TREND MICRO™

# Worry-Free™ Remote Manager

for Small and Medium Business

## Getting Started Guide for Resellers

Publication Date: March 2011

Document Version No.: 1.0

Service Name and Version No.: Trend Micro™ Worry-Free™ Remote Manager 2.6

The user documentation for Trend Micro™ Worry-Free™ Remote Manager is intended to introduce the main features of the service. You should read it prior to using the service.

Detailed information about how to use specific features within the service are available in the online help and the Knowledge Base at the Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

# Contents

## Chapter 1: Introducing Worry-Free Remote Manager



## Chapter 2: Getting Started



## Chapter 3: Preparing the Service Infrastructure

## Chapter 4: Understanding the Dashboard



## Chapter 5: Monitoring Threat Status

## Chapter 6: Monitoring System Status



## Chapter 7: Managing Networks

## Chapter 8: Managing Worry-Free Remote Manager Agents



## Chapter 9: Managing Reports



## Appendix A: Troubleshooting and FAQ

## Appendix B: Getting Help



## Index

# Chapter 1

# Introducing Worry-Free Remote Manager

Trend Micro™ Worry-Free™ Remote Manager (WFRM) is a robust console for providing managed security services to small and medium businesses.

This chapter discusses the following topics:

# What is Worry-Free Remote Manager

Trend Micro™ Worry-Free™ Remote Manager (WFRM) enables you to monitor the health of multiple managed networks via multiple, managed products and services. Worry-Free Remote Manager allows reseller administrators to issue commands to manage critical aspects of network security.

WFRM is hosted on regional Trend Micro Data Center servers where resellers obtain an account. Resellers can use Worry-Free Remote Manager to establish customer accounts, monitor customer networks, and manage security using the WFRM console.

Worry-Free Remote Manager (WFRM) presently monitors the following products:

- Worry-Free Business Security Standard (WFBS-S) (formerly CS) versions 5.x, 6.x, 7.x
- Worry-Free Business Security Advanced (WFBS-A) (formerly CSM) versions 5.x, 6.x, 7.x
- Worry-Free Business Security Services (WFBS-SVC) version 3.x

**Note:** WFBS-S/WFBS-A and WFBS-SVC are collectively referred to as WFBS(ALL)[1] where appropriate.

- Trend Micro™ Hosted Email Security version 1.x[2]

**Note:** WFBS-S/WFBS-A, WFBS-SVC, and Hosted Email Security are collectively referred to as "managed products" and/or "managed services" in this document.

Worry-Free Remote Manager has a monitoring dashboard that allows resellers to look into the following aspects of network security:

- WFBS(ALL):
  - Virus, network virus, and spyware/grayware incidents
  - Spam and phishing incidents
  - Unauthorized computer changes
  - Outbreak situations
  - License and update status of security products
  - Disk usage on desktops, servers, and Exchange servers (WFBS-S/WFBS-A only)
  - Key security indicators
- Hosted Email Security:
  - Total Email Message Traffic
  - Accepted Email Message Size
  - Threat Summary
  - Top Spam Recipients
  - Top Virus Recipients

**Note:** For detailed information on Hosted Email Security and WFBS(ALL), see the documentation for those products.

Worry-Free Remote Manager offers a structured view of customer networks and allows resellers to issue commands and manage the following aspects of network security:

- Component updates and updates to the managed server

1. WFBS(A), WFBS(S), and WFBS-SVC are collectively referred to as WFBS(ALL) where appropriate.
2. InterScan Messaging Hosted Security was renamed to Hosted Email Security in WFRM 2.2 SP1.

- Vulnerability assessment
- Damage cleanup
- Automatic outbreak response
- Firewall and real-time scan settings
- Manual scans

Worry-Free Remote Manager also supports comprehensive reporting features and allows resellers to subscribe individuals to automatically generated reports.

# Worry-Free Remote Manager Features

Worry-Free Remote Manager allows resellers to monitor and manage multiple protected networks from a single console by communicating with an Agent that runs on the managed servers. In addition, it offers event monitoring based on key security indicators.

