Trend Micro™
Worry-Free Business Security 8.0

Best Practice Guide
Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Copyright © 2012 Trend Micro Incorporated. All rights reserved.

No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Authors: Portia Gantioque
Editorial: Nadia Trivinio

Released: December 2012
# Table of Contents

Chapter 1: Product Description .......................................................... 5  
  1.1. Security Server ........................................................................... 5  
  1.2. Smart Scan Server ....................................................................... 5  
  1.3. Security Agents............................................................................... 6  
  1.1 > Web Console .............................................................................. 6  
  1.2 > What’s New in Worry-Free Business Security 8.0 ....................... 7  

Chapter 2: Planning ........................................................................... 8  
  2.1 > Planning Guide........................................................................... 8  
  2.2 > Protection Component Considerations ....................................... 8  
  2.3 > The Typical Small Business Network ....................................... 10  
  2.4 > Deploying WFBS 8.0 on a Windows Small Business Network .... 11  

Chapter 3: Installation ..................................................................... 13  
  3.1 > Recommended Hardware .......................................................... 13  
      3.1.1 Typical or Minimal vs. Custom Installation ......................... 14  
      3.1.2 Use the WFBS 8.0 Downloader ............................................ 16  
      3.1.3 Recommendations for Installation .................................... 16  
  3.2 > Upgrade Considerations ............................................................ 19  
  3.3 > Migration From a 3rd Party Antivirus solution......................... 21  
  3.4 > IPv6 Requirements for Upgrades .............................................. 22  
  3.5 > Upgrade Best Practices ............................................................. 22  
      3.5.1 Previous Version Upgrades ................................................. 23  
  3.6 > Compatibility Issues ................................................................. 24  
  3.7 > WFBS Ports ............................................................................... 25  
  3.8 > IPv6 installation requirements .................................................. 26  

Chapter 4: Post Installation Management Task ................................ 28  
  4.1 > Post Installation Tasks ............................................................. 28  
  4.2 > Trend Micro Vulnerability Assessment ..................................... 30  

Chapter 5: Password Management .................................................. 39  
  5.1 > How to Reset the Console Administrator Password ................ 40  
  5.2 > How to Reset the Uninstall or Unload Security Agent Passwords 40  
  5.3 > Bypassing the Uninstall Password of a Security Agent ............ 41  

Chapter 6: Configuration ................................................................. 42  
  6.1 > Management Console Settings ............................................... 42  
  6.2 > INI Configuration Files ............................................................ 44  
  6.3 > Performance Tuning ................................................................. 45  
  6.4 > Import/Export Settings .............................................................. 47  
      6.4.1 How to Configure IPv6 addresses ...................................... 50  

Chapter 7: Backup and Disaster Recovery ...................................... 52  
  7.1 > Configuring Database flush in WFBS 8.0 ................................. 52  
  7.2 > Security Server Database Files ............................................... 52  
  7.3 > Security Server and Messaging Security Agent Configuration Files 53
Chapter 8: Behavior Monitoring .................................................................55
  8.1 > Default Settings for Behavior Monitoring ..............................................55
  8.2 > How to Properly Deploy Behavior Monitoring in WFBS 8.0 ...............55
    8.2.1 Trusted Program and Device Control ..................................................59
Chapter 9: Miscellaneous ..........................................................................62
  9.1 > Recommended Scan Exclusion List in Windows Platform ....................62
  9.2 > How to improve Update Process .............................................................65
  9.3 > Virtualization ........................................................................................69
  9.4 > Recommended Installation Adjustments for Special Environments .......70
  9.5 > Supported Upgrade procedure .................................................................70
  9.6 > Summary of Tools that can be used for Troubleshooting .....................72
Chapter 10: About Trend Micro .................................................................73
  10.1 > Contributors and Sources .................................................................73
  10.2 > Inserting Contact Information (for Resellers and Partners) ...............74
Chapter 1: Product Description

Worry-Free Business Security (WFBS) is comprised of the following:

1.1.1 Security Server

In the center of Worry-Free Business Security is the Security Server. The Security Server hosts the web, the centralized web-based management console for Worry-Free Business Security. The Security Server installs agents to clients on the network and along with the agents, forms an agent-server relationship. The Security Server enables:

- viewing security status information,
- viewing agents,
- configuring system security,
- downloading components from a centralized location

The security server also contains a database where it stores logs of detected Internet threats being reported to it by the agents.

The Security Server also performs these important functions such as:

- Installation, monitoring, and agent management.
- Downloads the components needed by agents (By default, the Security Server downloads components from the Trend Micro ActiveUpdate server, and then distributes them to agents).

1.1.2 Smart Scan Server

The Security Server includes a service called Scan Server, automatically installed during Security Server installation. As such, there is no need to install it separately. The Scan Server runs under the process name iCRCService.exe and appears as Trend Micro Smart Scan Service from Microsoft Management Console. When Security Agents use a scan method called Smart Scan, the Scan Server helps these agents run scans more efficiently. The Smart Scan process can be described as follows:

- The Security Agent scans the client for security threats using the Smart Scan Agent Pattern, a lightweight version of the traditional Virus Pattern. The Smart Scan Agent Pattern holds most of the threat signatures available on the Virus Pattern.
● Security Agent that cannot determine the risk of the file during the scan. It verifies the risk by sending a scan query to the Scan Server. It verifies the risk using the Smart Scan Pattern, which holds the threat signatures not available on the Smart Scan Agent Pattern.

● The Security Agent "caches" the scan query result provided by the Scan Server to improve the scan performance.

1.1.3 Security Agents

Agents protect clients from security threats. Clients include desktops, servers, and Microsoft Exchange servers. The WFBS agents are:

<table>
<thead>
<tr>
<th>Agent</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Agent</td>
<td>Protects desktops and servers from security threats and intrusions</td>
</tr>
<tr>
<td>Messaging Security Agent (Advanced only)</td>
<td>Protects Microsoft Exchange servers from email-borne security threats</td>
</tr>
</tbody>
</table>

Figure 1 WFBS Agents

An agent reports to the Security Server from which it was installed. To provide the Security Server with the very latest client information, the agent sends event status information in real time. Agents report events such as threat detection, startup, shutdown, start of a scan, and completion of an update.

1.1 Web Console

The web console is the central point for monitoring clients throughout the corporate network. It comes with a set of default settings and values that can be configured based on the security requirements and specifications. The web console uses standard Internet technologies, such as Java, CGI, HTML, and HTTP.

Use the web console to:

● Deploy agents to clients.
● Organize agents into logical groups for simultaneous configuration and management.
● Set antivirus and anti-spyware scan configurations, and start Manual Scan on a single group or on multiple groups.
● Receive notifications and view log reports for threat-related activities.
● Receive notifications and send outbreak alerts through email messages, SNMP Trap, or Windows Event Log when threats are detected on clients.
● Control outbreaks by configuring, and enabling Outbreak Defense.
### 1.2 What’s New in Worry-Free Business Security 8.0

<table>
<thead>
<tr>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Support</td>
<td>The Security Server, Security Agents, Messaging Security Agents (Advanced only), and Remote Manager Agent can now be installed on IPv6 clients.</td>
</tr>
<tr>
<td>Advanced Cleanup</td>
<td>When configured to run advanced cleanup, Security Agents can stop activities by rogue security software, also known as FakeAV. The agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV behavior. Enable advanced cleanup on Security Agents when configuring the Manual Scan and Scheduled Scan settings.</td>
</tr>
<tr>
<td>Action against probable virus/malware</td>
<td>For probable virus/malware, the default action is &quot;Deny Access&quot; during Real-time Scan and &quot;Pass&quot; during Manual Scan and Scheduled Scan. If these are not the preferred actions, it can be changed to Quarantine, Delete, or Rename.</td>
</tr>
<tr>
<td>Security Agent Installation Path</td>
<td>During the Security Server installation, a window appears prompting to specify the installation path where Security Agents are installed. In previous versions and the Security Server installation has been completed, the installation path cannot be changed. However, in this version, the installation path from the web console can be changed by navigating to Preferences → Global Settings → System → Security Agent Installation directory section. After changing the path, new Security Agents will be installed to this path.</td>
</tr>
<tr>
<td>Support Vmware Solution</td>
<td>Microsoft Hyper-V 3.0 and Vmware Workstation 8.0 are now supported.</td>
</tr>
<tr>
<td>New client architecture</td>
<td>Single platform for OfficeScan and WFBS</td>
</tr>
<tr>
<td>Security Server Database</td>
<td>Frequent flushing of database to reduce instance of HTTPDB crash.</td>
</tr>
<tr>
<td>Client Shutdown after Scheduled Scan</td>
<td>A new setting in the web console (Scans → Scheduled Scan → Schedule tab) allows agents to initiate a shutdown of the client after completing a Scheduled Scan. This setting can only be configured from the web console, and is not available to users with Scheduled Scan privileges.</td>
</tr>
<tr>
<td>Notification</td>
<td>A button is available to test notification on the Security Server.</td>
</tr>
<tr>
<td>Mac Client Protection</td>
<td>Support for MAC OS 10.8 – Mountain Lion</td>
</tr>
<tr>
<td>New Client Language UI</td>
<td>New button to switch languages</td>
</tr>
<tr>
<td>Server UI for Tmproxy Exclusion</td>
<td>Add Server UI for user to add process image name for Tmproxy</td>
</tr>
</tbody>
</table>
Chapter 2: Planning

2.1 > Planning Guide

These are basic key questions that need to be answered prior to the actual deployment:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the existing company policies that need to be considered prior to migration or deployment?</td>
<td>Identify these to guide the deployment process according to the company policies.</td>
</tr>
<tr>
<td>Are there any remote networks that are dependent on the main corporate network? What is the network bandwidth for these remote connections?</td>
<td>Remote networks with low bandwidth can influence the Security Agent deployment method. Client packages can be used in order to deploy Security Agents to remote clients.</td>
</tr>
<tr>
<td>How many clients are situated in the main office and the remote offices?</td>
<td>This will identify the location and number of update agents on the main and remote office.</td>
</tr>
<tr>
<td>Is there an existing desktop antivirus solution on the network? Is there a previous version of Worry-Free Business Security or Client/Server Messaging Security installed on the network?</td>
<td>Migration from third party antivirus solutions and previous Worry-Free Business Security version should be carefully planned. WFBS 5/5.1, 6.0, 7.0 can be upgraded to WFBS 8.0. If CSM 3.x is used, upgrade to WFBS 6.0 is needed before upgrading to WFBS 8.0.</td>
</tr>
<tr>
<td>Are there any other antivirus programs installed on the server where Worry-Free Business Security will be installed?</td>
<td>Third party antivirus management programs may create errors in the Worry-Free Business Security 7.0 installation. Uninstall the third party antivirus management program prior to installing WFBS 8.0.</td>
</tr>
<tr>
<td>On which server will WFBS 8.0 Security Server be installed? What is this server's current role in the network? What are the applications that run on this server?</td>
<td>Knowing server performance is vital in order to decide if WFBS 8.0 Security Server should be hosted on an existing or a new server.</td>
</tr>
</tbody>
</table>

Table 1: Planning Guide

2.2 > Protection Component Considerations

In order to have a successful implementation of WFBS, there are several things necessary to consider regarding the components that will be protected.

