



TREND MICRO

Worry-Free Business Security

Services v3.5

Best Practices Guide

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
www.trendmicro.com

Volume Technical Product Marketing



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the latest version of the applicable user documentation.

Trend Micro, the Trend Micro t-ball logo, and Worry-Free are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2010 Trend Micro Incorporated, Volume Technical Product Marketing. All rights reserved.

Trend Micro™ Worry-Free™ Business Security Services – Best Practices Guide provides best practice guidelines to resellers and customers deploying Worry-Free Business Security Services. Detailed information about how to use specific features in the software is available in the Online Help and in the *Trend Micro™ Worry-Free™ Business Security Services User's Guide*.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. You can also evaluate this document on the following Web site:

www.trendmicro.com/download/documentation/rating.asp

DOCUMENT PROFILE:

Product: Trend Micro™ Worry-Free™ Business Security Services 3.5

Document Title: Worry-Free™ Business Security Services v3.5 – Best Practices Guide v1.0

Document Filename: BP - WFBS-SVC 3.5 - v1.0

Document Release Date: September 16, 2010

Team: Volume Technical Product Marketing

Author: Randy Jeff N. Licsi, CISSP, Senior Technical Product Engineer

Contents

Preface	5
Chapter 1: Introduction	6
What is Worry-Free Business Security Services?	6
Features and Benefits	7
Chapter 2: Product Registration.....	8
Logon Information	8
Chapter 3: Initial Configuration	10
Default Configuration.....	10
Installer Management	11
Deploying via Active Directory	11
Package URL.....	15
Chapter 4: Installation	16
Worry-Free Business Security Services Agent System Requirements	16
Uninstall Existing AV Product.....	16
Ports.....	17
Chapter 5: Management Console	18
Agent Reporting Time.....	18
Day-to-Day Management	18
Live Status	18
System Status	19
License Status.....	19
Agents Installed.....	20
Customize Columns	20
Scans Tab	21
Reports Tab	22
Log Query	23
Notifications	23
IM Content Filtering.....	23
Chapter 6: The Client Console.....	24
Accessing the WFBS-SVC – Client/Server Security Agent Console.....	24
Component Update.....	24
Personal Firewall.....	25
Chapter 7 – Worry-Free Remote Manager Integration	26
Creating a Customer and WFBS-SVC Service in WFRM	26

Chapter 8: Password Management	31
Recovering a Lost WFBS-SVC Console Password.....	31
Setting an Uninstall and Unload Agent Password.....	31
Chapter 9: Performance Tuning	33
Active and Normal Agents	33
Manually Setting the Active Agent	33
Account Recommendations/Limit.....	34
Update Bandwidth.....	35
About Trend Micro	36

Preface

Welcome to the *Trend Micro Worry-Free Business Security Services - Best Practices Guide*. This document is designed to help resellers and customers develop a set of best practices for deploying and managing Worry-Free Business Security Services.

The document is also designed to be used in conjunction with the following guides:

- *Trend Micro Worry-Free Business Security Services - User's Guide*
- *Trend Micro Worry-Free Business Security Services - Reviewer's Guide*

–Volume Technical Product Marketing

Chapter 1: Introduction

What is Worry-Free Business Security Services?

Trend Micro™ Worry-Free™ Business Security Services (WFBS-SVC) is an in-the-cloud security service for small business. It works with on-premise Client/Server Security Agents (CSAs) to help small businesses automatically detect, monitor, and prevent Web, Virus, and Spyware threats on file servers, PCs, and notebooks. No on-premise server is required to host the service, saving maintenance and hardware costs. Trend Micro security experts host the WFBS-SVC Server in the Trend Micro Data Center and update the service for you.

WFBS-SVC provides a centralized Web management console, readily available through your browser, which allows you to view dashboard Live Status information for threats, security incidents, system updates, and your license across all managed clients. It also allows you to manage clients by groups; execute manual and scheduled scans; create reports and store them in PDF format; and administer the system for multiple PCs and notebooks. Used in conjunction with Worry-Free Remote Manager, you can also manage multiple customers. Altogether, WFBS-SVC is

- **Safer:** It protects multiple PCs/notebooks located in or out of the office with a single antivirus, anti-spyware business solution.
- **Smarter:** It stops viruses and other threats without users having to configure settings or maintain updates.
- **Simpler:** You can centrally manage and check the status of protected clients anywhere (no server required).

Features and Benefits

As a member of the Trend Micro Worry-Free Business Security Family, Worry-Free Business Security Services provides a number of key benefits to small business users. Designed to be the simplest to deploy among the family, users can be up and running and protected in a matter of minutes.

Table 1 - WFBS Hosted Features and Benefits

Features	WFBS Services	WFBS Standard	WFBS Advanced
Server Required		✓	✓
Web Management Console	✓	✓	✓
Client Console and Agent Updates	✓	✓	✓
Smart Scan	✓	✓	✓
File Reputation	✓	✓	✓
Web Reputation	✓	✓	✓
Antivirus, Anti-spyware, Anti-rootkits, Anti-bots, Firewall	✓	✓	✓
Anti-phishing	✓	✓	✓
POP3 Anti-spam	✓	✓	✓
TrendSecure	✓	✓	✓
Instant Messaging Content Filtering	✓	✓	✓
Damage Cleanup Services	✓	✓	✓
Reports	✓	✓	✓
Behavior Monitoring	✓	✓	✓
Managed by Worry-Free Remote Manager (in-the-cloud)	✓	✓	✓
Intuit QuickBooks Protection	✓	✓	✓
URL Filtering	✓	✓	✓
Location Awareness		✓	✓
Email Message Content Filtering			✓
IMAP Anti-spam			✓
Attachment Blocking			✓
Email Reputation (IP Addresses), Exchange 2007 Support, bundled with Trend Micro Hosted Email Security (Inbound Filtering) (aka InterScan Messaging Hosted Security)			✓

Chapter 2: Product Registration

Logon Information

Though logging onto Worry-Free Business Security Services (WFBS-SVC) is a simple process, you should keep several things in mind to get the best results:

To provide better performance, WFBS-SVC data centers are situated in four regions around the world. When registering for a trial account or purchasing the product, select the appropriate region where the WFBS-SVC clients will be installed. This will enable the WFBS-SVC agents to update signature files from nearby update servers. It will also provide better Web Console performance.

To register for a Trial version of Worry-Free Business Security Services in specific regions, click the appropriate link below:

NABU: <http://forms.trendmicro.com/services/index.php?dom=us&productID=WFSBWXE3X>

APAC:

<http://forms.trendmicro.com/services/index.php?dom=apac&productID=WFSBWXE3X>

AU: <http://forms.trendmicro.com/services/index.php?dom=au&productID=WFSBWXE3X>

DE: <https://imperia.trendmicro-europe.com/de/products/sb/worry-free-business-security-hosted/download/index.php>

UK: <https://imperia.trendmicro-europe.com/uk/products/sb/worry-free-business-security-hosted/download/index.php>

FR: <https://imperia.trendmicro-europe.com/fr/products/sb/worry-free-business-security-hosted/download/index.php>

IT: <https://imperia.trendmicro-europe.com/it/products/sb/worry-free-business-security-hosted/download/index.php>

ES: <https://imperia.trendmicro-europe.com/es/products/sb/worry-free-business-security-hosted/download/index.php>

EMEA: <https://imperia.trendmicro-europe.com/emea/products/sb/worry-free-business-security-hosted/download/index.php>

Trend Micro Trial Registration Login

Sign into your Trend Micro service account
By signing up you can purchase or trial additional TM services without needing to re-enter profile information

Logon ID:

Password:

[Forgot your password?](#)
[Need help with your account?](#)

Create new account
First time user? or Do not have a Trend Micro service account? Create a new account to activate your online service.

