
<td>N/A</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\HTTPDB</td>
<td>Full control</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Log</td>
<td>Full control</td>
<td>N/A</td>
<td>N/A</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Temp</td>
<td>Full control</td>
<td>N/A</td>
<td>R</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Private</td>
<td>Full control</td>
<td>N/A</td>
<td>N/A</td>
<td>Full control</td>
<td>RX</td>
</tr>
<tr>
<td>\PCCSRV\Download</td>
<td>Full control</td>
<td>N/A</td>
<td>R</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Web</td>
<td>Full control</td>
<td>N/A</td>
<td>R</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Web\Cgi</td>
<td>Full control</td>
<td>N/A</td>
<td>RX</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Web\OSCE\Web\console</td>
<td>Full control</td>
<td>RX</td>
<td>N/A</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Web\OSCE\web\console\RemoteInstallCGI</td>
<td>Full control</td>
<td>N/A</td>
<td>R</td>
<td>Full control</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Web\OSCE\web\console\ClientInstall</td>
<td>Full control</td>
<td>N/A</td>
<td>RX</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>\PCCSRV\Virus</td>
<td>Full control</td>
<td>N/A</td>
<td>RW</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
There are times that the permission might have been changed accidentally. To reset the permissions back to default:

1. Open command prompt
2. Browse to the OfficeScan server’s PCCSRV folder (i.e. drive:\Program Files\Trend Micro\OfficeScan\PCCSRV)
3. Run the following command: SVRSVCSETUP.EXE -setprivilege

3. **Sizing Summary**

**Important Note:** This information can be used as a starting reference. Actual performance will vary depending on features enabled, topology, performance tweaks, and scan-exclusions as outlined throughout this best practice document.

The recommendations below can be used as a guideline to determine the location and number of OfficeScan servers needed to effectively manage your Local / Wide Area Network.

1. A single OfficeScan server is recommended to manage up to approximately 5,000 – 8,000 clients and Integrated Scan Server can manage 3000 smart clients. Stand Alone Scan Server is recommended for clients over 3000.

2. OfficeScan servers managing clients across the WAN is recommended to be installed on sites with the healthiest bandwidth (typically datacenters or head offices).

3. Consider installing a local OfficeScan server for sites with approximately 500 or more clients. This is recommended if WAN bandwidth is limited for a particular site.

4. An Update Agent is a regular OfficeScan client that is designated to replicate update information from an OfficeScan server for the purposes of distributing the update information to other OfficeScan clients.
Sample OfficeScan Deployment Architecture

Sample Deployment Architecture
This table can be used as a template to scope the different sites and generate an architecture proposal.

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>No. of CLIENTS</th>
<th>Office Scan INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORTH AMERICA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td>1400</td>
<td>OSCE Server for North America WAN</td>
</tr>
<tr>
<td>New York</td>
<td>1000</td>
<td>Integrated Scan Server for North America</td>
</tr>
<tr>
<td>Chicago</td>
<td>600</td>
<td>Local OSCE Server</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>500</td>
<td>Local OSCE Server</td>
</tr>
<tr>
<td>Dallas</td>
<td>71</td>
<td>Update Agent</td>
</tr>
<tr>
<td>San Jose</td>
<td>52</td>
<td>Update Agent</td>
</tr>
<tr>
<td>Memphis</td>
<td>35</td>
<td>Update Agent</td>
</tr>
<tr>
<td>Toronto</td>
<td>1200</td>
<td>Local OSCE Server</td>
</tr>
<tr>
<td>Dallas</td>
<td>25</td>
<td>Update Agent</td>
</tr>
</tbody>
</table>
### 3.1. Smart Protection Server Layout (Standalone)

Trend Micro recommends using Standalone Smart Protection Server if the number of smart clients will be more than 3000 instead of Integrated Smart Protection Server. Customers can also choose to install Standalone Smart Protection Server if they do not want to use Integrated Smart Protection Server.

If there are a lot of users at each site then the load can be distributed by adding more Standalone Smart Protection Servers.

If the latency is huge between the branch office and the main office, it is recommended to install a Smart Protection Server (standalone) on the branch office. If Smart Protection Server (standalone) cannot be installed or there are no available hardwares then it would be best to switch the clients to conventional scan.

### Smart Protection Server Sizing Recommendations
### 3.1.1. Load Balancing

Smart Protection Servers can be setup in order to achieve load balancing. Load balancing will help ensure http requests can be distributed among the Smart Protection Servers.

There are two ways to achieve load balancing from OfficeScan console:

1. **Random** – This will ensure that clients will randomly choose a Smart Protection Server from the list.
2. **Based on IP range** – Smart clients will update from the Smart Protection Server list they have been assigned to.

### 3.1.2. Deployment Recommendations

**Smart Protection Server Redundancy**

Smart Protection Servers should always be installed in redundant pairs to avoid WAN saturation in the event of a hardware failure.
Full System Scans

Initial scans require more requests to the Smart Protection Server as seen in the tables below. Clients should schedule their first scheduled scan in phases, especially when their Smart Protection Server is centrally located. Running scheduled scans in batches will increase capacity and normalize iCRC network utilization.

Performance Data: 1st Scheduled Scan Only

<table>
<thead>
<tr>
<th>Platform</th>
<th>Network Bandwidth</th>
<th>Concurrent Connection</th>
<th>Transaction Rate per Second</th>
<th>Latency TTFB (ms)</th>
<th>Throughput (bytes per second)</th>
<th>Network Usage Inbound/Outbound (mbps)</th>
<th>CPU Usage (%)</th>
<th>Memory Usage (MB)</th>
<th>Maximum Total User Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMEX v3.5 with 4 vCPUs</td>
<td>1G</td>
<td>5,180</td>
<td>2,022</td>
<td>235</td>
<td>861,13 5</td>
<td>12 / 16</td>
<td>98.4</td>
<td>1,020</td>
<td>20,700</td>
</tr>
<tr>
<td>VMEX v3.5 with 2 vCPUs</td>
<td>1G</td>
<td>2,880</td>
<td>1,200</td>
<td>128</td>
<td>511,28 9</td>
<td>7 / 9</td>
<td>99.2</td>
<td>707</td>
<td>11,500</td>
</tr>
<tr>
<td>VM Server with 2 vCPUs</td>
<td>1G</td>
<td>1,980</td>
<td>860</td>
<td>200</td>
<td>366,02 5</td>
<td>5 / 6</td>
<td>99.1</td>
<td>663</td>
<td>7,900</td>
</tr>
<tr>
<td>VMEX v4.0 with 8 vCPUs</td>
<td>1G</td>
<td>10,980</td>
<td>3,888</td>
<td>288</td>
<td>1,660,3 60</td>
<td>24 / 31</td>
<td>99.88</td>
<td>1,860</td>
<td>43,900</td>
</tr>
<tr>
<td>VMEX v4.0 with 4 vCPUs</td>
<td>1G</td>
<td>6,180</td>
<td>2,371</td>
<td>390</td>
<td>1,011,7 31</td>
<td>15 / 19</td>
<td>98.12</td>
<td>1,269</td>
<td>24,700</td>
</tr>
<tr>
<td>VMEX v4.0 with 2 vCPUs</td>
<td>1G</td>
<td>3,080</td>
<td>1,262</td>
<td>322</td>
<td>538,35 3</td>
<td>8 / 10</td>
<td>99.34</td>
<td>845</td>
<td>12,300</td>
</tr>
<tr>
<td>Hyper-V with 4 vCPUs (*)</td>
<td>1G</td>
<td>1,420</td>
<td>590</td>
<td>70</td>
<td>252,02 7</td>
<td>2 / 3</td>
<td>66.31</td>
<td>511</td>
<td>5,600</td>
</tr>
<tr>
<td>Hyper-V with 2 vCPUs (*)</td>
<td>1G</td>
<td>1,075</td>
<td>362</td>
<td>431</td>
<td>154,22 5</td>
<td>2 / 2</td>
<td>95.05</td>
<td>499</td>
<td>4,300</td>
</tr>
</tbody>
</table>

*Transaction rate: 0.5 Requests/Sec

Performance Data: Repeat Scheduled Scan or Real Time Scanning

<table>
<thead>
<tr>
<th>Platform</th>
<th>Network Bandwidth</th>
<th>Concurrent Connection</th>
<th>Transaction Rate per Second</th>
<th>Latency TTFB (ms)</th>
<th>Throughput (bytes per second)</th>
<th>Network Usage Inbound/Outbound (mbps)</th>
<th>CPU Usage (%)</th>
<th>Memory Usage (MB)</th>
<th>Maximum Total User Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMEX v3.5 with 4 vCPUs</td>
<td>1G</td>
<td>4,680</td>
<td>1,413</td>
<td>207</td>
<td>601,629</td>
<td>13 / 18</td>
<td>98.9</td>
<td>1,006</td>
<td>93,600</td>
</tr>
<tr>
<td>VMEX v3.5 with 2 vCPUs</td>
<td>1G</td>
<td>2,380</td>
<td>797</td>
<td>123</td>
<td>339,137</td>
<td>7 / 10</td>
<td>98.9</td>
<td>664</td>
<td>47,600</td>
</tr>
<tr>
<td>VM Server with 2 vCPUs</td>
<td>1G</td>
<td>1,580</td>
<td>562</td>
<td>172</td>
<td>239,216</td>
<td>5 / 7</td>
<td>99.1</td>
<td>634</td>
<td>31,600</td>
</tr>
<tr>
<td>VMEX v4.0 with 8 vCPUs</td>
<td>1G</td>
<td>10,850</td>
<td>2,692</td>
<td>97</td>
<td>1,149,211</td>
<td>26 / 35</td>
<td>99.86</td>
<td>1,718</td>
<td>211,600</td>
</tr>
<tr>
<td>VMEX v4.0 with 4 vCPUs</td>
<td>1G</td>
<td>5,580</td>
<td>1,654</td>
<td>262</td>
<td>70,569</td>
<td>16 / 21</td>
<td>98.65</td>
<td>1,230</td>
<td>111,600</td>
</tr>
<tr>
<td>VMEX v4.0 with 2 vCPUs</td>
<td>1G</td>
<td>2,580</td>
<td>854</td>
<td>64</td>
<td>364,098</td>
<td>8 / 10</td>
<td>96.45</td>
<td>782</td>
<td>51,600</td>
</tr>
<tr>
<td>Hyper-V with 4 vCPUs (*)</td>
<td>1G</td>
<td>1,280</td>
<td>385</td>
<td>78</td>
<td>164,651</td>
<td>2 / 3</td>
<td>63.49</td>
<td>449</td>
<td>25,600</td>
</tr>
<tr>
<td>Hyper-V with 2 vCPUs (*)</td>
<td>1G</td>
<td>1,058</td>
<td>224</td>
<td>311</td>
<td>95,290</td>
<td>1 / 2</td>
<td>91.84</td>
<td>500</td>
<td>21,100</td>
</tr>
</tbody>
</table>

*Transaction rate: 0.004 Requests/Sec
3.2. Integrated Smart Protection Server Best Practices

- When opting to use the Integrated Smart Protection Server, make sure that it is actually installed and running. If Integrated Smart Protection Server is not properly installed then smart clients will be disconnected and will not be utilizing the cloud technology properly.

**WARNING!** If you are using Microsoft IIS as your Web Server, monitor the IIS logs generated by Integrated Smart Protection Server. With an environment of around 1000 machines, the daily log size can easily go up to 250MB. IIS doesn’t delete old IIS logs by default and this can easily consume all the available free space on the OfficeScan server.

Make sure the above setting “Do not save encrypted pages to disk” is not enabled in IE in order to check for whether Integrated Smart Protection Server is running or not. After checking the setting above, type the URL below into your browser:

https://Officescan_server:port/tmcss/?LCRC=08000000BCB3080092000080C4F01936D430000

Once you enter you should see the following pop up which will confirm that Integrated Smart Protection Server is running.
1. Ensure that OfficeScan clients can query at least two Scan servers. This avoids the creation of single-point of failure. In order to take advantage of cloud technology fully, all clients must be online and connected to a Smart Protection Server. To add Smart Protection Servers go to [Smart Scan | Scan Source] then choose [Internal Clients] tab. Choose a standard list or a customer list based on IP address then click on Notify All Clients to push this setting.