Worry-Free Remote Manager offers the following features:

- Live Threat Status (see page 1-3)
- Live System Status (see page 1-4)
- License Status (see page 1-4)
- Network Management (see page 1-4)
- Reporting (see page 1-4)

## Live Threat Status

The Worry-Free Remote Manager dashboard provides the status of the following aspects of network security:

WFBS(ALL)

- Outbreak Defense
- Antivirus
- Anti-spyware
- Web Reputation
- Behavior Monitoring
- Network Viruses
- Anti-spam
- URL Filtering (WFBS-S/WFBS-A 6.x and up only)
- Device Control (WFBS-S/WFBS-A 7.x only)

Hosted Email Security

- Total Email Message Traffic
- Accepted Email Message Size
- Threat Summary
- Top Spam Recipients
- Top Virus Recipients

Worry-Free Remote Manager provides details about these aspects including statistical data such as the number of infected computers and virus/malware incidents. Reseller administrators can also check detailed information including the names of affected computers or the threats.

### Live System Status

Reseller administrators can check the following system-related aspects of network security through the Worry-Free Remote Manager dashboard:

- Outdated Client Desktops
- Outdated Exchange Servers
- Outdated Managed Servers
- Unusual System Events (presently, only low disk usage is under this category)

### License Status

Reseller administrators can view the following license-related details:

- Total seats purchased
- Number of seats in use
- Expired licenses, including date of expiry
- Expiring licenses, including number of days before expiration

### Network Management

Worry-Free Remote Manager offers a structured view of managed networks and allows reseller administrators to issue commands and manage the following critical aspects of network security:

- Component updates and updates to the managed server
- Vulnerability assessment
- Automatic outbreak response
- Damage cleanup
- Firewall and real-time scan settings
- Manual scans

### Reporting

In addition to notifications for security events, Worry-Free Remote Manager can automatically generate and send reports at regular intervals. Reports can be defined by the reseller according to customer, product, frequency and content and saved in various formats. Presently, 512MB of storage is available for saved reports.

## What's New in this Release

**Worry-Free Remote Manager version 2.6 includes the following new features:**

- Support for Worry-Free Business Security Services version 3.5 Service Pack 1
- Enhanced scalability to manage several thousand customers
- Improved user interface that includes pagination, search, and additional right-click options
- Features that enable partners to manage their own profiles

**Worry-Free Remote Manager version 2.5 includes the following new features:**

- Support for Worry-Free Business Security (WFBS-S/WFBS-A) 7.0
- New Dashboard for quickly finding and fixing problems
- More intuitive wizard for adding customers
- New license report that tracks license status across customers
- Support for the Autotask ticketing system (see www.autotask.com)

**Worry-Free Remote Manager version 2.2 includes the following new features:**

- Support for Worry-Free Business Security Services (WFBS Hosted) starting with version 3.0
- Support for the Kaseya ticket system (added in version 2.1 SP1; see www.kaseya.com)
- Enhanced dashboard and notification settings
- Interscan Messaging Hosted Security (IMHS) is renamed to Hosted Email Security (added in version 2.2 SP1)

**Worry-Free Remote Manager version 2.1 includes the following new features:**

- Support for WFBS-S/WFBS-A version 6.0
- Enhanced installation of the WFRM Agent from a WFBS-S/WFBS-A server
- Real time WFBS-S/WFBS-A Security Settings status on the WFRM console
- WFRM console displays URL Filtering status from WFBS-S/WFBS-A 6.0

# Overall Infrastructure

Worry-Free Remote Manager consists of three basic parts:

- The Reseller
- The Trend Micro Data Center
- The Customer Network

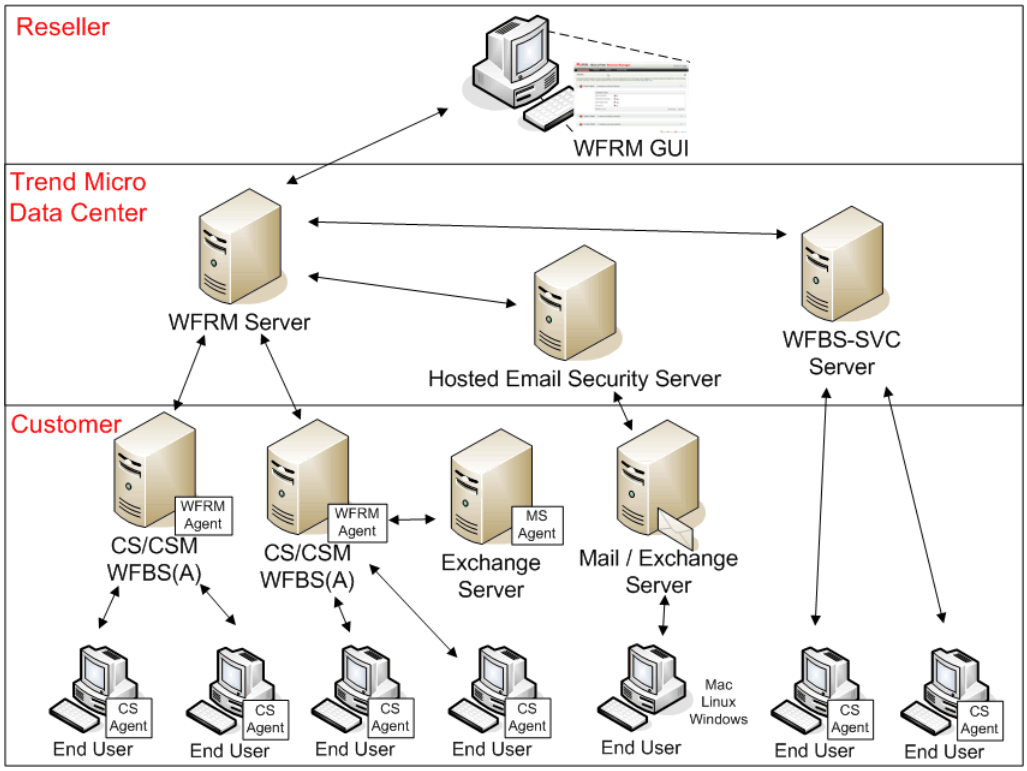



**FIGURE 1-1. Worry-Free Remote Manager Overall Architecture**

The reseller accesses a Trend Micro Data Center (currently on four continents) through the Worry-Free Remote Manager console via the Internet. No installation of the console is required by the reseller. From the console, the reseller can administer customer security.

Each customer needs to be added and configured on the console by the reseller. Each WFBS-S/WFBS-A managed server has a WFRM Agent installed which allows communication to and from the Worry-Free Remote Manager servers. Since Hosted Email Security and WFBS-SVC are hosted at the Trend Micro Data Center, no Agents need to be installed. Instead, Hosted Email Security and WFBS-SVC need to be registered on the WFRM console for each customer.

The WFRM Agent, which can be installed from the WFRM console, runs on the WFBS-S/WFBS-A managed server inside the customer's network. The Agent sends information to the WFRM server where you can access the data from your console 24/7 using an Internet connection.

## About WFBS-S, WFBS-A and WFBS-SVC

Worry-Free Business Security Standard (WFBS-S), Worry-Free Business Security Advanced (WFBS-A), and Worry-Free Business Security Services (WFBS-SVC) are comprehensive, centrally-managed solutions for small- and medium-sized business.

WFBS-S provides client-side antivirus and firewall protection for desktops and servers. Worry-Free Business Security Advanced (WFBS-A) includes the same features as WFBS-S but provides an anti-spam and email threat solution for mail servers running Microsoft Exchange Server. WFBS-S and WFBS-A include a server-side component for monitoring and managing client protection from a central location.

Worry-Free Business Security Services provides most of the advantages of WFBS-S. And because WFBS-SVC is a hosted service, you can centrally manage security from anywhere without the need to add, install, configure, or maintain a server. Trend Micro security experts host and constantly update the service for you.