Important: Make sure that all hardware/software requirements are met. Check the minimum requirements found in the Getting Started Guide and the Administrator Guide, or in the readme file that comes with the installation package.
### Security Server

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>New server or an existing multi-role server?</td>
<td>A new server would primarily need to meet the basic hardware/software requirements. An existing multi-role server will need a performance evaluation before WFBS (Worry-Free Business Security Server) is installed.</td>
</tr>
<tr>
<td>Server Role: Microsoft SBS or member server?</td>
<td>Microsoft SBS has Microsoft Exchange on the same server as the SBS Server. Trend Micro WFBS 8.0 automatically detects Microsoft Exchange when it is installed on the same box. For member servers, administrators need to select and add Microsoft Exchange servers during, or after the Security Server installation in order to install the Messaging Security Agent.</td>
</tr>
<tr>
<td>Displacement: Migration from a 3rd party Antivirus solution</td>
<td>A Migration plan is necessary for existing third party antivirus solutions. Although WFBS 8.0 supports automatic third party client protection uninstallation, administrators need to manually uninstall 3rd party antivirus software on the management server. To determine the list of antivirus products that can be uninstalled, refer to EN-1060980 open tmuninst.ptn on the Security Server installation disk. This file can be opened by any text editor e.g. notepad at \Trend Micro\Security Server\PCCSRV\Admin.</td>
</tr>
<tr>
<td>Migration from a previous WFBS/CSM version</td>
<td>Like 3rd party antivirus solutions, previous CS/CSM versions need a migration/upgrade process.</td>
</tr>
</tbody>
</table>

### Messaging Security Agent

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Microsoft Exchange on the same server as the Security Server?</td>
<td>Worry-Free Business Security 8.0 installation automatically detects Microsoft Exchange installation on the same box.</td>
</tr>
<tr>
<td>Is there an existing messaging protection solution for Microsoft Exchange?</td>
<td>Third party antivirus solutions for Microsoft Exchange needs to be removed prior to the Messaging Security Agent installation.</td>
</tr>
</tbody>
</table>

### Security Agent

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displacement: Is there an existing 3rd party Antivirus?</td>
<td>Migrate clients by stages. First, migrate several clients and then continue by department or by a designated number of PCs. Then, uninstall the 3rd party antivirus management server. This method will have minimum impact on business operations.</td>
</tr>
<tr>
<td>Scheduling Deployment</td>
<td>Schedule migration/installation and deployment during off-peak hours. A long weekend/holiday is the best time for migrating and deploying WFBS 8.0.</td>
</tr>
<tr>
<td>Client types: office and out-of-office</td>
<td>Administrators can have a different set of privileges for office and out-of-office clients. This allows mobile clients the flexibility that they need, such as for scheduled updates and update from the Internet.</td>
</tr>
</tbody>
</table>

Table 2: Planning Component
2.3 The Typical Small Business Network

Figure 1 shows a typical small business network. A majority of small businesses use Microsoft Small Business Server because it comes with the necessary network applications for a small business such as mail, collaboration, and remote access. The network is typically flat, with 1-2 servers, and less than 75 other computers.

Internet connectivity is provided by a leased line/DSL or cable connection, depending on what is available on the area. A commercial off-the-shelf firewall provides network address translation and VPN connectivity. The network is usually managed by a single person, usually not full time.

On some occasions, a remote office or home network needs access to the main office. A point-to-point VPN connection is made available for this purpose. Mobile computers can access essential office services using SBS’ Remote Web Workplace.

Figure 2 Typical SBS Network
2.4 > Deploying WFBS 8.0 on a Windows Small Business Network

Figure 2 above summarizes the deployment strategy for the typical small business network previously described.

Install WFBS 8.0’s Security Server (SS) on the Microsoft SBS if a single server on the network is used. Otherwise, it can be uninstalled on another available underutilized server.

Messaging Security Agent (MSA) can be installed remotely once the security Server is installed. MSA needs to reside on the server hosting of the Microsoft Exchange.

Security Agents (SA) can be installed on local and remote computers using several methods. Refer to the WFBS8_Installation_and_Upgrade guide for the preferred client deployment method.

An update agent for remote networks can be specified. The update agent acts as the update source for specified computers and is responsible for pulling out the updates from the WFBS 8.0 server. This reduces bandwidth, since only the update agent computers download the updates for the entire remote network.

Special firewall policies need to be added if the remote computer’s SA is necessary to communicate back to the SS. This is not a requirement as remote computers will download updates from Internet when not connected to the office. Any security logs will be uploaded once
the mobile computer returns back to the office network. To make the SS to report an up-to-date security events from remote clients, ports need to be opened on the firewall and redirect (forward) it to the WFBS 8.0 server IP. These ports are documented in Figure 2.
3.1 > Recommended Hardware

The following are the recommended setup to maximize performance of Worry-Free business security.

For the list of minimum requirements in deploying, refer to the ff. documents:

System requirements:
http://docs.trendmicro.com/all/smb/wfbs-s/v8.0/en-us/wfbs_8.0_sysreq.pdf

For Installation and Deployment Guide:
http://docs.trendmicro.com/all/smb/wfbs-s/v8.0/en-us/wfbs_8.0_iug.pdf

- Security Server
  Memory:
  32 Bit: Conventional Scan: 1GB; Smart Scan: 2GB
  64 Bit: Conventional or Smart Scan: 2GB

  Available Disk Space: 11GB total
  4.1GB for the Security Server program files
  6.9GB for Security Server operations

  **NOTE** 11GB is exclusively for the Security Server. Additional disk space is necessary because the Security Agent will also be installed on the same computer as the Security Server (installing the Messaging Security Agent is optional).

- Security Agent
  Smart Scan:
  - 450MB total for Security Agents
  300MB for the Security Agent program files
  150MB for Security Agent operations

- 800MB total for Update Agents
  300MB for the Update Agent program files
500MB for Update Agent operations

- Conventional Scan:
700MB total for Security Agents
400MB for the Security Agent program files
300MB for Security Agent operations

1050MB total for Update Agents
400MB for the Update Agent program files
650MB for Update Agent operations

3.1.1 Typical or Minimal vs. Custom Installation

The typical installation method automatically makes decisions about the installation by selecting default values for certain pre-configuration questions. To change the default values, a custom installation is necessary. Below is a table of the installation steps available for typical and custom installations.

![Figure 4: Typical Installation Workflow](image-url)
Figure 5 - Custom Installation Workflow
3.1.2 Use the WFBS 8.0 Downloader

WFBS installer packages can be downloaded using a downloader utility. There are several advantages on using the utility:

- The downloader utility uses multiple connections to download the package.
- The download can be paused/resumed if needed.
- It checks the available disk space prior to downloading.
- It verifies the MD5 hash of the downloaded package to detect corrupted downloads.

- The downloader uses proxy setting configured on the browser (IE). It does not support the proxy auto config script file, therefore IE needs to be explicitly pointed to the server IP address or hostname.

![Trend Micro Worry-Free Business Security Setup](image)

Figure 6 Downloader tool

3.1.3 Recommendations for Installation

Installation of WFBS 8.0 requires some planning. Recommendations include the following:

1. Before deploying WFBS 8.0, plan the order of how the installation will progress. To learn more about the deployment options available for WFBS 8.0, refer to the Administrator’s Guide.

2. On the average, a typical fresh installation of WFBS 8.0 Security Server takes 15-25 minutes. Typical install invokes prescan. This can affect the time. Also, if during Prescan, there are detected malwares, it requires user intervention in selecting the desired action for the detected viruses.

3. The Messaging Security Agent (MSA) installs in about the same amount of time, while a Security Agent (SA) can be installed in 5-10 minutes. Typically, a small company can roll out all the WFBS components in a single day.
4. Schedule the installation off peak hours, preferably after a system backup so that in the event of any possible failure, all system settings can be recovered.

5. Uninstall any 3rd Party antivirus management component on the server that will host the Worry-Free Business Security Server. If this server is also a Microsoft Exchange Server, uninstall any 3rd party antivirus solution for Exchange.

6. Prior to installing WFBS, consider the following disk recommendations:
   ○ If possible, install WFBS on a partition other than the boot partition. If the system has two disks, install WFBS on the disk not hosting the boot/system partition. It improves the overall disk performance.
   ○ WFBS server components require 4.1GB of disk space for installation and another 6.9GB for operation. Ensure there is sufficient space to host the installation directory.

7. During the Security Server installation process, there are other options which needs to be selected:
   ○ Pre-scanning - This basic pre-scan is recommended. However, it is also recommended that a scan is initiated after the pattern and engine files have been updated.
   ○ Fully Qualified Domain Name (FQDN) – prior to WFBS 8.0, the FQDN setting is automatically detected by the setup program and cannot be changed. On an SBS network, the FQDN is defaulted to the internal FQDN of the SBS server. In WFBS 8, an option to specify an externally-accessible FQDN. Setting this value to an externally-accessible FQDN allows remote Security Agents to upload log information while outside the company network. Choose the appropriate IP addressing, either IPv4 or IPv6 for the Security Server. Check the IPv6 Limitations before deploying using IPv6 addressing. Refer to Security Server IPv6 requirements in Installation and Upgrade Guide.
   ○ Target Directory - Choose a directory with more than 11GB of free space
   ○ IIS vs. Apache - Use IIS for integrated Windows Authentication - Recommended. Use Apache when IIS is not available on the hosting server.