2. Do not use Smart Scan as the default scanning method at the root level. Always use Conventional Scan as the root level scanning method. When you're selecting OfficeScan clients to use Smart Scan, always choose a regular domain instead of a root level. If root level is selected as Smart Scan method, before a new client is installed, and if this client is placed in a domain where it uses Conventional Scan, it will download Conventional Scan components.

   WARNING! When a client is switched from Smart Scan to Conventional Scan, OfficeScan client will download full pattern file if a conventional pattern file is not present or is more than 14 patterns behind.

3. Make sure Computer Location settings have correct settings OfficeScan clients can connect to. Computer Location setting can be reached by [Networked Computers | Computer Location]. The default setting is “Client connection status”. OfficeScan clients that can connect to the OfficeScan server or any of the reference servers are located internally, which means if these clients use smart scan, they will connect to a local Smart Protection Server. If connection cannot be established, these clients will be located externally and connect to the Trend Micro Global Smart Protection Server. If “Gateway IP address” setting is applied and the client computer’s gateway IP address matches any of the gateway IP addresses you specified on the Computer Location screen, the computer’s location is internal. Otherwise, the computer’s location is external.

3.3. Configuration

Majority of the product default configurations provide substantial security with a consideration on server/network performance. The information below are different recommendations, and can be used as an additional reference to either enhance security, or achieve better performance.
NOTE: Following notifications in UI shows these features are turned off by default on Windows Server platforms.

**Behavior Monitoring Settings**

- **OfficeScan automatically disables this feature on Windows server platforms. Refer to the Online Help for more information.**
- **Behavior Monitoring supports only 32-bit platforms.**

**Device Control Settings**

- **OfficeScan automatically disables this feature on Windows server platforms. Refer to the Online Help for more information.**
- **Device Control supports only 32-bit platforms.**

**Client Self-protection**

- **IMPORTANT:** OfficeScan automatically disables this feature on Windows server platforms. Refer to the Online Help for more information.
- Protect files in the OfficeScan client installation folder
- Protect OfficeScan client processes
- Protect OfficeScan client registry keys
- Protect OfficeScan client services

To turn on these features administrators should enable “Unauthorized Change Prevention Service” (TMBMSRV.EXE) and “Firewall Service” under “Additional Service Settings” for server platforms as needed.

*Path: Networked Computers -> Client Management -> Settings -> Additional Service Settings.*

**WARNING:** Enabling or disabling the Firewall service temporarily disconnects the clients from the network. Ensure that you change the settings only during non-critical hours to minimize network interruptions.

Administrators can turn on “Unauthorized Change Prevention Service” on a single server platform by enabling/disabling it through “Additional Service Settings”. Administrators can also enable/disable “Unauthorized Change Prevention Service” on Workstations by selecting a root/domain/single client/multi-select client.
3.3.1. Management Console

<table>
<thead>
<tr>
<th>SECURITY COMPLIANCE</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Assessment</td>
<td>***Select an OfficeScan domain to run compliance report on the clients to see which clients are incompatible with server. In “Scan Compliance” view, specify one or both of the following: • Number of days a client has not performed Scan Now or Scheduled Scan • Number of hours the remote or scheduled scan task has been running</td>
</tr>
<tr>
<td>Compliance Report</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Compliance Report</td>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td>Scheduled Compliance Report</td>
<td><em><strong>Report can show status of OfficeScan client services, components, Scan compliance, and settings to find incompliant clients. This can be run on daily basis if needed. Trend Micro recommends enabling on-demand assessment to perform real-time queries for more accurate results. You can also disable on-demand assessment wherein OfficeScan queries the database instead of each client. This option may be quicker but produces less accurate results.</strong></em></td>
</tr>
<tr>
<td></td>
<td>a. The SMTP setting in notification page is needed for sending the scheduled compliance report to user. Follow these steps to complete the settings:</td>
</tr>
<tr>
<td></td>
<td>Go to Notification &gt; Administrator Notifications &gt; General Settings page, fill in the fields “SMTP server”, “Port number” and “From” in Email Notification section and click Save.</td>
</tr>
<tr>
<td></td>
<td>2. “Scan Compliance” view uses the configurations that were used to do manual assessment last time.</td>
</tr>
</tbody>
</table>

Outside Server Management
Define
Active Directory Scope

Advanced Settings
Specify Ports

Declare a computer unreachable by checking port

***Select OU’s containing less than 1000 account of computers for performance baseline then increase and decrease number of computers according to performance

***Make sure to add all OSCE server communication ports
135

***Different port can be chosen but make sure it is a common port that will be available on all
<table>
<thead>
<tr>
<th>Settings</th>
<th>the computers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable scheduled query for once a week to find out clients that do not have OfficeScan client.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SCAN METHODS</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Methods</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Conventional Scan</strong></td>
<td><em><strong>Conventional scan leverages anti-malware and anti-spyware components stored locally on endpoints.</strong></em></td>
</tr>
<tr>
<td><strong>Smart Scan</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Smart Scan now is default at the ROOT domain level. Smart Scan method should be selected at the Domain level so this way if a user installs a client it is easier to move from conventional scan to Smart scan.</strong>*</td>
</tr>
<tr>
<td></td>
<td><strong>Smart Scan leverages anti-malware and anti-spyware signatures stored in-the-cloud.</strong>*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MANUAL SCAN SETTINGS</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virus / Malware Scan Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Target Tab</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Files to scan</strong></td>
<td></td>
</tr>
<tr>
<td>All Scannable</td>
<td><em><strong>Selecting All Scannable Files improves security by only scanning all known to potentially carry malicious code. Using this setting also allows you to utilize True File Type scanning.</strong></em></td>
</tr>
</tbody>
</table>

| **Scan Settings** |                           |
| **Scan Hidden Folders** | Enabled                     |
| **Scan Network Drive** | Enabled                     |
| **Scan compressed files** | Enabled                     |
| **Scan OLE objects** |                           |
| **Detect exploit code in OLE files** |                           |

| **Virus/Malware Settings only** |                           |
| **Scan Boot Area** | Enabled                     |
| **CPU Usage** | Medium                     |
| **Scan Exclusions** | Enable Scan Exclusion |
| **Refer to section 6.6 Recommended Scan-Exclusion List for recommendations on files** |
Apply scan exclusion settings to all scan types
Exclude directories where Trend Micro products are installed

**Action Tab**

**Virus/Malware**
- Use Active Action
- Customize action for probable virus/malware
- Back up files before cleaning
- Enable system clean up for probable virus/malware

**Spyware/Grayware**
- Clean

**REAL-TIME SCAN SETTINGS**
- Enable virus / malware scan
- Enable spyware / grayware scan

**Target Tab**

**User Activity on Files**
- Scan files being created/modified and retrieved

**Files to scan**
- File types scanned by Intelliscan

**Scan Settings**
- Scan floppy disk during system shutdown
- Scan Network Drive
- Scan Compressed Files
- Scan OLE Objects

Notes and Recommendations
- **Enable virus / malware scan**
- **Enable spyware / grayware scan**
- **Create/modified and retrieved**
- **File types scanned by Intelliscan**
- **Enabled**
- **Scan Compressed Files**
- **Scan OLE Objects**

and directories to exclude.

Disabled
Enabled

Enabled
***This setting will utilize the Trend Micro recommended settings for each type of virus/malware.

Enabled
***Select Quarantine to have the ability to restore any files that are needed.

Enabled

Enabled

Enabled

Enable virus / malware scan
Enable spyware / grayware scan

Created/modified and retrieved
***In cases where the system is heavily accessed such as File servers, it may be advisable to select Scan files being created / modified but only use this option if the server performance is affected.

Enabled
***Selecting intelliscan slightly improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows you to utilize True File Type scanning.

Disabled
***For additional security, it is recommended that this setting be enabled. Note that in some environments, this setting may cause performance issues, please disable if issues are encountered.

Enabled
***Scanning 2 layers is reasonable. Increasing the level may cause performance issues. Compressed files are scanned in real-time when extracted.

Enabled
***Scanning 3 layers is reasonable.
Detect exploit code in OLE files

**Virus/Malware Scan Settings Only**
Enable Intellitrap

**Scan Exclusion**
Enable Scan Exclusion

Apply scan exclusion settings to all scan types
Exclude directories where Trend Micro products are installed

**Action Tab**
**Virus/Malware**
Use Active Action

Customize action for probable virus/malware

Back up files before cleaning
Display a notification message on the client computer when virus/malware is detected

Display a notification message on the client computer when probable virus/malware is detected

Enable system clean up for probable virus/malware

**Spyware Grayware**
Clean
Display a notification message on the client computer when virus/malware is detected

Enable system clean up for probable virus/malware

**SCHEDULED SCAN SETTINGS**

Enable Virus / Malware Scan

Enable spyware/grayware scan

**Target Tab**
**Schedule**
Weekly on Friday 12pm

**Files to scan**
All Scannable Files

**Notes and Recommendations**

Enabled
***This setting heuristically identifies malware by checking Microsoft Office files for exploit code.

Enabled
***Turn off this setting on special cases if users regularly exchange/access compressed executable files in real-time.

Enabled
***Refer to 6.6 Recommended Scan-Exclusion List for recommendations on files and directories to exclude.

Disabled
Enabled

Enabled
***This setting will utilize the Trend Micro recommended settings for each type of virus/malware.

Enabled
***Select Quarantine to be able to restore any files that are needed

Enabled
***Turn off this setting to avoid end users to see popup messages which can generate helpdesk calls.

Disabled
***Turn off this setting to avoid end users to see popup messages which can generate helpdesk calls.

Enabled
**Suggested to scan during lunch time or after office hours if machine remain turned on.**

Enabled
***Selecting All Scannable Files improves security by only scanning all known to**
Scan settings
Scan compressed files

Scan OLE objects
Detect exploit code in OLE files

Virus/Malware Settings Only
Scan Boot Area
CPU Usage
Medium

Scan Exclusions
Enable Scan Exclusion

Apply scan exclusion settings to all scan types
Exclude directories where Trend Micro products are installed

Action Tab
Virus/Malware
Use Active Action

Customize action for probable virus/malware

Back up files before cleaning
Display a notification message on the client computer when virus/malware is detected

Display a notification message on the client computer when probable virus/malware is detected.

Enable system clean up for probable virus/malware

Spyware/Grayware
Clean
Display a notification message on the client computer when virus/malware is detected

Enable system clean up for probable virus/malware

**Scan Now Settings**
Enable Virus / Malware Scan

**Notes and Recommendations**
Enabled

**Scan settings**
- Scan compressed files
- Scan OLE objects
- Detect exploit code in OLE files

**Virus/Malware Settings Only**
- Scan Boot Area
- CPU Usage: Medium

**Scan Exclusions**
- Enable Scan Exclusion

**Action Tab**
- Virus/Malware
  - Use Active Action
  - Customize action for probable virus/malware
  - Back up files before cleaning
  - Display a notification message on the client computer when virus/malware is detected
  - Display a notification message on the client computer when probable virus/malware is detected.
  - Enable system clean up for probable virus/malware

**Spyware/Grayware**
- Clean

**Notes and Recommendations**
- Enable Virus / Malware Scan

**Notes and Recommendations**
- Enable Virus / Malware Scan

**Scan settings**
- Scan compressed files
- Scan OLE objects
- Detect exploit code in OLE files

**Virus/Malware Settings Only**
- Scan Boot Area
- CPU Usage: Medium

**Scan Exclusions**
- Enable Scan Exclusion

**Action Tab**
- Virus/Malware
  - Use Active Action
  - Customize action for probable virus/malware
  - Back up files before cleaning
  - Display a notification message on the client computer when virus/malware is detected
  - Display a notification message on the client computer when probable virus/malware is detected.
  - Enable system clean up for probable virus/malware

**Spyware/Grayware**
- Clean

**Notes and Recommendations**
- Enable Virus / Malware Scan
<table>
<thead>
<tr>
<th>Section</th>
<th>Setting</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Spyware/grayware scan</strong></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Target Tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Files to Scan</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Type scanned by Intelliscan</td>
<td>Enabled</td>
<td>“Selecting Intelliscan slightly improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows you to utilize True File Type scanning.”</td>
</tr>
<tr>
<td><strong>Scan Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan compressed files</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Scan OLE objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect exploit code in OLE files</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Virus/Malware Settings Only</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan Boot Area</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td><strong>CPU Usage</strong></td>
<td>Medium</td>
<td>“Minimizes the slowdown of PCs when a scan is initiated. It is not recommended to run manual scan during working hours due to high CPU usage.”</td>
</tr>
<tr>
<td><strong>Scan Exclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Scan Exclusion</td>
<td>Enabled</td>
<td>“Refer to section 6.6 Recommended Scan-Exclusion List for recommendations on files and directories to exclude.”</td>
</tr>
<tr>
<td>Apply scan exclusion settings to all scan types</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Exclude directories where Trend Micro products are installed</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td><strong>Action Tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Virus/Malware</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Active Action</td>
<td>Enabled</td>
<td>“This setting will utilize the Trend Micro recommended settings for each type of virus/malware.”</td>
</tr>
<tr>
<td>Customize action for probable virus/malware</td>
<td>Enabled</td>
<td>“Select Quarantine to be able to restore any files that are needed”</td>
</tr>
<tr>
<td>Back up files before cleaning</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Enable system clean up for probable virus/malware</td>
<td>Enables</td>
<td></td>
</tr>
<tr>
<td><strong>Spyware/Grayware</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clean</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td><strong>UPDATE AGENT SETTINGS</strong></td>
<td></td>
<td>Notes and Recommendations</td>
</tr>
</tbody>
</table>
Component Updates
Domain Settings
Client programs and hot fixes

Client can act as Update Agent

Component Updates, Domain Settings, and Client programs and hotfixes should be selected to take full advantage of Update Agents to save bandwidth and to speed up deployment.

