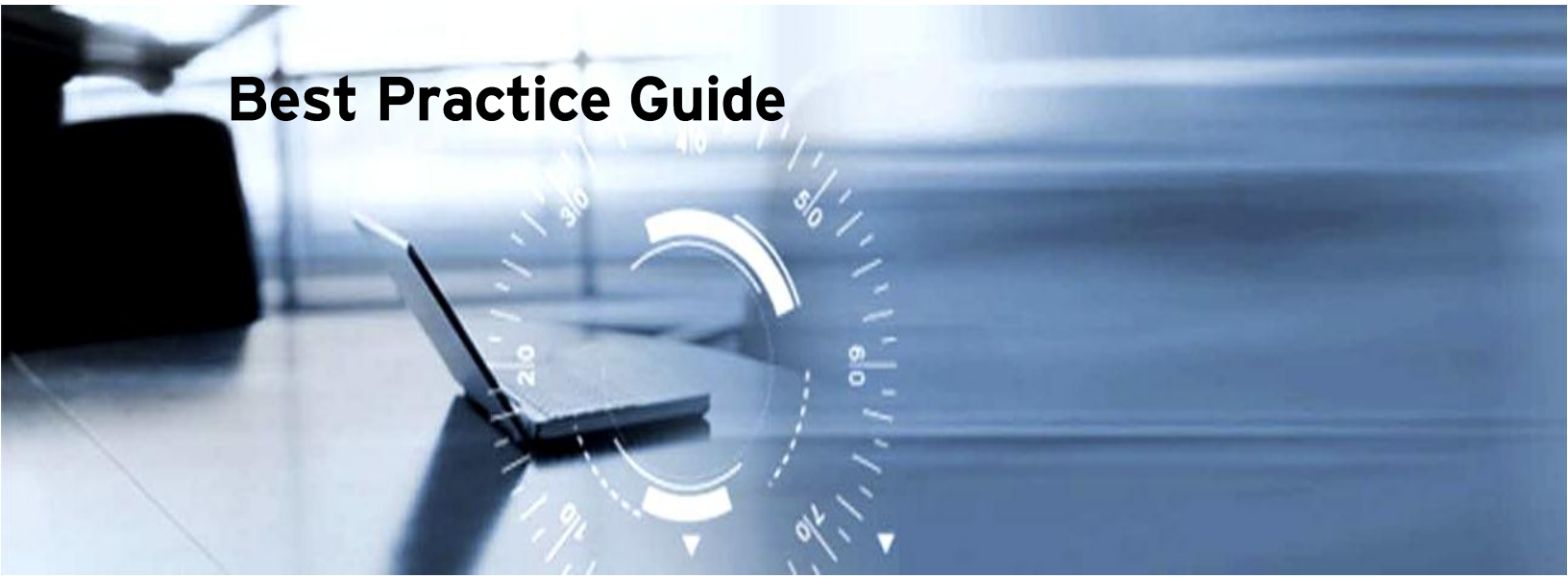
Trend Micro™ Worry-Free Business Security 9.0

Best Practice Guide



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

Authors: : Oliver John Maño Tony Dong, Richard De Leon, Cyrus Ramos
Contributors: Trumpet Huang, Noah Hsieh, Raquel Linquico, Henry Hung
Editorial: Nadia Trivinio

Released: March 2014
Revised: February 2015

Table of Contents

Chapter 1: Product Description

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

1.1 > Security Server

The Security Server is at the center of Worry-Free Business Security. It hosts the centralized web-based management console for WFBS. It installs agents to computers in 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 contains a database of detected Internet Threats, logged/reported by the agents.The Security Server also performs these important functions such as:

- Installation, monitoring, and management of agents
- 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).

1.1.1 Smart Scan Server

The Security Server includes a service called Scan Server, which is automatically installed during Security Server installation. 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.
- If the Security Agent cannot determine the risk of the file during the scan. It verifies the risk by sending a scan query to the Scan Server. The Scan Server 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.

1.1.2 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 > Security Agents

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

Agent	Description
Security Agent	Protects desktops and servers from security threats and intrusions
Messaging Security Agent (Advanced only)	Protects Microsoft Exchange servers from email-borne security threats.

Table 1 WFBS Agents

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

1.3 > What's New in Worry-Free Business Security 9.0

Features	Description
New Platform Support	The Security Server and Security Agent can now be installed on Windows 8.1 and Windows Server 2012 R2. It now supports Internet Explorer 11
Microsoft Exchange support	The Messaging Security Agent (Advanced only) now supports Microsoft Exchange Server 2010 SP3 and Exchange Server 2013

Features	Description
Mobile Device Security	The integration of the Messaging Security Agent with Exchange 2010 and Exchange 2013 can now support mobile device data protection and access control. It provides security to mobile devices without installing an app. It has the following features: Device Access Control • Allow access to the Exchange server based on user, operating system, and / or email client • Specify the access granted to specific mailbox components Device Management • Perform a device wipe on lost or stolen devices • Apply security settings to specific users including: ○ Password strength requirements ○ Automatic device lock after being inactive ○ Encryption ○ Unsuccessful sign-in data purge
Mac OS support	Trend Micro Security for Mac supports Mac OS X 10.9 Mavericks
Detection improvements	These are features included in the product to enhance its detection against new malware threats: • Memory Scan for real-time scan • Known and potential threats detection for Behavior Monitoring Blocking • Browser Exploit Protection • Newly-encountered program download detection
New Virtualization Support	• Citrix Presentation Server 5.0 • XenServer 6.1/6.2 • XenClient 2.0/2.1 • VMware ESX 5.1/5.5 • Vmware Workstation 9/10 • Microsoft Windows Server 2012 R2 Hyper-V
Activation Code enhancement	Post-paid Activation Code support
Performance improvements	• Security agent installation and uninstallation is now relatively faster. • Deferred Scan for Real-time Scan is now available
Usability improvements	• Global and group Approval/Block lists for Web Reputation and URL Filtering • IP exception list for Web Reputation and URL Filtering in the Global Settings • Removal of ActiveX from Client Tree and Remote installation page • Customizable Outbreak Defense • Outlook 2013 and Windows Live Mail 2012 support for Trend Micro Anti-Spam Toolbar • Configure Update Agent to update from Trend Micro ActiveUpdate • Stop Server updates • Keep patterns when upgrading the Server and Agent • Help Link and Infection Source virus logs • WFBS re-introduces global URL Approved and Blocked lists for administrators

Table 2 WFBS 9.0 new features and improvements

Chapter 2: Planning

2.1 > Planning Guide

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

Questions	Answers
What are the existing company policies that need to be considered prior to migration or deployment?	Identify these to guide the deployment process according to the company policies.
Are there any remote networks that are dependent on the main corporate network? What is the network bandwidth for these remote connections?	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.
How many clients are situated in the main office and the remote offices?	This will identify the location and number of update agents on the main and remote office.
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?	Migration from third party antivirus solutions and previous Worry-Free Business Security version should be carefully planned. WFBS 6.0, 7.0 and 8.0 can be upgraded to WFBS 9.0. If CSM 3.x/5.x is used, upgrade to WFBS 6.0 first before upgrading to WFBS 9.0.
Are there any other antivirus programs installed on the server where Worry-Free Business Security will be installed?	Third party antivirus management programs may create errors in the Worry-Free Business Security 9.0 installation. Uninstall the third party antivirus management program prior to installing WFBS 9.0.
On which server will WFBS 9.0 Security Server be installed? What is this server's current role in the network? What are the applications that run on this server?	Knowing server performance is vital in order to decide if WFBS 9.0 Security Server should be hosted on an existing or a new server.

Table 3: 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.

Scenario	Recommendation
Security Server	
New server or an existing multi-role server?	The server which will host the Worry-Free Business Security Server should meet the basic hardware/software requirements.
Server Role: Microsoft SBS or member server?	A Windows Small Business Server setup includes several installed components by default like Microsoft Exchange etc. Worry-Free Business Security 9.0 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.
Displacement: Migration from a 3rd party Antivirus solution	A Migration plan is necessary for existing third party antivirus solutions. Although WFBS 9.0 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.
Migration from a previous WFBS/CSM version	Like 3rd party antivirus solutions, previous CS/CSM versions need a migration/upgrade process.
Messaging Security Agent	
Is Microsoft Exchange on the same server as the Security Server?	Worry-Free Business Security 9.0 installation automatically detects Microsoft Exchange installation on the same box.
Is there an existing messaging protection solution for Microsoft Exchange?	Third party antivirus solutions for Microsoft Exchange need to be removed prior to the Messaging Security Agent installation.
Security Agent	
Displacement: Is there an existing 3rd party Antivirus?	Migrating clients should be done 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.

Scheduling Deployment	Schedule migration/installation and deployment during off-peak hours. A long weekend/holiday is the best time for migrating and deploying WFBS 9.0
Client types: office and out-of- office	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.