8. **Remote Installation** is one of the easiest deployment options for Worry-Free Business Security. Take note of the following points when using this deployment option:
   - The Windows “Server” system service should be started
   - For Windows XP Professional computers, Simple File Sharing must be disabled. Remote Installation on Windows XP Home computers is not supported.
   - For computers running Windows Vista, 7, 8 and 2012, the following should be performed before the Remote Install:
     ○ The “Remote Registry” system service should be started.
○ User Access Control (UAC) should be disabled Allow File and Print Sharing through the Windows Firewall Exception.

![Figure 7 Allow File and Printer Sharing on Windows Firewall](image)

**NOTE** Auto pcc, Login Script, TMVS and Client Package deployment is not supported on terminal sessions.

9. A single Security Server installation can manage up to 2,500 clients. If there is more clients, Trend Micro suggests installing more than one Security Server. If the security server manages clients, the bandwidth consumption in the network can be possibly high (especially when Smart Scan is enabled on the server).

Verify if sections identified on the network between Security Agents and the Security Server as “low-bandwidth” or “heavy traffic”, Security Agents can be specified to act as update sources (Update Agents) for other agents. This helps distribute the burden of deploying components to all agents.

For example, if the network is segmented by location, and the network link between segments experiences a heavy traffic load, Trend Micro recommends allowing at least one Security Agent on each segment to act as an Update Agent.

10. Internet Explorer Enhanced Security Configuration - Internet Explorer’s Enhanced Security Configuration can cause the WFBS web console to be inaccessible. Add the URL: http://servername:port as an allowed site in order to access the WFBS web console.

11. Update the scan engine and pattern files immediately. By default, WFBS 8.0 initiates an update task after installation.

12. Check installation success. Access the WFBS 8.0 web console


15. Create different client/server agent groups and customize settings such as client privileges, scan settings, directory exclusions etc.

16. Management Console publishing (Optional) - Publish the secured web console on the firewall. It allows users secure web access to the WFBS web console.

### 3.2 > Upgrade Considerations

1. If upgrading from a previous version of WFBS, perform the upgrade procedure in the Security server in about 20-30 minutes. The Security Agent (SA) and Messaging Security Agent (MSA) computers are automatically upgraded. The component versions can be verified on the SA computers by right-clicking the SA system tray icon and selecting **Component Versions**.

2. After installing, uninstalling or upgrading an SA computer, make sure to restart the system. The restart deletes any temporarily files that were previously tagged as locked. Upgrade of firewall and proxy drivers requires a restart and the SA notifies the user by a popup.

3. Assuming there is an existing WFBS installation on a Windows 2003/SBS 2003 server and there is a need to move the Security Server to a new machine, the following can be performed:
   
   3.1. Before installing WFBS 8.0 on the new server, take note of the client port used by the Security Agent. Configure the new server to use the same client port to talk back to the SA. In the figure below, the client port is port 52660.

   ![Figure 8: WFBS Client and Server Port](image)

   **NOTE**: this is randomly chosen by the installer when the Security Server is installed. Additionally, take note of the server port. The default is 8059.

   **IMPORTANT**: YA Custom Installation is necessary to allow the specification of the client port used by the old server. Using typical installation would allow the installer to use a random port.

3.2. Install WFBS 8.0 Security Server on the new server. The WFBS installer allows the installation of MSA and SA on the same server.
3.3. Once the new WFBS Security Server is installed, the SAs needs to be moved to the new Security Servers. There are two ways to do this:

**Online Clients** – For online clients, the Move feature can be used on the old Security Server to move SA to the new Security Server. Select the clients to move, and then click the Move icon.

Specify the IP address of the new Security Server and the server port. The default server port is 8059.
Wait for a few minutes, then check the clients’ status in the WFBS management console.

**Offline Clients** -- the Move function cannot be used for offline clients. To automatically move offline clients when they get online and logs in to the network, the ipXfer utility can be used found in the

\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\IpXfer

Directory of the Security Server. Add this line to the user logon script so that it automatically executes when user logs onto the domain. The utility has the following syntax:

```plaintext
ipXfer.exe -s Server_Name -p Server_Port [-c Client_Port]
ex: ipXfer.exe -s 172.20.0.2 -p 8059 -c 49273
```

Verify if the clients are reporting to the new Security Server. To verify, open the SA console and click the green icon on the bottom right. The Security Server that the agent is reporting to is listed on the “Connected to Server” section.

### 3.3 > Migration From a 3rd Party Antivirus solution:

1. Check if the 3rd party antivirus software can be uninstalled automatically by Trend Micro Security Agent setup.


2. If the antivirus software is listed under **Anti-virus software that WFBS can detect and uninstall** section, the WFBS agent setup can be run on top. Otherwise, manually uninstall the antivirus software from the system’s Add/Remove Programs.
3. If the antivirus software is listed under “Anti-virus software that WFBS can detect, but cannot uninstall” section, these software can be detected by the WFBS agent setup, but it has to be manually uninstalled from the system’s Add/Remove Programs.

Not all other antivirus software not listed in the list will be detected by the WFBS agent setup. Any antivirus software must be uninstalled before running the WFBS agent setup to avoid any conflict on the system. i.e. BSOD due to drivers’ conflict.

4. If the uninstallation of the antivirus software failed, contact the software vendor. Trend Micro Security Agent setup only launches the software’s uninstallation program.

5. If the antivirus software are not listed in either “Anti-virus software that WFBS can detect but cannot uninstall” or “Anti-virus software that WFBS can detect and uninstall” sections, Trend Micro Support can help modify the WFBS agent installer to detect these antivirus software.

Before contacting Trend Micro Technical Support, prepare the existing antivirus software’s installer. Otherwise, if the installer cannot be retrieve, there is still an option to manually uninstall it from the system’s Add/Remove Programs.

### 3.4 IPv6 Requirements for Upgrades

The IPv6 requirements for the Security Server are as follows:

- The Security Server to be upgraded must be installed on Windows Server 2008, SBS 2008/2011, 7, and Vista. Security Servers on Windows XP, Server 2003, and SBS 2003 cannot be upgraded because these operating systems only support IPv6 addressing partially.

- The Security Server must already be using an IIS web server. Apache web server does not support IPv6 addressing.

Assign an IPv6 address to the Security Server. In addition, the server must be identified by its host name, preferably its Fully Qualified Domain Name (FQDN). If the server is identified by its IPv6 address, all clients currently managed by the server will lose connection with the server. If the server is identified by its IPv4 address, it will not be able to deploy the agent to pure IPv6 clients.

Verify that the Security Server host machine’s IPv6 or IPv4 address can be retrieved, for example, the “ping” or “nslookup” command.

### 3.5 Upgrade Best Practices

The client settings can be preserved when upgrading to the newest version of WFBS.

To ensure that that the existing settings can be easily restored if the upgrade is unsuccessful, Trend Micro recommends the following:

- Backing up the Security Server database
  - Deleting all log files from the Security Server
  - Backing up configuration files.
Refer to section 7.3 for the Security Server and Messaging Security Agent Configuration Files to back-up.

**Backing Up the Security Server Database**

Procedure:

2. In Windows Explorer, go to the Security Server folder and copy the contents of \PCCSRV\HTTPDB to another location (such as a different folder on the same server, to another computer, or to a removable drive).
3. Deleting Log Files from the Security Server
4. Procedure
   5.2. Set Delete Logs Older Than to 0 for a log type.
   5.3. Click Delete.
   5.4. Repeat steps 2 to 3 for all log types.

**3.5.1 Previous Version Upgrades**

This product version supports upgrades from any of the following WFBS or WFBS Advanced versions:

- 7.x (7.0 and 7SP1)
- 6.x (6.0, SP1, SP2, and SP3)

This product version does not support upgrades from any of the following:

- All upgrades that supported Windows 2000
- Client/Server Messaging Security 3.6 (except for Japanese version)
- Client/Server/Messaging Security 3.5
- Client/Server/Messaging Security 3.0
- Client/Server Security 3.0
- Client/Server Suite 2.0
- Client/Server/Messaging Suite 2.0
- WFBS 5.x
- OfficeScan or ScanMail for Microsoft Exchange
- One language to another
Forbid upgrade is not supported since WFBS 7.x. We can only delay upgrade or upgrade all agents immediately.

### 3.6 > Compatibility Issues

This section explains compatibility issues that may arise with certain third-party applications. Always refer to the documentation of all third-party applications that are installed on the same computer (which the Security Server and other Worry Free components will be installed.

<table>
<thead>
<tr>
<th>Application</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Endpoint Security Software</td>
<td>Before installing the Security Server, Trend Micro recommends manually removing other endpoint security software from the target computer, this may block the installation or influence the Security Server’s performance after installation.</td>
</tr>
<tr>
<td>Security Applications in Windows SBS and EBS 2008</td>
<td>WFBS is compatible with both Windows Small Business Server (SBS) 2008, and Windows EBS (Essential Business Server) 2008. However, some security applications that are either installed with or managed through these operating systems may conflict with WFBS. For this reason, you may need to remove these security applications.</td>
</tr>
<tr>
<td>Messaging Security Agent and Forefront</td>
<td>The Messaging Security Agent cannot be installed on Microsoft Exchange servers that have Forefront (Microsoft Forefront Security for Exchange Server) installed. Uninstall Forefront and ensure that the Microsoft Exchange Information Store service is started before installing the Messaging Security Agent.</td>
</tr>
<tr>
<td>Security Agents and OneCare</td>
<td>Although the Security Server can be installed with Microsoft Windows Live™ OneCare for Server, the Security Agent cannot be installed with the OneCare client. The Security Agent installer will automatically remove OneCare from clients.</td>
</tr>
<tr>
<td>Databases</td>
<td>Scanning databases may decrease the performance of applications that access the databases. Trend Micro recommends excluding databases and their backup folders from Real-time Scan. If there is a need to scan a database, perform a Manual Scan or schedule a scan during off-peak hours to minimize the impact.</td>
</tr>
<tr>
<td>Other Firewall Applications</td>
<td>Trend Micro recommends removing or disabling any other firewall applications prior to installing the WFBS firewall, including: Windows Internet Connection Firewall (ICF) Windows Firewall (WF) However, if there is a need to run ICF or any other third-party firewall, add the Trend Micro Security Server listening ports to the firewall exception list (see for information on listening ports and refer to the firewall documentation for details on how to configure exception lists).</td>
</tr>
</tbody>
</table>

Table 3 Application Compatibility List
3.7 > WFBS Ports

WFBS uses the following ports:

**Server listening port (HTTP port):**

Used to access the Security Server. By default, WFBS uses one of the following:

- IIS server default website: The same port number as the HTTP server’s TCP port.
- IIS server virtual website: 8059
- Apache server: 8059

**Client listening port:**

A randomly generated port number through which the Security Agent and Messaging Security Agent receive commands from the Security Server.