Figure 1 - WFBS Hosted Main Page

Upon successful registration, Trend Micro will send your WFBS-SVC account information to your email address. Take time to read the User's Guide for an overview of the functions in WFBS-SVC.

Chapter 3: Initial Configuration

Default Configuration

The **Computers** tab in the main menu allows you to deploy clients with predefined settings. By default, there are two computer groups – the Server and the Desktop groups. Since newly installed clients will use these groups' settings after installation, it is a good idea to configure the settings of these groups according to your company's security requirements. (You can also add additional groups to cluster specific settings.) Consider the following before deploying clients.

The default scanning method is set for Smart Scan. Smart Scan reduces the need for clients to download virus definitions. It also consumes less client memory than Conventional Scan, so you can use the Smart Scan Method for computers with less memory. Consider setting Conventional Scan for server/clients that won't be able to connect to the Internet for a long time.

The default Antivirus and Anti-spyware settings are recommended. If you have applications that you trust that use data files that you know won't host malicious code, it is a good idea to put them in the Exclusions configuration screen. These could be databases, multimedia files, or other files that can introduce scanning delays.

Figure 2 - Exclusions Settings

By default, mapped drives are not scanned. Do not enable mapped drive-scanning on clients with persistent static mappings to server shares as this will lead to multiple scanning jobs.

Server and Desktop groups have different Web Reputation settings. It is advisable to keep the default Web Reputation configurations for maximum security.

We encourage enabling Behavior Monitoring to prevent malicious system changes. This adds a layer of security, since Behavior Monitoring does not depend upon virus definitions, but rather blocks application behavior that violates certain rules.

Plan groups accordingly. You may want to have more granular settings by creating multiple groups, or simplify settings by using the default Server and Desktop groups. Note that the more groups you create, the more administrative overhead you will incur.

New groups appear alphabetically below the default groups, with Server groups appearing at the top of the tree. Aside from planning for the group's configuration settings, also consider their names as they appear in the tree. Groups can be renamed.

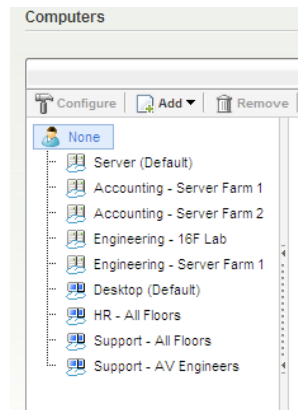


Figure 3 – New Group Names are listed alphabetically

Installer Management

The package management feature of previous releases was simplified for this release. There is now only a single installation package bound to a WFBS-SVC account. The installation process is triggered by a downloader, which downloads the package for installation. You must use this installer on systems that you want to report to your WFBS-SVC account.

Deploying via Active Directory

The WFBS-SVC has an MSI package which can be deployed using Active Directory. You can follow the following procedure if your environment has an Active Directory domain. The following procedure was tested on an SBS 2003 server.

1. Open the WFBS-SVC Console.
2. Navigate to the **Computers** tab, and then click **Add Computers**.
3. Click the expansion box for **Additional Installation Options**. The screen shows the 2 installation packages.

4. Select the package used for Conventional Installation by clicking the Download URL at the top of the panel.

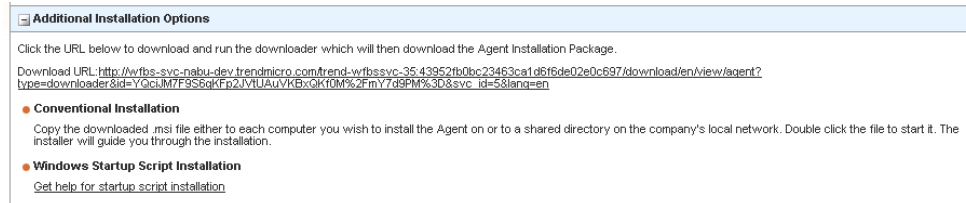


Figure 4 - MSI Download Link

5. The downloaded MSI package should be placed on a file server accessible to the computers you want to install with WFBS-SVC.
6. Create a shared folder on your SBS server or any available file server and make sure that the UNC path is accessible from the computers you are installing with WFBS-SVC.
7. At minimum, give the “Domain Computers” and the “Domain Users” security group **Read** permissions to the share.
8. WFBS-SVC is also bundled with a VBS script which can be used to deploy the application during logon. Locate the example script by clicking the **Administration** tab and selecting **Tools**.
9. In the Administrative Tools panel, download the file **WFBS-SVC Example Deployment Script.vbs**.



Figure 5 - Deployment Script Sample

10. Edit the sample script using Notepad, such that the installer path points to the UNC path of the MSI installer you created earlier. To do this, edit the line of the script that reads **pathOfWFBSInstaller="HostedAgent.MSI"** and replace the text between the double quotes with the path to your MSI file. Example [\\MySBSserver\ClientApps\WFBS-SVC_Agent_Installer.msi](#). Then save the updated file.
11. Open **Active Directory > Users and Computers** and select the **OU** for the computers you want to deploy with WFBS-SVC. If you don't have an OU for Computer accounts, create a new one and move the computer accounts from the default “Computers” folder to the newly created OU.

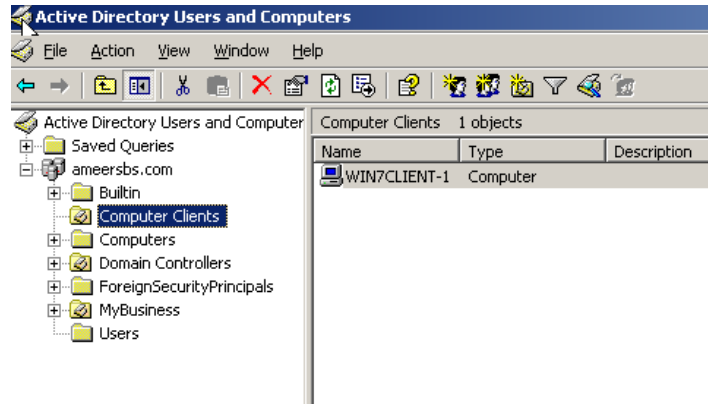


Figure 6 - Computer Account OU

12. Right click the OU for the computer accounts (in this example – the **Computer Clients** OU), then click **Properties | Group Policy | Open**. This opens the Group Policy Management console.
13. Right click the **Computer Clients** OU again, then click **Create and Link GPO here**.