- Enabled
- Enabled
- Enabled

PRIVILEGES AND OTHER SETTINGS

Privileges Tab

Roaming Privileges
- Enable Roaming mode

Scan Privileges
- Configure Manual Scan Settings
- Configure Real-time Scan Settings
- Configure Scheduled Scan Settings

Scheduled Scan Privileges
- Postpone Scheduled Scan
- Skip and stop scheduled Scan

Firewall Privileges (if you have firewall activated)
- Display the Firewall tab on the Client console
- Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message
- Allow clients to send firewall logs to the OfficeScan server

Behavior Monitoring Privileges
- Display the Behavior Monitoring tab on the client console.

Mail Scan Privileges
- Display the Mail Scan tab on the client console

Notes and Recommendations

- Disabled
- "It is highly recommended to disable this function as it will allow users to stop communication between OfficeScan server and client. This Roaming privilege allows users to isolate their systems to avoid getting notified by the server for scans or updates. This function has nothing to do with the ability to update when the machine is off the network, such as taking a laptop home."
- Disabled
- "Enable this to allow users to configure their own scan setting."
- Disabled
- "Enable this to allow users to configure their own scan setting."
- Disabled
- "Enable this to allow users to configure their own scan setting."
- Disabled
- "Enable this to allow users to stop the Scheduled scan when it is triggered."
- Disabled
- "Enable this to allow users to stop the Scheduled scan when it is triggered."
- Enabled
- Disabled
- "Enable this to allow users to configure their own firewall settings other than what is set on the OfficeScan server"
- Disabled
- "Keep this disabled unless necessary as it will increase traffic between OSCE server and Clients."
- Disabled
- "Since most enterprise does not use POP3, this tab can be hidden to users to avoid confusion. If this setting is allowed then users..."
can install this tool using OSCE client GUI.

**Toolbox Privileges**
Display the Toolbox tab on the client console and allow users to install Check Point Secure Client Support

**Proxy Settings Privileges**
Allow the Client user to Configure proxy Settings

**Component Update Privileges**
Perform Update Now

Enable Scheduled Update

**Uninstallation**
Require a password for the user to uninstall the OfficeScan client

**Unloading**
Require a password for the user to unload the OfficeScan client

**Other Settings Tab**

**Update Settings**
Clients download updates from the Trend Micro ActiveUpdate Server

Enable Scheduled Update

Clients can update components but not upgrade the client program or deploy hot fixes

**Web Reputation Settings**
**Behavior Monitoring Settings**
Display a notification when a program is blocked.

**Scheduled Scan Settings**
Display a notification before a scheduled scan occurs

**Client Security Settings**
High: Restrict users from accessing OfficeScan client files and registries

**POP3 Email Scan Settings**
Scan POP3 email

**Client Console Access Restriction**
Do not allow users to access the client console from the system tray or Windows Start menu

**Restart Notification**
Display a notification message if the client computer needs to restart to finish cleaning infected files.

**ADDITIONAL SERVICES**

<table>
<thead>
<tr>
<th>Service</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Change Prevention Service</td>
<td>Enabled **Unauthorized Change Prevention Service regulates application behavior and verifies program trustworthiness. Behavior Monitoring, Device Control, Certified Safe Software Service, and Client Self protection all require this service. If an Administrator wants to allow this service on a server then a single server must be chosen to view the option to enable this service. <strong>WARNING: Enabling this service will temporarily disconnect the OfficeScan client from the network.</strong></td>
</tr>
<tr>
<td>Firewall Service</td>
<td>Enabled <strong>This setting will turn on the firewall service on the OfficeScan clients.</strong></td>
</tr>
</tbody>
</table>

**WEB REPUTATION**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>External clients tab</td>
<td>Enabled <strong>Enable this feature to protect clients from web threats when they are not connected to the internal network. Enabling this will provide them protection from accessing malicious</strong></td>
</tr>
</tbody>
</table>
Enable assessment

**Security Level**

Medium

**Untested URLs**

Block pages that have not been tested by Trend Micro

**Client Log**

Allow Clients to Send Logs to the OfficeScan Server

**Internal clients tab**

Enable Web Reputation Policy

Enable Assessment

Use Smart Protection Server Web Reputation Service

Use only Smart Protection Servers, do not send queries to Smart Protection Network

**Security Level**

Low

**Untested URLs**

Block pages that have not been tested by Trend Micro

**Client Log**

Allow Clients to Send Logs to the OfficeScan Server

**BEHAVIOR MONITORING**

Enable Malware Blocking

---

*Notes and Recommendations*

- **Enable assessment**
  - Disabled
  - ***Administrator can enable assessment to monitor the type of detections before deploying Web Reputation. When assessment is turned on OfficeScan will not take any action.***

- **Security Level**
  - Medium

- **Untested URLs**
  - Block pages that have not been tested by Trend Micro
  - Enabled

- **Client Log**
  - Allow Clients to Send Logs to the OfficeScan Server
  - Enabled

- **Internal clients tab**
  - Enable Web Reputation Policy
  - Enabled

  - ***If there is already a web security on the gateway, this may be turned off.***

  - Enable Assessment
  - Disabled

  - ***Administrator can enable assessment to monitor the type of detections before deploying Web Reputation. When assessment is turned on OfficeScan will not take any action.***

  - Use Smart Protection Server Web Reputation Service
  - Enabled

  - ***Internet traffic usage is lowest and browsing info is kept in house. Security level is always 'low'.***

  - Use only Smart Protection Servers, do not send queries to Smart Protection Network
  - Enabled

  - ***This will give the most up to date protection from Trend Micro but browsing info will be revealed to Trend Micro. Support security levels are “high”, “medium”, and “low”***

- **Security Level**
  - Low

- **Untested URLs**
  - Block pages that have not been tested by Trend Micro
  - Enabled

- **Client Log**
  - Allow Clients to Send Logs to the OfficeScan Server
  - Enabled

- **Enable Malware Blocking**
  - Enabled

  - ***Enable this setting to protect your clients from specific threats, threat types and threat families through behavior analysis.***
Enable Event Monitoring

**Policies (Under Event Monitoring if Enabled)**

** The “Assess” action will log events that violate the policy but will not take action. To avoid interfering with normal activity, it is recommended that administrators start with this action set for all policies. This would help them define the proper action they need to take once data is available.

- Duplicated System File: Assess
- Hosts File Modification: Assess
- Suspicious Behavior: Assess
- New Internet Explorer Plugin: Assess
- Internet Explorer Setting Modification: Assess
- Security Policy Modification: Assess
- Program Library Injection: Assess
- Shell Modification: Assess
- New Service: Assess
- System File Modification: Assess
- Firewall Policy Modification: Assess
- System Process Modification: Assess
- New Startup Program: Assess

**Exceptions (Approve/Block)**

***Enter the full path of programs you would want to exempt from Behavior Monitoring or directly Block.

**DEVICE CONTROL**

**Notes and Recommendations**

Enabled device control

Block autorun function on USB devices

**Device**

Plug-in Devices (USB)
Optical Disks
Floppy Disks
Network Resource

**Notification**

Display a notification message on the client
Computer when OfficeScan detects unauthorized Device access

**Device Access Control**

Grant full access to all device types
Allow to be run from devices

**Exceptions (Approve/Block)**

**CLIENT GROUPING**

NetBIOS domain

***Only used during installation of a client
### Custom Client Groups

<table>
<thead>
<tr>
<th>Automatic Client Grouping</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| ***Can be used anytime to group clients***

<table>
<thead>
<tr>
<th>Schedule Domain Creation</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| ***Administrators can create client grouping according to Active Directory or IP***

#### Schedule Domain Creation

- Enabled
- Performing scheduled domain creation creates a domain in the client tree. This may take a long time to complete, especially if the scope is broad. However, this does not move existing clients to this domain. Custom client grouping must be used.
- To move the clients, refer to manual sort client or OfficeScan can automatically move clients when the following events occur:
  1. Client installation,
  2. Clients reload
  3. Clients change IP addresses
  4. Clients enable or disable roaming mode

### Global Client Settings

#### Scan Settings

**Configure scan settings for large compressed files**

<table>
<thead>
<tr>
<th>Do not scan files in the compressed file if the size exceeds</th>
<th>10MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Manual Scan to the Windows shortcut menu on client computers</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Exclude the OfficeScan server database folder from Real-time Scan**

| Exclude Microsoft Exchange server folders from scanning | Enabled |

#### Virus/Malware Scan Settings only

- Clean/Delete infected files within compressed files
- Clean/Delete infected files within compressed files

#### Spyware/Grayware Scan Settings Only

- Enable Assessment Mode

#### Scan for Cookies

<table>
<thead>
<tr>
<th>Scan for Cookies</th>
<th>Enabled</th>
</tr>
</thead>
</table>

**Enabled**

- This enhances performance on scanning compressed files and prevents OfficeScan from taking time and resource scanning every content of a compressed file. When compressed files are extracted, realtime scan will still scan the files.

**Disabled**

- Enable this function to allow users to right-click on files or folders to perform a manual scan.
- Prevent OfficeScan database from getting corrupted.
- Prevent OfficeScan from interfering with the mails being processed by the Exchange server and the antivirus that scans the mail traffic.

**Enabled**

- Turn this on with a recommended of at least 3 weeks to allow administrator to assess the detection of spyware in the network. Any detection will not have any action taken on them. This allows admin to monitor and verify if there are any false positive detections specially on home grown applications.

**Enabled**

- Turn on to allow cookie scanning and...
Cleaning

Scheduled Scan Settings
- Count Cookie into spyware log:
  - Disabled
  - ***Turn this off to prevent logs generated from cookie detection to overpopulate the virus log database.

  - Scheduled Scan Settings
  - Remind users of the Scheduled Scan
    - 10 minutes before it runs
    - ***This setting only applies to users who have the privilege to control Scheduled scans.

  - Postpone Scheduled Scan for up to
    - 1 hour
    - ***This setting only applies to users who have the privilege to control Scheduled scans.

  - Automatically stop Scheduled Scan when scanning lasts more than
    - Disable

  - Skip Scheduled Scan when a wireless computer’s battery life is less than
    - Enable
    - ***Enable this setting (20 percent) when there is a number of laptop users in your environment to save battery life.

  - Resume a missed scheduled scan
    - Enable

Firewall Log Settings (If you have firewall activated)
- Send firewall logs to the server every
  - 4 hours
  - ***If it is really needed, set this to Daily or every 4 to 8 hours to prevent clients from saturating the network by sending logs at short intervals regularly.

- Update the OfficeScan firewall driver only after a system reboot
  - Enabled
  - ***This setting will let clients update the firewall driver settings during reboot. This way there will be no loss of network connectivity. This setting applies to only updates/upgrades done through OfficeScan server.

Behavior Monitoring Settings
- Automatically allow program if client does not respond within X seconds.
  - 30
  - ***If timeout is reached, BM will “allow” the program.

- Enable Certified Safe Software Service
  - Disabled
  - ***When enabled, the OSCE client will query the Trend Micro back-end servers via the Internet to reduce BM false alarms.

