Best Practice Configurations for Worry-Free Business Security (WFBS) 7 Std/Adv

Worry-Free Business Security (WFBS) 7 Standard/Advance offers several layers of protection to make your machine secure. This document guides you on how to make the best out of those features and make your network protected from the latest threat the Internet could offer.

Web Reputation

Web Reputation is an in-the-cloud service capable of detecting and blocking Web-based security risks, including phishing attacks. Accessed sites are classified and assigned credibility scores that reflected their potential for either becoming infection vectors or somehow involved in a malware / spyware's lifecycle. WFBS uses these credibility scores to regulate access to these sites.

Firewall

Firewall manages connections to and from Security Agents by means of rules. Currently, WFBS implements two types of rules, Access rules and Generic Stream Scanning rules. In Access Rule, you can define the kinds of packets that are blocked and are allowed to pass. Generic Stream Scanning rules detect network viruses and are defined in firewall patterns. By enabling the Firewall, you have the option to enable Intrusion Detection System that identifies patterns in network packets that may indicate an attack on the client.

Behavior Monitoring

Behavior Monitoring protects the machine by preventing any authorized real-time changes in the system files and registries. Instead of file signature, this feature monitors the behavior of the files and sees if they exhibit similar to a malware. With that, it proactively stops unknown malware and continuously monitors malicious activities and blocks questionable programs.

Device Control

Device Control allows administrators to block autorun programs on USB flash memory or USB hard disk. It also controls access to external storages and network resources connected to computers.

Smart Scan

Smart Scan is a technology from Trend Micro that utilizes a central scan server on your network to take the burden of scanning off your clients and reduce the amount of network traffic. Enable Smart Scan to let the Smart Scan Server download all the necessary scan components and scan clients. The Smart Scan Server is installed automatically with the WFBS Advanced server. You do not need to install it separately.

Smart Feedback

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others.

NOTE : There is no need to re-apply if already configured

Configuring Smart Scan

How to enable or disable the Smart Scan function in Worry Free Business Security (WFBS) Standard / Advanced 6.0
http://esupport.trendmicro.com/pages/How-to-enable-or-disable-the-Smart-Scan-function-in-Worry-Free-Business-Security-(WFBS)-Standard--Advanced-60.aspx
Changing the Scan Method in Worry-Free Business Security (WFBS) Standard / Advanced 6.0
http://esupport.trendmicro.com/pages/Changing-the-Scan-Method-in-Worry-Free-Business-Security-Standard--Advanced-60.aspx
Frequently Asked Questions (FAQs) about Smart Scan in Worry-Free Business Security (WFBS) Standard / Advanced 6.0
http://esupport.trendmicro.com/pages/Frequently-Asked-Questions-(FAQs)-about-Smart-Scan-in-Worry-Free-Business-Security-(WFBS)-Standard--Advanced-60.aspx

Configuring Real Time Scan Settings

1. From the Security Server, open the Security Dashboard
2. Click **Security Settings** tab
3. Highlight group under My Company
4. Click **Configure**
5. Click on **Antivirus/Anti-spyware**
6. Tick the Enable real-time antivirus / anti-spyware checkbox
7. Under **Target** tab, select Intelliscan then choose "Read or write"
8. Expand **Advanced Settings**
9. Tick the Enable IntelliTrap checkbox
10. Tick Scan compressed files: up to 1 or more layers of compression
11. Under **Action** tab, select Customized action for the following detected threats
12. Click Restore Defaults button
13. Select Delete or Quarantine for Probable malware
14. Click Save for any changes
15. Click on **Firewall**
16. Tick the Enable Firewall checkbox for both In Office and Out of Office.
17. Click on Save for any changes
18. Click on **Web Reputation**
19. Tick the Enable Web Reputation for both In Office and Out of Office
20. For In Office and Out of Office, select Medium for Security Level
21. Click Save for any changes
22. Click on **Behavior Monitoring**
23. Tick the Enable Behavior Monitoring, Enable Intuit Quickbooks Protection and Enable Malware Behavior Blocking checkboxes
24. Click Save for any changes
25. Click on **Device Control**
26. Tick the Enable Device Control and Enable USB Autorun Prevention checkboxes
27. Configure access permissions and exceptions for your devices.
28. Click Save for any changes
29. Repeat steps to your other groups as necessary