**Important:** Today’s cyber criminals use HTTP and direct their attacks at ports 80 and/or 8080 – commonly used in most organizations as the default Transmission Control Protocol (TCP) ports for HTTP communications. If the organization is currently using one of these ports as the HTTP port, Trend Micro recommends using another port number.

**Scan Server ports:**

Used by the Scan Server to communicate with Security Agents for scan queries.

**NOTE** To find out which port the Security Agents are using to connect to the Scan Server, open ..\PCCSRV\SSCFG.ini in the folder where the server is installed.

<table>
<thead>
<tr>
<th>PORT TYPE</th>
<th>IIS DEFAULT</th>
<th>IIS VIRTUAL</th>
<th>PRE-INSTALLED APACHE</th>
<th>NEW APACHE INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SSL port</td>
<td>Non-SSL port on web server</td>
<td>First open port in range 8082 to 65536</td>
<td>Non-SSL port on web server</td>
<td>Non-SSL port on web server</td>
</tr>
<tr>
<td>SSL port</td>
<td>SSL port on web server</td>
<td>First open port in range 4345 to 65536</td>
<td>N/A</td>
<td>SSL port on web server</td>
</tr>
<tr>
<td>Using SSL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL port</td>
<td>First open port in range 4345 to 65536</td>
<td>First open port in range 4345 to 65536</td>
<td>N/A</td>
<td>First open port in range 4345 to 65536</td>
</tr>
<tr>
<td>Not using SSL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 13: Scan Server Ports
Trend Micro Security (for Mac) Communication port:
Used by the Trend Micro Security (for Mac) server to communicate with Mac clients. The default is port 61617.

**NOTE** | Trend Micro Security (for Mac) is a WFBS plug-in and is licensed separately. Contact your Trend Micro representative for inquiries about this plug-in.

SMTP port:
Used by the Security Server to send reports and notifications to administrators through email. The default is port 25.

Proxy port:
Used for connections through a proxy server.

### 3.8 > IPv6 installation requirements

IPv6 support for Worry-Free Business Security started in version 8.0. Earlier WFBS versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading the Security Server, Security Agents, and Messaging Security Agents that satisfy the IPv6 requirements.

**Security Server IPv6 Requirements**
The IPv6 requirements for the Security Server are as follows:

- The server must be installed on Windows Server 2008/2012, SBS 2008/2011, 7, 8, and Vista. It cannot be installed on Windows XP or Server/SBS 2003 because these operating systems only support IPv6 addressing partially.
- The server must use an IIS web server. Apache web server does not support IPv6 addressing.
- If the server manages IPv4 and IPv6 agents, it has both IPv4 and IPv6 addresses, and must be identified by its host name. If a server is identified by its IPv4 address, pure IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.
- If the server manages only IPv6 agents, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.
- Verify that the host machine’s IPv6 or IPv4 address can be retrieved, for example, the “ping” or “nslookup” command.
- If the Security Server is being installed to a pure IPv6 computer, set up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Security Server and the Internet to allow the server successfully connect to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.
Security Agent Requirements
The Security Agent must be installed on:

- Windows Vista (all editions)
- Windows Server 2008 (all editions)
- Windows 7 (all editions)
- Windows SBS 2011
- Windows 8 (all editions)
- Windows Server 2012 (all editions)

It cannot be installed on Windows Server/SBS 2003 and Windows XP because these operating systems only support IPv6 addressing partially.

It is preferable for a Security Agent to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 addressing.

Messaging Security Agent Requirements
The Messaging Security Agent (Advanced only) must be installed on a dual-stack or pure IPv6 Microsoft Exchange server. It is preferable for a Messaging Security Agent to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 Addressing.
Chapter 4: Post Installation Management Task

4.1 Post Installation Tasks

1. Move clients and servers to the appropriate domain/group - Move clients to the proper Groups through the WFBS management console. Notify clients so that settings take effect. Replicate settings from one group for efficiency.

2. Assign Update Agents on remote sites. Assign Update sources to groups of clients. This will reduce WAN bandwidth consumption. Administrators can also use this strategy in order to deploy updates by network segments. This method used in conjunction with scheduled updates will effectively distribute update traffic.


4. Add Update Agents.

Figure 14: Update Source Configuration
5. Enable Alternative Update Sources.

![Enable Alternative Update Sources Screen](image1)

6. Add Client/Server Security Agent IP address range to Update Agents.

![Add Alternate Update Source Screen](image2)

7. Reorder Update Sources if necessary.
4.2 > Trend Micro Vulnerability Assessment

Trend Micro Vulnerability Assessment offers threat – virus correlation and maps vulnerabilities to Microsoft patches. Scan and perform actions periodically in order to mitigate threats.


2. Set the schedule for Vulnerability Scans and click Save.
Trend Micro Vulnerability Scanner

TMVS (Trend Micro Vulnerability Scanner) tracks unprotected servers and clients, it also offer protection component installation option. This helps administrators detect and take actions on unprotected hosts. An account with administrative privilege on the target PCs is needed to run TMVS.

**WARNING!** DO NOT run TMVS (Trend Micro Vulnerability Scanner) on servers with Terminal Services. TMVS may trigger false alerts from Intrusion Detection Systems.

**TO RUN/SCHEDULE A VULNERABILITY SCAN:**

1. On the local server, execute:
   
   Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\TMVS\TMVS.exe
2. An on-demand Vulnerability Scan can be initiated. Set and schedule vulnerability scans.

3. Under the **Settings** Menu, additional configuration options can be specified. Note that the Security Server is automatically detected by the tool.

![Figure 22: TMVS Settings](image)

- The Auto-install Client/Server Security Agent installation needs an account that has administrative rights on the target PCs.

- Trend Micro Vulnerability Scanner can even scan other 3rd party antivirus protection components.

**DEPLOYING SA VIA TMVS WITH WINDOWS FIREWALL ENABLED**

If the Install SA option does not work, ensure that the **File and Print Sharing Exception** under Windows Firewall is checked. This can be configured on the client computer's Windows Firewall settings.
If the customer has an Active Directory domain, Firewall settings can be configured using a Group Policy Object to multiple computers. This allows user to enable the firewall exception without having to visit each of the client computers. Refer to the Microsoft KnowledgeBase document for instructions on below:


Enable the Allow File and Print Exception Setting, under Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall.
Certificates

If Internet Explorer 7 is used, a certificate error appears on the first time the WFBS console is used. Proceed and click Continue to this Website or to prevent the browser error from appearing again, the Security Server certificate can be installed.

To install the server certificate:

1. On the Certificate Error message, click Continue to this website.

2. Click the Certificate Error bar on the right side of the IE7 address bar. The Untrusted Certificate message window displays.

3. Click View Certificates to open the Certificate window.

Figure 24: Untrusted Certificate Popup
4. Click Install Certificate > Next > Next > Finish.

5. Click Yes when the Security Warning prompt appears.

How to Properly Deploy Behavior Monitoring

When deploying Behavior Monitoring feature in WFBS 8 make sure to address the following:

1. Set up and deploy a pilot environment that matches the production environment as closely as possible.
2. Ensure that the following are included in the pilot environment:
   - Business applications
   - Custom developed applications
   - Critical applications used by groups or individuals (such as Payroll, Inventory, Accounting and Database applications)

3. Deploy the Client/Server Security Agents into the pilot environment with the features that will be enabled.

4. Allow the pilot environment to run for a reasonable amount of time (a “soak time”) with the standard applications running and with an average daily use.

5. Identify system-intensive applications:

   Trend Micro provides a standalone performance tuning tool to help identify applications that could potentially cause a performance impact during deployment. Trend Micro recommends running the **TMPerfTool**, available from Trend Micro Technical Support, on a standard workstation image and/or a few target workstations during the pilot process to determine any potential software or driver conflicts that may cause disruptions during the final deployment of the Behavioral Monitoring and Device Control features.

   **TO USE THE TMPerfTool:**

   1. Obtain a copy of the TMPerfTool Utility from the program directory of the Security Server under \Trend Micro\Security Server\PCCSRV\Admin\Utility\TMPerfTool
   2. Choose the proper version based on the platform of the Security Agent being tested (32-bit or 64-bit). Place the TMPerfTool.exe file in the BM folder under the **Client Security Agent** directory (%ProgramDir%/Trend Micro/BM).
   4. Click Analyze when the system or applications start to slow down.
   5. When a red highlighted row appears, it means that the TMPerfTool found the resource-intensive process.
   6. Select the highlighted row and click Exclude.
   7. After excluding the process, verify if the system or application performance improves, then perform one of the following:
      - If the performance drops again, it means that the root cause is found.
   8. Note the name of the application.
   9. Click **Stop**.
   10. Review the applications and associated processes that have been identified as conflicting.
These will automatically be added to the Exceptions list in the Behavior Monitoring configuration. Review the list and make any necessary modifications. To add an additional application:

a. Open the WFBS console.

b. Go to Security Settings > Select a group > Configure > Behavior Monitoring.

c. Under Exceptions section, add the applications.

NOTE In this release, UNC paths are now supported in the Behavior Monitoring Exception List. This will allow to allow or block programs running from network drives.

Figure 27: BM Exception

**Trusted Programs**

There may be some programs that are active and consume many resources such as a database server or a backup program. If performance issues occur even after the programs have been excluded from Behavior Monitoring, the program can be further excluded from real-time scanning to prevent added performance issues.