Alert Settings
- Show the alert icon on the Windows taskbar if the virus pattern file is not updated after X days
  - 5
  - Enabled
  - ***When firewall is enabled, it is suggested to have this turned on so that whenever the firewall driver is updated, the client may be notified to reboot for the update to take effect, otherwise, without reboots, the firewall may not function properly with the updated component.

- Display a notification message if the client computer needs to restart to load a kernel mode driver
  - Enabled

OfficeScan Service Restart
- Automatically restart an OfficeScan client service if the service terminates unexpectedly
  - Enabled

- Restart the service after
  - 1 minute

- If the first attempt to restart the service fails, retry
  - 6 times

- Reset the restart failure count after
  - 1 hour
**Client Self-protection**
- Protect files in the OfficeScan client installation folder: **Enabled**
  
  ***To prevent other programs and even the user from modifying or deleting OfficeScan files, it is recommended to enable this setting.***
- Protect OfficeScan client processes: **Enabled**
  
  ***To prevent all attempts to terminate OSCE related processes, it is recommended to enable this setting.***
- Protect OfficeScan client registry keys: **Enabled**
  
  ***To prevent other programs and even the user from modifying, deleting, or adding new entries related to the OSCE registry and subkeys, enable this setting.***
- Protect OfficeScan client services: **Enabled**
  
  ***To prevent OfficeScan services from being stopped.***

**Reserved Disk Space**
- Reserve X MB of disk space for updates: **60**
  
  ***To allow enough disk space on client side for updates.***

**Network Virus Log Consolidation**
- Enable OfficeScan clients to consolidate network virus logs and send them to the OfficeScan server hourly: **Enabled**
  
  ***This minimizes bandwidth usage by consolidating the logs first before sending them together to the OfficeScan server.***

**Virus/Malware Log Bandwidth Settings**
- Enable OfficeScan clients to create a single virus/malware log entry for reoccurring detection of the same virus/malware within an hour: **Enabled**
  
  ***This allows clients to send only a single log to server on multiple detection of viruses detected on the same location, same virus for a period of time.***

**Proxy Configuration**
- Automatically detect settings: **Enabled**
  
  ***To allow auto detection of proxy for updates, this can be enabled.***
- Use automatic configuration script: **Disabled**
  
  ***To allow use of proxy scripts for connection, this can be enabled.***

**Updates**
- Download only pattern files from the Activeupdate server when performing updates: **Enabled**
  
  ***Administrators can use this setting to let OfficeScan clients to update only patterns from the Trend Micro Active Updatesite.***

**COMPUTER LOCATION**

<table>
<thead>
<tr>
<th>Computer Location</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| Client Connection status (edit reference server list) | **Enabled**

  ***OfficeScan clients will try to communicate with reference servers to determine if their status will be online or offline if the OfficeScan server is not available.***

| Gateway IP address | **Disabled**

  ***Gateway addresses can be entered instead of reference list to determine whether OfficeScan clients are online or offline.***

| Mac address (optional) | **Disabled** |
## CONNECTION VERIFICATION

<table>
<thead>
<tr>
<th>Scheduled Verification</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Scheduled Verification</td>
<td>Enabled Daily at 10:30am</td>
</tr>
</tbody>
</table>

"This allows the server to recheck the status of the clients that are in the network, it is ideal to set it to run on a schedule where most clients are already online.

## SMART PROTECTION SOURCES

<table>
<thead>
<tr>
<th>Smart Protection Sources</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Clients</strong></td>
<td></td>
</tr>
<tr>
<td>Use the standard list</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

"Use this setting if all Smart Protection Servers are reachable through the same network connection for the entire environment. Ensure that there is a minimum of 2 Smart Protection Servers reachable for all clients.

Order

"The setting will configure the clients to check the Scan Servers in the order specified on the list. (Integrated Smart Protection Server will always be last)

Random

"If all Scan Servers are equal in performance, availability and location, the random setting will allow the clients to load balance between all of the Smart Protection Servers on the list.

Use customer lists based on client IP address

"Use this setting to customize which Smart Protection Server clients will use. It is recommended that each sub site will have its own Smart Protection Server.

Use standard list if customer list becomes unavailable

"To help ensure full redundancy in situations where the customer Smart Protection Server list is unavailable, the client should check the standard list

**Integrated Server**

"Check box should be enabled if the Integrated Smart Protection Server will be used. The Integrated Smart Protection Server should not be used to support more than 3000 clients in a primary role. If more than 3000 clients need to be supported a Stand-Alone Smart Protection Server should be installed in the environment and the Integrated Smart Protection Server should be used for backup purposes only.

<table>
<thead>
<tr>
<th>Update Settings</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable scheduled updates</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Smart Feedback</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Protection Network</td>
<td></td>
</tr>
</tbody>
</table>

"When enabled, Trend Micro Smart Feedback shares threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new
### UPDATES

#### SERVER

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| **Scheduled Update**     | Enable scheduled update of the OfficeScan server
|                           | Update Schedule

**Enabled**

**Hourly**

***It is best to check on a more regular basis to get the latest updates.***

#### NETWORKED COMPUTERS

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic Update</strong></td>
</tr>
</tbody>
</table>
|                           | **Event-Triggered Update**
|                           | Initiate component update on clients immediately after the OfficeScan server downloads a new component
|                           | Include roaming client(s)
|                           | Let clients initiate component update when they restart and connect to the OfficeScan server (roaming clients are excluded)
|                           | Perform Scan Now after update (excluding roaming clients)

**Enabled**

***Turn this on so that the updates can be deployed immediately to the clients once the OfficeScan server finished updating.***

**Disabled**

***If you have the roaming privilege turned off, this is not necessary.***

**Enabled**

***There are instances where the clients are offline when the server updated from the internet. This function will allow clients to get their updates from the server when they are back online.***

**Disabled**

***It is not extremely necessary to do a full scan right after performing an update. The scheduled scan is normally sufficient.***

**2 or 4 hours**

**Enabled**

***Depending on the number of clients that the server manages, you can set this from 2 hours to every 4 hours. This is the setting to configure clients on how often they will check for updates from the OfficeScan server, the update agent or the Internet.***

#### Update Source

**Standard Update Source**

**Enabled**

***Enable this if No update agents will be used***

**Customized Update Source**

**Enabled**

***Administrators can allow clients to get updates from OfficeScan servers if Update Agents are not available***

**Disabled**

***This setting can be turned on if bandwidth is healthy enough to provide back up updates to Update Agents***

**Enabled**

***Domain settings are small enough to allow clients to go to OfficeScan server to get updates from as long as Update Agents are not available.***

**Disabled**

***This setting should not be turned on unless OfficeScan clients are allowed to**
Upgrade from OfficeScan server. This might cause bandwidth problems depending on the network.

Enabled

**Enable this to have update agents always update from the OfficeScan server**

**LOGS**

**LOG MAINTENANCE**

Enable Scheduled Deletion

Enable

***Enable this to maintain a manageable size of log and prevent performance issue on the OSCE server when retrieving logs. If Control Manager is used the logs are also sent to Control Manager, hence there is no need to keep 2 copies of logs. You can get reports from Control Manager. Ensure all Log types are selected.

Logs to Delete

Logs Older than 7 days

***To Keep the log database small enough for efficiency.

Log Deletion Schedule

Daily @ 2am

***It is advisable to have this checked everyday. The Time suggested is 2am so that the traffic to server is low and can be purged before the system backup kicks off. OfficeScan Server automatically does database maintenance during midnight, so avoid scheduling during this time.

**NOTIFICATIONS**

**ADMINISTRATOR NOTIFICATIONS**

Standard Notifications

Virus/Malware

Send notifications only when the action on the virus/malware is unsuccessful

Enable

***Enable this to only notify when an action failed on the virus/malware.

Spyware/Grayware

Send notifications only when the action on the virus/malware is unsuccessful

Enable

***Enable this to only notify when an action failed on the spyware/grayware.

Outbreak Notifications

Virus/Malware

Enable

***Enable this to alert administrators when infections are starting to grow.

1

100

24 hrs

Spyware/Grayware

Enable

***Enable this to alert administrators when infections are starting to grow.

1

100

24 hrs

Firewall Violations

Enable

***Enable this to alert administrators when infections are starting to grow.
Monitor Firewall violations on networked computers

IDS Logs
Firewall Logs
Network Virus Logs
Time Period

Shared Folder Session
Monitor Shared Folder session on your network

Shared Folder Sessions
Time Period

**ADMINISTRATION**

**User Accounts**

User Roles

**Active Directory**

**Active Directory Integration**
Active Directory Domains

**Encrypt Active Directory Credentials**

**Scheduled Synchronization**
Enable Scheduled Active Directory synchronization

**Proxy Settings**

**Internal Proxy**

**Client Connection with the OfficeScan Server Computer**
Use the following proxy settings when clients connect to the OfficeScan server and the Integrated Smart Protection Server.

**Client Connection with the Local Smart Protection Servers**
Use the following proxy settings when clients connect to the local Smart Protection Servers.

**External Proxy**

**Notes and Recommendations**

User accounts are used to logon to OSCE web console. These accounts are assigned privileges as deemed appropriate. Use this section to add custom accounts or Active Directory accounts.

User roles define a list of operations that a user can perform. These operations are roughly tied to the navigation menu. Use this section to assign/create/modify roles for a user or a windows group. This would give the account permission to perform operations defined in that group.

Add Active Directory domains OfficeScan will associate with the client tree.

Specif an encryption key and file path to ensure an additional layer of protection for your Active Directory credentials.

Administrators can set the scheduled synchronization daily.

This should be disabled all the time unless the OfficeScan clients require connection to an intranet proxy to communicate with the OfficeScan Server.

This should be disabled all the time unless the OfficeScan clients require connection to an INTRANET proxy to communicate with the local Smart Protection Server.
### OfficeScan Server Computer Updates
Use a proxy server for pattern, engine, and license updates

Enabled

***Enable this option and fill out the fields when a proxy server is required to download updates from the internet.

### Client Connection with Trend Micro Servers
Specify proxy server authentication credentials the client will use to connect to the Trend Micro Global Smart Protection Server and Web reputation servers.

Enabled

***Fill this out if the proxy server used requires authentication credentials.

### Inactive Clients
Enable automatic removal of inactive clients

Enabled

***Enable this function to allow OfficeScan to remove old clients that are inactive for X days. Whenever these clients come back online, they will automatically be added and show up in the console.

Automatically remove a client if inactive for X days

7 days

### Quarantine Manager
Quarantine folder capacity

10240MB

***Please note that the Quarantine folder on the OfficeScan server does not cleanup by itself. It is important to clean the folder up on a regular basis.

Maximum size for a single file

5 MB

### Web Console Settings

#### Web Console Auto Refresh
Enable Auto Refresh

Enabled

***Set it for 30 seconds

#### Web Console Timeout Setting
Enable Timeout Setting

Enabled

***Set it for 30 minutes

### Database Backup

#### Database Backup Schedule
Enable Scheduled Database Backup

Daily @ 3AM

***OfficeScan Server does database maintenance usually at midnight, and it is best not to interfere with the maintenance so it is recommended either to set the time few hours before or few hours after Midnight after log purging.

### NOTE:
It is recommended that during a virus outbreak, to utilize the Outbreak prevention policy feature in OfficeScan. This feature allows you to control and contain an outbreak by blocking the ports, shared folders, and protect files that malwares are using to propagate and infect.

### 3.3.2. INI Configuration Files

A. OfcScan.ini
3.4. Performance Tuning

A. OfficeScan Server (ofcscan.ini) Parameters

The parameters below can be added or edited to further improve the performance of the OfficeScan server.

