Best Practice Configurations for Worry-Free Business Security (WFBS) Std/Adv 8.0

Apply the latest patch(es) for WFBS

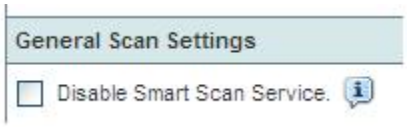
WFBS-Advanced
WFBS-Standard

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 (via PMAC).

Configuring Smart Scan

Smart Scan is a new technology from Trend Micro that utilizes a central scan server on your 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 on Save
5. Still on the WFBS web console, go to Security Settings
6. Select the group that you want to configure
7. Click on Configure
8. Select *Smart Scan*
9. Click Save

Difference between Smart Scan and Conventional Scan:
http://esupport.trendmicro.com/solution/en-us/1053817.aspx

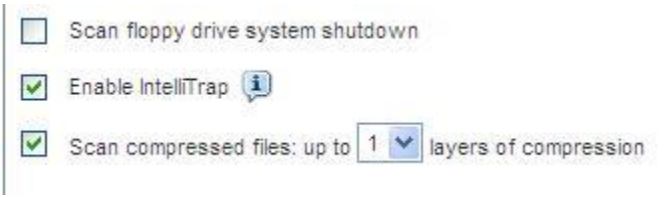
Frequently Asked Questions (FAQs) about Smart Scan in Worry-Free Business Security (WFBS):
http://esupport.trendmicro.com/pages/Frequently-Asked-Questions-(FAQs)-about-Smart-Scan-in-Worry-Free-Business-Security-(WFBS)-Standard--Advanced-60.aspx

Configuring Real Time Scan Settings

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

   Note: The speed of scanning files might degrade a little bit once this change is made.

7. Then choose *Read or write* for the condition
8. Expand Advanced Settings and enable *Scan POP3 messages*
9. Also, make sure that *Enable IntelliTrap* is checked
10. Check *Scan compressed files*: up to *1 or more* layers of compression



11. Under the Action tab, select *ActiveAction*
12. Check *Set action of Probable malware* and select *Quarantine* to ActiveAction

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

14. Click Save for any changes

Configuring Manual Scan Settings

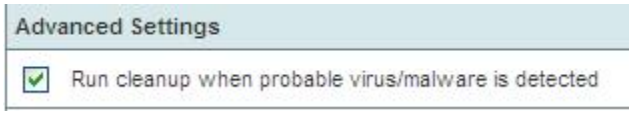
1. On the WFBS web console, go to Scans > Manual Scan
2. Click on the name of the group that you want to configure
3. Under the Target tab, select *All scannable files*

   Note: The speed of scanning files might degrade a little bit 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. Under Action tab, select the preferred CPU Usage
8. For Malware Detections, select *ActiveAction*
9. Check *Set action of Probable malware* and select *Quarantine* to ActiveAction

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



10. Click Save for any changes
11. Repeat steps to your other groups as necessary

Configuring Scheduled Scan Settings

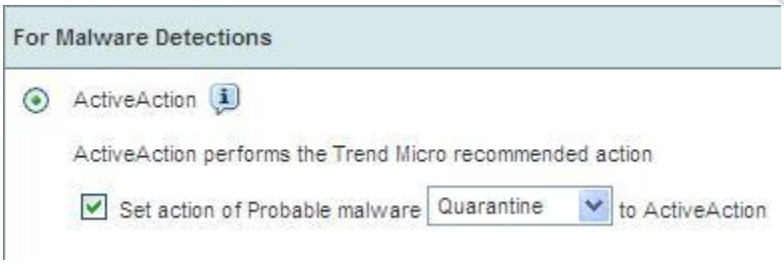
1. On the WFBS web console, go to Scans > Scheduled Scan
2. Click on the name of the group that you want to configure

3. Under the Target tab, select *All scannable files*

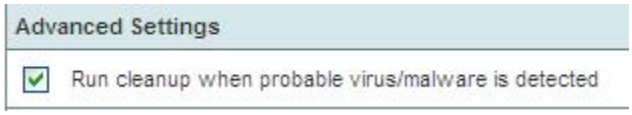
   Note: The speed of scanning files might degrade a little bit once this change is made.

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. Under Action tab, select the preferred CPU Usage
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 on Save for any changes
11. Make sure all groups are checked to have scheduled scan
12. Under Schedule tab, select the preferred frequency of the scheduled scan
13. Repeat steps to the other groups as necessary

Summary of the Settings that were changed on the Different Types of Scans

	Real Time Scan	Manual Scan	Scheduled Scan
All scannable files will be scanned	O	O	O
Condition (read or write)	O	X	X
Scan POP3 messages	O	X	X
Intellitrap enabled	O	X	X

Scan compressed files	O	O	O
Scan mapped drives	X	O	X
Run advanced cleanup (for FakeAV)	X	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 = means the specified feature needs to be changed or was changed
X = means that the specified feature doesn't apply or doesn't need to be changed

Enable Other Features (WRS, BM and DAC)

WRS stops web-based threats based on the URL that a user attempts to access. **BM** regulates application behavior and verifies program trustworthiness. **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*
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. Go to *Behavior Monitoring* and enable the Behavior Monitoring feature
5. Put a check mark on *Enable Malware Behavior Blocking*
6. Click on Save
7. Go to *Device Control* and enable device control
8. Make sure that *Enable USB Autorun Prevention* is checked
9. Configure the Permissions depending on your needs or work environment
10. Click Save for any changes
11. Repeat steps to your other groups as necessary

Configuring Location Awareness

Your ability to define an endpoint machine's internal/external status and apply different policies allows you to manage mobile endpoint machines more flexibly.

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 your internal gateway then click Add
4. Click Save

Configure the scanning of compressed/decompressed files

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

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

1. You can always check it from the WFBS web console under the 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

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 Security Dashboard, go to Preferences tab > Smart Protection Network
2. Check *Enable Trend Micro Smart Feedback*
3. Check *Enable feedback of suspicious program files*
4. Enter your type of Industry (optional)
5. Click Save

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

Keeping your Microsoft operating system always updated is very important. Users should apply these software updates regularly to avoid attacks leveraging old (but reliable) or new vulnerabilities. This is not limited to MS updates only -- other 3rd party applications (like *Adobe*, *Java*, etc.) should be updated too.

You can read more about this free tool from Microsoft and get the installer here:

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

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. They should also be wary of downloading, executing or accessing files/links that are from social media sites like *Facebook*.