Table 4: Planning Component

2.3 > The Typical Small Business Network

Figure 2 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

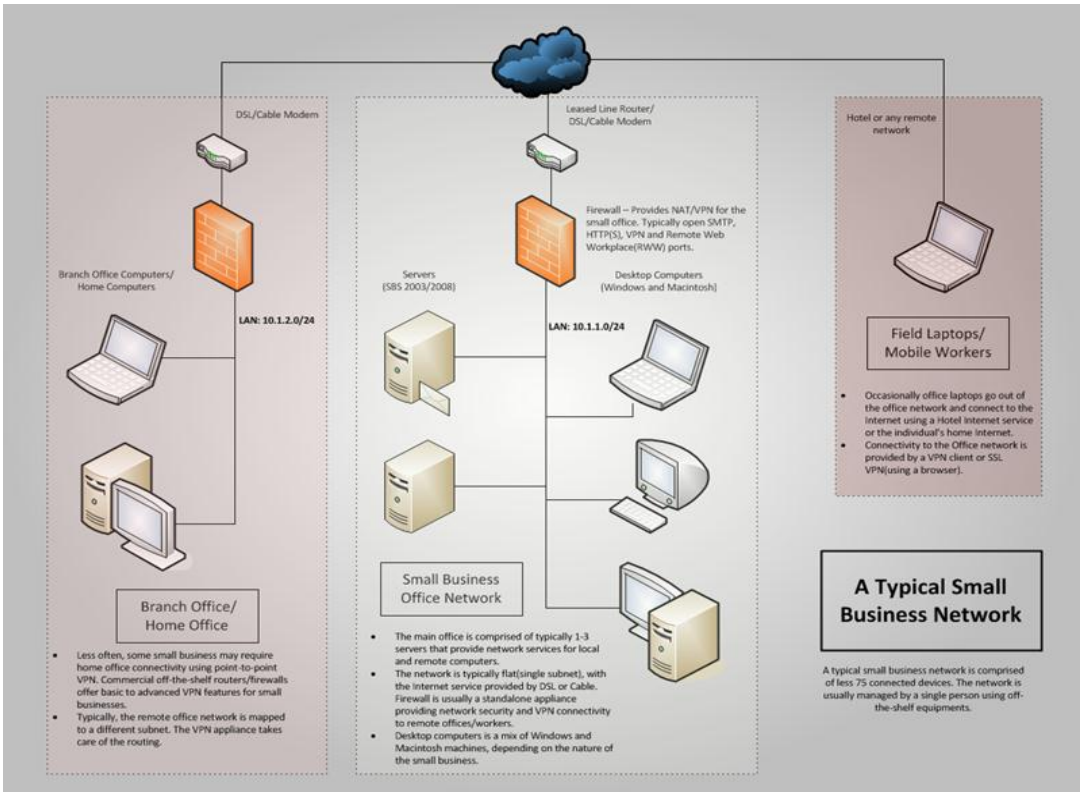


Figure 1 Typical SBS Network

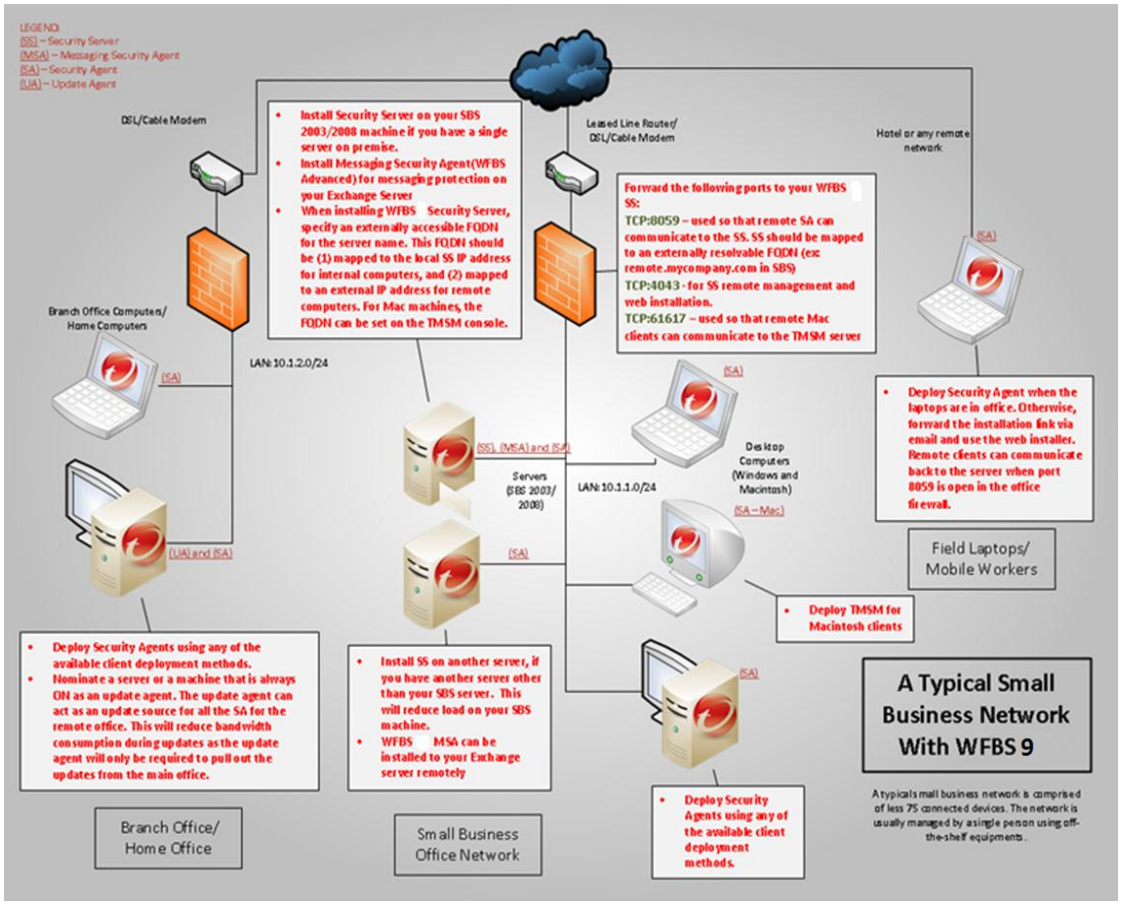


Figure 2 Typical Small Business Network with WFBS 9.0

2.4 > Deploying WFBS 9.0 on a Windows Small Business Network

Figure 1 above summarizes the deployment strategy for the typical small business network previously described.

Install WFBS 9.0's Security Server (SS) on the Microsoft SBS if a single server on the network is used. Otherwise, it can be installed on another available under-utilized 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 WFBS9_Installation_and_Upgrade guide for the preferred client deployment method.

An Update Agent (UA) for remote networks can be specified. It acts as the update source for specified computers and is responsible for pulling out the updates from the WFBS 9.0 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 report an up-to-date security event from remote clients, ports need to be opened on the firewall and redirect (forward) it to the WFBS 9.0 server IP. These ports are documented in Figure 1

Chapter 3: Installation

3.1 > Recommended Hardware

The following are the recommended setup to maximize performance of WFBS.

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

System requirements:

http://docs.trendmicro.com/all/smb/wfbs-s/v9.0/en-us/wfbs_9.0_sysreq.pdf

Security Server

Memory:

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

Available Disk Space:

- 4.1GB for the Security Server program files
- 6.9GB for Security Server operations
- 11 GB total

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.

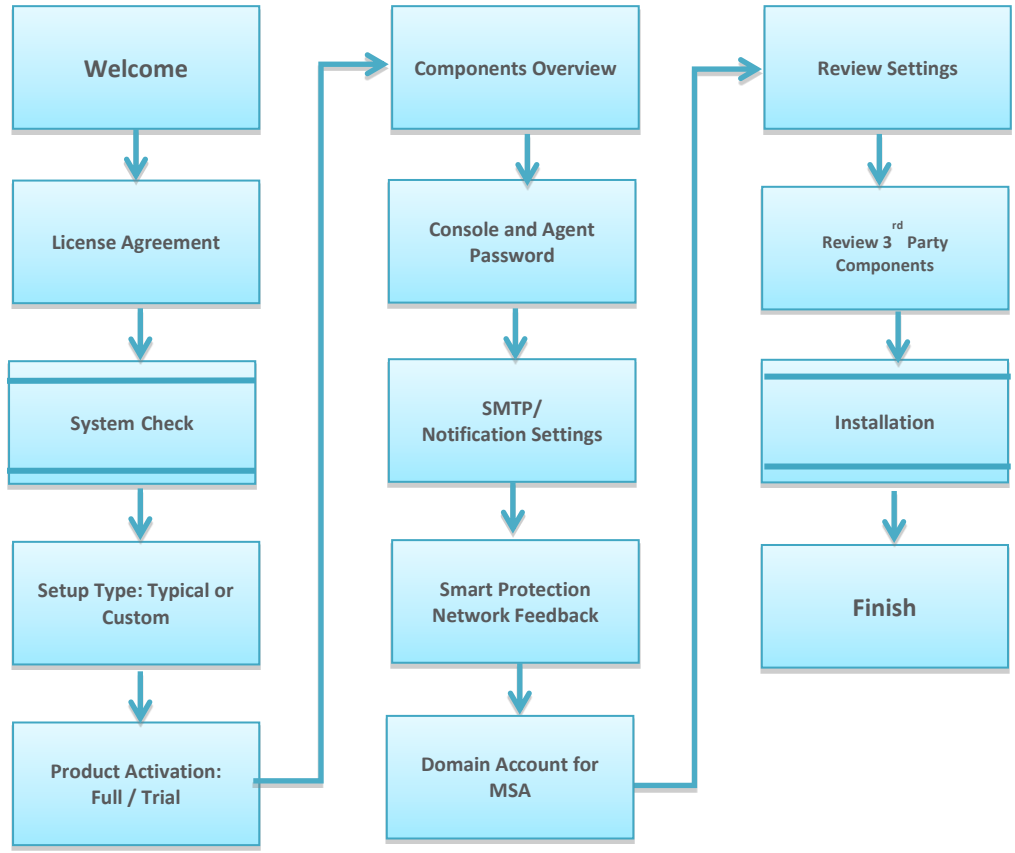


Figure 3: Typical Installation Workflow

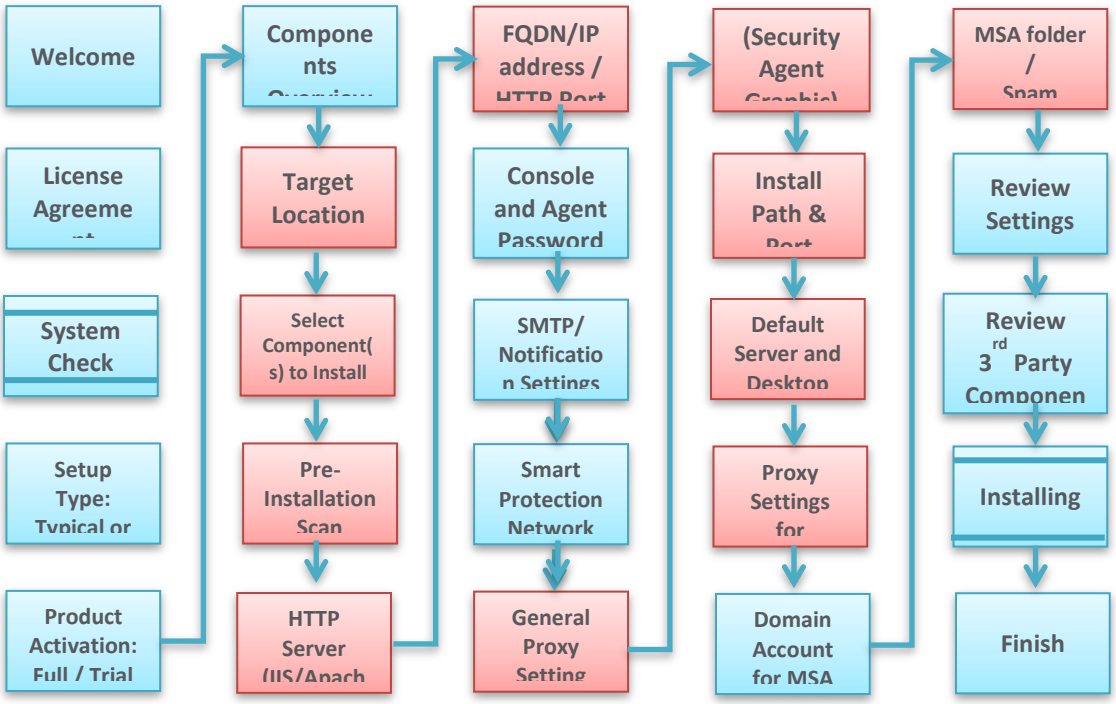


Figure 4 - Custom Installation Workflow

3.1.2 Use the WFBS 9.0 Downloader

WFBS installer packages can be downloaded using a downloader utility. There are several advantages when 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.

Figure 5 Downloader tool

3.1.3 Recommendations for Installation

Installation of WFBS 9.0 requires some planning. Recommendations include the following:

1. Before deploying WFBS 9.0, plan the order of how the installation will progress. To learn more about the deployment options available for WFBS 9.0, refer to the Administrator's Guide.
2. On the average, a typical fresh installation of WFBS 9.0 Security Server takes 15-25 minutes. Typical installation invokes prescan and can affect the time. During prescan, if 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 as WFBS 9.0 Security Server installation, 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 during 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 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. By doing these, it improves the overall disk performance.
- WFBS server components require 4.1GB of disk space for installation and another 6.9GB for operation. Ensure that 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 initiated after the pattern and engine files have been updated.
- Fully Qualified Domain Name (FQDN) – prior to WFBS 9.0, 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 9, 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 WFBS. 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, 8.1, 2012 and 2012 R2 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.
  - For Windows 8, 8.1, 2012 and 2012 R2: Modify the following registry key to turn off User Account Control (Reboot is required to let setting take effect.): [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "EnableLUA"=dword:00000000.