<table>
<thead>
<tr>
<th>PARAMETER (ofcscan.ini)</th>
<th>USAGE / NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command_Handler_Maxium_Thread_Number</td>
<td>This OfficeScan server parameter controls the number of threads responsible for receiving client communications. Default value is 20. Add the parameter under [INI_SERVER_SECTION] of ofcscan.ini to modify default setting. Recommended value is 20 multiplied by the number of CPUs. NOTE: the word Maximum is intentionally misspelled.</td>
</tr>
<tr>
<td>DB_MEM_OPT_MAX</td>
<td>Increase the server database cache to improve performance. Recommended value is at 10% of available memory.</td>
</tr>
</tbody>
</table>
Increase the number of Command Handler threads
1. Edit `<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\ofcscan.ini`
2. Add the parameter `Command_Handler_Maximum_Thread_Number=` under `[INI_SERVER_SECTION]` section and set its value to `20 x Number of CPUs`
3. Restart the `OfficeScan Master Service`

Increase Database Cache to improve performance
1. Edit `<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\ofcscan.ini`
2. Locate the entry `DB_MEM_OPT_MAX = 10240` and set its value to be at least 10% of available memory.
3. Restart the `OfficeScan Master Service`

Verify Connection Thread Count Parameter
1. Go to the `[INISERVER_SECTION]` section.
2. Look for the `VerifyConnectionThreadCount=16` parameter.
3. This value is dependent on the network capacity. If you have a 100 Mbps intranet, entering a value of 64 or 128 is acceptable.

4. Backup and Disaster Recovery

   NOTE: Section below applies only to OfficeScan itself. Integrated Scan Server components will not be backed up.

4.1. OfficeScan Server Database Files
The OfficeScan server can be set to automatically backup client database information. This is configurable via the web-based management console under [Administration | Database Backup] section. This process copies all database files under [ `<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\HTTPDB`] to either a local or remote location. It is recommended to do a Daily backup especially during client deployment. The schedule can be changed to Weekly after the deployment is complete. It is also recommended to configure the backup to start at 2:00 AM when client interaction is minimal and the process does not coincide with other OfficeScan scheduled tasks. It is recommended to use the OfficeScan built-in backup function to do the backup for the database. Using third party application to backup the database may cause system instability or database corruption.

4.2. OfficeScan Server Configuration Files
It is also recommended to manually backup the OfficeScan server configuration files which can be used to recover from a server disaster.

OfficeScan Server and Firewall configuration Files
`\PCCSRV\Ofcscan.ini` – Server configuration information
In an event of server corruption, the OfficeScan server settings can be restored by following the procedure below.

**Restoring OfficeScan Server Configuration**

This procedure assumes that the OfficeScan server is being restored to the same host, using the same FQDN and IP address.

1. Stop the OfficeScan Master Service and WWW Publishing Service.
2. Restore the backup database files under \Program Files\Trend Micro\OfficeScan\PCCSRV\HTTPDB
3. Restore the OfficeScan server and Firewall policy configurations
   - \Program Files\Trend Micro\OfficeScan\PCCSRV\Ofcscan.ini
   - \Program Files\Trend Micro\OfficeScan\PCCSRV\Private\Ofcserver.ini
   - \Program Files\Trend Micro\OfficeScan\PCCSRV\Private\Ous.ini
   - \Program Files\Trend Micro\OfficeScan\PCCSRV\Private\PFW directory
   - \Private\SortingRuleStore\SortingRule.xml
   - \Private\AuthorStore folder – RBA User Profile
   - \Private\vdi.ini
4. From the command prompt, go to \Program Files\Trend Micro\OfficeScan folder and run the command srvsvcsetup.exe –setprivilege.
5. Restart the OfficeScan Master Service and WWW Publishing Service.

4.3. OfficeScan Client Configuration Settings

**Saving the Client Configuration Settings**

1. Log on to the OfficeScan Management Console
2. Go to Networked Computers | Client Management
3. To save the Global Domain settings, highlight the OfficeScan Server domain; To save just the domain level setting, highlight only the subdomain; To save only a specific client’s setting, highlight the client.
4. Once highlighted, select Settings | Export Settings
5. Click on the Export button and save the file.

**Restoring the Client Configuration Settings**

1. Log on to the OfficeScan Management Console
2. Go to Networked Computers | Client Management
3. To restore the Global Domain settings, highlight the Officescan Server domain; To restore just the domain level setting, highlight only the subdomain; To restore only a specific client’s setting, highlight the client.

4. Once highlighted, select **Settings | Import Settings**

5. Browse to the DAT file saved previously that you want to restore, then click in **Import** button

6. Put a check to **Apply to all Domains** or **Apply to all computers belonging to the selected domain(s)**

7. Click on the **Apply to Target** button

---

5. **Behavior Monitoring**

Trend Micro™ OfficeScan™ protects enterprise networks from malware, network viruses, Web-based threats, spyware, and mixed threat attacks. Behavior Monitoring and Device Control are some of the new OfficeScan features that proactively aim to prevent malware attacks.

This document aims to increase knowledge about Behavior Monitoring and Device Control and help readers avoid potential issues during deployment.

---

5.1. **Behavior Monitoring Overview**

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or installed software. Behavior Monitoring is composed of the following sub-features:

- **Malware Behavior Blocking**
- **Event Monitoring**

---

5.1.1. **Malware Behavior Blocking**

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time and as programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

**Note:** To help ensure that this feature does not interfere with critical applications, OfficeScan leaves this feature disabled on server platforms, even when it is enabled through the console. To enable this feature on a server computer, select an individual server and go to **Settings -> Additional Service** to enable this option. For instructions, see the Administrator’s Guide.

*Figure 1-1: Malware Behavior Blocking setting*

---

**Tip:** Before deploying Malware Behavior Blocking, Trend Micro recommends running a pilot deployment. See **Deploying Behavior Monitoring and Device Control** for more information.
5.1.2. Event Monitoring

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It uses a policy-based approach where system areas are monitored for certain changes, allowing administrators to regulate programs that cause such changes.

If attempts to change the system are made, Event Monitoring will:
- Refer to the Event Monitoring policies and perform the configured action.
- Notify the user or administrator

Use the Event Monitoring if you have specific system protection requirements that are above and beyond what is provided by Malware Behavior Blocking.

**Figure 1-2: Event Monitoring setting**

![Event Monitoring settings](image)

The following Event Monitoring policies define which events it checks for and how it handles each event.
<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
<th>Default Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicated System File</td>
<td>Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.</td>
<td>Assess</td>
</tr>
<tr>
<td>Hosts File Modification</td>
<td>The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirected to infected, non-existent, or fake Web sites.</td>
<td>Assess</td>
</tr>
<tr>
<td>Suspicious Behavior</td>
<td>Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.</td>
<td>Assess</td>
</tr>
<tr>
<td>New Internet Explorer Plugin</td>
<td>Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.</td>
<td>Assess</td>
</tr>
<tr>
<td>Internet Explorer Setting</td>
<td>Many virus/malware programs change Internet Explorer settings, including the home page, trusted Web sites, proxy server settings, and menu extensions.</td>
<td>Assess</td>
</tr>
<tr>
<td>Security Policy Modification</td>
<td>Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.</td>
<td>Assess</td>
</tr>
<tr>
<td>Program Library Injection</td>
<td>Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.</td>
<td>Assess</td>
</tr>
<tr>
<td>Shell Modification</td>
<td>Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow</td>
<td>Assess</td>
</tr>
<tr>
<td>Events</td>
<td>Description</td>
<td>Default Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>malicious programs to track the programs used and start alongside legitimate applications.</td>
<td></td>
</tr>
<tr>
<td>New Service</td>
<td>Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.</td>
<td>Assess</td>
</tr>
<tr>
<td>System File Modification</td>
<td>Certain Windows system files determine system behavior, including startup programs and screensaver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.</td>
<td>Assess</td>
</tr>
<tr>
<td>Firewall Policy</td>
<td>The Windows firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access the network and the Internet.</td>
<td>Assess</td>
</tr>
<tr>
<td>System Process</td>
<td>Many malicious programs perform various actions on built-in Windows processes. These actions can include terminating or modifying running processes</td>
<td>Assess</td>
</tr>
<tr>
<td>Process Modification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Startup Program</td>
<td>Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.</td>
<td>Assess</td>
</tr>
</tbody>
</table>

Administrators can choose to perform one of the following actions to respond to monitored events:

- **Assess**: Always allow processes associated with an event but record this action in the logs for assessment.

  **NOTE**: *Use this option during initial deployment to assess the impact of enabling Behavior Monitoring features.*

- **Allow**: Always allow processes associated with an event

- **Ask When Necessary**: Prompts users to allow or deny processes that may have violated Behavior Monitoring policies. If selected, a prompt asking users to allow or deny the process and add to the
Allowed Programs or Blocked Programs appears. If users do not respond within the time period specified in the Behavior Monitoring settings screen, OfficeScan automatically allows the process to continue.

- **Deny**: Always block processes associated with an event and record this action in the logs

### 5.1.3. Enabling Behavior Monitoring

**Path:** Networked Computers > Client Management > Settings > Behavior Monitoring Settings

To enable Malware Behavior Blocking or Event Monitoring, select the following options:

- **Enable Malware Behavior Blocking** (workstation default: on; server default: off)
- **Enable Event Monitoring** (workstation default: on; server default: off)

**Note:** Since Malware Behavior Blocking is enabled by default, Trend Micro strongly recommends identifying system-intensive applications and adding them to the exception list before deploying OfficeScan. For more information, see How Behavior Monitoring and Device Control Can Affect Performance.

Behavior Monitoring settings can be applied to specific entities in the client tree or all entities (root). If you are applying settings to the root, you need to select one of the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain (domains not yet created during configuration).

- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

### 5.2. Device Control Overview

Device Control regulates access to external storage devices and network resources. Device Control helps prevent the propagation of malware on removable drives and network shares and, combined with file scanning, helps guard against security risks.

**Figure 1-3: Device Control settings**

Notification messages are displayed on the endpoints when device control violations occur. Administrators can modify the default notification message.

**Note:** To help ensure that this feature does not interfere with critical applications, OfficeScan leaves this feature disabled on server platforms, even when it is enabled through the console. To enable this feature on a server computer, select an individual server and go to **Settings -> Additional Service** to enable this option. For instructions, refer to the Administrator’s Guide.

### 5.2.1. Using Device Control

**Path:** Networked Computers > Client Management > Settings > Device Control
To configure Device Control:

1. Select the **Enable device control** option.

2. Choose whether to block or allow the AutoRun function (autorun.inf) on USB devices connected to the computer.

3. Select the permissions for each device type.

### Table 1-2: Device permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Files on the Device</th>
<th>Incoming Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full access</td>
<td>Operations allowed: Copy, Move, Open, Save, Delete, Execute</td>
<td>Operations allowed: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This means that a file can be saved, moved, and copied to the device.</td>
</tr>
<tr>
<td>Read and write only</td>
<td>Operations allowed: Copy, Move, Open, Save, Delete</td>
<td>Operations allowed: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>Operation blocked: Execute</td>
<td></td>
</tr>
<tr>
<td>Read and execute only</td>
<td>Operations allowed: Copy, Open, Execute</td>
<td>Operations blocked: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>Operations blocked: Save, Move, Delete</td>
<td></td>
</tr>
<tr>
<td>Read only</td>
<td>Operations allowed: Copy, Open</td>
<td>Operations blocked: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>Operations blocked: Save, Move, Delete, Execute</td>
<td></td>
</tr>
<tr>
<td>No access</td>
<td>Any attempt to access the device or network resource is automatically blocked.</td>
<td>Operations blocked: Save, Move, Copy</td>
</tr>
</tbody>
</table>

**Note:** The antivirus feature in OfficeScan complements Device Control. For example, if Device Control allows a file to open from a regulated device but OfficeScan detects that the file is infected, a scan action will still be performed on the file to eliminate the malware.
4. Select whether to display a notification message on the client computer when OfficeScan detects unauthorized device access.

5. If you selected domain(s) or client(s) on the client tree, click Save to apply settings to the domain(s) or client(s). If you selected the root icon 🌟, choose from the following options:

- **Apply to All Clients**: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.
- **Apply to Future Domains Only**: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

### 5.2.2. How Behavior Monitoring and Device Control Can Affect Performance

The Behavior Monitoring and Device Control features both use the Trend Micro Unauthorized Change Prevention Service (running under the process name TMBMSRV.EXE). These features use TMBMSRV.EXE to monitor for system events and check these events against rules to determine whether certain application activities are unwanted.

TMBMSRV.EXE delivers highly beneficial behavior-based security functionality, particularly the capability to check applications for suspicious behavior (Behavior Monitoring) and control access to storage devices (Device Control). Its monitoring mechanism, however, can strain system resources, especially when the computer is running applications that cause numerous system events. To prevent impacting system performance, Trend Micro recommends configuring OfficeScan so that these “system-intensive” applications are not monitored by TMBMSRV.EXE.