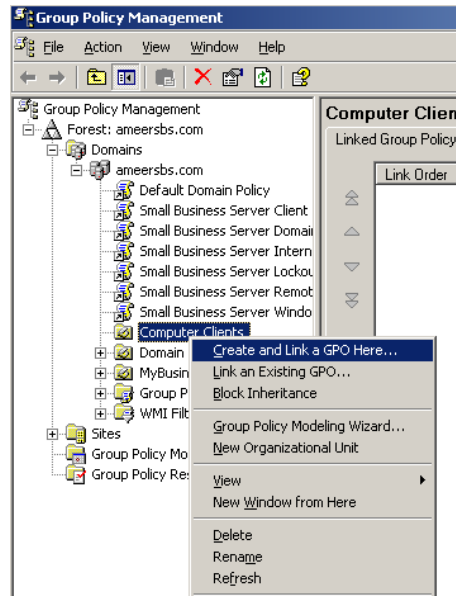


Figure 7 - Create GPO Menu Item

14. Give the GPO a name, and then click **OK**.
15. In the **Scope** tab of the GPO, make sure the “Domain Computers” Group is included in the **Security Filtering** section.
16. Select the newly created GPO and then click **Edit**. The **Group Policy Object Editor** appears.

17. Under **Computer Configuration**, click **Windows Settings | Scripts (Startup/Shutdown)**, then double click **Startup**.
18. Click **Show Files** to open the folder where the Startup Script should be copied.
19. Copy the VBS script you edited earlier into this directory.

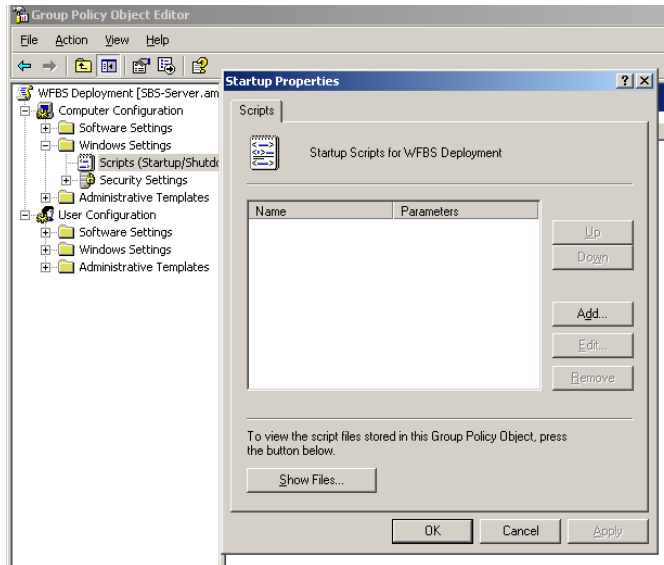


Figure 8 - Specify Script Location

20. Click **Add** then browse to the location of the script from the previous step.
21. Leave the Script Parameters blank and click **OK**. Then close the GPO Editor.

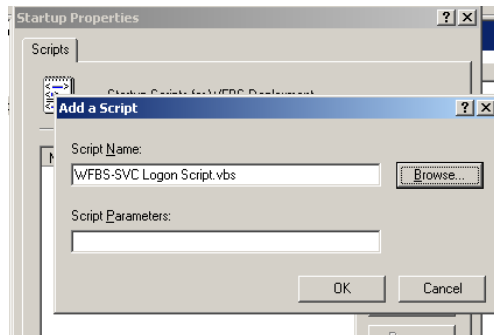


Figure 9 - Add Script Dialog Box

22. The WFBS-SVC CSA agent will be automatically installed when a user logs in the computer.

Package URL

You can use the email template below to deploy the WFBS-SVC agent via email. The body of it is generated whenever you use the **Copy Text** or **Use My Default Email** buttons in the Web Installation panel when you add computers.

Dear Sir/Madam,

Click the URL to install the Trend Micro Client/Server Security Agent. The installer will guide you through the installation.

Client/Server Security Agent

Download URL: <http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/en/view/agent?type=installer&id=riby2cWbWVxx3yRa6yMnEM0C6xKgi0lyhZ24b8Qx&lang=en>

Regards,

Administrator

Chapter 4: Installation

Worry-Free Business Security Services Agent System Requirements

The WFBS-SVC Agent supports the following operating systems:

Table 2 - System Requirements

Item	Minimum Specifications	
Operating System	Series or Family	Supported Service Packs or Releases
	Windows 2000	SP3 or SP4
	Windows Small Business Server (SBS) 2000	No service pack or SP1a
	Windows XP Home	SP2 or SP3
	Windows XP Tablet PC	SP2 or SP3
	Windows XP	SP2 or SP3
	Windows Server 2003 R2 (with Storage Server 2003)	No service pack
	Windows Server 2003 (with Storage Server 2003)	SP2 or SP2
	Windows SBS 2003 R2	No service pack
	Windows SBS 2003	No service pack
	Windows Vista	Sp1 or SP2
	Windows Home Server	No service pack
	Windows Server 2008 R2	No service pack
	Windows Server 2008	SP1 or SP2
	Windows SBS 2008	No service pack
	Windows Essential Business Server (EBS) 2008	No service pack
Windows 7	No service pack	

Uninstall Existing AV Product

Though the WFBS-SVC installation package can uninstall 3rd party antivirus products, it's best to manually uninstall existing AV products by running their uninstall programs.

After doing so, reboot the computer before installing the WFBS-SVC agent.

Ports

If you installed WFBS-SVC agents on multiple segments separated by firewalls, you need to open the following ports. The following ports are automatically exempted from the WFBS-SVC firewall policy.

Table 3 - WFBS Hosted Ports

Service	Port	Protocol
Agent Download	61116	TCP
Agent Broadcast	61117	UDP
Agent Discover	61118	UDP
Agent Broadcast	61119	UDP
Pattern Update	80	TCP

Chapter 5: Management Console

Agent Reporting Time

Agent reporting time has been greatly improved on this version. Agents appear in the management console almost instantaneously after a successful installation. Configuration changes on the management console also take only a few minutes to propagate to the client.

Day-to-Day Management

Live Status

The **Live Status** Tab provides an overview of the security posture of all the WFBS-SVC agents. The **Threat Status** panel summarizes the Outbreak Defense, Antivirus, Anti-spyware, Web Reputation, URL Filtering, Behavior Monitoring, and Network Virus status of your agents.