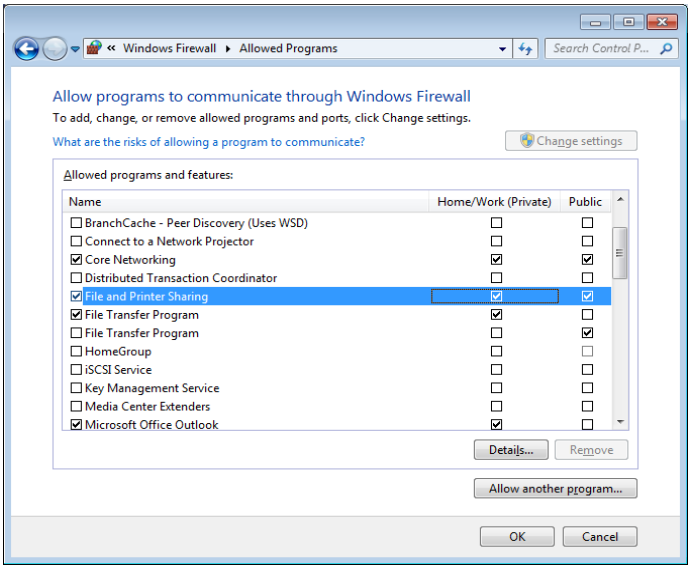


Figure 6 Allow File and Printer Sharing on Windows Firewall

NOTE Autopcc, 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 are more clients, Trend Micro suggests installing more than one Security Server. If the security server manages clients, bandwidth consumption in the network can increase 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 9.0 initiates an update task after installation.
12. Check installation success. Access the WFBS 9.0 web console
13. Download the test file from: http://eicar.org/anti_virus_test_file.htm
14. Configure the settings for the Security Server and Messaging Security Agent after installation.
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, the upgrade procedure in the Security server takes 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 via popup message.
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:

   Online Clients – For online clients, the Move feature can be used on the old Security Server to move SA to the new Security Server:

   3.1. In WFBS 9 Management Console Security Settings page, just select the clients to move, click **Manage Client Tree** and then click Move icon.

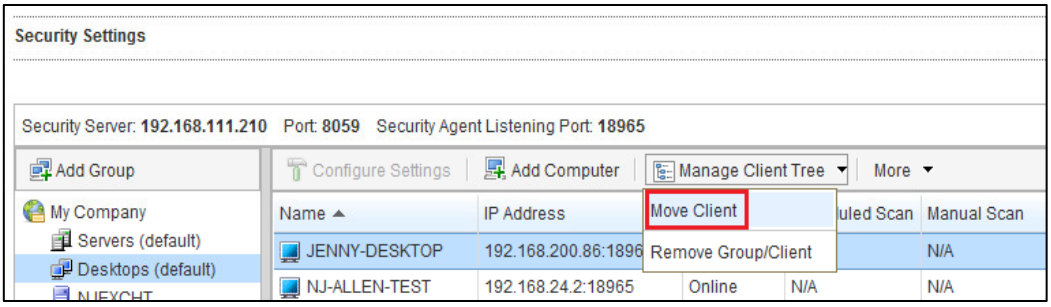


Figure 7: Select SAs to Move

   3.2. Specify the IP address or computer name of the new Security Server and the server port. The default server port is 8059.