**TO ADD A PROGRAM TO THE TRUSTED PROGRAMS LIST:**

1. From the Security Settings page, click on the group that contains machines with the application to be excluded. Click Configure.
2. Click on Trusted Programs.
3. Type in the full file path to the specific program executable.
4. Click Add to Trusted Program List.
Install Latest Patches


When a major hotfix, service pack, or patch release occurs, a notification is displayed on the Live Status page of the WFBS dashboard.
Chapter 5: Password Management
5.1 > How to Reset the Console Administrator Password

Trend Micro recommends using strong passwords for the web console. A strong password is at least eight characters long, has one or more uppercase letters (A-Z), has one or more lowercase letters (a-z), has one or more numerals (0-9), and has one or more special characters or punctuation marks (!@#$%^&,.:;?). Strong passwords never are the same as the user’s login name or contain the login name in the password itself. They do not consist of the user’s given or family name, birth dates, or any other item that is easily identified with the user.

**PROCEDURE**

1. Navigate to Preferences > Password. Or alternatively go to shortcut option under Start > Programs > Trend Micro Worry-Free Business Security > Console Password Reset Tool.

![Figure 29: Console Password Reset Tool window](image)

2. Update the following options as required:
   - Old password
   - New password
   - Confirm password: Re-type the new password to confirm.

3. Click Save.

5.2 > How to Reset the Uninstall or Unload Security Agent Passwords

Unlike the Console Administrator Password that can be manually reset if there is a physical access to the system, the Uninstall and Unload passwords for the Security Agent can only be reset from
the Administrator Console. therefore there is a need access to the Administrator account. If there is no access to the console, refer to the previous section.

To specify/clear a password during agent unload or removal, go to Preferences | Global Settings | Desktop/Server and set a password. Refer to Figure 30 below.

![Figure 30: Security Agent Uninstall/Unload Password](image)

5.3 > Bypassing the Uninstall Password of a Security Agent

In the event that there is a need to uninstall a Security Agent, and the Uninstall Password is unavailable, either of the two can be performed:

1. On the computer where SA will be uninstalled, launch cmd.exe and run the following command: `msiexec /x {0A07E717-BB5D-4B99-840B-6C5DED52B277} /qf DASH331=1`

2. Set HKLM\Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc\Allow Uninstall to 1, then remove the Security Agent from Windows Add/Remove program.
# Chapter 6: Configuration

## 6.1 Management Console Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Scan Settings</td>
<td></td>
</tr>
<tr>
<td><strong>Scan Compressed Files</strong></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Add compressed files or file extensions that should not be scanned to the scan exclusion list.</td>
</tr>
<tr>
<td></td>
<td>• Recommended 2nd layer</td>
</tr>
<tr>
<td><strong>CPU Usage</strong></td>
<td>• Low</td>
</tr>
<tr>
<td></td>
<td>• This setting helps minimize computer slowdown when scanning occurs during peak hours. To improve performance, consider running Manual Scan during off-peak hours.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>• ActiveAction</td>
</tr>
<tr>
<td>Realtime Scan Settings</td>
<td></td>
</tr>
<tr>
<td><strong>User activity on files</strong></td>
<td>• Scan files being created, modified, retrieved, or executed.</td>
</tr>
<tr>
<td></td>
<td>• This option ensures that files introduced to and originating from the computer are safe to access.</td>
</tr>
<tr>
<td><strong>CPU Usage</strong></td>
<td>• Low</td>
</tr>
<tr>
<td></td>
<td>• This setting helps minimize computer slowdown when scanning occurs during peak hours. To improve performance, consider running Manual Scan during off-peak hours.</td>
</tr>
<tr>
<td><strong>Scan Compressed Files</strong></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Add compressed files or file extensions that will not be scanned to the scan exclusion list.</td>
</tr>
<tr>
<td><strong>Scan Target</strong></td>
<td>• File types scanned by IntelliScan</td>
</tr>
<tr>
<td></td>
<td>• IntelliScan improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows the utilization of true file-type scanning.</td>
</tr>
<tr>
<td><strong>Scan Compressed Files</strong></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Add compressed files or file extensions that will not be included in the scan exclusion list.</td>
</tr>
</tbody>
</table>
### Recommended 2nd layer

**CPU Usage**
- **Low**
- This setting helps minimize computer slowdown when scanning occurs during peak hours.

**Action**
- **ActiveAction**

**Allow users to postpone or cancel Scheduled Scan**
Disabled users may cancel the scan if this setting is enabled. Consider enabling only on selected computers. For example, enable the option on a shared computer used for presentations. This allows the user to cancel the scan if scanning will occur during a presentation.

**Scan Exclusion Settings**

**Scan Exclusions**
- **Enabled**
- Database and encrypted files should generally be excluded from scanning to avoid performance and functionality issues. Also, add files that are causing false-positives and files that many users are reporting as safe. See Chapter 10.1 for recommended scan exclusions in Windows Platform.

**Web Reputation Settings for External Clients**

**Web Reputation Policy**
- **Enabled**
- This setting ensures that clients are protected from web-based threats even if they are outside the corporate network.

**Security Level**
- **Medium**

**Web Reputation Settings for Internal Clients**

**Web Reputation Policy**
- **Enabled**

**Security Level**
- **Medium**

**Allow clients to send logs to the Trend Micro Security Server**
Enabled if there is no need to monitor websites that users are accessing. This setting generates traffic between the server and clients.

**Web Reputation Approved URL List**

**Approved URL List**
Add URLs that the users think are safe to access.
Also access the following page if there is a possibility that a URL has been misclassified: [http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx](http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx)

**Server Updates**

**Update schedule**
- Daily or Hourly

**Update source**
Setting up the Trend Micro ActiveUpdate server and maintaining a custom update source may be a tedious process and requires additional computing resources.

**Standard Notifications**

**Criteria**
Send a notification only when the scan action was not performed successfully. Select this option to limit the amount of email notifications that is received, and focus only on security events that requires attention.

**Email**
Add all Trend Micro Security and WFBS administrators in the organization as email recipients.

**Outbreak Notifications**

**Criteria**
Query sources: 1
Rejections: 100
Time period: 24 hours

**Email**
Add all Trend Micro Security and WFBS administrators in the organization as email recipients.

**Client-Server Notification**

**Server name and listening port**
Avoid changing when clients have been registered to the server or clients will have to be redeployed.

**Proxy Settings**
Clients do not typically communicate with the server through an intranet proxy. Also avoid changing when...
<table>
<thead>
<tr>
<th>External Proxy Settings</th>
<th>clients have been registered to the server or clients will have to be redeployed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Settings</td>
<td>Enabled if the Trend Micro Security Server connects to the Trend Micro ActiveUpdate server through a proxy server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Log Maintenance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled deletion of logs</td>
<td>Enabled</td>
</tr>
<tr>
<td>Logs to delete</td>
<td>• Logs older than 7 days</td>
</tr>
<tr>
<td>Log deletion schedule</td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Schedule the deletion during off-peak hours.</td>
</tr>
</tbody>
</table>

### 6.2 > INI Configuration Files

This KB can be checked for Ofcscan.ini listing and definitions for each of the configuration entry in the ofcscan.ini file: [http://esupport.trendmicro.com/solution/en-US/1061403.aspx](http://esupport.trendmicro.com/solution/en-US/1061403.aspx)
## 6.3 > Performance Tuning

<table>
<thead>
<tr>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Disable TSC at startup | 1. Open the ..\PCCSRV\ofcscan.ini file using a text editor like Notepad.  
2. Under Global Setting section, add the "DisableTSCAtStart=1" parameter to disable the TSC.exe process.  
3. Save and close the file.  
4. Log on to the WFBS console.  
5. Deploy the new configuration to all clients:  
6. Click Security Settings > Configure > Domain Configure > Client Privileges.  
7. Click Save.  

   The "dtas=dword:00000001" registry is created in the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCCillinNTCorp\CurrentVersion\Misc of the Security agent. |
| Delay Real-time Scan service startup | 1. Open the Registry Editor (regedit.exe).  
2. Go to the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCCillinNTCorp\CurrentVersion\Real Time Scan Configuration\ hive.  
3. Change the value of the registry key "NTRIScanInitSleep" to "180000" (DWORD, Decimal).  

   Note: The unit is in milliseconds. The value "180000" will delay the start of the Real Time Scan for 3 minutes. |
| Increase Pagepool | Notes:  
This registry key will not work with Windows Vista or Windows Server 2008.  
This workaround will not work if there is a startup option "/3GB" in the boot.ini file for Windows XP and Windows Server 2003.  

   a. Open the Registry Editor.  

   Important: Always create a backup before modifying the registry. Incorrect registry changes may cause serious issues. Should this occur, restore it by referring to the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe. |
serious issues. Should this occur, restore it by referring to the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

b. Change the value of "PagedPoolSize" to "0xFFFFFFFF".
c. Restart the computer.

UADuplicationOptValue =128
1. Open the ..\PCCSRV\ofcscan.ini file using a text editor like Notepad.
2. Under Global Setting section, make sure that the entry "UADuplicationOptValue " is set to "128"
3. Save and close the file.

Deploy the settings to clients:
4. Log on to the WFBS console.
5. Deploy the new configuration to all clients:
6. Click Security Settings > Configure > Domain Configure > Client Privileges.
7. Click Save.

Command_Handler_Maxium_Thread_Number
-This Security server parameter controls the number of threads responsible for receiving client communications. Default value is 20. 
NOTE: the word Maxium is intentionally misspelled.

1. Edit <drive>:\ Program Files \ Trend Micro \ Security Server \ 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.

DB_MEM_OPT_MAX
Increase the server database cache to improve performance.
1. Edit <drive>:\ Program Files \ Trend Micro \ Security Server \ PCCSRV \ ofcscan.ini
2. Locate the entry DB_MEM_OPT_MAX = 10240 and set its value to be at least 10% of available memory.

VerifyConnectionThreadCount=16
Verify Connection Thread Count
1. Go to the [INI_SERVER_SECTION] section of ..\Pccsrv\ofcscan.ini
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.

Preventing HTTPDB crash
1. Make sure that the HTTPDB folder is not being backed up by any third party backup software, this may cause the database to be corrupted. Use the database backup feature of WFBS and point the third party software to back up the backup copy instead.

For the database backup settings, refer to this article: Changing the settings for the database backup of WFBS.

Note: The weekly database backup during Sundays at 5:00AM is the recommended database backup setting.

2. Enable Virus Log Deletion.
a. Open the WFBS console.
b. Go to Reports > Maintenance.
3. **Enlarge the database cache.**
   a. Go to the `..\Trend Micro\Security Server\PCCSRV` folder.
   b. Open the `ofcscan.ini` file with a text editor like Notepad.
   c. Under the `[INI_DBFILE_SECTION]`, look for the "DB_MEM_OPT_MAX" and change the default value "10240(KB)" to 10% of the Security Server's free memory.
   d. Save the changes.