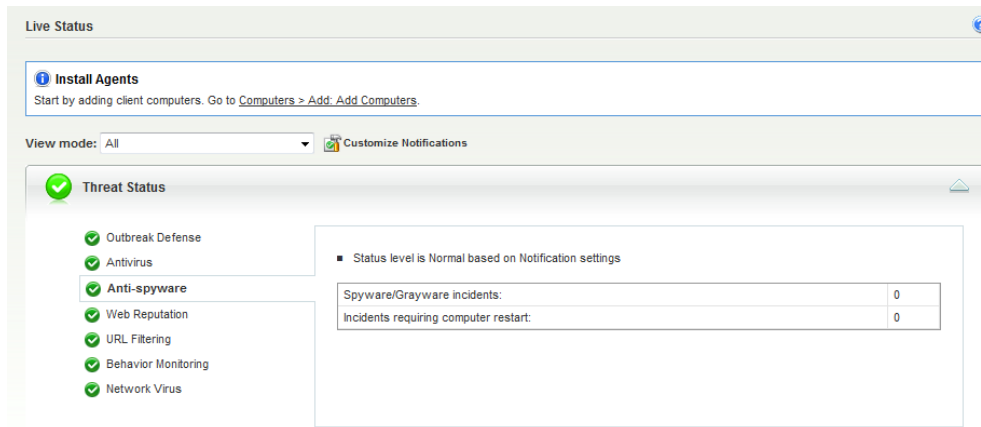


Figure 10 - Threat Status Panel

A red icon means that you need to perform an action to prevent further risk in your network. Once the appropriate action has been completed, (for example, doing a manual scan or manually deleting an infected file), click **Reset Counter** to clear the threat log and restore the icon to green status.

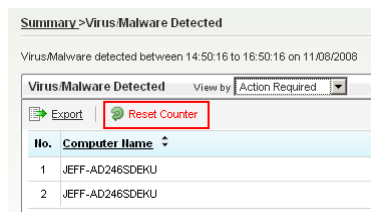


Figure 11 - Reset Counter

System Status

The **System Status** section provides a summary of the virus update deployment of your organization. By clicking the number link generated for the Outdated computers (Component Status), you can update the computers in a few clicks.

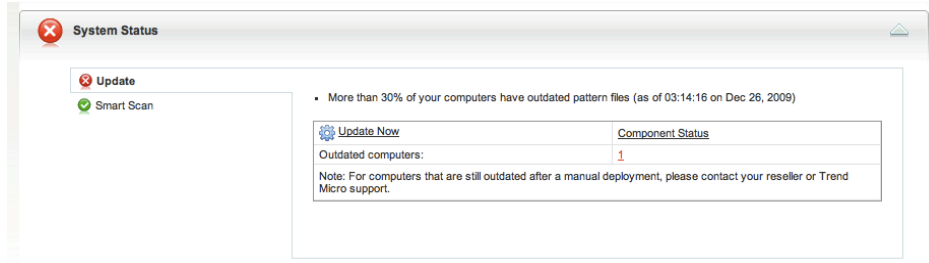


Figure 12 - System Status Section

License Status

If the **License Status** section turns yellow, it means that you need to consider adding licenses for your clients.

WFBS-SVC back end servers provides a 20% seat allowance. This means that if you have 10 licenses, you can still add 2 agents above your license limit. Adding more agents would fail. We recommend adding licenses when you have 80% license usage if you are still in the process of deploying the products.

If you go over the license limit the following will be imposed to your WFBS-SVC account:

1. If a new user clicks the agent installation link, the agent will still be installed.
2. However, these newly installed agents won't be allowed to report to the management console. Since the agents will not report to the console, you cannot configure any client-side settings.
3. The agents will not receive any updates.

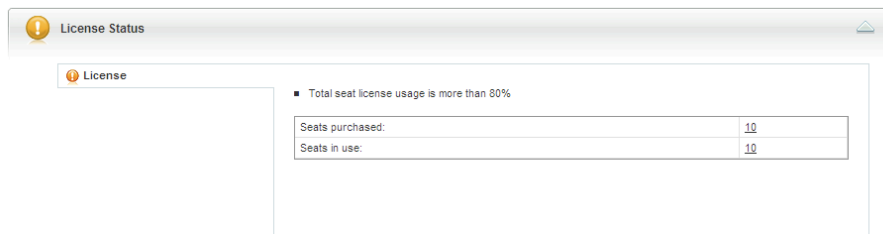


Figure 13 - License Section

Agents Installed

You can view all the agents you have installed in the **Computers** section (previous versions show it in the **License** screen). This is also where you set configuration settings for each of your security groups.

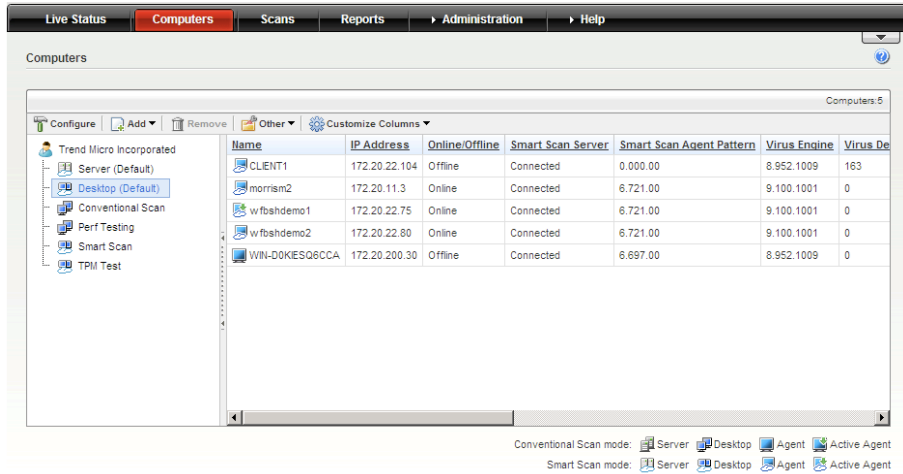


Figure 14 - Computers Tab

Customize Columns

By default, the Web management console displays all the column fields for a group in the Group Information Table. Using the **Customize Columns** dropdown menu (shown below in the Command menu), you can limit the columns to display the most useful information using the checkboxes.

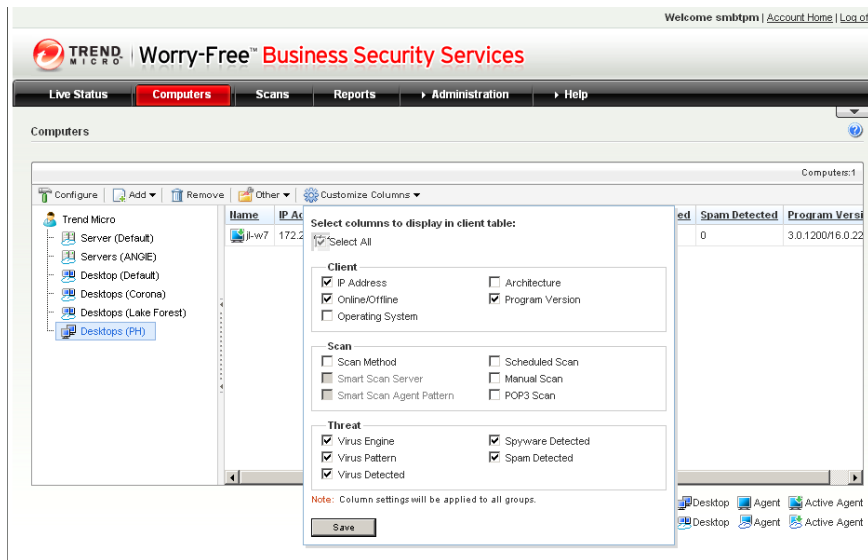


Figure 15 - Customize Columns

We recommend displaying the following:

- IP Address
- Online/Offline State
- Program/Virus Pattern/Virus Engine Version
- Virus/Spyware/Spam Detected

Scans Tab

The **Scans** tab allows you to configure Manual and Scheduled Scans. Note that you can also do an on-demand scan from the **Computers** tab.