Figure 8: Specify Security Server IP/name and Server Port

   3.3. Wait for a few minutes, then check the clients' status in the WFBS management console.

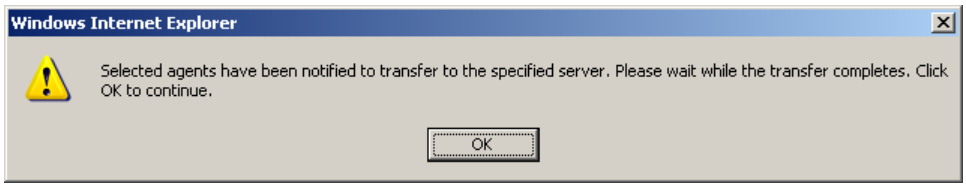


Figure 9: Confirmation Message

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. The tool can be found under `..\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:

```
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. Check the following Knowledgebase article:

   http://esupport.trendmicro.com/solution/en-US/1060980.aspx

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.

   NOTE 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 such as BSOD due to driver 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 is 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 2008/2012, 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

1. Stop the Trend Micro Security Server Master Service.
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).

Deleting Log Files from the Security Server

1. Go to **Reports** > **Maintenance** > **Manual Log Deletion**.

2. Set **Delete Logs Older Than** to **0** for a log type.
3. Click **Delete**.
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:

- 8.x (8.0 and 8 SP1)
- 7.x (7.0 and 7 SP1)
- 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
- Forbidding 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.

Application	Recommendation
Other Endpoint Security Software	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.
Security Applications in Windows SBS and EBS 2008	WFBS is compatible with both Windows Small Business Server (SBS) 2008, and Windows EBS (Essential Business Server) 2008. However,

Application	Recommendation
	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.
Messaging Security Agent and Forefront	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.
Security Agents and OneCare	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.
Databases	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.
Other Firewall Applications	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).

Table 5 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' 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: *Cyber criminals use HTTP and direct 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.

Port Type	IIS Default	IIS Virtual	Pre-Installed Apache	New Apache Installation
Non-SSL port	Non-SSL port on web server	First open port in range 8052 to 65536	Non-SSL port on web server	Non-SSL port on web server
SSL Port using SSL	SSL port on web server	First open port in range 4345 to 65536	N/A	SSL port on web server
SSL Port not using SSL	First open port in range 4345 to 65536	First open port in range 4345 to 65536	N/A	First open port in range 4345 to 65536

Table 6 Scan Server Port

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 2008/2012/2012 R2, SBS 2008/2011, 7, 8/8.1 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 successful connection to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.

Security Agent IPV6 Requirements

The Security Agent must be installed on:

- Windows Vista (all editions)
- Windows 7 (all editions)
- Windows 8 (all editions)
- Windows 8.1 (all editions)
- Windows Server 2008 (all editions)
- Windows SBS 2011
- Windows Server 2012 (all editions)
- Windows Server 2012 R2 (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 IPV6 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

3.9 > TMSM Server Deployment

TMSM does not support deployment on a Windows Domain Controller (DC). This is because of the Network Service account being used by TMSM hard-code for SQL TMSM instance installation. Microsoft SQL Server has a limitation that prevents it from running SQL Server services on a DC under a local privilege account which includes both Network Server and Local Server. See the following link for more information:

http://msdn.microsoft.com/en-us/library/ms143506.aspx#DC_Support

DO THE FOLLOWING WHEN UPGRADING TMSM SERVER:

1. Recreate the kahaDB of activeMQ:
   1.1. Rename /Security Server/Addon/TMSM/Apache-activemq/data folder
   1.2. Execute restart_TMSM.bat under /Security Server/Addon/TMSM folder. A new 'data' folder will be created automatically.
2. Check if:
   2.1. Broker.cert in the following locations if it has the same file size, modification date, and contents:
   - ..\TMSM\TMSM_HTML\ActiveUpdate\ClientInstall\tmsminstall.mpkg.zip/Contents\Resources\conf\broker.pem
   - ..\TMSM\apache-activemq\conf\broker.pem

   2.2. The following information are reflected in ..\TMSM\TMSM_HTML\ActiveUpdate\ClientInstall\tmsminstall.mpkg.zip/Contents\Resources\conf\ServerInfo.plist
   - Server current IP should be the same as current TMSM server
   - Password after <string>!CRYPT! is the same as the one in: ..\Trend Micro\Security Server\Addon\TMSM\ServerInfo.plist
3. If the information is not the same:
   - Manually unzip tmsminstall.mpkg.zip to a folder
   - Replace the two files in ..\TMSM\apache-activemq\conf
   - Compress the folder to tmsminstall.mpkg.zip
4. Use the new tmsminstall.mpkg.zip a new installation.

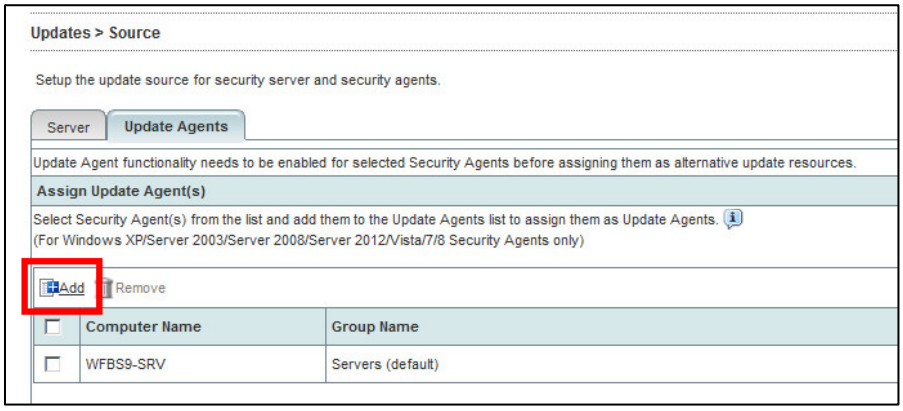
Chapter 4: Post Installation Management Task

4.1 > Post Installation Tasks

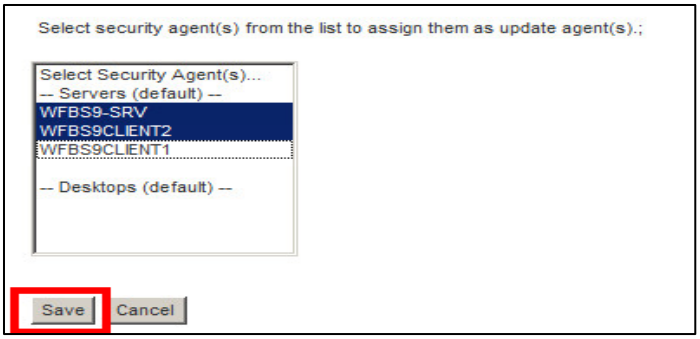
1. Move clients and servers to the appropriate domain/group - Move clients to the proper Groups through the WFBS management console. Notify clients so that settings take effect. Replicate settings from one group for efficiency.
2. Assign Update Agents on remote sites. Assign Update sources to groups 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.

   2.1. In the WFBS console, go to **Updates** > **Source** > **Update Agents** tab.

   2.2. Click **Add**



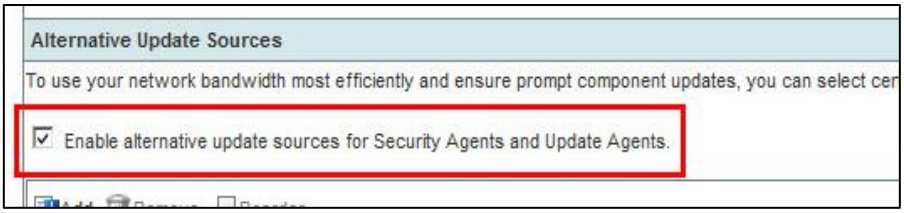
3. Select the Security Agents that will act as Update Agent then click **Save**.



3.1. Choose whether the update agents will download update components directly from the server or from the Internet through Trend Micro Activeupdate Server.

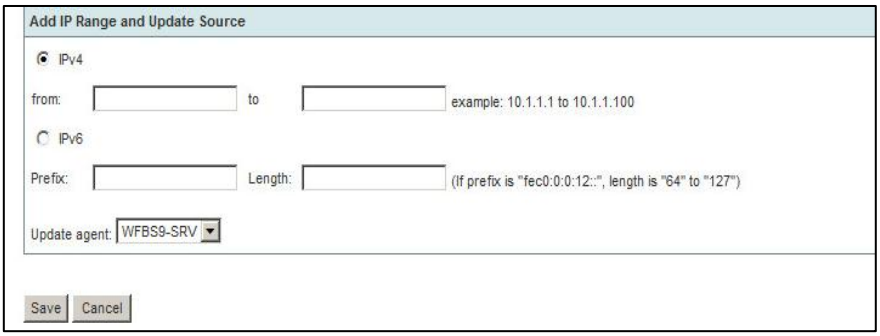
3.2. In the **Alternative Update Sources** section, select **Enable alternative update sources for Security Agents and Update Agents**.

NOTE Disabling this option prevents Security Agents from updating from Update Agents effectively switching update source back to the Security Server.

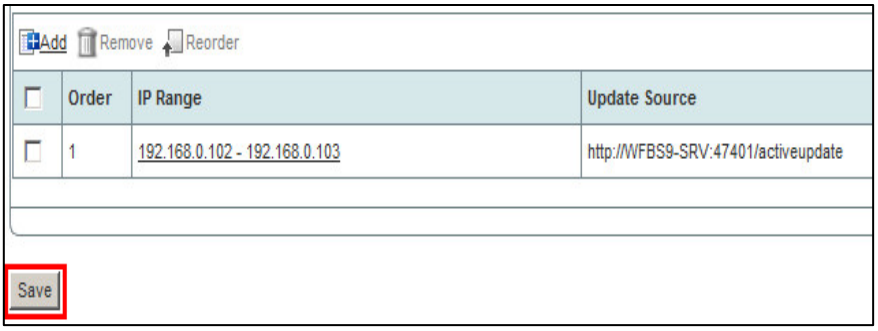


3.3. Click **Add**. A new screen opens.

3.4. Type the IP addresses of the Security Agents that will update from an Update Agent, select the update agent from the dropdown box and then click **Save**