### 5.2.3. Deploying Behavior Monitoring and Device Control

Running TMBMSRV.EXE and system-intensive applications on the same computer can affect system performance and disrupt critical applications. It is for this reason that a properly managed deployment of Behavior Monitoring and Device Control is recommended.

To ensure smooth deployment of OfficeScan with Behavior Monitoring and Device Control:

- Set up and deploy a pilot environment.
- Identify system-intensive applications.
- Add system-intensive applications to the Behavior Monitoring exception list.

#### Step 1: Preparing a Pilot Environment

Before performing a full-scale deployment, conduct a pilot deployment in a controlled environment. A pilot deployment provides opportunity to determine how features work and, most importantly, how Behavior Monitoring and Device Control can affect your endpoints.

The pilot process should result in:

- A better understanding of the implications of deploying the new Behavior Monitoring and Device Control features.
- A better understanding of applications that may conflict with these features.
- A list of applications that can be added to the Behavior Monitoring exception list.
When setting up the pilot environment:

- Prepare an environment that matches the production environment as closely as possible.
- Ensure that the following are included in the pilot environment:
  - Business applications
  - Custom applications
  - All network applications used by groups or individuals (such as payroll, inventory, accounting, and database applications)
- Deploy the OfficeScan clients into the pilot environment with the features that you intend to enable. For example, Behavior Monitoring and Device Control may both be enabled.
- Allow the pilot environment to run for a reasonable amount of time (give sufficient “soak time”) with the standard applications running and with average daily use.

Step 2: Identifying System Intensive Applications

Trend Micro provides a standalone performance tuning tool to help identify applications that could potentially cause a performance impact. The TMPerfTool tool, available from Trend Micro technical Support, should be run on a standard workstation image and/or a few target workstations during the pilot process to preempt performance issues in the actual deployment of Behavioral Monitoring and Device Control.

To identify system intensive applications:
1. Unzip the TMPerfTool.zip file.
2. Place the TMPerfTool.exe file in the OfficeScan default installation folder (%ProgramDir%/Trend Micro/OfficeScan Client) or in the same folder as the TMBMCLI.dll file.
4. Click Analyze when the system or applications start to slow down. If a red highlighted row appears, it means that the TMPerfTool found the system-intensive process.
5. Select the highlighted row and click Exclude.
6. After excluding the process, verify if the system or application performance improves. If the performance improves, select the process row again and click Include. If the performance drops again, it means you found a system-intensive application. Perform the following:
   a) Note the name of the application.
   b) Click Stop.
   c) Click Report and save the .xml file in your specified folder.
   d) Review the applications that have been identified as conflicting and add the applications to the Behavior Monitoring exception list.

Step 3: Adding System-Intensive Applications to the Behavior Monitoring Exception List

The Behavior Monitoring exception list is a user-configurable list of approved and blocked programs that are not monitored by Behavior Monitoring and Device Control. These features automatically allow approved programs to continue—approved programs are still checked by other OfficeScan features. Blocked programs are never allowed to run.

Trend Micro strongly recommends adding system-intensive applications to the Behavior Monitoring exception list to reduce the likelihood of performance issues from occurring. System-intensive applications can cause TMBMSRV.EXE (the service used by both Behavior Monitoring and Device Control) to consume very high amounts of CPU resources and disrupt critical applications.
To add programs to the exception list:

*Path:* Networked Computers > Client Management > Settings > Behavior Monitoring Settings

1. Type the full path of the program under **Exceptions**.

   **Note:** Separate multiple entries with semicolons (;). The exception list supports wildcards and UNC paths.

2. Click **Approved Programs** or **Blocked Programs**

   **Note:** All exceptions apply to both Behavior Monitoring and Device Control. Add only verified programs to the Approved Programs list to ensure network security.

3. If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to the domain(s) or client(s). If you selected the root icon 🌑, choose from the following options:

   1. **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.

   2. **Apply to Future Domains Only:** Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

### 5.3 Alternative Ways to Prevent Performance Impact

To prevent TMBMSRV.EXE from affecting performance, you can disable the service itself or disable both Behavior Monitoring and Device Control.

**Warning:** Disabling the Behavior Monitoring, Device Control, and other features may put your network at risk from new and suspicious attacks. Perform these actions only as a last resort.

You can disable Behavior Monitoring and Device Control from the Web console or from the registry.
5.3.1 Disabling Features from the Web Console

Behavior Monitoring
Path: Networked Computers > Client Management > Settings > Behavior Monitoring Settings
To disable Behavior Monitoring, deselect the following options:
- Enable Malware Behavior Blocking
- Enable Event Monitoring
If you selected domain(s) or client(s) on the client tree, click Save to apply settings to those domain(s) or client(s). If you selected the root icon 🥇, choose from the following options:
  - Apply to All Clients
  - Apply to Future Domains Only

Device Control
Path: Networked Computers > Client Management > Settings > Device Control
To disable Device Control, deselect Enable Device Control.
If you selected domain(s) or client(s) on the client tree, click Save to apply settings to the domain(s) or client(s). If you selected the root icon 🥇, choose from the following options:
  - Apply to All Clients
  - Apply to Future Domains Only

5.3.2 Stopping the Service
Disable Behavior Monitoring and Device Control by stopping the Trend Micro Unauthorized Change Prevention Service (TMBMSRV.EXE). Perform this task directly on each endpoint.

Note: Starting and stopping services directly overrides settings on the console. However, these changes will not take effect if the Client Self-Protection feature is enabled. Disable Client Self-Protection before starting or stopping OfficeScan services. See the Administrator’s Guide for more information.

To stop the service:
1. Open the Services console. Click Start > Run. Type SERVICES.MSC and click Open.
2. In the Services console, stop Trend Micro Unauthorized Change Prevention Service.

6. Miscellaneous

6.1 Product Communication Ports
6.3 Update Architecture and Network Usage

6.3.1 The Update Process

**OfficeScan Server**

The process starts with the OfficeScan server downloading update packages. The server can be configured to get updates from several locations:

- **Trend Micro's Active Update Server** (Internet) – Default method. It uses standard HTTP GET request to download update packages from the Internet. This only
requires the HTTP port (80) to be open from the OfficeScan server to the Internet. This can be triggered manually or on scheduled basis (Hourly, Daily, Weekly, or Monthly). Recommended setting is Hourly.

- **Trend Micro Control Manager** (TMCM) server – Control Manager notifies the OfficeScan server when an update is available for download. OfficeScan will then check its **Update Source** [ Updates | Server Update | Update Source ] setting to know where it should download the package via HTTP. By default, the Update Source is set to the Internet (Trend’s Active Update server). This can be pointed to the Control Manager server if desired (i.e. http://<server fqdn or ip address>/tvcsdownload/activeupdate).

- **Custom Update Source** (Other update source). Similar to the Internet update method except that the admin re-creates an Active Update (web) server and sets the OfficeScan server to point to the HTTP location (i.e. http://<server fqdn or ip address>/activeupdate). Control Manager and peer OfficeScan servers can service such request.

**Update Agent**

When the update package has been downloaded, the OfficeScan server notifies its **Update Agents** first that a new package is available. The Update Agents would then compare version information and download the package from its designated OfficeScan server as needed. The OfficeScan server waits for an acknowledgement command for the verification or download/update process to complete. If no acknowledgement is received, the OfficeScan server will wait to reach a timeout value before notifying the rest of its clients. Default timeout is 10 minutes and is configurable in **Timeout for update agent** parameter using SvrTune.exe [ Tools | Administrative Tools | Server Tuner ]. All communications are done through CGI commands via HTTP protocol. The OfficeScan server listens on its web server management port (typically 80 or 8080) while the Update Agents listen on its pre-configured port (randomly generated or manually defined during the OfficeScan server installation).

**OfficeScan Client**

Once the Update Agent notification process is completed, the OfficeScan server notifies the rest of its clients. Notification process is done by batches. The number by batch is configurable in **Maximum Client Connections** using SvrTune.exe [ Tools | Administrative Tools | Server Tuner ] utility. Once notified, clients would check for updates in the order below.

**OfficeScan Client Update Source Order**

1. Update Agent
2. OfficeScan Server
3. Trend Micro’s Active Update Server (Internet)

Privileges can be set to allow clients to update from the OfficeScan server when its Update Agent is unavailable. This setting is global and can be enabled under [ Updates | Client Deployment | Update Source | Update from OfficeScan server if all customized sources are not available or not found ].

**NOTE:** SvrTune.exe only controls the number of clients notified by the OfficeScan server at a given time after OfficeScan server completed an update. When OfficeScan clients are the ones who initiated the update, for example via ‘Scheduled Update’, the OfficeScan server will handle the client update request and the ones it cannot is queued in IIS for later processing. (IIS can process concurrently 256 cgi requests at a time, this is the default configuration.)

Individual or group of clients (OfficeScan Domain) can also be given privileges to download updates directly from the Internet. Highlight the client or Domain from the [ Clients ] main window and enable the option under [ Clients | Client Privileges/Settings | Update Settings | Download from the Trend Micro ActiveUpdate Server ].
**Integrated Smart Protection Server**

- **Trend Micro’s Active Update Server** (Internet) – Default method. It uses standard HTTP GET request to download update packages from the Internet. This only requires the HTTP port (80) to be open from the OfficeScan server to the Internet. This can be triggered manually or on scheduled basis (*Hourly* or *every 15 minutes*). Recommended setting is *Hourly*.

- **Trend Micro Control Manager** (TMCM) server – Control Manager notifies the OfficeScan server when an update is available for download. OfficeScan will then check its *Update Source* [Updates | Server Update | Update Source] setting to know where it should download the package via HTTP. By default, the *Update Source* is set to the Internet (Trend’s Active Update server). This can be pointed to the Control Manager server if desired (i.e. `http://<server fqdn or ip address>/tvcsdownload/activeupdate`).

**NOTE:** Before connecting OfficeScan 10.5 to TMCM 3.5 or 5.0 make sure following hotfixes are installed on TMCM to support Smart Scan.

- **TMCM 5.0 Patch 3 + Hotfix 1740**
- **TMCM 3.5 Patch 6 + Hotfix 1599**

- **Custom Update Source** (*Other update source*). Similar to the Internet update method except that the admin re-creates an Active Update (web) server and sets the OfficeScan server to point to the HTTP location (i.e. `http://<server fqdn or ip address>/officescan/download`). Control Manager and peer OfficeScan servers can service such request.

### 6.2.2 Network Usage (Bandwidth Consumption)

OfficeScan generates network traffic when the server and client communicate with each other. Server initiated communications are mainly CGI commands sent through HTTP protocol and are only a few kilobytes in size. The clients, on the other hand, generate traffic as they upload information and pull component updates. Below is a summary of the different types of communications within OfficeScan.

**Server Initiated Traffic**
- Notification on configuration changes
- Notification on component updates

**Client Initiated Traffic**
- Client start-up information
- Uploading virus, event, firewall and web reputation logs
- Infected files to be quarantined on the OfficeScan server (network usage depends on quarantined file size)
- Downloading program and pattern file updates

Probably the most significant data transfer is when a client performs a pattern file update. To reduce network traffic generated during this process, OfficeScan uses a feature called incremental updates. Instead of downloading the full pattern each and every time, only the differences (deltas) are downloaded for up to 14 previous versions for virus definitions and 7 previous versions for spyware, network, and damage cleanup patterns. These new patterns are merged with the old pattern file as they are received by the OfficeScan client. An incremental pattern may range from 1 kilobyte to several megabytes (i.e. 3 MB) depending on version increment (how far the delta is to the latest version).

To further save WAN bandwidth, specific clients can be promoted as an Update Agent to service peer clients. This implies that each client won’t have to individually pull incremental updates from the OfficeScan server. The Update Agent host replicates the complete engine and pattern packages (full
The engine and pattern packages are downloaded every time an update is available. To verify the latest size, simply log in to the OfficeScan server and view the size property of the folders below:

<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\Download\Engine
<drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\Download\Pattern

The Engine and Pattern subfolders in the OfficeScan server are copied over to the Update Agent host under <drive>:\Program Files\Trend Micro\OfficeScan Client\ActiveUpdate folder.

For locations with limited bandwidth connectivity, an ini flag (UADuplicationOptValue) can be enabled in the OfficeScan server to change the behavior of the Update Agent. Instead of downloading the complete engine and pattern packages, only the latest increment (one version older) is downloaded. The Update Agent then generates its own full pattern file as well as the 7 incremental files.