Figure 16 - Scans Tab

Reports Tab

The **Reports** tab allows you to configure one-time and scheduled reports. You can specify an email address where the report will be sent after it has been generated. Reports are also stored on the in-the-cloud WFBS-SVC Server.

Reports > New Report

Report Name

Report name:* December Report

Report Schedule

One-time
 Weekly
 Monthly

From: 2009-12-19
yyyy-mm-dd

To: 2009-12-26
yyyy-mm-dd

Send Report

Send the report to: jeff@licsi.com

For example, user1@example.com; user2@example.com (Separate multiple entries with a semicolon)

Note: Reports are sent out as PDF attachments to the specified recipients.

Generate Cancel

Figure 17. New Report

The generated report contains the following information:

1. Desktop/Server Virus Summary
2. Desktop/Server Spyware/Grayware Summary
3. Top 5 Desktops with Virus Detections
4. Top 5 Servers with Virus Detections
5. Top 10 Network Viruses Detected
6. Top 10 Computers Attacked by Network Viruses
7. Top 5 Desktops with Spyware/Grayware Detections
8. Top 5 Servers with Spyware/Grayware Detections
9. Top 10 Computers Violating Web Threat Protection Policies
10. Top 5 Programs Violating Behavior Monitoring Policies
11. Top 10 Computers Violating Behavior Monitoring Policies

The reports are generated in PDF format. Disable any popup blockers, since the PDF report is opened in a new window.

Generate a report at least once a month to keep a history of the security status of your protected network.

Log Query

Each WFBS-SVC agent (CSA) sends logs at predefined intervals. You can query management and desktop/server logs from the **Reports** menu. The logs can be exported to CSV format.

Date/Time	Computer Name	Virus/Malware Name	File Name	Path	Scan Type	Action Taken
12/07/2007 14:50:32	[Client removed]	PHP_TEST_VIRUS	Test_php.php	E:\test_virus\Virus...	Real-time Scan	Virus successfully detected, but cannot be cleaned. File was quarantined
11/07/2007 14:50:32	[Client removed]	PHP_TEST_VIRUS	Test_php.php	E:\test_virus\Virus...	Real-time Scan	Virus successfully detected, but cannot be cleaned. File was quarantined
10/07/2007 14:50:32	[Client removed]	PE_TestVir-NME	PE_TestVir-NME.exe	E:\test_virus\Virus...	Real-time Scan	Virus successfully detected, but cannot be cleaned. File was quarantined
09/07/2007 14:50:32	[Client removed]	PHP_TEST_VIRUS	Test_php.php	E:\test_virus\Virus...	Real-time Scan	Infected file was successfully quarantined
08/07/2007 14:50:32	[Client removed]	PE_TestVir-NME	PE_TestVir-NME.exe	E:\test_virus\Virus...	Real-time Scan	Virus successfully detected, but cannot be cleaned. File was quarantined

Figure 18 - Virus/Malware Logs

Logs are kept for 15 days in the WFBS-SVC agent computers. Adjust this according to your log retention requirement.

Notifications

WFBS-SVC now includes a robust notification system. This system can send event notifications at certain thresholds. Notification settings are globally applied so you may need to fine-tune the settings at certain times. WFBS-SVC can notify individuals from 17 types of events.

IM Content Filtering

WFBS-SVC can filter words and phrases from the following popular IM applications.

1. America Online® Instant Messenger (AIM) 6 (builds released after March 2008 are not supported)
2. ICQ® 6 (builds released after March 2008 are not supported)
3. MSN™ Messenger 7.5, 8.1
4. Windows Messenger Live™ 8.1, 8.5
5. Yahoo!™ Messenger 8.1

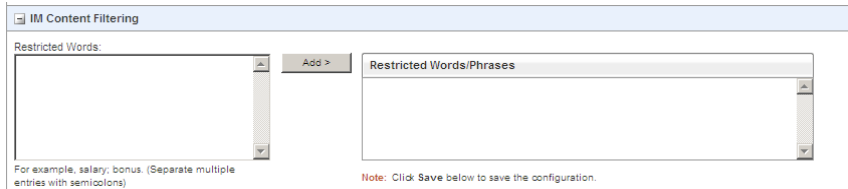


Figure 19 - IM Content Filtering under General Tab


Chapter 6: The Client Console

Accessing the WFBS-SVC – Client/Server Security Agent Console

The Worry-Free Business Security Hosted (WFBS-SVC) – Client/Server Security Agent (CSA) Console can be accessed by double-clicking the system tray icon on the client. This opens the Agent console, allowing you to see the number of files scanned and the last detected files. You can also access the CSA console in the Trend Micro Client Security Agent Program group created during the installation.

Component Update

If you encounter problems with the product, especially virus detection issues, it's a good practice to check the version of all installed components and compare it with the latest components listed at <http://www.trendmicro.com/download/pattern.asp>. The WFBS-SVC Active Agent automatically downloads the latest components available. However, beta signature files (virus definitions not yet available to Trend Micro's update server) can be installed manually.



Component	Version	File Name
Main Program	3.5.1050	PccNMon.exe
Virus Scan Engine (32-bit)	9.150.1013	VSApNt.sys
Smart Scan Agent Pattern	7.423.00	icrc\$oth.423
IntelliTrap Exception Pattern	0.575.00	TmwWhite.575
Behavior Monitoring Driver (32-bit)	2.80.1063	tmactmon.sys
Behavior Monitoring Core Service (32-bit)	2.80.1080	tmbsrv.exe
Policy Enforcement Pattern	1.192.00	tmpolicy.ptn
Digital Signature Pattern	1.261.00	tmwlchk.ptn
Behavior Monitoring Configuration Pattern	1.176.00	tmbscfg.ptn
Behavior Monitoring Detection Pattern	1.209.00	tmtd.ptn
IntelliTrap Pattern	0.141.00	Tmblack.141
Spyware Scan Engine (32-bit)	6.2.3012	Ssapi32.dll
Spyware Pattern	9.71	ssapiptn.da6
URL Filtering Engine	3.0.1029	Tmufeng.dll
Smart Feedback Engine	2.5.1028	Tmfeng.dll
Anti-rootkit Driver (32-bit)	2.80.1063	Tmcomm.sys
Virus Cleanup Engine (32-bit)	6.3.1015	TSC.EXE
Virus Cleanup Template	1092	Tsc.ptn
Vulnerability Assessment pattern	115	TMVAmain.ptn

Figure 20 – Version Information

Personal Firewall

WFBS-SVC comes with a personal firewall and a default set of policies. To tune the policies according to your requirements, you can configure the rules by opening the CSA console, selecting the **Security Protection** tab and selecting the **Firewall** drop-down menu. The status of the personal firewall can also be changed by right-clicking the system tray icon. We recommend enabling the firewall component when you are using a public Internet connection.