3.5. Click **Save** to apply new settings



4.2 > Trend Micro Vulnerability Assessment

Trend Micro Vulnerability Assessment offers threat – virus correlation and maps vulnerabilities to Microsoft patches. Use this tool to assess security risks in a network. The information generated by the tool gives a clear guide on how to resolve known vulnerabilities. To use this feature, do the following:

1. In the WFBS management console, go to **Outbreak Defens**e.
2. In the Vulnerable Computer(s) section, click **Scheduled Assessment**

3. To turn on scheduled vulnerability assessments, select **Enable Scheduled Vulnerability Prevention**
4. In the Schedule section, select the frequency of vulnerability assessments:

- Daily
- Weekly
- Monthly
- Start Time

5. In the Target section, select the group(s) to assess for vulnerabilities:

- All groups: All groups in the Security Group Tree
- Specified groups: Server or desktop groups in the Security Group Tree.

6. Click **Save**.

4.3 > Trend Micro Vulnerability Scanner

TMVS (Trend Micro Vulnerability Scanner) detects installed antivirus software, searches for unprotected computers on the network, and offers an option to install the Security Agent. 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, go to the following folder and open TMVS.exe:

   `..\Trend Micro\Security Server\PCCSRV\Admin\Utility\TMVS`

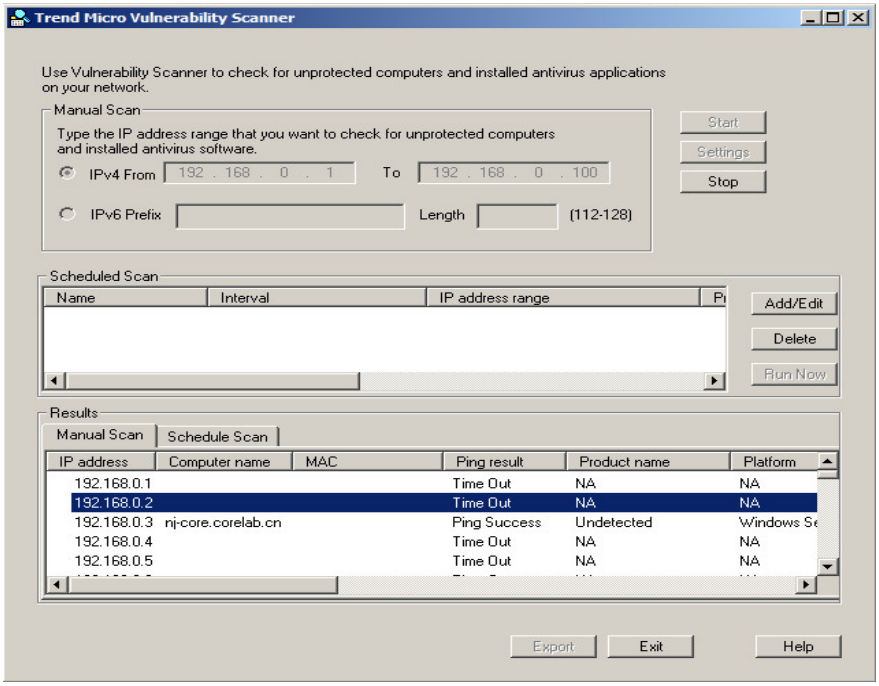


Figure 10 TMVS Window

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.

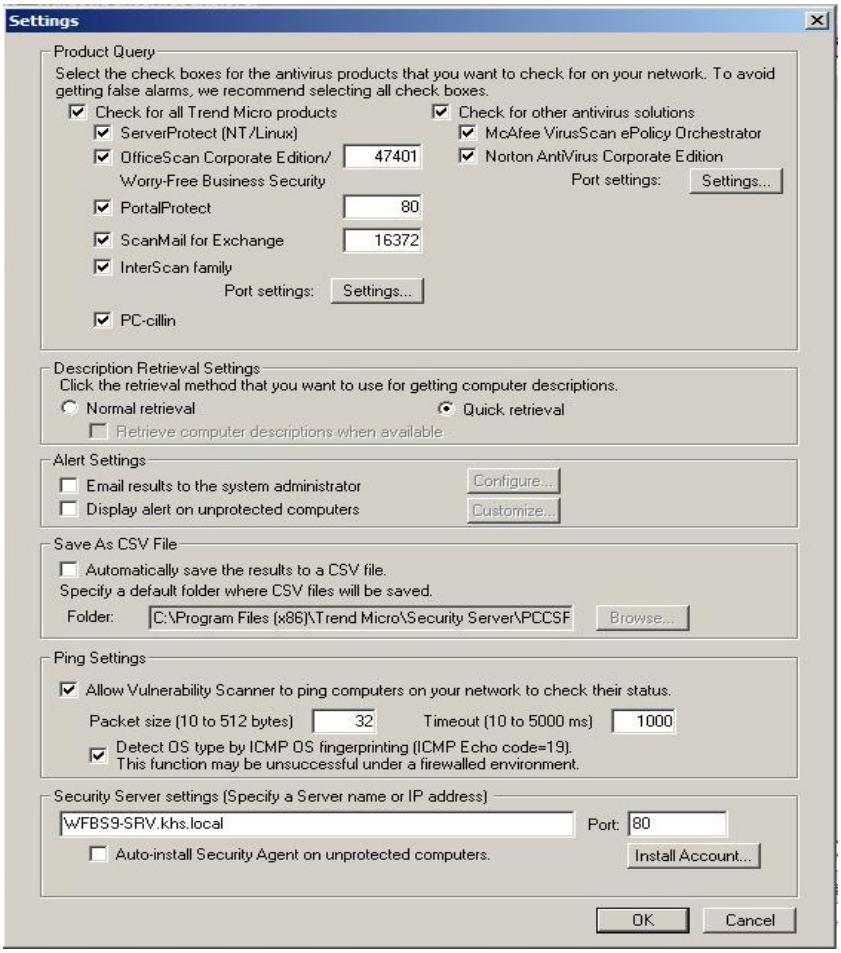


Figure 11: TMVS Settings

- 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 detect 3rd party antivirus protection components.

Deploying Security Agent 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.

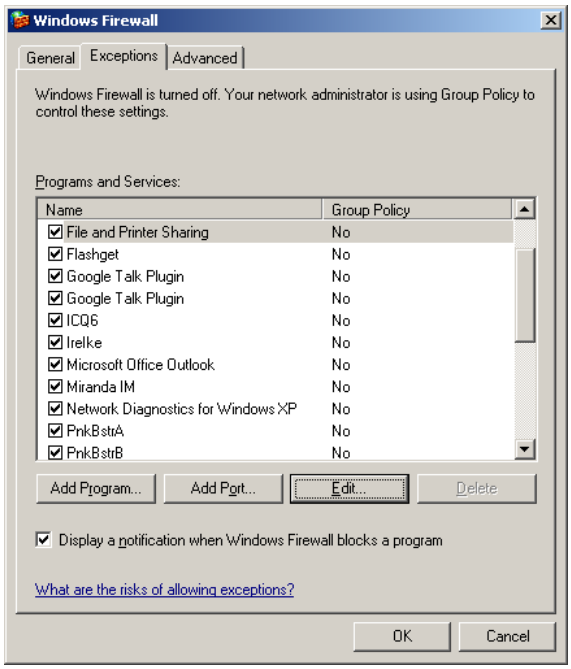


Figure 12: File and Print Sharing Exception

In an Active Directory domain, Firewall settings can be configured using a Group Policy Object to multiple computers. This allows users to enable the firewall exception without having to visit each of the client computers. Refer to the Microsoft Knowledge Base document for instructions on below:

http://technet.microsoft.com/en-us/library/bb490626.aspx

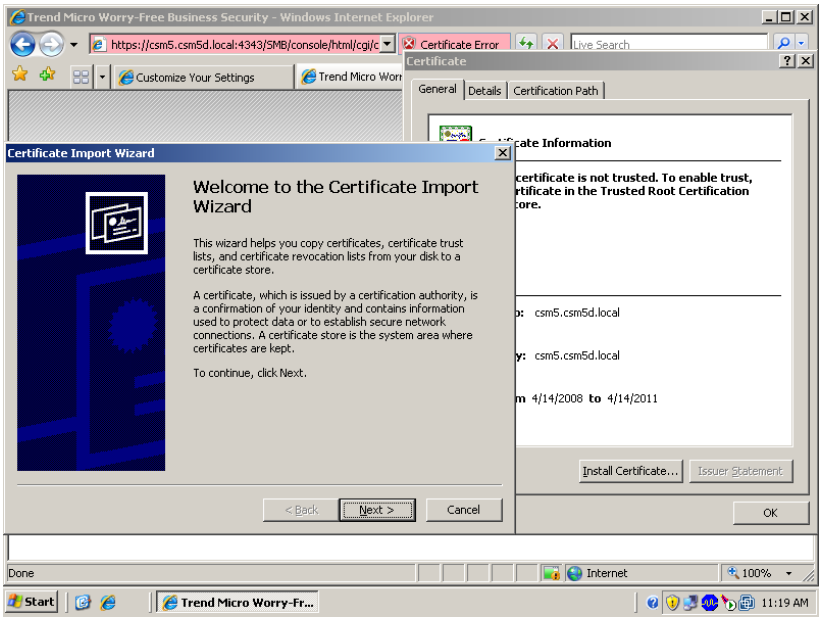
Enable the **Allow File and Print Exception** setting, under Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall.

4.4 > 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. Here's how 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.



4. Click **Install Certificate** > **Next** > **Next** > **Finish**.
5. Click **Yes** when the Security Warning prompt appears.

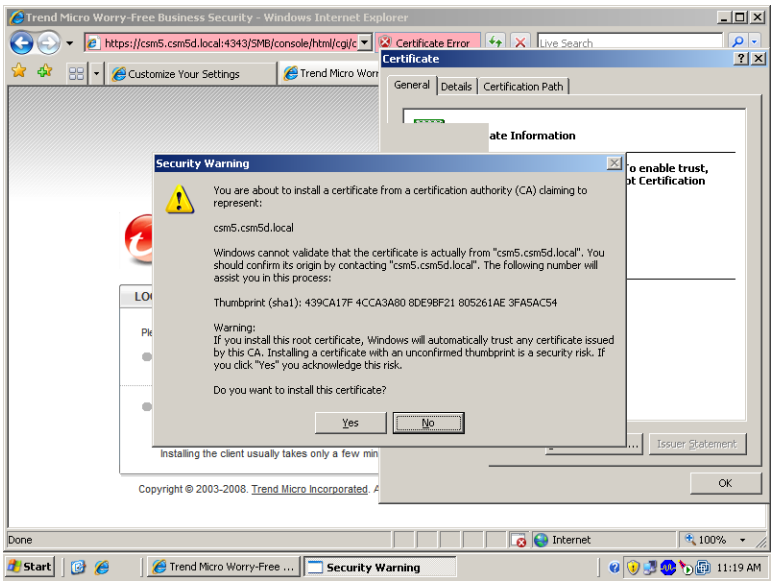


Figure 13: Security Warning

4.5 > Properly Deploying Behavior Monitoring

When deploying Behavior Monitoring feature, 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.

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 by using TMPerftool.

TMPerfTool

Use this performance tuning tool to help identify applications that could potentially cause a performance impact during deployment. Trend Micro recommends running the TMPerfTool 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 TMPerTool 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).
3. Double-click **TMPerfTool.exe**.
4. Put a checkmark on the terms of license agreement box then click **OK**.
5. Click **Analyze** when the system or applications start to slow down.
6. When a red highlighted row appears, it means that the TMPerfTool found the resource-intensive process.
7. Select the highlighted row and click **Exclude**.
8. 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.

9. Note the name of the application.
10. Click **Stop**.
11. 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:

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

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

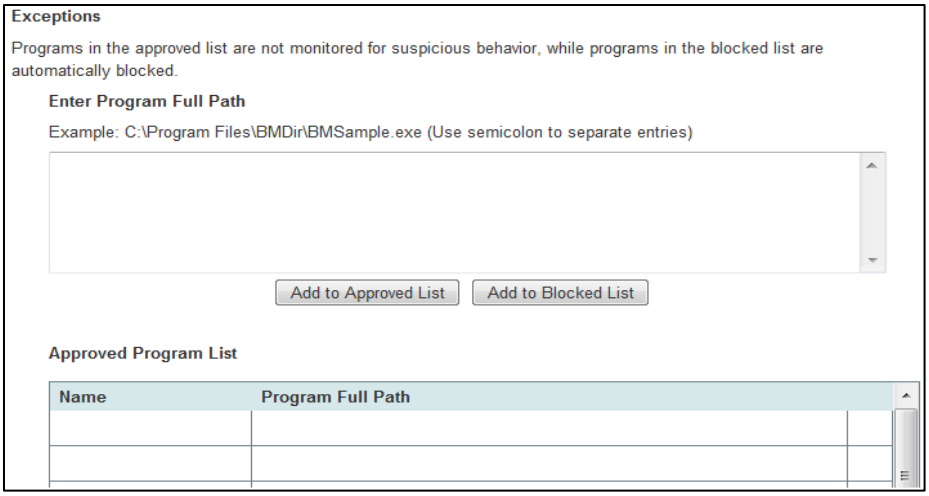


Figure 14: BM Exception

4.6 > 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 Settings**.
2. Click on **Trusted Program**.
3. Type in the full file path to the specific program executable.
4. Click **Add** to Trusted Program List.
5. Click **Save**.

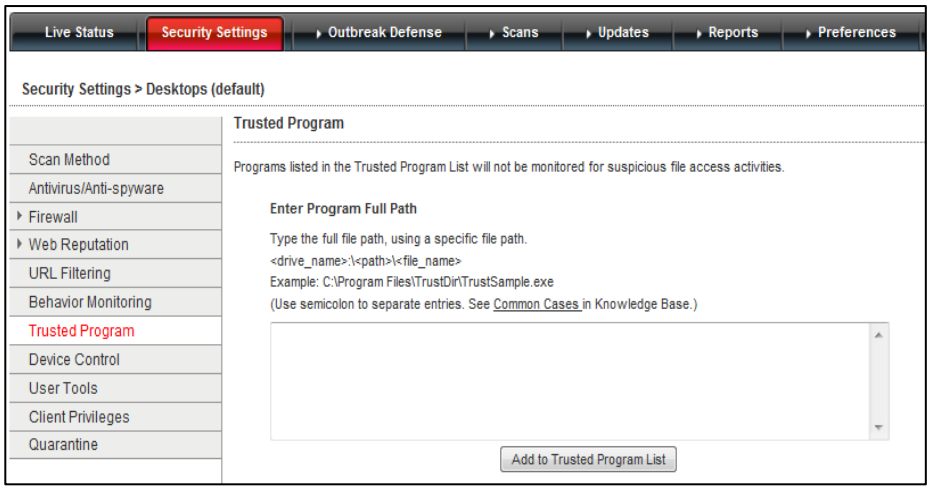


Figure 15: Trusted Programs

4.7 > Install Latest Patches

Most Trend Micro patches are applied to the Security Server. The Security Server then automatically updates the Client/Server Security Agents. Monitor and update to the latest Trend Micro WFBS 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 has:

- At least eight characters long, has one or more uppercase letters (A-Z),
- One or more lowercase letters (a-z),
- One or more numerals (0-9),
- One or more special characters or punctuation marks (!@#$%^&,.:;?)

Strong passwords should not be the same as the user's login name or contain the login name in the password itself. It should not consist of the user's given or family name, birth dates, or any other information that is easily identified with the user.

PROCEDURE

1. In the WFBS management console, navigate to **Preferences** > **Password**. Or alternatively go to shortcut option under **Start** > **Programs** > **Trend Micro Worry-Free Business Security Server** > **Console Password Reset Tool**

Figure 16: Console Password Reset Tool window

2. Type in the user's Windows account and password then click **Next**

3. In the next window, enter the following information

- New password
- Confirm password

4. Click **Change Password**

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. Refer to the previous section if there is no access to the console.

To specify/clear password during agent unload or removal, go to **Preferences** > **Global Settings** > **Desktop/Server** and set password. Refer to Figure 17 below.

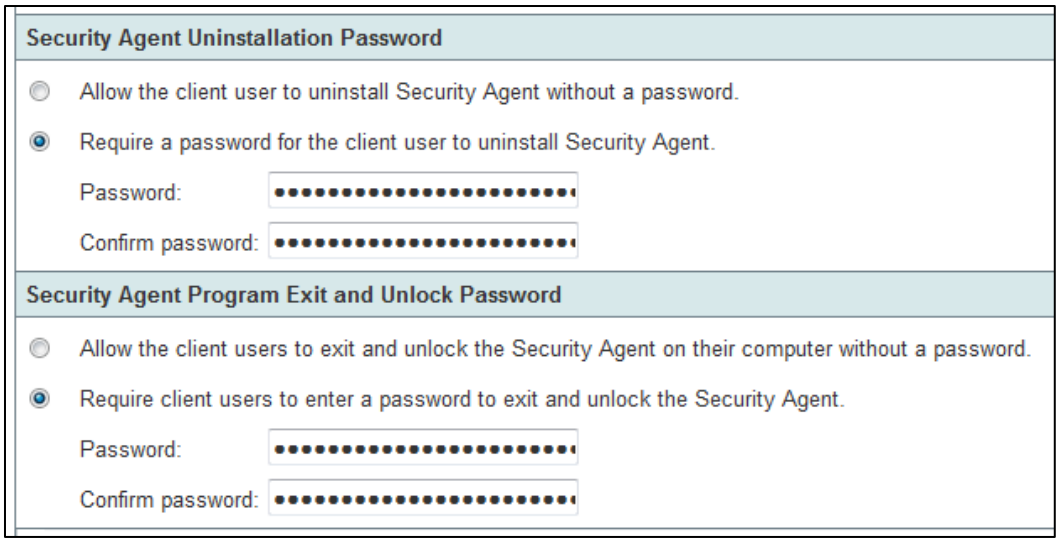


Figure 17: Security Agent Uninstall/Unload Password

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, any of the following procedures can be performed:

- Use the Security Agent Uninstall Tool:

  http://esupport.trendmicro.com/solution/en-us/1057237.aspx

- On the computer where the Security Agent will be uninstalled, set the value of "Allow Uninstall" to 1 in registry editor. Then remove Security Agent from the control panel. This entry can be found under:
  - For 32-Bit OS:

    HKLM\Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc\
  - For 64-Bit OS:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc\
- On the computer where the Security Agent will be uninstalled, launch cmd.exe with elevated privilege (Run as Administrator) and run the following command:

  ```
  For 64-bit OS:

  msiexec /x {A38F51ED-D01A-4CE4-91EB-B824A00A8BDF} /qf DASH331=1

  For 32-bit OS:

  msiexec /x {C1F6E833-B25E-4C39-A026-D3253958B0D0} /qf DASH331=1
  ```

Chapter 6: Configuration

6.1 > Security Server Management Console Settings

Settings	Recommendation
Manual Scan Settings	
Scan Compressed Files	• Enabled • Add compressed files or file extensions that should not be scanned to the scan exclusion list. • Recommended: 2 compression layers
CPU Usage	• Low • This setting helps minimize computer slowdown when scanning occurs during peak hours. To improve performance, consider running Manual Scan during off-peak hours
Action	Use ActiveAction
Realtime Scan Settings	
User activity on files	Read or Write should be selected. This option ensures that files introduced to and originating from the computer are safe to access.
Scan Compressed Files	• Enabled • Add compressed files or file extensions that will not be scanned to the scan exclusion list. • Recommended: 2 compression layers
Action	Use ActiveAction
Display a notification message when a security risk is detected	Enabled. Notifications allow users to take immediate action. Consider disabling only if the notifications are generating a large number of support calls.
Scheduled Scan Settings	
Scheduled Scan	• Enabled • Weekly • Schedule the scan during off-peak hours to improve the scanning performance and avoid potential computer slowdown.
Scan Target	All scannable files

Settings	Recommendation
Scan Compressed Files	• Enabled • Add compressed files or file extensions that will not be included in the scan exclusion list. • Recommended: 2 compression layers
CPU Usage	Low. This setting helps minimize computer slowdown when scanning occurs during peak hours.
Action	Use ActiveAction
Allow users to postpone or cancel Scheduled Scan	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 (Out of Office)	
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
Browser Exploit Prevention New	Enabled
Web Reputation Settings for Internal Clients (In Office)	
Web Reputation Policy	Enabled
Security Level	Medium
Browser Exploit Prevention New	Enabled
Web Reputation and URL Filtering Approved 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://global.sitesafety.trendmicro.com
Server Updates	
Update schedule	Daily or Hourly
Standard Notifications	
Criteria	Send a notification only when the scan action was not performed

Settings	Recommendation
	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.
Client-Server Notification	
Server hostname 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 clients have been registered to the server or clients will have to be redeployed
External Proxy Settings	
Proxy Settings	Enabled if the Trend Micro Security Server connects to the Trend Micro ActiveUpdate server through a proxy server
Log Maintenance	
Scheduled deletion of logs	Enabled
Logs to delete	Logs older than 7 days
Log deletion schedule	Weekly Schedule the deletion during off-peak hours.
Global Settings > Desktop/Server	
Location Awareness	Enable location awareness (affects In/Out of Office settings of Firewall, Web Reputation, and frequency of scheduled updates). Specify all Gateway IP and MAC Addresses. The Security Server identifies the location of a client based on the Security Server gateway information.
General Scan Settings	Check the following options: • Exclude shadow copy sections • Exclude the Security Server database folder • Exclude the Microsoft Exchange server folders when installed on Microsoft Exchange Server • Exclude the Microsoft Domain Controller folders
Virus Scan Settings	• Configure Scan Settings for large compressed files • Do not scan if extracted size is over 2 MB • Scan the first 100 files in the compressed file • Clean compressed files • Scan up to 3 OLE layer(s)
Spyware/Grayware Scan Settings	• Scan for cookies • Add cookie detections to the Spyware log

Settings	Recommendation
Web Reputation and URL Filtering New	Define the URLs the user wants to allow or block access. Note: Allowing or Blocking a URL includes all of its sub domains. (Separate multiple entries with semicolons). Process Exception List: Add critical processes the user wants to be excluded from Web Reputation and URL Filtering. Note: Consider updating the process exception list during off-peak hours as it resets active HTTP connections for a few seconds. IP Exception List: Add trustworthy IP addresses the user wants to be excluded from Web Reputation and URL Filtering.

6.2 > Performance Tuning

Description	Procedure
Disable TSC at startup **- Add/Change value to 1 to disable the Damage Cleanup service from executing whenever the Security Agent's real-time scan starts up. This is helpful for systems with low resource to speed up the bootup/startup time.**	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. 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. The "dtas=dword:00000001" registry is created in the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-CillinNTCorp\CurrentVersion\Misc of the Security agent.
Delay Real-time Scan service startup	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\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration\ hive. 3. Change the value of the registry key "NTRtScanInitSleep" to "180000" (DWORD, Decimal). *Note: The unit is in milliseconds. The value "180000" will delay the start of the Real Time Scan for 3*

Description	Procedure
	minutes.
Increase Pagepool	This registry key will not work with Windows Vista or Windows Server 2008 and above. This workaround will not work if there is a startup option "/3GB" in the boot.ini file for Windows XP and Windows Server 2003. 1. 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. 2. Change the value of "PagedPoolSize" to "0xFFFFFFFF". 3. Restart the computer.
UADuplicationOptValue =128 **- Enable this feature to allow Update Agents to download only one incremental file from the Security server and allow it to automatically generate full pattern and the rest of the incremental files. This will help minimize bandwidth usage.**	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. 3. Restart the Security Server Master Service.
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. 3. Restart the Security Server Master Service.
VerifyConnectionThreadCount=16 **This is the number of threads that will be used for verifying**	1. Go to the [INI_SERVER_SECTION] section of ..\Pccsrv\ofcscan.ini 2. Look for the VerifyConnectionThreadCount=16 parameter.

Description	Procedure
client-server communication	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. c. Go to the Auto Log Deletion tab. d. Set Delete Logs Older Than to "14 Days" for all Log Types. e. Click Save. 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. 5. Restart the Trend Micro Security Server Master Service.

6.3 > 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 9.0 Administrator's Guide.

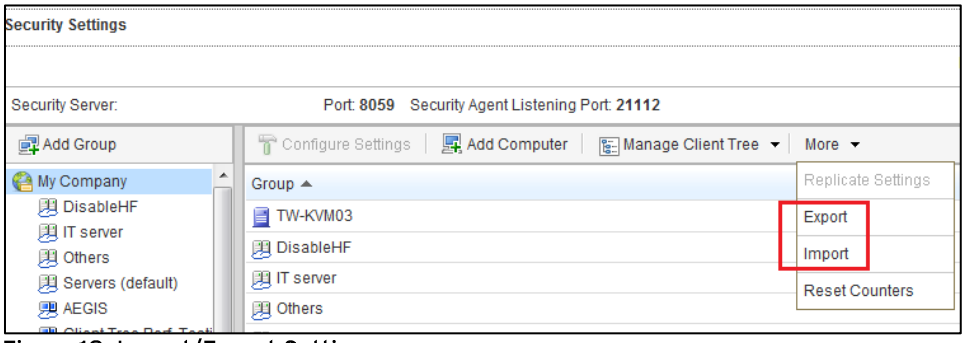


Figure 18: Import/Export Settings

Your 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 27). This allows the Security Server's general (as well as its default group security) settings to be saved. This scope can be selected if there are multiple Security Servers in the company. It can, also, be used to create a backup of the settings of the Security Server.

   Note that this option does not save any custom groups' settings. If there's a need to have a full back up, then export the settings per custom group.

   By design, WFBS 9.0 will NOT export company-specific settings like Proxy, SMTP, Location Awareness, etc. (refer to the unchecked boxes in Figure 28).

2. Per Group settings - select the custom group in the WFBS 9.0 Security Settings Network Tree (refer to Figure 27). It allows the Security Settings defined for the group to be saved.

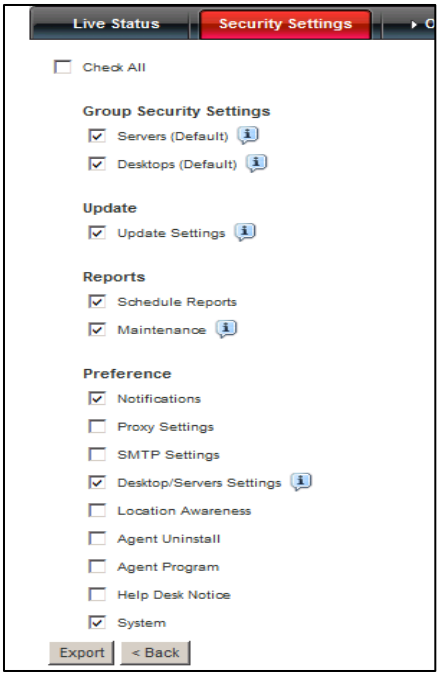


Figure 19 Company Settings - Import Export

NOTE The exported file is encrypted. The exported configuration's filename will be in the format – <Security Server FQDN/IP>_90_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 9.0 checks the following information before importing a saved configuration:

- If the scope of the exported file doesn't match the target import scope. Configurations exported under Company or per group scope can only be imported on Company 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 > Messaging Security Agent Console Settings

Settings	Recommendation
Antivirus	
Real-time antivirus	Enabled
Action	Use ActiveAction
Anti-Spam	
Email Reputation	• Enable real-time anti-spam (email reputation) • Service Level: Advanced
Content Scanning	• Enable real-time anti-spam (content scanning) • Spam detection level: Medium • Detect Phishing: Checked
Web Reputation Settings	
Web Reputation	Enabled
Security Level	Medium

Table 7 Recommended MSA Console Settings

NOTE For Content Filtering, Data Loss Prevention, Attachment Blocking and Mobile Security, settings such as allow or block list, rules and policies would depend on business security requirements.

Chapter 7: Backup and Disaster Recovery

7.1 > Configuring Database Flush

The database flush is now configurable. This allows setting a schedule for flushing data from the memory to the disk and resolve issues associated with 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:

   ```
   DB_ENFORCE_DBFLUSH_PERIOD={y}
   ```

   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.

   NOTE
   If DB_ENFORCE_DBFLUSH_PERIOD is between 1 and 300, then set the time to 300.
   If DB_ENFORCE_DBFLUSH_PERIOD is larger 86400, then set the time to 86400.
   If you set DB_ENFORCE_DBFLUSH_PERIOD to 0, it will skip the enforced flush.

5. Save and close the file.
6. Restart the Security Server Master Service using the Services console.

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 `Database Backup` registry hive:

   For 32-bit OS: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup

   For 64-bit OS: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432node\TrendMicro\Database Backup

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 follow the steps below. Otherwise, proceed to Step 5.

   a. On the right pane, look for "Frequence" 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 "DayOfWeek" 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 ..\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 ..\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: Enhance Protection Against Malware

8.1 > Apply the Latest Patches for WFBS

Make sure to apply the latest patches for WFBS. There is no need to re-apply if the latest patch has been installed already. Patches can be downloaded from the Trend Micro website (URLs specified below) or Live Status in the WFBS console.

- WFBS-Advanced

  http://downloadcenter.trendmicro.com/index.php?prodid=39

- WFBS-Standard

  http://downloadcenter.trendmicro.com/index.php?prodid=40

NOTE There is no need to re-apply if the latest patch has been installed already. Patches can be downloaded from the Trend Micro website (URLs specified above) or sometimes they appear on the WFBS web console's Live Status page.

8.2 > Apply the Latest Patches for Microsoft OS And Other Applications

Keeping the Microsoft operating system always updated is very important. Updates should be applied to avoid attacks leveraging old (but reliable) or new vulnerabilities. Configure WFBS Vulnerability Scanner to perform an assessment on all computers to detect unpatched machines :

1. On the WFBS web console, go to **Outbreak Defense**
2. Under **Vulnerable computer(s)**, click on **Schedule Assessment**
3. Check **Enable Scheduled Vulnerability Prevention**
4. Select the preferred schedule (once a week is recommended)
5. Select the target groups
6. Click **Save**

This is not limited to Microsoft updates only -- other 3rd party applications such as Adobe, Java, and others should be updated as well. Run Microsoft Baseline Security Analyzer once a month to check for machines that have unpatched 3rd party applications. Refer to the link below for more information about this tool:

http://www.microsoft.com/download/en/details.aspx?id=7558

8.3 > Security Agent Pattern Files

This can be checked from the WFBS web console under the **Security Settings** tab. The Trend Micro Vulnerability Scanner (TMVS.exe) can also be utilized to check if there is an AV installed and what pattern is in use.

1. On the WFBS web console, go to **Preferences** > **Management Tool**s
2. Click on **Vulnerability Scanner** to launch another window with all the information and steps on how to use TMVS.exe

8.4 > Enable Smart Feedback

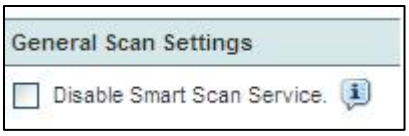
Trend Micro Smart Feedback provides continuous communication between Trend Micro products as well as Trend Micro 24/7 threat research centers and technologies. Each new threat identified during the routine reputation checking of one customer automatically updates the Trend Micro threat databases to help better protect all customers.

1. On the WFBS web console, go to **Preferences** > **Smart Protection Network**
2. Check Enable **Trend Micro Smart Feedback**
3. Check Enable feedback of suspicious program files
4. Enter the type of Industry (optional)
5. Click **Save**

8.5 > Enable SmartScan

Smart Scan is a technology that utilizes a central scan server on the network to take the burden of scanning off your endpoint machines. Smart Scan leverages threat signatures that are stored in the cloud.

1. Login to the WFBS web console
2. Go to **Preferences** > **Global Settings** > **Desktop/Server** tab
3. Under **General Scan Settings** section, make sure that **Disable Smart Scan Service** is NOT checked



4. Click **Save**
5. Still on the WFBS web console, go to **Security Settings**
6. Select the group to configure
7. Click on **Configure Settings**

8. Under Scan Method, make sure that **Smart Scan** is selected
