

Best Practice Configurations for Worry-Free Business Security (WFBS) Std/Adv 6

Apply the Latest Patch(es) for WFBS

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

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](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](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/AntiSpyware
6. Tick the Enable real-time antivirus / anti-spyware checkbox
7. Under Target tab, select All Scannable files then choose "Scan files being created/modified or retrieved"
8. Expand Advanced Settings
9. Tick or check the Enable IntelliTrap checkbox
10. Tick Scan compressed files: up to 1 or more layers of compression
11. Under Action tab, select Perform the same action for all detected Internet threats
12. Select Clean and Delete or Quarantine for the first and second action
13. For Spyware/Grayware Detections select Clean for the action
14. Click Save for any changes
15. Click on Web Reputation
16. Tick the Enable Web Reputation for either In Office or Out of Office
- 17 For In Office and Out of Office, select Medium for Security Level
18. Click Save for any changes
19. Click on Behavior Monitoring
20. Tick the Enable Behavior Monitoring



ANTI-SPYWARE



ANTI-SPAM



ANTIVIRUS



WEB REPUTATION



ANTI-PHISHING



WEB FILTERING

21. Tick the Enable Intuit Quickbooks Protection
22. Click Save for any changes
23. 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. Expand Advanced Settings
8. Tick the Enable IntelliTrap checkbox
9. Tick the Scan boot area checkbox
10. Under Action tab, select the preferred CPU Usage
11. For Virus Detections, select Perform the same action for all detected Internet threats
12. Select Clean and Delete or Quarantine for the first and second action
13. For Spyware/Grayware Detections select Clean for the action
14. Click Save for any changes
15. 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
6. Expand Advanced Settings
7. Tick the Enable IntelliTrap checkbox
8. Tick the Scan boot area checkbox
9. Under Action tab, select the preferred CPU Usage
10. For Virus Detections, select Perform the same action for all detected Internet threats
11. Select Clean and Delete or Quarantine for the first and second action
12. For Spyware/Grayware Detections select Clean for the action
13. Click Save for any changes
14. Make sure all groups are checked to have scheduled scan.
15. Under Schedule tab, select the preferred frequency of the scheduled scan.
16. Click Save for any changes
17. Repeat steps to your other groups as necessary

Configuring Location Awareness for Web Reputation Service (WRS)

1. From the Security Dashboard, go to Preferences -> Global Settings -> Desktop/Server tab
2. Tick or check the Enable location awareness
3. Enter the IP address of your internal gateway then click Add.
4. Click Save.



ANTI-SPYWARE



ANTI-SPAM



ANTIVIRUS



WEB REPUTATION



ANTI-PHISHING



WEB FILTERING

Apply Enhanced GeneriClean

1. Verify if Enhanced GeneriClean is applied or not
2. Go to c:\program files\trend micro\officescan\pccsrv\admin\tsc.ini
3. Look for this section [secured policy], if it exists, it means Enhanced GeneriClean is applied. Else, it has not been applied:
[secured policy]
DisableTaskMgr=1
DisableRegistryTools=1
NoRun=1
NoCloseKey=1
NoFind=1
DisallowRun=1
FirewallDisableNotify=0
UpdatesDisableNotify=0
AntiVirusDisableNotify=0
FirewallOverride=0
AntiVirusOverride=0
NoAutoUpdate=0
AUOptions=1
EnableFirewall=0
6. Open the PCCSRV\Autopcc.cfg\apnt.ini file.
7. Look for the "admin\tsc.ini" line. If it does not exist, add it.
8. Save and close the file.
9. Wait 2-3 minutes and the hotfixnt.txt will be automatically generated.
10. The Security Server will now notify the Security Agents and deploy the tsc.ini file.
11. If hotfixnt.txt was not automatically generated, please restart the Security Server Master Service.

Disable roaming mode

Trend Micro recommended to not to set the machines in roaming mode since it won't get configuration being set on the security server.

If the client had already enabled roaming mode, please do the following on the client machine:

Option 1:

1. Right-click the Trend Micro icon from the system tray.
2. Select Disable Roaming Mode

Option 2:

1. Open the registry editor (Start > Run > Type in "regedit")

Important: Before editing the registry, make sure you understand how to restore it if a problem occurs.

For more information, view the Restoring the Registry Help topic in Regedit.exe or Restoring a Registry Key Help topic in Regedt32.exe. Making incorrect changes to your registry can cause serious system problems. Always make a back up copy before making any registry changes. Refer on the link below on how to create and restore the Windows registry backup:

<http://esupport.trendmicro.com/Pages/Creating-and-restoring-the-Windows-system-registry-backup.aspx>

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

On the right pane, double click on ForceMobile and set the value data to 0



To remove the privilege to set a machine to roaming mode, please do this from the Security Server:

1. Click Security Settings tab from the Security Dashboard
2. Highlight the group under My Company where the machine is located
3. Click Configure
4. Go to the Client Privileges section
5. Select the Enable Roaming option.

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.

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.

Checking for unprotected computer using Trend Micro Vulnerability Scanner

1. Navigate to \Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\TMVS and run TMVS.exe
2. Click on Settings
3. Under Save As CSV section, check the box to that says "Automatically save the result to a CSV file".
4. You may specify the path where to save the log file.
Default directory where the log file will be created is at C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\TMVS
5. Click OK
6. Specify the IP ranges you have on the Network
7. Click on Start

8. You may open the CSV file using Microsoft Excel to check the machines that are unprotected.

Note: You may also use this CSV file to check for machines that are out of dated in terms of Pattern file and scan engine.

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).



ANTI-SPYWARE



ANTI-SPAM



ANTIVIRUS



WEB REPUTATION



ANTI-PHISHING



WEB FILTERING

Run Microsoft Baseline Security Analyzer 2.1 once a month to check for Unpatched PC

1. Download the tool on the link below

<http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en#Instructions>

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 Local Computer Policy | Administrative Template | System | System Restore
4. Double-click "Turn off System Restore," set it to Enabled, then click OK.
5. Close the policy and exit Active Directory Users and Computers. The changes will take effect on the next policy refresh.

Disable AutoRun

1. Click on Start then Run
2. Type in GPEDIT.MSC then hit ENTER.
3. Go to Local Computer Policy | Administrative Template | System
4. On the right pane, double-click Turn off Autoplay
5. When you are in the properties dialog box, click Enabled
6. Choose All drives from the drop-down list underneath.
7. Click on OK.

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.



ANTI-SPYWARE



ANTI-SPAM



ANTIVIRUS



WEB REPUTATION



ANTI-PHISHING



WEB FILTERING