**Enabling Smart Duplicate for Update Agents**

1. Edit <drive>:\Program Files\Trend Micro\OfficeScan\PCCSRV\ofcscan.ini
2. Locate the parameter UADuplicationOptValue and set value to 128.
3. Save changes on the INI file.
4. Log on to the Management Console Clients | Global Client Settings
5. Click on Save button.

**NOTE:** To disable Smart Duplicate if bandwidth is not an issue, configure the parameter as follows: UADuplicationOptValue=64

**Sample computation of bandwidth usage:**

Given: An incremental update is 300Kb

A full compressed pattern is 45MB

For an Update Agent using regular incremental updates, it downloads the full pattern file and 7 incremental files from the OfficeScan server

Total size downloaded = 7x(300kb incremental) + 45Mb full Pattern

= 2.1MB + 45Mb

= 47.1Mb

For an Update Agent configured for Smart Duplicate, it downloads only one incremental the full pattern file and generates its own full pattern and incremental, therefore

Total size download = 300Kb

Saves you 46.8Mb of transfer over the WAN link.

### 6.4 Virtual Desktop Infrastructure (VDI)

OfficeScan 10.5 supports two types of VDI environment: Citrix XenDesktop 4 and VMWare View 4. Following two features have been added:

- **VM Awareness** – to avoid all VM clients in the same physical machine to do on-demand scan or component update at the same time.
• Whitelist Cache Mechanism – to reduce scan time of on-demand scan.

6.4.1 Golden Image Preparation

When deploying VDI, the following tasks need to be completed on the Golden Image.

1. Copy the TcacheGen.exe utility to the Golden Image.
2. Use TcacheGen to create a whitelist of files and folders in the Golden Image. The tool will scan files and folders in the Golden Image and add them into the OfficeScan Whitelist to reduce scanning load on the machine.
3. Use TcacheGen to clear the GUID key found in the OfficeScan Client Registry Hive: HKEY_Local_Machine\Software\TrendMicro\Pc-cillinNTCorp\CurrentVersion\GUID
4. Set the value of VDIEnabled=1 in OfficeScan registry hive: HKEY_Local_Machine\Software\TrendMicro\Pc-cillinNTCorp\CurrentVersion\MISC.
5. Proceed to complete the Golden Image creation.

6.4.2 Install the VDI Support in OfficeScan server Plugin Manager

1. Open the OfficeScan Console >> Plug-in Manager. Download and install the VDI Support component.
2. Click on the Manage Program button to configure VDI Support.

Trend Micro VDI Support

Trend Micro VDI Support delivers immediate protection on VDI Environment.

Manage Program  | Current version: 1.0.1000  | Uninstall

3. Choose between VMWare vCenter Server on Citrix XenServer
4. Enter the server connection information.

Virtual Desktop Management Method

- VMware vCenter™ Server
- Citrix XenServer™

Citrix XenServer Connection Setting 1

- Enable this connection

XenServer IP address: 10.2.168.67
Username: root
Password: **********************

5. Click the save button.
6. Check the vdi_list.ini to confirm the setting is applied correctly.
7. Adjust the VDI parameters depending on the actual need.
We can control 2 very resource intensive actions from the OfficeScan Client namely On-demand Scan and Component Updates.

**VDI.ini parameter’s description and their recommended values are:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache_Time_Seconds</td>
<td>This is the VDI client cache used by the OfficeScan server. When VDI client performs a scan/update, OfficeScan server uses the cache information to respond. After the default value of 300 seconds, OfficeScan server will query XenServer/vCenter to update cache information.</td>
<td>300</td>
</tr>
<tr>
<td>Cache_Time_Error_Seconds</td>
<td>When OfficeScan server tries to query XenServer/vCenter to get updated cache information but couldn’t (Failed), within 30 secs, OfficeScan server will use old cache to respond to clients’ request and will not try the query again within the elapse time.</td>
<td>30</td>
</tr>
<tr>
<td>Controller_Counts</td>
<td>The number of VDI Client tasks controlled by OfficeScan server, currently we have 2 types, (00) is for on-demand scan and (01) is for update.</td>
<td>2</td>
</tr>
<tr>
<td>Controller_00_MaxRunningSeconds</td>
<td>Within 300 seconds, if the on-demand scan client didn’t respond to the OfficeScan server, the OfficeScan server considers the scan task completed and will allow the next client to run on-demand scan.</td>
<td>300</td>
</tr>
<tr>
<td>Controller_00_MaxConcurrentGuests</td>
<td>Only one client can run on-demand scan at the same time.</td>
<td>1</td>
</tr>
<tr>
<td>Controller_00_BaseWaitingTime</td>
<td>If the MaxConcurrentGuests value is reached, other requesting VDI clients need to wait 10 secs and then 10+10 secs, 10+10+10 secs, till it reaches MaxWaitingTime value.</td>
<td>10</td>
</tr>
<tr>
<td>Controller_00_MaxWaitingTime</td>
<td>Used by BaseWaitingTime to determine how long VDI Client should wait before trying to contact the OfficeScan server.</td>
<td>30</td>
</tr>
<tr>
<td>Controller_00_TaskName</td>
<td>Name of the VDI Client Task</td>
<td>ODScan</td>
</tr>
<tr>
<td>Controller_01_MaxRunningSeconds</td>
<td>Within 600 seconds, if the updating client didn’t respond to the OfficeScan server, the</td>
<td>600</td>
</tr>
</tbody>
</table>
### 6.4.3 Performance Related Items

To mitigate performance issue, you should comply with the best practices below when running OfficeScan 10.5 client in VDI environment.

1. Suggest to first set scan mode to smart scan, and then deploy OfficeScan client to VDI.
2. Do not switch between conventional scan and smart scan on VDI guest environment. This is because scan type change will trigger full pattern update immediately on the guest environment causing Disk I/O congestion if occurring on multiple VM images at the same time.
3. When Smart Protection Server is offline, OfficeScan clients will add files into a queue list (suspicious list). When the Smart Protection Server comes back online, all the machines will perform a scan base on this list and can cause performance issue. Make sure to have a backup Smart Protection Server to ensure the Smart Scanning is available at all times.
4. Pattern Update rollback is very Disk I/O intensive and should be done as seldom as possible.
5. Take special caution deploying program updates or hotfix to VDI Clients. Deploy to a few machines at a time to minimize performance impact.
6. AEGIS is should be disabled in VDI environment and this should be done when golden image is prepared. This can help improve performance in VDI environment.
7. Enable/Disable firewall should not be performed on all clients at the same time; otherwise it will have heavy disk I/O usage.
8. If many clients are enabled to act as update agent at the same time then this will have heavy disk I/O and CPU, and will need long time to enable. It is recommended to avoid enabling many clients to act as update agents at the same time.

### 6.5 Recommended Installation Adjustments for Special Environments

#### 6.5.1 Migration of Unsupported Platforms

In OfficeScan 8.0/10.0, there are several OS platforms that were dropped. Among these platforms are the Windows 95/98/ME, Windows NT and IA64 architecture.

After an upgrade of previous versions of OfficeScan server to version 10.5, the OfficeScan clients that are unsupported will not appear in the management console. The OfficeScan server will generate a list of these clients into a file `C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupCln.txt`.

To continue updating and managing these clients, a tool (`clientmover.exe`) has been provided to migrate the clients to a version of OfficeScan server that supports these clients.

**In order to migrate:**

1. Setup an older version of OfficeScan server i.e. version 7.3
2. From the OfficeScan 10.5 server, in the command prompt, go to `C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Admin\Utility\Clientmover` folder
3. Run the tool with the following parameters:


**Where:**

/P is the path of the unsupported client list generated by the OfficeScan 10.5 server.

/S is the older version of Officescan server that these clients will be moved to and the server port.

/N – allows you to notify and then move the clients to the previous version of the OfficeScan server

/V – verifies if the tool successfully moved the clients.

/F – force the notification or verification without checking the current client status.

**Example:**

ClientMover /P:‖C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupcln.txt‖ /S:10.20.30.40:8080 /N /V

4. The result of the move will be logged into a file under C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\. The log file name is in the following format:

   unsupcln.txt.log.{date_time}

**Example:**

unsupcln.txt.log.20061201_162502

### 6.5.2 Citrix Environment

#### 6.5.2.1 Installation of Officescan Clients on Citrix Servers

b. Installation of Officescan Clients on Citrix servers may need some special configuration due to the architectural limitation of Officescan Clients. This includes the issue wherein a session of a Citrix client generates a PCCNTMON.exe process created on the Citrix Server. If there are 500 Citrix clients connected, there may be 500 PCCNTMON.exe process running. This may use up the Citrix Server resource.

In the previous version of Officescan, tweaks on ini file and registry is needed to workaround the issue. For this version, you just need to do the following:

1. Login to the Officescan Server Management console
2. Go to **Networked computers| Client Management**
3. From the Client tree, expand the domain and highlight the Citrix Servers (hold down CTRL key to select multiple servers)
4. On the top menu, select **Settings | Privileges and Other Settings | Other Settings**
5. Put a check mark on **"Do not allow users to access the client console from the system tray or Windows Start menu"**
6. Click on **Save** button

**Note:** The only minimal side effect for this configuration is that there will be no popup messages that will come up on the Citrix Servers whenever a virus/malware, spyware/grayware, or web threats are detected
c. When the OfficeScan client is installed to a Citrix server, Citrix clients currently connected to the Citrix server may become disconnected.

To address this issue, do the following before installing the client:

1. Open Registry Editor on the Citrix server.
   Important: Always back up the whole registry before making any modifications. Incorrect changes to the registry can cause serious system problems.
2. Go to HKLM\SOFTWARE\TrendMicro\NSC\TmProxy\WhiteList
3. Click Edit > New > Key and name the key “IIS”.
4. Under this new key, create the following value:
   Type: String value
   Name: ProcessImageName
   Value: w3wp.exe

6.5.2.2 Citrix Known Issues

A. Unsupported Citrix Features and Functions

1. The OfficeScan client on the Citrix server cannot be published. To allow users to access the OfficeScan client, publish the Citrix Server desktop through the Citrix Access Management Console (CMC). When published, users need to:
   a. Launch the desktop from the Citrix client Web interface.
   b. In the Citrix desktop session, open the OfficeScan client program from Start > Programs > Trend Micro OfficeScan Client > OfficeScan Client.
   c. Launch the OfficeScan client console from the system tray icon.
2. The OfficeScan client cannot be streamed because the OfficeScan client profile created by Citrix Streaming Profiler does not function correctly during streaming. This means that some functions may appear to execute properly from the client console but may actually not run anything in the backend.
   Other programs published and streamed on the Citrix server are expected to work properly.

B. Scanning

1. A drive or folder on a computer running Windows 2003 contains a file infected with virus/malware and the drive or folder is mapped to the Citrix server. When the infected file is opened during a Citrix client session, Real-time Scan may be unable to detect the virus/malware on the file if the mapped drive has the same drive name, for example (C:\, in a multi-user environment.

To resolve this issue:

   d. Open Registry Editor.
   Important: Always back up the whole registry before making any modifications. Incorrect changes to the registry can cause serious system problems.

   e. Go to
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TmPreFilter
      and add the following value:
      Type: Multi-string value (REG_MULTI_SZ)
Name: DependOnService
Value: Cdm

f. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TmFilter\Parameters and add the following value:

Type: DWORD value (REG_DWORD)
Name: CitrixOn2003Support
Value: Any number except zero

If you are using remote desktop, add the following value to the same key:

Type: DWORD value (REG_DWORD)
Name: MsRemoteDesktopSupport
Value: Any number except zero

g. Restart the machine for the changes to take effect.

h. When the OfficeScan client detects a security risk during a particular user session, the notification message for the security risk displays on all active user sessions.
Warn users about this limitation or disable the notification if you do not want the notifications displaying on all user sessions.
Security risk can be any of the following:
• Virus/Malware
• Spyware/Grayware
• Firewall policy violation
• Web Reputaion policy violation

i. Updates
When manual update is in progress in one Citrix client session, other active sessions cannot launch manual update.

Trend Micro recommends disabling manual update from the OfficeScan server Web console so users cannot run manual update. Aside from manual update, clients get updated through scheduled update or event-triggered update.