9. Click **Save**

For more information about this feature, visit the following links:

Difference between Smart Scan and Conventional Scan

Frequently Asked Questions (FAQs) about Smart Scan in Worry-Free Business Security (WFBS):

8.6 > Configure Scan Types

Configuring Scan options involves settings the target files to scan and the action that will be taken againt threats. Scheduled scan is disabled by default. If Scheduled scan is enabled, make sure to run scan during off-peak time for your clients.

Real Time Scan

1. On the WFBS web console, go to **Security Settings**
2. Select the group that you want to configure
3. Click on **Configure Settings**
4. Go to **Antivirus/Anti-spyware**
5. Make sure that the **Enable real-time Antivirus/Anti-spyware** is checked
6. Under the Target tab, select **All Scannable files**
7. Choose **Read or write** for the condition
8. Expand **Advanced Settings** and enable **Scan POP3 messages**
9. Make sure that **Enable IntelliTrap** is checked
10. Also, enable the **Memory Scan** so that packed malware process/es running in the memory will be scanned and taken care of
11. Check **Scan compressed files: up to 2 or more layers of compression**
12. Under the Action tab, select **ActiveAction**
13. Check **Set action of Probable malware** and select **Quarantine** to **ActiveAction**

14. Expand Advanced Settings and put a check mark on **Run cleanup when probable virus/malware is detected**

15. Click **Save** for any changes

ENABLE NEWLY ENCOUNTERED PROGRAM DOWNLOAD DETECTION

This feature is a detection improvement in common clients to prevent 0-day attacks. This feature leverages Behavior Monitoring and Web Reputation, thus both must be enabled in order for the feature to function properly.

1. Log in to the WFBS Security Server console.
2. Go to **Security Settings** > **Desktop (defaults)** > **Configure Settings**.
3. On the left pane, click **Web Repuation** and make sure it is enabled.
4. Go back to the left pane and select **Behavior Monitoring**.
5. Make sure that the **Enable Behavior Monitoring** checkbox is ticked. Tick the **Prompt users before executing newly encountered programs through HTTP or email applications** option as well.
6. Click **Save**.

Manual Scan

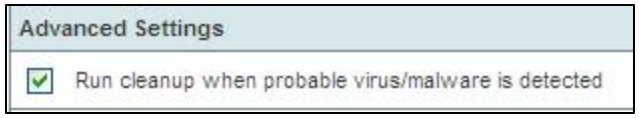
1. On the WFBS web console, go to **Scans** > **Manual Scan**
2. Click on the name of the group to configure
3. Under the **Target** tab, select **All scannable files**.

NOTE The speed of scanning files may degrade once this change is made

4. Check the **Scan mapped drives and shared folders on the network**
5. Check the **Scan compressed files: up to 2 or more layers of compression**
6. Expand **Advanced Settings**, put a check mark on **Run advanced cleanup (For FakeAV)**

7. For Malware Detections, select **ActiveAction**
8. Check **Set action of Probable malware** and select **Quarantine to ActiveAction**

9. Under **Advanced Settings**, put a check mark on **Run cleanup when probable virus/malware is detected**



10. Click **Save** to apply changes
11. Repeat steps to the other groups as necessary

Scheduled Scan Settings

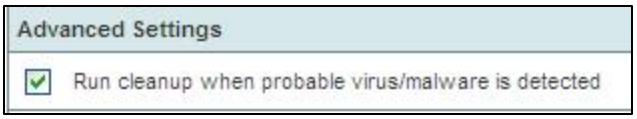
1. On the WFBS web console, go to **Scans** > **Scheduled Scan**
2. Click on the name of the group to configure
3. Under the **Target** tab, select **All scannable files**. Scan time may increase once this option is enabled.

NOTE The speed of scanning files may degrade once this change is made

4. Check the **Scan compressed files: up to 2 or more layers of compression**
5. Expand **Advanced Settings**, put a check mark on **Run advanced cleanup (For FakeAV)**

6. For Malware Detections, select **ActiveAction**
7. Check **Set action of Probable malware** and select **Quarantine to ActiveAction**

8. Under **Advanced Settings**, put a check mark on **Run cleanup when probable virus/malware is detected**



9. Click on **Save** to apply changes
10. Make sure all groups are checked to have the scheduled scan enabled
11. Under **Schedule** tab, select the preferred frequency of the scheduled scan
12. Repeat steps to the other groups as necessary

Summary of the Settings Changed on the Different Types of Scans

	Real Time Scan	Manual Scan	Scheduled Scan
All scannable files will be scanned	X	O	O
Condition (read or write)	O	N/A	N/A
Scan POP3 messages	O	N/A	N/A
Scan mapped drives	X	O	N/A
Intellitrap enabled	O	N/A	N/A
Memory Scan	O	N/A	N/A
Newly encountered program download detection	O	N/A	N/A
Scan compressed files	O	O	O
Run advanced cleanup (for FakeAV)	N/A	O	O
Active action	O	O	O
Set action of probable malware to active action (quarantine)	O	O	O
Run cleanup when probable virus/malware is detected	O	O	O

O = enabled

X = disabled or other setting is applied

N/A = not applicable

8.7 > Enable Behavior Monitoring

Behavior Monitoring regulates application behavior and verifies program trustworthiness. It also uses a separate pattern file to determine if the behavior of a particular file is similar to a malware.

NOTE It is highly recommended to enable this feature gradually or to deploy on a controlled environment first to be sure that it will not cause any conflict on 3rd party or home-grown applications. If such issues occur, contact Trend Micro Technical Support for assistance.

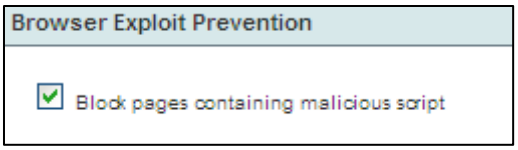
1. On the WFBS web console, go to **Security Settings**
2. Select the group that you want to configure and click on **Configure Settings**

3. Go to Behavior Monitoring and enable the B**ehavior Monitorin**g feature
4. Ensure that the following are enabled:
   4.1. Enable Malware Behavior Blocking for known and potential threats
   4.2. Prompt users before executing newly encountered programs downloaded through HTTP or email applications
5. Click **Save**
6. Repeat steps to the other groups as necessary

8.8 > Enable Web Reputation Service and Device Access Control

Web Reputation Service (WRS) stops web-based threats based on the URL that a user attempts to access. Device Access Control (DAC) regulates access to external storage devices and network resources connected to computers.

1. On the WFBS web console, go to **Security Settings**
2. Select the group that you want to configure and click on **Configure Settings**
3. Go to **Web Reputation** and put a check mark on **Enable Web Reputation for both In Office and Out of Office** (click on **Save** on each)
4. Enable **Browser Exploit Prevention for both In Office and Out of Office** (click on **Save** on each)



5. Click on **Save**
6. Go to **Device Control** and enable device control
7. Make sure that **Enable USB Autorun Prevention** is checked
8. Configure the permissions depending on the needs or work environment
9. Click **Save** for any changes
10. Repeat steps to the other groups as necessary

8.9 > Configure Location Awareness

The administrator's ability to define an endpoint machine's internal/external status and apply different policies will allow more flexible management **of mobile endpoint machines.**

1. **On the WFBS web console, go to Preferences > Global Settings > Desktop/Server** tab
2. Put a check mark on **Enable location awareness**
3. Enter the IP address of the internal gateway, then click **Add**
4. Click **Save**

8.10 > Configure Scanning of Compressed/Decompressed Files

This will let the Security Agents scan the files inside a compressed archive (.zip files, etc.)

1. On the WFBS web console, go to **Preferences** > **Global Settings** > **Desktop/Server** tab
2. Under **Virus Scan Settings**, change the value of **Do not scan if extracted size is over** to **20 MB**
3. Change the value of **Scan the first __ files in the compressed file** to **100**
4. Check **Clean compressed files**
5. Click **Save**

8.11 > User Education

Malware authors often use social engineering to trick users into doing what they want. Educate users not to open suspicious links or files especially from instant messengers, emails from unidentified users and from pop-up windows. Be wary on downloading, executing or accessing files/links that are from social media sites like Facebook.

The following links are useful for user education:

- Best practices in preventing virus infection

  http://esupport.trendmicro.com/solution/en-US/1104639.aspx
- Preventing Ransomware infection

  http://esupport.trendmicro.com/solution/en-US/1099580.aspx

Chapter 9: Miscellaneous

9.1 > Recommended Scan Exclusion List in Windows Platform

Database and encrypted type files should generally be excluded from scanning to avoid performance and functionality issues. Below are exclusions to consider depending on the type of machine you are installing the Security Agent. For other software, contact the vendor about their recommendation.

Application	Directory
Cisco CallManager	..\Call Manager ..\Call Manager Serviceability ..\Call Manager Attendant
Citrix Exclusions	Exclude these file extensions to avoid any performance problems: *.LOG, *.DAT, *.TMP, *.POL, *.PF 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.
Cluster Servers	Q:\ (Quorum drive) C:\Windows\Cluster
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.
General Exclusions for Windows platforms and Domain Controllers	Refer to this Microsoft article about virus scanning recommendations for Enterprise computers that are running currently supported operating system: http://support.microsoft.com/kb/822158
Mapped Drives / Shared Folders	This option is best disabled otherwise, it may create unnecessary network traffic when the end users access remote paths or mapped network drives. Consider disabling this function if all workstations have WFBS client installed and are updated to the latest virus signature.
Microsoft Exchange Server	Exchange 2003 Refer to this Microsoft article: Overview of Exchange Server 2003 and antivirus software Exchange 2007

Application	Directory
	Refer to this Microsoft article: File-Level Antivirus Scanning on Exchange 2007 Exchange 2010 Refer to this Microsoft article: File-Level Antivirus Scanning on Exchange 2010 Exchange 2013 Refer to this Microsoft article: Anti-Virus Software in the Operating System on Exchange Servers
Microsoft IIS 6.0, 7.0, and above server	Web Server log files should be excluded from scanning. For IIS 6.0: C:\Windows\System32\LogFiles C:\Windows\System32\IIS Temporary Compressed Files For IIS 7.0 and above: C:\Inetpub\logs C:\inetpub\temp\IIS Temporary Compressed Files
Microsoft Internet Security and Acceleration Server (ISA)	Refer to: http://technet.microsoft.com/en-us/library/cc707727.aspx
Microsoft Lync	Follow the scan exclusion guidelines for Microsoft Lync: Microsoft Lync 2010: Specifying Antivirus Scanning Exclusions Microsoft Lync 2013: Antivirus Scanning Exclusions for Lync Server 2013
Microsoft Operations Manager Server (MOM)	Refer to http://support.microsoft.com/kb/975931
Microsoft Sharepoint	Refer to http://support.microsoft.com/kb/952167
Microsoft SQL Server	Refer to http://support.microsoft.com/kb/309422
Microsoft Systems Management Server (SMS)	SMS\Inboxes\SMS_Executive Thread Name SMS_CCM\ ServiceData SMS\Inboxes Please refer to Microsoft article http://support.microsoft.com/kb/327453 for more information.
Microsoft Windows System Update Server (WSUS)	Refer to http://technet.microsoft.com/en-us/library/dd939908(WS.10).aspx#av
MySQL	MySQL main directory - ..\mysql\ MySQL Temporary Files - Uses the Windows system default, which is usually C:\Windows\Temp\
Novell Zenworks	..\Novell\Zenworks Exclude the following files: NalView.exe, RMenf.exe, ZenNotifyIcon.exe, ZenUserDaemon.exe, casa.msi, dluenf.dll, fileInfo.db, lcredmgr.dll, objInfo.db Exclude the following extensions: .APPSTATE, .LOG, .TMP, .ZC
Oracle	.dbf - Database file .log - Online Redo Log .rdo - Online Redo Log .arc - Archive log

Application	Directory
	.ctl - Control files
Other Trend Micro Products	Make sure the checkbox for "Do not scan the directories where Trend Micro products are installed." is enabled in WFBS Exclusion List settings (Security Settings > *Group name* > Configure Settings > Antivirus/Anti-spyware > Exclusions).
SAP	SAP ABAP or Java installs: \usr\sap\ SAP Content Server Install: \SAPDB\ SAP Printer Server: SAPSprint.exe Servers where are SAPGui is installed: Isagent.exe During SAP installs or upgrades, it is recommended to exclude the base SAPinst directories and subdirectories: ...\SAPinst_instdir\
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
Trendmicro Scanmail for Exchange	Refer to this article: http://esupport.trendmicro.com/solution/en-us/1055703.aspx
VMWare	Other file extension types that should be added to the exclusion list include large flat and designed files, such as VMWare disk partition. Scanning VMWare partitions while attempting to access them can affect session loading performance and the ability 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.
Microsoft Hyper-V	Hyper-V files: Virtual Machine Configuration Files C:\ProgramData\Microsoft\Windows\Hyper-V Virtual Machine VHD Files: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks C:\ClusterStorage Snapshot Files: C:\ProgramData\ProgramData\Microsoft\Windows\Hyper-V\Snapshots Virtual Machine Processes: Vmms.exe Vmwp.exe
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

Application	Directory
	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.

For updated exclusion list, please refer to the link below:

http://esupport.trendmicro.com/solution/en-us/1059795.aspx

9.2 > How to improve Update Process

Lack of free space may prevent the Security Server from updating. Security Server requires 4.1 GB disk space for program files and 6.9 GB for operation. Take into consideration the disk space that will be used by the Security Agent and the Messaging Security Agent.

9.2.1 Disk Cleaner Tool

To save disk space, use the Disk Cleaner Tool to delete unused backup, log, and pattern files from the following directories:

```
<Security Agent>\AU_Data\AU_Temp\*
<Security Agent>\Reserve\*
<Security Server>\PCCSRV\TEMP\* (except hidden files)
<Security Server>\PCCSRV\Web\Service\AU_Data\AU_Temp\*
<Security Server>\PCCSRV\wss\*.log
<Security Server>\PCCSRV\wss\AU_Data\AU_Temp\*
<Security Server>\PCCSRV\Backup\*
<Security Server>\PCCSRV\Virus\* (Delete quarantined files older than two weeks, except
  NOTVIRUS file)
<Security Server>\PCCSRV\ssaptpn.* (keep the latest pattern only)
<Security Server>\PCCSRV\lpt$vpn.* (keep the latest three patterns only)
<Security Server>\PCCSRV\icrc$oth.* (keep the latest three patterns only)
<Security Server>\DBBackup\* (keep latest two subfolders only)
<Security Server>\AU_Data\AU_Temp\*
<Security Server>\Debug\*
<Security Server>\engine\vsapi\latest\pattern\*
```

NOTE An administrator privilege is needed to run this tool on the Security Server. If 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. Go to: ..\Trend Micro\Security Server\PCCSRV\Admin\Utility
2. Double-click the **TMDiskCleaner.exe** file.
3. Click **Delete Files** to start the cleaning of unused files.

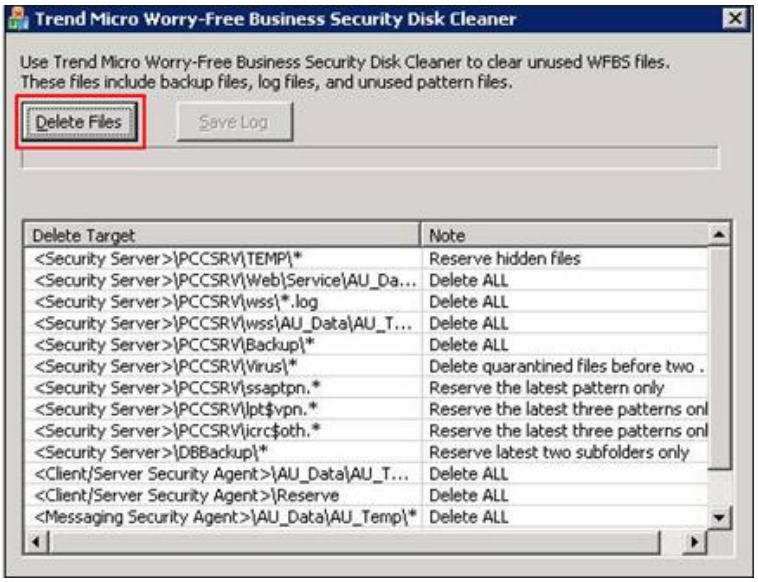


Figure 20 Disk Cleaner Tool

4. Once the cleanup process is finished, click **Save Log**.

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

Via command line:

1. Open a command prompt window.
2. Go to: ..\Trend Micro\Security Server\PCCSRV\Admin\Utility
3. Run the following command: `TMDiskCleaner.exe /<condition>`

/hide - Execute tool in the background.

/log – Works only when "/hide" is set. Saves the DiskClean.log file to current folder.

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:

1. Go to **Start** > **Programs** > **Accessories** > **System Tools** > **Scheduled Tasks**.
2. Double-click **Add Scheduled Task**.
3. When the Scheduled Task Wizard window appears, click **Next**.
4. Select **TMDiskCleaner.exe**.

5. Specify the frequency of the cleanup, the time, and the user account that will be used to run the tool.

Figure 21 Scheduled task to run TmDiskCleanner tool

5. Go back to the Scheduled Task window, right-click **TMDiskCleaner** and select **Properties**.
6. On the **Run** field, specify "/hide /log" as shown below.

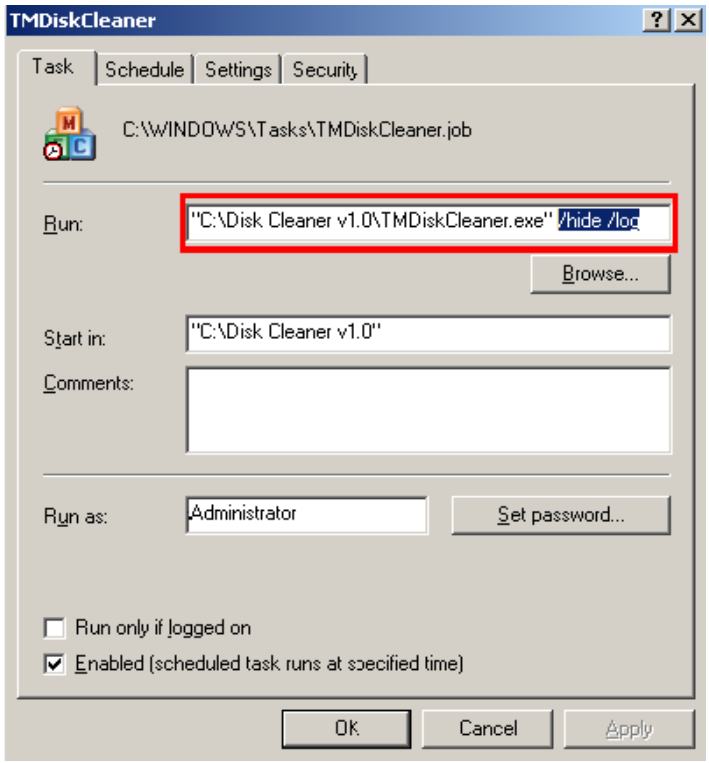


Figure 22 Properties of TMDiskCleaner Tool

7. Click **Apply**.

9.2.2 Update Agent

An Update Agent is a Security Agent that can receive updated components from the Security Server or ActiveUpdate server and then deploy to other Security Agents. For networks segmented by location, Trend Micro recommends allowing at least one Security Agent on each segment to act as an Update Agent to save bandwidth. See the link below on how to setup an Update Agent:

http://esupport.trendmicro.com/solution/en-us/1057531.aspx

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\PFW

  Name: 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 XP SP2 and below
- Windows NT server / workstation
- Intel IA64 (Itanium)
- Windows 2000 series

When planning an upgrade to version 9.0, 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 9.0
- 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 9.0 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 9.0:

- WFBS 6.x, 7.x, 8.x → WFBS 9.0
- CSM 3.0 → CSM 3.6 → WFBS 5.x → WFBS 6.x → WFBS 7.x → WFBS 8.0 → WFBS 9.0

WFBS 9.0 supports direct upgrade from WFBS 6.x, 7.x, and 8.x. 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 9.0. Alternatively, uninstall both Security Server and Client/Server Security Agent and then do a fresh install of WFBS 9.0.

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.

NOTE The following steps work only on Windows Server 2003 and below, but not on Windows Server 2008.

   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.
8. Create a daily/weekly scheduled scan of the roaming profiles in off-peak hours on the fileserver.

9.6 > How to Configure IPv6 addresses

The web console allows user 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
- 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.

9.7 > Summary of Tools that can be used for Troubleshooting

Table below lists the tools that can be used for troubleshooting WFBS.

Troubleshooting	Tools
Installation/Uninstallation	Uninstall Tool - for manual uninstallation of Security Agent. Downloader Tool - for downloading WFBS 9.0 installer when the installer gets corrupted after completing Gmer and RCMToolPack - for finding third-party driver conflicting with the installation and collecting tmcomm.log respectively.
Offline Clients/Not showing in console	Change GUID Tool - for changing the GUID of Security Agent when you want to clone the machine IPxFer tool - for transferring Security Agents (SA) from one Security Server to another
Update	Disk Cleaner Tool - for deleting unused WFBS files such as backup files, log files and unused pattern files to free up disk space
Console	Console Recovery Tool - for resolving several console issues Console Password Reset Tool - for resetting the WFBS management console password
Performance	TMPerfTool and Xperf Tool - for identifying applications that are resource-intensive or that have heavy I/O
Crash	ADPlus and Dr. Watson Tools - for debugging crash issues
Database	SrvDiag Tool - for recreating the Security Server Website and Database of WFBS.
Malware	Anti-Malware tools - for cleaning infection and getting logs/system information
Debugging	Case Diagnostic Tool - for collecting information needed by Trend Micro Technical Support

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.

10.1 > 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.
2. {Security Server installation folder} is typically C:\Program Files\Trend Micro\Security Server.
3. Open contact_info.ini using a text editor such as Notepad and then type the relevant contact information. Save the file.
4. 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.