4. **Enlarge the command handler's thread number.**
   a. In the `..\Trend Micro\Security Server\PCCSRV\ofcscan.ini` file, look for the `[INI_SERVER_SECTION]` and add a "Command_Handler_Maxium_Thread_Number" entry.

   **Note:** The "Command_Handler_Maxium_Thread_Number" entry does not exist by default. Depending on the number of CPUs, set the value of this entry to 20 times the number of the Security Server's CPU.

   b. Save the changes.


---

6.4 > **Import/Export Settings**

**Import/Export Feature Scope**

The Import/Export feature allows an administrator to replicate an existing server’s configuration to another server. This saves deployment time since there is no need to configure individual security features’ setting. The feature is available under the Security Settings tab. For more information on how to import and export the configuration, refer to the WFBS 8.0 Administrator’s Guide.
You configuration on two levels can be exported, namely:

1. Company settings – Select the root icon (My Company) on the Security Settings Network Tree (refer to Figure 29). This allows the Security Server’s general settings to be saved and default group security settings. This scope can be selected if there is are multiple Security Servers in the company. It can also be used to create a backup of the settings of the server. Note that this option does not save any custom groups’ settings, so to have a full backup, a need to do per policy export for every custom group that must be created.
By default, WFBS 8.0 will NOT export company-specific settings like Proxy Settings, SMTP settings; Location Awareness, etc. (refer to the unchecked boxes of Figure 30). If there is a need to apply an exported server setting to another company, make sure those are unchecked. However if there is a need, apply the settings to another WFBS 8.0 server in the organization (which will have general settings in common with the source server), then check all the boxes so that all the general settings are included in the exported settings.

2. Per Group settings - select the custom group in the WFBS 8.0 Security Settings Network Tree (refer to Figure 30). It allows the Security Settings defined for the group to be saved.

NOTE: The exported file is encrypted. The exported configuration’s filename will be in the format - <Security Server FQDN/IP>_70_YYYYMMDD.dat for a company level scope and WFBS Policy_<Group>_YYYYMMDD.dat for a group setting scope. It might be sufficient to distinguish the purpose of the exported file from the filename itself, but it is recommended that you create appropriate documentation for future use.
Error Handling/Limitations

WFBS 8.0 checks the following information before importing a saved configuration:

- If the exported file is imported using a different scope than export, the import attempt will fail. Configurations exported under Company scope or per group scope can only be imported on Company scope and per group scope respectively.
- If the exported file is corrupted.
- If the exported file is exported from a different version.
- If the language is not the same as that of the target server.

6.4.1 How to Configure IPv6 addresses

The web console allows users to configure an IPv6 address or an IPv6 address range. The following are some configuration guidelines.

- Worry-Free Business Security accepts standard IPv6 address presentations.

For example:

2001:0db7:85a3:0000:0000:8a2e:0370:7334
2001:db7:85a3:0:0:8a2e:370:7334
2001:db7:85a3::8a2e:370:7334
::ffff:192.0.2.128

- Worry-Free Business Security also accepts link-local IPv6 addresses, such as:

fe80::210:5aff:feaa:20a2

**WARNING!** Exercise caution when specifying a link-local IPv6 address because even though Worry-Free Business Security can accept the address, it might not work as expected under certain circumstances. For example, agents cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets.
- For IPv6 address ranges, a prefix and prefix length are usually required. For configurations that require the server to query IP addresses, prefix length restrictions apply to prevent performance issues that may occur when the server queries a significant number of IP addresses.
- Some settings that involve IPv6 addresses or address ranges will be deployed to agents but agents will ignore them. For example, if the Update is configured.
- Agent list and included an Update Agent identified by its IPv6 address, pure IPv4 agents will ignore this Update Agent and connect to IPv4 or dual-stack Update Agents, if any.

This topic enumerates places in the web console where IP addresses are shown.

- Security Groups Tree
Whenever the Security Groups Tree displays, the IPv6 addresses of pure IPv6 agents display under the IP address column. For dual-stack agents, their IPv6 addresses display if they used their IPv6 address to register to the server.

**NOTE**  
The IP address that dual-stack agents use when registering to the server can be controlled in the Preferred IP Address section in Preferences > Global Settings > Desktop/Server tab.

When the agent settings are exported to a file, the IPv6 addresses also display in the exported file.

- **Logs**
- The IPv6 addresses of dual-stack and pure IPv6 agents display on the logs.
- Refer to [EN-1095282](#) for the settings and components that IPv6 supports.
- Check this KB for [IPv6 Limitations](#).

---

*Worry-Free Business Security 8.0 Best Practice guide Book*
Chapter 7: Backup and Disaster Recovery

7.1 > Configuring Database flush in WFBS 8.0

You the database flush can now be configured, and its frequency in WFBS 8.0. This allows setting a schedule for flushing data from the memory to the disk and resolve issues related to corrupted database.

To configure the database flushing and customized the frequency of the database flush, do the following:

1. Go to `\PCCSRV\` folder of the Security Server (SS).
2. Open the ofcscan.ini. with a text editor (e.g. Notepad).
3. Find "INI_DBFILE_SECTION".
4. Under the "INI_DBFILE_SECTION" section, find the following and assign the appropriate values:
   
   ![Image]

   Where y = value from 300 to 86400 seconds. This is the frequency of the flush process and the default value is 7200.

By default, the database process runs the flush task every two hours after the latest flush.

5. Save and close the file.

For corrupted database, recreate DB by performing this article:

How to recreate the HTTPDB database in Worry-Free Business Security (WFBS)

7.2 > Security Server Database Files

WFBS is set to automatically back up the database weekly on Sundays at 5 AM system time. To change the directory where the backup is placed and the scheduled back-up frequency, perform the following:
1. Open the Registry Editor (regedit.exe).

**Important:** Always create a backup before modifying the registry. Incorrect registry changes may cause serious issues. Should this occur, restore it by referring to the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

2. Go to the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup registry hive.

3. On the right pane, double-click BackupPath and then change the path where the backup will be placed.

4. If there is a need to specify when to perform a backup, please do Steps 4a - 4c. Otherwise, proceed to Step 5.
   a. On the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup registry hive.
   b. On the right pane, look for "Frequency" and set the preferred value based on the following:
      "1" for Monthly
      "2" for Weekly
      "3" for Daily
   c. On the right pane, look for "DaysOfWeek" and set the preferred value based on the following.
      "0" - for Sunday
      "1" - for Monday
      "2" - for Tuesday
      "3" - for Wednesday
      "4" - for Thursday
      "5" - for Friday
      "6" - for Saturday

5. Close the Registry Editor.

### 7.3 > Security Server and Messaging Security Agent Configuration Files

The following are the important files and/or folders to back up before upgrading:

**Security Server:**
- Ofcscan.ini - This file contains the global settings. This can be found in the C: Program Files\Trend Micro\Security Server\PCCSRV folder.
• Ous.ini - This file contains the update source table for component deployment. This can be found in the ..\Trend Micro\Security Server\PCCSRV folder.

• Private folder - This contains the firewall settings and license information. This can be found in the ..\Trend Micro\Security Server\PCCSRV folder.

• HTTPDB folder - This contains the server and client settings and information. This can be found in the ..\Trend Micro\Security Server\PCCSRV folder.

• TMOPP folder - This contains the Outbreak Defense settings. This can be found in the ..\PCCSRV\Web folder.

• OfcPfw.dat - This file contains the personal firewall settings. This can be found in the ..\PCCSRV\Pccnt\Common folder.

• OfcPFw.dat file - This one contains the firewall deployment settings. This can be found in the ..\PCCSRV\Download folder

**MESSAGING SECURITY AGENT:**
The following can be found in the C: Program Files\Trend Micro\Messaging Security Agent folder.

• Config folder - This contains the XML files used for generating MSA databases.

• EUQ folder - This contains the End User Quarantine logs and configuration files.

• Data folder - This contains the database configuration such as MSA rules, reports, etc.

• Storage folder - This storage area allows the configuration of dedicated storage for archives, backups, and quarantined items on a filter basis. It enables administrators to relocate resource intensive storage areas on separate partitions or hard drives.
Chapter 8: Behavior Monitoring

8.1 Default Settings for Behavior Monitoring

Behavior monitoring is disabled by default in server platform to avoid performance impact against certain server-based environment, based on capacity, loading and applications on the server.

8.2 How to Properly Deploy Behavior Monitoring in WFBS 8.0

When deploying the Behavior Monitoring feature in WFBS 8 make sure to address the following:

1. Set up and deploy a pilot environment that matches the production environment as closely as possible.

**NOTE** The pilot environment is where testers ensure that all applications work as expected in network and security conditions that match the conditions of the production environment.
2. Ensure that the following are included in the pilot environment:
   - Business applications
   - Custom developed applications
   - Critical applications used by groups or individuals (such as Payroll, Inventory, Accounting and Database applications)

3. Deploy the Client/Server Security Agents into the pilot environment with the features that will be enabled.

   **NOTE** The Behavior Monitoring and Device Control features may both be enabled.

4. Allow the pilot environment to run for a reasonable amount of time (a “soak time”) with the standard applications running and with an average daily use.

5. Identify system-intensive applications:

6. Trend Micro provides a standalone performance tuning tool to help identify applications that could potentially cause a performance impact during deployment. Trend Micro recommends running the **TMPerfTool**, available from Trend Micro Technical Support, on a standard workstation image and/or a few target workstations during the pilot process to determine any potential software or driver conflicts that may cause disruptions during the final deployment of the Behavioral Monitoring and Device Control features.

7. **To use the TMPerfTool:**

   1. Obtain a copy of the TMPerfTool Utility from the program directory of the Security Server under `\Trend Micro\Security Server\PCCSRV\Admin\Utility\TmPerfTool`
   2. Choose the proper version based on the platform of the Security Agent being tested (32-bit or 64-bit). Place the TMPerfTool.exe file in the BM folder under the **Client Security Agent** directory (`%ProgramDir%/Trend Micro/BM`).
4. Click Analyze when the system or applications start to slow down.