6.5.2.3 Citrix Exclusions
Refer to section 6.6 Recommended Scan-Exclusion List for recommendations on files and directories to exclude.
6.5.2.4 Citrix Firewall Port

Refer to section 6.7 Some Server Common Ports for recommendations on Citrix ports to open.

6.5.3 Installation of OfficeScan Clients on Cisco Callmanager

The following are needed to be configured as recommended to support Cisco Callmanager:

2. Configure Real-time Scan Settings
   a. Login to the OfficeScan Management console
   b. Go to Networked Computers| Client Management
   c. From the Client tree, expand the domain and highlight the Cisco Callmanager Clients
   d. On the top menu, select Settings | Real-time Scan Settings
   e. Under the Scan Settings in the Target tab, configure “Do not scan compressed files if the number of compression layers exceeds” to scan only 1 layer
   f. In the Action tab, uncheck the following:
      
      Display a notification message on the client computer when virus/malware is detected
      
      Display a notification message on the client computer when spyware/grayware is detected
   g. Click on Save button

3. Configure Client Privileges and Settings
   a. Login to the OfficeScan Management console
   b. Go to Networked Computers| Client Management
   c. From the Client tree, expand the domain and highlight the Cisco Callmanager Clients
   d. On the top menu, select Settings | Privileges and Other Settings
   e. Uncheck the following:
      
      Display the Mail Scan tab on the client console and allow users to install/upgrade Outlook mail scan
      
      Display the Toolbox tab on the client console and allow users to install Check Point SecureClient Support
   f. Click on Save button

4. Configure Scan Exclusions
   a. Login to the OfficeScan Management console
   b. Go to Networked Computers| Client Management
   c. From the Client tree, expand the domain and highlight the Cisco Callmanager Clients
   d. On the top menu, select Settings | Real-time Scan Settings
   e. Under the Scan Exclusion in the Target tab, enable the following:
Enable scan exclusion
Apply scan exclusion settings to all scan types

f. Add the following folders to the Scan Exclusion List (Directories)
   - Drive:\Program Files\Call Manager
   - Drive:\Program Files\Call Manager Serviceability
   - Drive:\Program Files\Call Manager Attendant

g. Click on Save button

5. Configure Update Settings
   a. Login to the OfficeScan Management console
   b. Go to Updates | Networked Computers | Automatic Update
   c. Uncheck “Perform Scan Now after update (excluding roaming clients)”
   d. Click on Save button

6. Turn off Scheduled Scan for Virus/Malware and Spyware/Grayware
   a. Login to the OfficeScan Management console
   b. Go to Networked Computers | Client Management
   c. From the Client tree, expand the domain and highlight the Cisco Callmanager Clients
   d. On the top menu, select Settings | Scheduled Scan Settings
   e. Under the Virus/Malware Scan tab, uncheck “Enable virus/malware scan”
   f. Under the Spyware/Grayware Scan tab, uncheck “Enable spyware/grayware scan”
   g. Click on Save button

7. Turn off/disable OfficeScan Firewall
   As much as possible, do not activate firewall on the OfficeScan server when Callmanager will be managed. If already activated and OSCE clients are installed, you need to disable the firewall from the Product Registration Page, then reinstall the OfficeScan clients installed on the Callmanager servers

6.6 Recommended Scan-Exclusion List
Database and encrypted type files should generally be excluded from scanning to avoid performance and functionality issues. Below are exclusions to consider depending on the type of machine you are installing the OfficeScan client on.

General Exclusions for all Windows platforms

Pagefile.sys
*.pst
%systemroot%\System32\Spool (replace %systemroot% with actual directory)
%systemroot%\SoftwareDistribution\Datastore (replace %systemroot% with actual directory)
%allusersprofile%\NTUser.pol
%Systemroot%\system32\GroupPolicy\registry.pol
Microsoft Active Directory Domain Controller

<drive>:\ WINNT \ SYSVOL
<drive>:\ WINNT \ NTDS
<drive>:\ WINNT \ ntfrs
<drive>:\ WINNT \ system32 \ dhcp
<drive> : \ WINNT \ system32 \ dns

Microsoft IIS Server

Web Server log files should be excluded from scanning. By default, IIS logs are saved in
<drive>: \ WINNT \ system32 \ LoggerFiles
<drive>: \ WINNT \ system32 \ IIS Temporary Compressed Files

Microsoft IIS 7.0 Server

Web Server log files should be excluded from scanning. By default, IIS logs are saved in
<drive>:\inetpub\logs\n
Domino Data Directory

The data directory is used to store Domino email messages. Repeated scanning of this folder while it is
being updated with new messages is not an efficient way to scan locally stored email. Use virus
scanning applications like ScanMail for Domino to handle email viruses. By default, the Domino data
directory for a non-partitioned installation is <drive>: \ Lotus \ Domino \ Data.

Cisco CallManager

- Drive:\Program Files\Call Manager
- Drive:\Program Files\Call Manager Serviceability
- Drive:\Program Files\Call Manager Attendant

Microsoft SQL Server

Because scanning may hinder performance, large databases should not be scanned. Since Microsoft
SQL Server databases are dynamic, exclude the directory and backup folders from the scan list. If it is
necessary to scan database files, a scheduled task can be created to scan them during off-peak hours.
<drive>: \ Program Files \ Microsoft SQL Server \ MSSQL \ Data
<drive>: \ WINNT \ Cluster (if using SQL Clustering)
Q:\ (if using SQL Clustering)
C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Data
File extensions to exclude: .mdf, .ldf, .ndf, .bak, .tm

Cluster Servers

- Q:\ (Quorum drive)
- C:\Windows\Cluster

Microsoft SharePoint Portal Server

<drive>: \ Program Files \ SharePoint Portal Server
<drive>: \ Program Files \ Common Files \ Microsoft Shared \ Web Storage System
<drive>: \ Windows \ Temp \ Frontpagetempdir
M:\

Microsoft SharePoint Servers Foundation 2010
Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions
Drive:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files
Drive:\Users\ServiceAccount\AppData\Local\Temp
Drive:\Users\Default\AppData\Local\Temp
Drive:\Users\the account that the search service is running as\AppData\Local\Temp
Drive:\WINDOWS\system32\LogFiles
Drive:\Windows\Syswow64\LogFiles

Microsoft SharePoint Server 3.0 / 2007 / 2010

Drive:\Program Files\Microsoft Office Servers
Drive:\Program Files\Common Files\Microsoft Shared\Web Service Extensions
Drive:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files
Drive:\Documents and Settings\All Users\Application Data\Microsoft\SharePoint\Config
Drive:\Windows\Temp\WebTempDir
Drive:\Documents and Settings\the account that the search service is running as\Local Settings\Temp\n
Drive:\WINDOWS\system32\LogFiles

Reference: http://support.microsoft.com/kb/952167

Microsoft Systems Management Server (SMS)

SMS \ Inboxes \ SMS_Executive Thread Name
SMS_CCM \ ServiceData

Microsoft Operations Manager Server (MOM)

<drive>: \ Documents and Settings \ All Users \ Application Data \ Microsoft \ Microsoft Operations Manager
<drive>: \ Program Files \ Microsoft Operations Manager 2005

Microsoft Internet Security and Acceleration Server (ISA)

<drive>: \ Program Files \ Microsoft ISA Server \ ISALogs
<drive>: \ Program Files \ Microsoft SQL Server \ MSSQL$MSFW \ Data

Microsoft Windows System Update Server (WSUS)

<drive>: \ WSUS
<drive>: \ WsusDatabase

VMWare
Other file extension types that should be added to the exclusion list include large flat and designed files, such as VMWare disk partition. Scanning VMWare partitions while attempting to access them can affect session loading performance and the ability interact with the virtual machine. Exclusions can be configured for the directory(ies) that contain the Virtual Machines, or by excluding *.vmdk and *.vmem files.

Microsoft Exchange Server
Exclude the directory or partition where MS Exchange stores its mailbox. Use virus scanning applications like ScanMail for Exchange to handle email viruses. Installable File System (IFS) drive M must also be excluded to prevent the corruption of the Exchange Information Store.
Mapped Drives / Shared Folders
This option is best disabled. If it is enabled, it may create unnecessary network traffic when the end users access remote paths or mapped network drives. It can severely impact the user’s experience. Consider disabling this function if all workstations have OfficeScan client installed, and updated to the latest virus signature.

Volume Shadow Copies
Backup process takes longer to finish when real-time scan is enabled. There are also instances when real-time scan detects an infected file in the volume shadow copy but cannot enforce the scan action because volume shadow copies have read-only access.

It is also advisable to apply the latest Microsoft patches for the Volume Shadow Copies service: http://support.microsoft.com/kb/833167

Citrix Exclusions
On Citrix systems following extensions have been causing performance problems. Exclude these file extensions to avoid any performance problems.

*.*LOG, *.*DAT, *.*TMP, *.*POL, *.*PF

Novell Zenworks
C:\Program Files\Novell\Zenworks
Exclude the following files: NaIView.exe, Rmenf.exe, ZenNotifyIcon.exe, ZenUserDaemon.exe, casa.msi, duenf.dll, fileInfo.db, lcredmgr.dll, objInfo.db
Exclude the following extensions: .APPSTATE, .LOG, .TMP, .ZC

Other Trend Micro Products
Make sure the check box for *Exclude from scanning the directories where Trend Micro products are installed* is enabled in OfficeScan's Exclusion List settings.

**Additional References:**

Microsoft SQL Server: [http://support.microsoft.com/kb/309422](http://support.microsoft.com/kb/309422)
Microsoft Exchange 2003: [http://support.microsoft.com/kb/823166](http://support.microsoft.com/kb/823166)
Microsoft Exchange 2000: [http://support.microsoft.com/kb/328841](http://support.microsoft.com/kb/328841)
Microsoft Sharepoint Portal Server: [http://support.microsoft.com/kb/320111](http://support.microsoft.com/kb/320111)
Microsoft Systems Management Server: [http://support.microsoft.com/kb/327453](http://support.microsoft.com/kb/327453)
Microsoft IIS: [http://support.microsoft.com/kb/817442](http://support.microsoft.com/kb/817442)
Domain Controllers: [http://support.microsoft.com/kb/822158/en-us](http://support.microsoft.com/kb/822158/en-us)

## 6.7 Some Common Server Ports

<table>
<thead>
<tr>
<th>Application</th>
<th>Ports</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>21</td>
<td>TCP</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>TCP</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
</tr>
<tr>
<td>WINS Replication</td>
<td>42</td>
<td>TCP</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>Web server</td>
<td>80</td>
<td>TCP</td>
</tr>
<tr>
<td>Kerberos Authentication</td>
<td>88</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>TCP</td>
</tr>
<tr>
<td>Windows Time Synchronization Protocol – NTP</td>
<td>123</td>
<td>UDP</td>
</tr>
<tr>
<td>RPC</td>
<td>135</td>
<td>TCP</td>
</tr>
<tr>
<td>NetBIOS Name, Netlogon and Browsing</td>
<td>137,138</td>
<td>TCP</td>
</tr>
<tr>
<td>NetBIOS Session</td>
<td>139</td>
<td>UDP</td>
</tr>
<tr>
<td>IMAP4</td>
<td>143</td>
<td>TCP</td>
</tr>
<tr>
<td>IMAP3</td>
<td>220</td>
<td>TCP</td>
</tr>
<tr>
<td>LDAP</td>
<td>389</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>SSL (Secure Sockets Layer) Web server</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td>Server message block (SMB) for Netlogon, LDAP conversion, and Microsoft Distributed File System (DFS) discovery</td>
<td>445</td>
<td>TCP</td>
</tr>
<tr>
<td>SQL Server</td>
<td>1433</td>
<td>TCP</td>
</tr>
<tr>
<td>PPTP</td>
<td>1723</td>
<td>TCP</td>
</tr>
<tr>
<td>Global Catalog LDAP</td>
<td>3268</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>Remote Desktop (Terminal Services)</td>
<td>3389</td>
<td>TCP</td>
</tr>
<tr>
<td>Citrix Server</td>
<td>1494,2598</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Note:** It is advisable to disable the firewall of the OSCE clients that are installed on the server platform.
## Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/16/2010</td>
<td>Document created</td>
<td>Alp Deveci, Jill Chua-Maceda, Jessie Prevost, Alwin Yu</td>
</tr>
<tr>
<td>9/9/2010</td>
<td>Edited and removed settings that changed since Beta</td>
<td>Alp Deveci</td>
</tr>
</tbody>
</table>