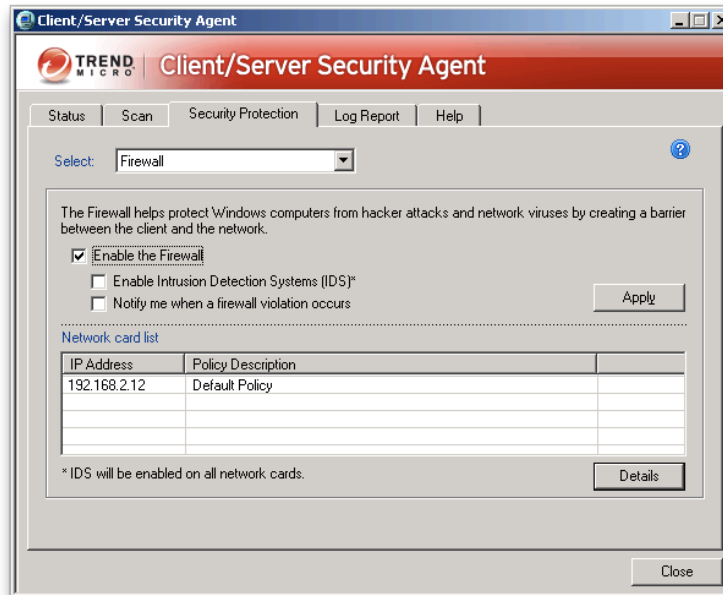


Figure 21 – CSA Firewall Configuration

Chapter 7 – Worry-Free Remote Manager Integration

Worry-Free Remote Manager (WFRM) installation integration allows resellers to easily get up and running with WFRM, to monitor multiple WFBS-S/A, Hosted Email Security (aka InterScan Messaging Hosted Security), and WFBS-SVC customers and companies from one easy-to-use Web-based console. WFBS-SVC 3.5 is supported for Worry-Free Remote Manager 2.5 and above

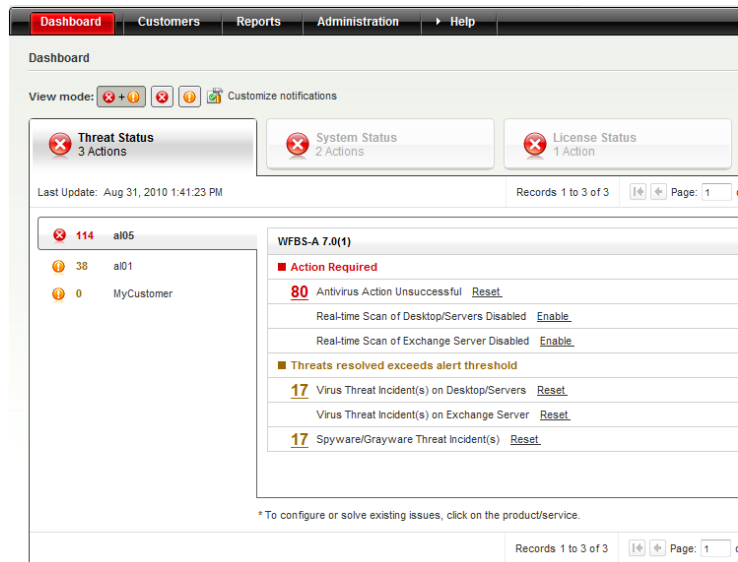


Figure 22 - Worry-Free Remote Manager Dashboard

Creating a Customer and WFBS-SVC Service in WFRM

If you are a reseller and want to have access to your customer WFBS-SVC installation, you need to create customer and service entries in your WFRM account for the customer. The process is illustrated in the following WFRM screenshots.

1. In the WFRM Console, select the **Customers** tab to open the **Customers** Network Tree.

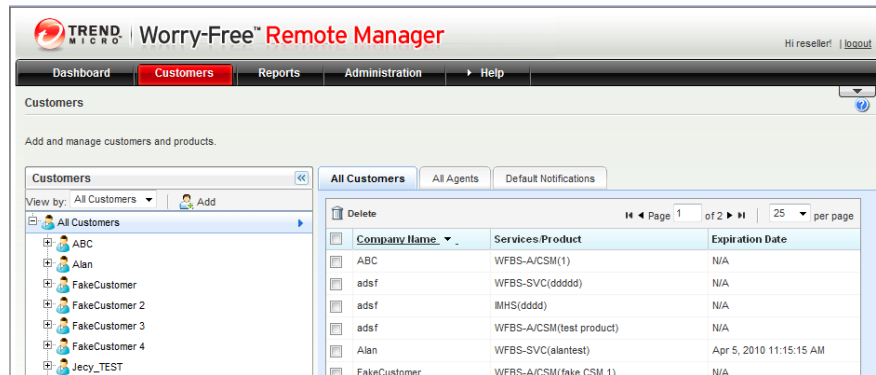


Figure 23. Customers

- In the **Customers** Network Tree menu, click the **Add** button to create a customer. The wizard walks you through the customer creation process.

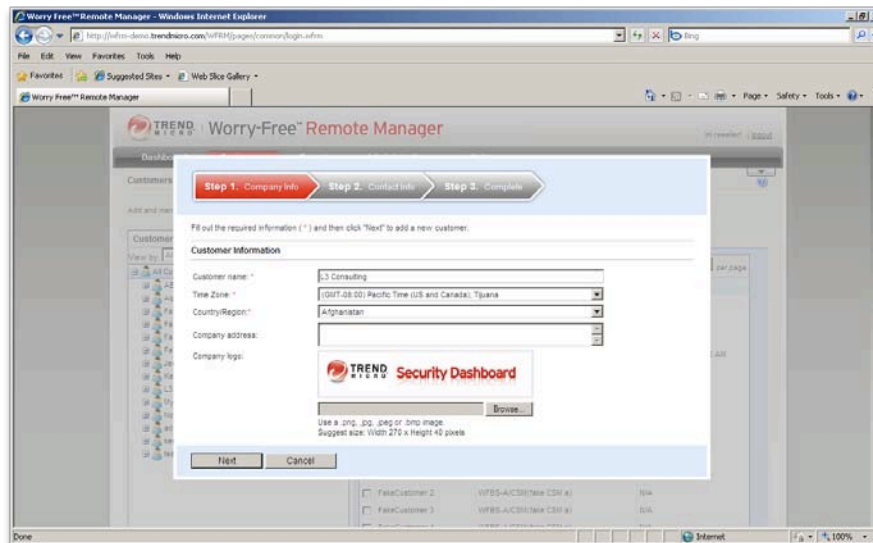


Figure 24 - Create a customer

- Select the customer name in the Network tree and in the **Purchased Product/Service** panel on the right, click **Add** to add a service entry for WFBS-SVC for that customer. Remember that WFBS-SVC 3.5 is only supported on WFRM v2.5 and above.