![Performance Tuning Tool](image)

**Figure 33 Performance Tuning Tool**

5. When a red highlighted row appears, it means that the TMPerfTool found the resource-intensive process.
6. Select the highlighted row and click the plus (+) sign button to add to the exception list.
7. After excluding the process, verify if the system or application performance improves, then do one of the following:
   - If the performance improves, select the process row again and click Include.
   - If the performance drops again, it means the root cause is found.
8. Note the name of the application
9. Click **Stop**.
10. Review the applications and associated processes that have been identified as conflicting.

To add an additional application:

   a. Open the WFBS console.
   b. Go to **Security Settings > Select a group > Configure > Behavior Monitoring**.
   c. Under **Exceptions** section, add the applications.

![Figure 36: Behavior Monitoring Approved/Blocked List](image)

8.2.1 **Trusted Program and Device Control**

There may be some programs that are active and consume numerous resources such as a database server or a backup program. If performance issues occur even after the programs have been excluded from Behavior Monitoring, the program can be further excluded from real-time scanning to prevent added performance issues.
To add a program to the Trusted Programs list:

1. On the Security Settings page, click on the group that contains machines with the app.
   Click **Trusted Programs**.
2. Enter the full file path to the specific program executable.
3. Click **Add to Trusted Program List**.

Besides Behavior Monitoring, the following are two additional features of AEGIS.
Device Control  Allows SAs to block autorun programs on USB flash memory or USB hard disk.

It also regulates access to external storage devices and network resources connected to computers.

**NOTE** USB and virtual CDs, DVDs, or floppy drives are regarded as CD/DVD/floppy devices—non-USB devices. Therefore, these will not be protected.

trusted

trusted program

We will not scan the application, if user set approved list in Trusted Program. So, if the application is malware, it will not be detected. It will add to both exclusion list of Behavior Monitoring and Real-Time Scan
### Chapter 9: Miscellaneous

#### 9.1 > Recommended Scan Exclusion List in Windows Platform

<table>
<thead>
<tr>
<th>Application</th>
<th>Directory</th>
</tr>
</thead>
</table>
| General Exclusions for all Windows platforms | Pagefile.sys * .pst  
%systemroot%\System32\Spool  
(replace %systemroot% with actual directory)  
%systemroot%\SoftwareDistribution\Datastore  
%systemroot%\SoftwareDistribution\Datastore  
%systemroot%\SoftwareDistribution\Datastore  
%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\LogFiles  
<drive>:\WINNT\system32\IIS Temporary Compressed Files |
| Microsoft IIS 7.0 and above Server | Web Server log files should be excluded from scanning. By default, IIS logs are saved in <drive>:\inetpub\logs\. |
| 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 locally scan stored email. Use virus scanning applications such as 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, they 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>:\WINNT\Cluster (if using SQL Clustering)  
<drive>:\Program Files\Microsoft SQL Server\MSSQL\Data  
O:\ (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 | O:\ (Quorum drive)  
C:\Windows\Cluster |
<table>
<thead>
<tr>
<th>Application</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Sharepoint Portal Server</td>
<td><code>&lt;drive&gt;:\ Program Files \ SharePoint Portal Server</code>&lt;br&gt;<code>&lt;drive&gt;:\ Program Files \ Common Files \ Microsoft Shared \ Web Storage System</code>&lt;br&gt;<code>&lt;drive&gt;:\ Windows \ Temp \ Frontpagemovdir</code>&lt;br&gt;<code>M:\</code></td>
</tr>
<tr>
<td>Microsoft SharePoint Servers Foundation 2010</td>
<td><code>Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions</code>&lt;br&gt;<code>Drive:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files</code>&lt;br&gt;<code>Drive:\Users\ServiceAccount\AppData\Local\Temp</code>&lt;br&gt;<code>Drive:\Users\Default\AppData\Local\Temp</code>&lt;br&gt;<code>Drive:\Users\&lt;the account that the search service is running as&gt;\AppData\Local\Temp</code>&lt;br&gt;<code>Drive:\WINDOWS\system32\LogFiles</code>&lt;br&gt;<code>Drive:\Windows\Syswow64\LogFiles</code>&lt;br&gt;Reference: <a href="https://docs.microsoft.com/en-us/sharepoint/security/server-side-security">Certain folders may have to be excluded from antivirus scanning when you use a file-level antivirus program in SharePoint</a>`</td>
</tr>
<tr>
<td>Microsoft Systems Management Server (SMS)</td>
<td><code>SMS \ Inboxes \ SMS_Executive Thread Name</code>&lt;br&gt;<code>SMS_CCM \ ServiceData</code></td>
</tr>
<tr>
<td>Microsoft Operations Manager Server (MOM)</td>
<td><code>&lt;drive&gt;:\ Documents and Settings \ All Users \ Application Data \ Microsoft \ Microsoft Operations Manager</code>&lt;br&gt;<code>&lt;drive&gt;:\ Program Files \ Microsoft Operations Manager 2005</code></td>
</tr>
<tr>
<td>Microsoft Internet Security and Acceleration Server (ISA)</td>
<td><code>&lt;drive&gt;:\ Program Files \ Microsoft ISA Server \ ISALogs</code>&lt;br&gt;<code>&lt;drive&gt;:\ Program Files \ Microsoft SQL Server \ MSSQL$\MSFW \ Data</code></td>
</tr>
<tr>
<td>Microsoft Windows System Update Server (WSUS)</td>
<td><code>&lt;drive&gt;:\ WSUS</code>&lt;br&gt;<code>&lt;drive&gt;:\ WsusDatabase</code></td>
</tr>
<tr>
<td>VMWare</td>
<td>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 to 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. &lt;br&gt;Hyper-V files:&lt;br&gt;<code>C:\ProgramData\Microsoft\Windows\Hyper-V</code>&lt;br&gt;Virtual Machine VHD Files:&lt;br&gt;<code>C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks</code>&lt;br&gt;Snapshot Files:&lt;br&gt;<code>C:\ProgramData\Microsoft\Windows\Hyper-V\Snapshots</code>&lt;br&gt;Virtual Machine Processes:&lt;br&gt;<code>Vmms.exe</code>&lt;br&gt;<code>Vmwp.exe</code></td>
</tr>
</tbody>
</table>
| Microsoft Exchange Server | `Exchange 5.5`<br>`<drive>:\ EXCHSRVR \ IMCData`<br>`<drive>:\ EXCHSRVR \ MDBData`<br>`Exchange 2000`<br>`<drive>:\ EXCHSRVR \ MDBData`<br>`<drive>:\ EXCHSRVR \ MTAData`<br>`<drive>:\ EXCHSRVR \ Mailroot`<br>`<drive>:\ EXCHSRVR \ SrsData`
###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 are 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. Refer to this Microsoft article: [A Volume Shadow Copy Service (VSS) update package is available for Windows Server 2003](https://support.microsoft.com/en-us/kb/923584).

###Symantec Backup Exec
*...\Symantec\Backup Exec\beremote.exe*
*...\Symantec\Backup Exec\beserver.exe*
*...\Symantec\Backup Exec\bengine.exe*
*...\Symantec\Backup Exec\benetns.exe*
*...\Symantec\Backup Exec\pvlsvr.exe*
*...\Symantec\Backup Exec\BkUpexec.exe*

File extension: *.BFK files

###Citrix Exclusions
On Citrix systems, the following extensions have been causing performance problems. Exclude these file extensions to avoid any performance problems: *.LOG, *.DAT, *.TMP, *.POL, *.PF.

Exclude the roaming profiles from scan on the fileserver.

Exclude the roaming profiles from the real-time scan on the fileserver.

Create a daily scheduled scan of the roaming profiles in off-peak hours.

###Novell Zenworks
Exclude the following files: NalView.exe, RMenf.exe, ZenNotifyIcon.exe, ZenUserDaemon.exe, casa.msi, dlienf.dll, fileInfo.db, lcredmgr.dll, objInfo.db

Exclude the following extensions: .APPSTATE, .LOG, .TMP, .ZC

###Other Trend Micro Products
Make sure the checkbox for "Do not scan the directories where Trend Micro products are installed." is enabled in WFBS's Exclusion List settings (Security Settings>Antivirus/Anti-spyware>Exclusions).

---

**Additional Recommended Exclusions**

Other frequently used Microsoft server applications may sometimes cause performance issues in some environments. Examples of these applications are Windows Software Update Services, Print Services, IIS, DHCP Server, DNS Server, WINS Server, SQL Server. Other applications such as VMWARE, Hyper-V, and Citrix may also cause high CPU usage when being scanned.
Refer to the Knowledge Base article below for information on how to exclude these programs from scanning.


9.2 › How to improve Update Process

Normal WFBS Security Server operations will use up disk space that may range from as low as 1.2GB up to 6.0 GB depending on the usage.

However, under some occasions when the Security Server is managing a lot of agents including the Messaging Security Agent, a disk usage of up to 9GB may occur.

Example: 9GB usage may occur when the Security Server of WFBS 6.0's Messaging Security Agent is installed, Smart Scan mode is enabled, and debugging is also enabled, all at the same time.

**NOTE** Lack of free space may cause the Security Server to stop updating.

To regularly free up disk space, the Disk Cleaner tool can be used to clear up unused WFBS files such as backup files, log files and unused pattern files.

To use the tool, do the following:

1. Download the Disk Cleaner under: ..\Trend Micro\Security Server\PCCSRV\Admin\Utility

**NOTE** An administrator privilege is needed to run this tool on the Security Server. If the operating system's User Access Control is enabled, a popup may appear asking for administrator privilege before the tool executes.

The Disk Cleaner can be used through any of the following:

- Via User Interface (UI) Mode
- Via command line

**Via User Interface (UI) Mode:**
1. Double-click the TMDiskCleaner.exe file.
2. Click Delete Files to start the cleaning of unused files.
3. Once the cleanup process is finished, click Save Log.

**NOTE** In UI mode, all cleaned files cannot be restored.

**VIA COMMAND LINE:**

4. Open a command prompt window.

5. Run the following command: TMDiskCleaner.exe [/hide] [/log] [/allowundo]

   - /hide - Execute tool in the background.

   - /log - Save the DiskClean.log file to the current folder.

Note: This parameter only works when "/hide" is set.