Configuring Manual Scan Settings

1. From the Security Server, open the Security Dashboard
2. Click **Scans | Manual Scan** tab
3. Click the name of the group
4. Under **Target** tab, select All Scannable files
5. Tick the Scan mapped drives and shared folders on the network
6. Tick the Scan compressed files: up to 2 or more layers of compression
7. Under **Action** tab, select the preferred CPU Usage
8. For Malware Detections, select Customized action for the following detected threats
9. Click Restore Defaults button
10. Select Delete or Quarantine for Probable malware
11. Click Save for any changes
12. Repeat steps to your other groups as necessary

Configuring Scheduled Scan Settings

1. From the Security Server, open the Security Dashboard
2. Click **Scans | Scheduled Scan** tab
3. Click the name of the group
4. Under **Target** tab, select All Scannable files
5. Tick the Scan compressed files: up to 2 or more layers of compression
9. Under **Action** tab, select the preferred CPU Usage
10. For Malware Detections, select Customized action for the following detected threats
11. Click Restore Defaults button
12. Select Delete or Quarantine for Probable malware
13. Click Save for any changes
14. Repeat steps to your other groups as necessary
15. Make sure all groups are checked to have scheduled scan.
16. Under **Schedule** tab, select the preferred frequency of the scheduled scan.
17. Click Save for any changes

Configuring Location Awareness

1. From the Security Dashboard, go to **Preferences** | **Global Settings** | **Desktop/Server** tab
2. Tick the Enable location awareness
3. Enter the IP address of your internal gateway then click Add.
4. Click Save for any changes.

Configure the scanning of compressed/decompressed files

1. On the Security Dashboard, go to Preferences > Global Settings
2. Click on the Desktop/Server tab
3. Under Virus Scan Settings, change the value of "Do not scan if extracted size is over" to 20 MB
4. Change the value of "Scan the first __ files in the compressed file" to 100
5. Click on Save down at the bottom

Configuring Security Server to get the latest updates from Trend Micro

1. Click **Updates** tab then **Scheduled** from the Security Dashboard.
2. Select all components under **Components** tab.
3. Click **Schedule** tab.
4. Select Hourly for Conventional Scan Updates.
5. Select Every 15 minutes for Smart Scan Updates.
6. Click Save for any changes.

Make sure all security agents are up-to-date with the latest engine/pattern

1. You can always check it from the Security Dashboard under Security Settings tab.
2. You can also run Trend Micro Vulnerability Scanner (TMVS.exe) to check if there's an AV installed and what pattern they are currently using.

Enable Smart Feedback

1. Click Preferences tab then Smart Protection Network from the Security Dashboard.
2. Click the Enable Trend Micro Smart Feedback.
3. Click the File Feedback.
4. Enter your type of Industry (optional).

Apply the Latest Patch(es) for WFBS

http://www.trendmicro.com/download/product.asp?productid=39

Run Microsoft Baseline Security Analyzer once a month to check for Unpatched PC

1. Download the tool on the link below
http://www.microsoft.com/download/en/details.aspx?id=7558
2. See more information on the link below
http://technet.microsoft.com/en-au/security/cc184924.aspx

Disable System Restore

NOTE: For detections with actions "Failed to clean, delete or quarantine" and located under SYSTEM VOLUME INFORMATION folder, please follow these steps:

1. Click on Start then Run
2. Type in GPEDIT.MSC then hit ENTER.
3. Go to Computer Configuration | Administrative Templates | System | System Restore
4. Double-click "Turn off System Restore," set it to Enabled, then click OK.
5. Close the Group Policy Object Editor. The changes will take effect on the next policy refresh.

Educate users not to click on links they do not trust

Do not open suspicious links or files especially from instant messengers, emails from unidentified users and from pop-up windows.