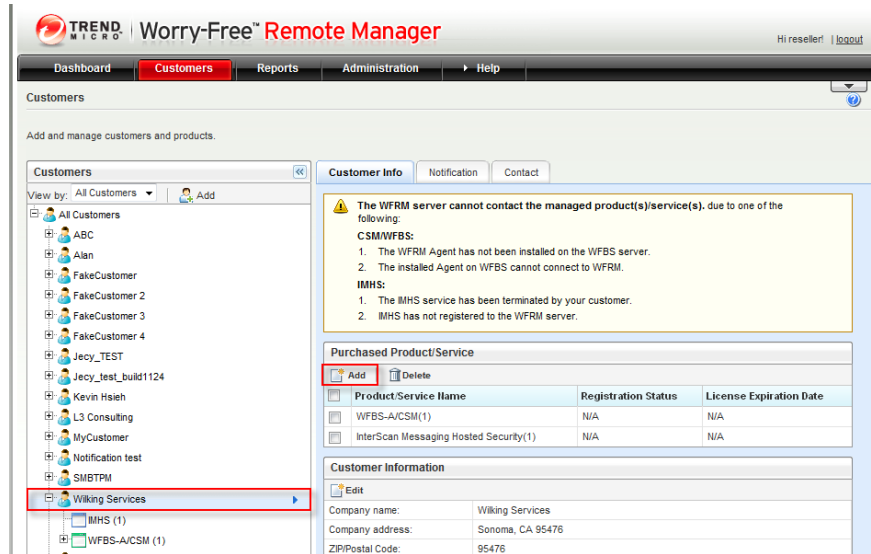


Figure 25. Add Purchased Product/Service

- The **Product/Service** wizard appears and walks you through the process to add the Service.

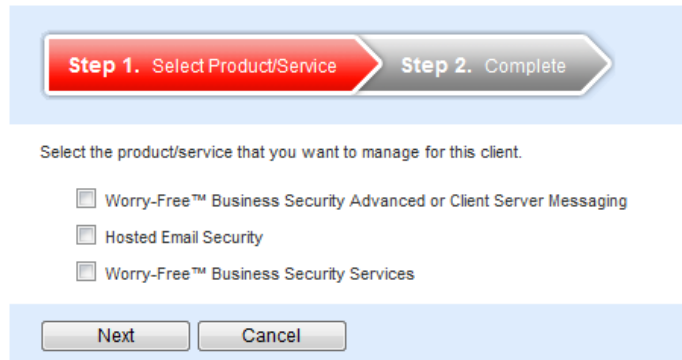


Figure 26 - Add a Service entry for WFBS-SVC

- Once WFBS-SVC has been added for the customer, you will then be provided with an Authorization Key.

Step 1. Select Product/Service Step 2. Complete

For SaaS services:	
Service Name	Authorization Key
Worry-Free Business Security Services	076B8061ED24-09B1370B-DEB1-CD29-60DC

Add the authorization key to the service console and start the connection between WFRM and the new services.

Save as txt file Send a copy to my email

Add additional product/service now OK

Figure 27 - WFRM AK generated for WFBS-SVC

6. Provide this Authorization Key to your customer, who will in turn enter the key into the WFBS-SVC Console.
7. The customer inputs the Authorization Key in the delegation field on the **Administration >Worry-Free Remote Manager** page.

Administration > Remote Manager

Remote Manager allows reseller to manage your security console anytime, anywhere. To start the service, please enter the Authorization Key you received from the reseller.

Remote Manager Delegation

You have not delegated management abilities to the reseller.

Please enter Authorization Key to delegate the service :

Enter Authorization Key

Connect

Figure 28 - Using the WFRM AK for Remote Manager Delegation

8. After a successful delegation, the reseller will be able to access the customer's WFBS-SVC account. The following WFBS-SVC features will be available from the WFRM Console:
 - SSO
 - Sync
 - Live Status
 - Threat Management

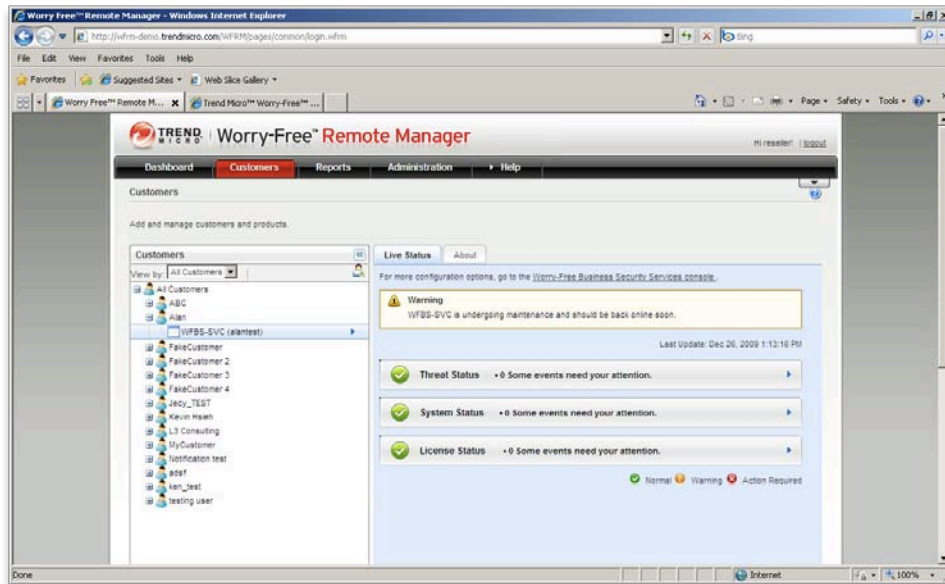


Figure 29 - Worry-Free Remote Manager > WFBS-SVC Features

Chapter 8: Password Management

Recovering a Lost WFBS-SVC Console Password

1. If you forget your WFBS-SVC Console password, visit the following link:

https://olr.trendmicro.com/registration/us/en-us/forget_pwd.aspx

Forgot Your Password?

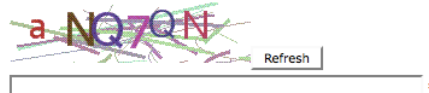
Please enter your logon name or e-mail address. You will receive a confirmation e-mail upon submitting the reset request. If you have any questions, please contact [Trend Micro](#).

Enter the logon ID or e-mail address that you have registered.

Logon ID or e-mail Address:

Verification Code:

(Type the code shown below. If you want to try another code, click 'REFRESH'.)



Enter the characters from the above image. The characters are case sensitive.

Submit

Figure 30. New Password Request

2. Input the appropriate information and click **Submit**. Instructions will be sent to the email account on how to reset the password.

Setting an Uninstall and Unload Agent Password

Starting WFBS-SVC 3.5, administrators can set an Uninstall and Unload password. These two passwords can be different and are set individually under the **Administration > Global Settings** tab. By default, no password is required to uninstall or unload the agent.