   - allow/undo - Move files to the Recycle Bin only.

   to run the Disk Cleaner in regular intervals, Windows Scheduled Tasks can be used. Perform the following:

   a. Go to Start > Programs > Accessories > System Tools > Scheduled Tasks.

   b. Double-click Add Scheduled Task.

   c. When the Scheduled Task Wizard window appears, click Next.

   d. Select TMDiskCleaner.exe.

   e. Specify the frequency of the cleanup, the time, and the user account that will be used to run the tool.
6. Go back to the Scheduled Task window, right-click TMDiskCleaner and select Properties.

7. On the Run field, specify "/hide /log" as shown below.
8. Click Apply.

The following directories will be cleaned:

- `<SA>\AU_Data\AU_Temp`*
- `<SA>\Reserve`
- `<SS>\PCCSRV\TEMP`* (except hidden files)
- `<SS>\PCCSRV\Web\Service\AU_Data\AU_Temp`*
- `<SS>\PCCSRV\wss\*.log`
- `<SS>\PCCSRV\wss\AU_Data\AU_Temp`*
- `<SS>\PCCSRV\Backup`*
- `<SS>\PCCSRV\Virus`* (Delete quarantined files older than two weeks, except NOTVIRUS file)
- `<SS>\PCCSRV\ssaptfn.xxx` (keep the latest pattern only)
- `<SS>\PCCSRV\lpt$vpn.xxx` (keep the latest three patterns only)
- `<SS>\PCCSRV\icrc$oth.xxx` (keep the latest three patterns only)
- `<SS>\DBBackup`* (keep latest two subfolders only)
- `<MSA>\AU_Data\AU_Temp`*
- `<MSA>\Debug`*
- `<MSA>\engine\vsap1\latest\pattern`*
9.3 > Virtualization

Virtualization creates specific conditions that must be accounted for:

- On Windows Vista/7/2008 guest operating systems running VMware ESX 3.5 servers, PccNTmon cannot render the SA console correctly. The system hangs and eventually crashes. To prevent this issue, go to Control Panel > Performance Information and Tools > Visual Effects and select "Adjust for best performance".

- Client/Server Security Agent supports Citrix Presentation Server™ 4.0/4.5/5.0 and Remote Desktop.

- WFBS-A supports VMware© ESX™ 3.0/3.5, VMware Server 1.0.3/2.0.1, VMware Workstation 6.0/6.5, and Microsoft Hyper-V™ Server 2008

- WFBS 8 now supports Microsoft Hyper-V 3.0 and Vmware Workstation 8.0

- On VMware clients, the SA firewall may block all incoming packets. To address this issue, add the following value to the client's registry:

  Key: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC\PFWName: EnableBypassRule

  Type: REG_DWORD
9.4 Recommended Installation Adjustments for Special Environments

Migration of Unsupported Platforms
Support for the following client platforms has been discontinued:

- Windows 95
- Windows 98
- Windows Me
- Windows NT server / workstation
- Intel IA64 (Itanium)
- Windows 2000 series

When planning an upgrade to version 8.0, check whether there are clients installed on these unsupported platforms. If there are clients running any of these supported platforms:

- Do not upgrade all servers to version 8.0
- Designate an existing CSM server, which is running a version prior to 5.1 to manage these clients
- Before upgrading, open the Web console and move the clients to the designated server. Alternatively, use the Client Mover tool

NOTE <WFBS installation directory>:\Trend Micro\Security Server\PCCSRV\Private\unsupclient.txt is generated if WFBS 8.0 is installed on a server with an older version of CSM.

9.5 Supported Upgrade procedure:
The following summarizes the supported upgrade procedure for WFBS 8.0:

- WFBS 6.x, 7.x → WFBS 8.0
- CSM 3.0 → CSM 3.6 → WFBS 5.x → WFBS 6.x → WFBS 7.x → WFBS 8.0

WFBS 8.0 supports direct upgrade from WFBS 6.x/7.x, and above. Direct upgrade preserves configuration settings. Environments running CSM 3.0 must upgrade to version 3.6 first before upgrading to WFBS 6.0, and then version 8.0. Alternatively, uninstall both Security Server and Client/Server Security Agent and then do a fresh install of WFBS 8.0.

Upgrade options can be classified into the following modes:

- In-place migration
- Deploys WFBS on an existing CSM server, and the installation program handles all the relevant changes.
New server migration Deploys WFBS to a separate server, and migrate supported agents from the existing server to the new server.

The second option presents the fewest issues. If an in-place migration happens on a server that manages unsupported clients, these clients will have to be migrated to another server running WFBS 6.0 SP3.

**Citrix Environment**

Many instances of the PccNTMon process will be created in the memory where the agent is installed. This happens when users access the computer from a terminal session.

To avoid this issue, do the following:

1. Open the Registry Editor using a text editor like Notepad.

   **Important:** Always create a backup before modifying the registry. Incorrect registry changes may cause serious issues. Should this occur, restore it by referring to the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

2. Look for the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC cillinNTCorp\CurrentVersion\Misc registry hive.

3. Change the value of the registry key "RCS" (REG_DWORD) to decimal "202". The default value is "101".

4. Set the TmPreFilter to run in MiniFilter-Mode.
   a. Look for the HKLM\SYSTEM\CurrentControlSet\Services\TmPreFilter\Parameters registry hive.
   b. Change the value of the "EnableMiniFilter" registry key to "1".
   c. Restart the computer.

5. Change the memory usage of the PagedPool.
   a. Go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management registry hive.
   b. Change the value of the "PagedPoolSize" registry key to "FFFFFFFF".
   c. Restart the computer. Memory management will be set.

6. Exclude the following file extensions from scanning on a Citrix and Terminal Server:
   - .LOG
   - .POL
   - .DAT
   - .PF
   - .TMP

7. Exclude the roaming profiles from the RealTime scan on the fileserver.

**NOTE**  The following steps work only on Windows Server 2003 and below, but not on Windows Server 2008.
8. Create a daily/weekly scheduled scan of the roaming profiles in off-peak hours on the fileserver.

### 9.6 Summary of Tools that can be used for Troubleshooting

Get the tools that can be used for troubleshooting WFBS issues in the following areas:

<table>
<thead>
<tr>
<th>Area</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation/Uninstallation</td>
<td><strong>Uninstall Tool</strong> - for manual uninstallation of Security Agent)</td>
</tr>
<tr>
<td></td>
<td><strong>Downloader Tool</strong> - for downloading WFBS 8.0 installer when the installer gets corrupted after completing</td>
</tr>
<tr>
<td></td>
<td><strong>Gmer and RCMToolPack</strong> - for finding third-party driver conflicting with the installation and collecting tmcomm.log respectively.</td>
</tr>
<tr>
<td>Offline Clients/Not showing in console</td>
<td><strong>Change GUID Tool</strong> - for changing the GUID of Security Agent when you want to clone the machine</td>
</tr>
<tr>
<td></td>
<td><strong>IPxFer tool</strong> - for transferring Security Agents (SA) from one Security Server to another</td>
</tr>
<tr>
<td>Update</td>
<td><strong>Disk Cleaner Tool</strong> - for deleting unused WFBS files such as backup files, log files and unused pattern files to free up disk space</td>
</tr>
<tr>
<td>Console</td>
<td><strong>Console Recovery Tool</strong> - for resolving several console issues</td>
</tr>
<tr>
<td></td>
<td><strong>Console Password Reset Tool</strong> - for resetting the WFBS management console password</td>
</tr>
<tr>
<td>Performance</td>
<td><strong>TM PerfTool and Xperf Tool</strong> - for identifying applications that are resource-intensive or that have heavy I/O</td>
</tr>
<tr>
<td>Crash</td>
<td><strong>ADPlus and Dr. Watson Tools</strong> - for debugging crash issues</td>
</tr>
<tr>
<td>Database</td>
<td><strong>SrvDiag Tool</strong> - for recreating the Security Server Website and Database of WFBS.</td>
</tr>
<tr>
<td>Malware</td>
<td><strong>SIC Tool</strong> - for collecting information about your system and pinpoint possible infections by an unknown malware</td>
</tr>
<tr>
<td></td>
<td><strong>Anti-Malware tools</strong> - for cleaning infection and getting logs/system information</td>
</tr>
<tr>
<td></td>
<td><strong>Trend Micro RootKit Buster</strong> - for scanning hidden files, registry entries, processes, drivers, services, ports, and the master boot record (MBR) to identify and remove rootkits.</td>
</tr>
<tr>
<td></td>
<td><strong>Trend Micro Anti-Threat Toolkit</strong> - for analyzing malware issues and cleaning infected computers.</td>
</tr>
<tr>
<td>Debugging</td>
<td><strong>Case Diagnostic Tool</strong> - for collecting information needed by Trend Micro Technical Support</td>
</tr>
</tbody>
</table>
Chapter 10: About Trend Micro

Trend Micro, Incorporated is a global leader in network antivirus and Internet content security software and services, focused on helping customers prevent and minimize the impact of network viruses and mixed-threat attacks through its award-winning Trend Micro Enterprise Protection Strategy. Trend Micro has worldwide operations and trades stock on the Tokyo Stock Exchange and NASDAQ.

Copyright © 2012 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, and Worry-Free are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

Legal Notice: Trend Micro licenses this product in accordance with terms and conditions set forth in the License Agreement inside the product package. If you wish to review the License Agreement prior to purchase, visit: www.trendmicro.com/license. If you (or the company you represent) do not agree to these terms and conditions, promptly return the product and package to your place of purchase for a full refund.

10.1 > Contributors and Sources

Additional explanations and testing materials were provided by the following subject matters: experts:

Tobias Firnges
PH Core Team
Denny Yen
KoFeng Lee

Hanna Rebay
SMB NABU/APAC Team
Raquel Linquico
Trumpet Huang

The content of this Best Practice guide Book is based on the information provided by WFBS PDG, product investigations from documents listed below:

- Best Practice Guide WFBS 7 0 SP1
- OSCE 10.6 Best Practice Guide
10.2 > Inserting Contact Information (for Resellers and Partners)

Resellers and partners can add their contact information to the Security Server web console by performing the following steps:

1. On the computer where the Security Server is installed, navigate to `{Security Server installation folder}\PCCSRV\Private`.

   `{Security Server installation folder}` is typically `C:\Program Files\Trend Micro\Security Server`.

2. Open `contact_info.ini` using a text editor such as Notepad and then type the relevant contact information. Save the file.

3. Log on to the Security Server web console and navigate to Preferences > Product License. A Reseller Information section is added to the Product License screen.