Agent Uninstallation

Allow the client user to uninstall the Security Agent without a password

Require the client user to enter a password to uninstall the Security Agent

Password: (4 to 20 characters (alphanumeric))

Confirm password:

Agent Shut Down (Unload)

Allow the client user to exit the Security Agent without a password

Require the client user to enter a password to exit the Security Agent

Password: (4 to 20 characters (alphanumeric))

Confirm password:

Save

Figure 31. Agent Uninstallation and Unload Passwords

On some occasions, you may need to uninstall a client security agent that was installed with a different account. In this case, if you don't know the password and you need to uninstall the agent perform the procedure at the following link:

<http://esupport.trendmicro.com/5/Bypassing-the-uninstallation-password-of-a-ClientServer-Security-Agent.aspx>

Chapter 9: Performance Tuning

Active and Normal Agents

After installation, an agent can be elected to be the Active Agent. The Active Agent serves as the contact window between the WFBS-SVC server and all WFBS-SVC Agents in a company. It is responsible for distributing updates and pattern files to other WFBS-SVC agents

The Active Agent periodically checks the WFBS-SVC server for component and pattern file updates. If there are updates, the Active Agent downloads the update and notifies Inactive Agents about the update. Some agents then download the update from the Active Agent. After these inactive agents are updated, they then proceed to update other agents that need to be updated. This prevents excessive utilization of the Active Agent's system resources.

The Active Agent election algorithm ensures there is always one Active Agent. If the computer hosting the current Active Agent becomes unavailable, all other WFBS-SVC agents immediately elect a new Active Agent.

Each agent connects to a channel. A channel is created for each of the following computer groups:

- OS architecture: an x64 and an x86 machine will be in a different channel.
- Hotfix ability: In the CSA group configuration, specifically on **Client Privileges | Update Settings**, clients with the ability to deploy agent and hotfix upgrades will belong to one channel, while clients with this setting disabled will belong to another channel.

For each of these channels, there are 4 conditions checked in deciding which computer becomes an Active Agent. These are:

1. Online/Offline status: Online has higher priority.
2. Program Version: Higher version has higher priority.
3. Priority: There are 3 priorities - high, medium, and low.
4. IP address: The higher IP, the higher the priority.

Each agent broadcasts its own information and each agent sequentially compares these 4 conditions.

Manually Setting the Active Agent

On some occasions, you may want to manually set the Active Agent role to a particular machine. This could be a machine that is always on or a machine with higher hardware specifications.

To manually set a computer as the Active Agent:

The computer needs to belong to a group with hotfix deployment enabled. Ensure that the “Disable agent upgrade and hotfix deployment” is unchecked.

1. Open Registry Editor on the computer you want to be the Active Agent.

2. Set the following registry entry to 0.
`\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\HostedAgent\Priority`
 (0=High, 1=Medium, 2=Low)
3. Restart the “Trend Micro Client/Server Security Agent” service.

You can verify which machine is the Active Agent by running the support tool – WhoIsAA.exe. The tool can be requested from SMB Technical Support or from SMB Technical Product Marketing.

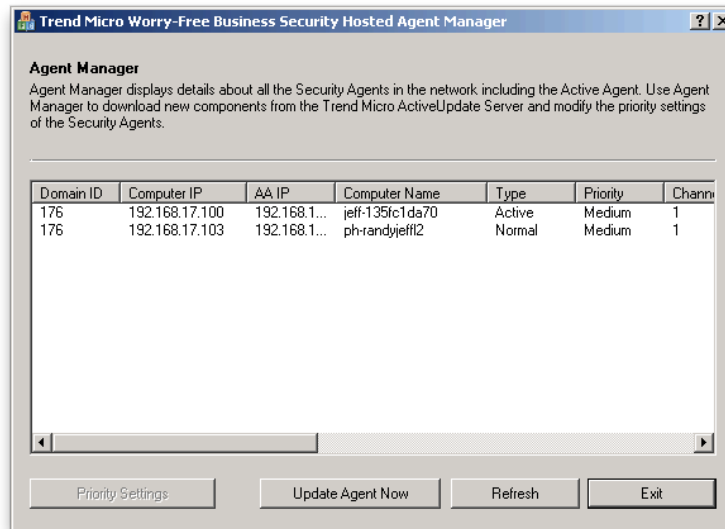


Figure 32 - WholsAA utility

We recommend setting the Active Agent to a computer/server that has a gigabit LAN connection. This will considerably increase the amount of clients that can concurrently pull updates.

Account Recommendations/Limit

We recommend the following account limits:

- Limit the number of computers to 2500 per WFBS-SVC account.
- Limit the number of computers per group to 250 as a best practice. If it is unavoidable, do not go beyond 500 computers per group as it can introduce delay in viewing the client tree.
- Limit the number of groups to what’s really needed by the organization. The more groups you create, the more management overhead will come with it.
- Use IE7/IE8 or Firefox in opening the management console, especially if viewing client trees with a large number of users. IE6 will introduce delays in showing the client tree.

Update Bandwidth

Active Agents conserve Internet bandwidth by propagating program and definition updates to other WFBS-SVC agents instead of each agent downloading via the Internet. In the table below, a worst case scenario is simulated by deploying a 75MB pattern file to all the agents. The pattern deployment time is estimated below on this scenario.

Table 4 - Full Pattern Deployment Time – Active Agent to WFBS-SVC Agents

75MB Full Pattern Download In Minutes (Active Agent to CSA Agents)	100 Agents	200 Agents	400 Agents	600 Agents	1000 Agents
100Mbps @ 80% Utilization	13.1 min.	26.2 min.	52.4 min.	78.6 min.	131.1 min.
1Gbps @ 80% Utilization	1.3 min.	2.6 min.	5.2 min.	7.9 min.	13.1 min.

After installation, all agents will download incremental updates and not full updates. Below is the estimated time for different number of agents. Note that this example is for a 1MB incremental pattern. Typically after installation, only incremental updates needs to be downloaded, so this is the usual update time after installation.

Table 5 - Incremental Pattern Deployment Time – Active Agent to WFBS-SVC Agents

1MB Incremental Pattern Download In Minutes (Active Agent to CSA Agents)	100 Agents	200 Agents	400 Agents	600 Agents	1000 Agents
100Mbps @ 80% Utilization	0.17 min.	0.35 min.	0.70 min.	1.05 min.	1.75 min.
1Gbps @ 80% Utilization	0.02 min.	0.03 min.	0.07 min.	0.10 min.	0.17 min.

With the current limit of 10 WFBS-SVC agents per Active Agent, a 1000 Agent network can have up to 100 Active Agents. To estimate the amount of bandwidth an update can incur, below is a table summarizing the update time for various Internet connection bandwidth. As stated previously, the 75MB download size is a worst case scenario while the usual update size is 500Kb-1MB for incremental updates.

Table 6 - Full/Incremental Update Time for an Active Agent

Number of Agents	Number of Active Agents	Internet Bandwidth (80% Utilization)	Time for AAs to download pattern in minutes	
			Full Pattern (75MB)	Incremental (1MB)
10	1	768Kbps	17.07	0.23
10	1	1.5Mbps	8.74	0.12
250	25	3.0Mbps	109.23	1.46
250	25	6.0Mbps	54.61	0.73
500	50	8.0Mbps	81.92	1.09
1000	100	8.0Mbps	163.84	2.18

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. You can reach Trend Micro at www.trendmicro.com.

Copyright © 2010 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, and Worry-Free are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.