---

**Note:** For information about WFBS(ALL) and WFBS-SVC, see the documentation at http://www.trendmicro.com/download.

---

WFRM monitors and manages WFBS-S/WFBS-A-protected networks by communicating with an Agent that runs on WFBS-S/WFBS-A servers.

Worry Free Remote Manager monitors and manages WFBS-SVC-protected networks by communicating with the WFBS-SVC server located at Trend Micro data centers.

## About Hosted Email Security

Trend Micro™ Hosted Email Security blocks spam, viruses, phishing, and other email threats before they reach your network. As a hosted solution, it requires no hardware or software to install and maintain and helps you reclaim IT staff time, end-user productivity, bandwidth, mail server storage and CPU capacity.

In addition, Trend Micro's worldwide team of experts manages all hot fixes, patches, updates and application tuning so that solution performance is continuously optimized.

---

**Note:** For information about Hosted Email Security, see the Hosted Email Security documentation at http://www.trendmicro.com/download

---

Worry Free Remote Manager monitors and manages Hosted Email Security-protected networks by communicating with the Hosted Email Security server located at Trend Micro data centers.

# About Kaseya

Beginning with version 2.1 SP1, WFRM can send event notifications to the Kaseya system. The following WFBS events can be sent to Kaseya:

- Agent Abnormal
- Outbreak Defense
- Antivirus
- Anti-spyware
- Web Reputation
- Behavior Monitoring
- Network Virus
- Anti-spam
- Outdated Managed Servers
- Unusual System Events
- License Expiration
- URL Filtering
- Device Control
- CS(M)/WFBS-S/WFBS-A Server Shutdown
- Exchange Server Shutdown

These events are sent to Kaseya in the form of email messages which are transformed into a Kaseya ticket. For this to occur, notification recipients need to be added to the WFRM console and several fields need to be made to Kaseya's ticketing system. See *Integrating Kaseya with WFRM* on page 3-16.

# About Autotask

With WFRM 2.5, WFRM can send the following WFBS event notifications to the Autotask system:

- Agent Abnormal
- Outbreak Defense
- Antivirus
- Anti-spyware
- Web Reputation
- Behavior Monitoring
- Network Virus
- Anti-spam
- Outdated Managed Servers
- Unusual System Events
- License Expiration
- URL Filtering
- Device Control
- WFBS-S/WFBS-A Server Shutdown
- Exchange Server Shutdown

These events are sent to Autotask in the form of email messages that are transformed into an Autotask ticket. For this to occur, you must add notification recipients to the WFRM console and several fields to Autotask's ticketing system. See *Integrating Autotask with WFRM* on page 3-21 for more details.

# Key Terminology

Knowing the following terms can help you work with this product more efficiently:

- **Agent** (WFBS-S/WFBS-A)**:** Installed on WFBS-S/WFBS-A servers, this program allows WFRM to monitor and manage WFBS-S/WFBS-A.
- **Assessment:** Regular checks done on data collected from customer networks to determine the health of monitored networks; these checks use key indicators called assessment indexes.
- **Assessment indexes:** The basis for security assessments; reseller administrators can customize these indexes individually to control assessment intervals, ranges, and notifications.
- **Client Security Agent (CSA):** The Agent that reports to the WFBS(ALL) server. The CSA sends event status information in real time. Agents report events such as threat detection, Agent startup, Agent shutdown, start of a scan, and completion of an update. The CSA provides three methods of scanning: real-time scan, scheduled scan, manual scan. Configure scan settings on Agents from the Web console.
- **Dashboard:** The dashboard in Worry-Free Remote Manager is the main page (first tab) that displays a summary of each network aspect that the console monitors.
- **Detection:** The discovery of a threat; a detection does not constitute a system infection, but simply indicates that malware has reached the computer. The detection of the same threat on different computers can constitute an outbreak.
- **Event:** The occurrence of a condition in a monitored domain.
- **Infection:** The condition in which a threat is able to run its payloads in a computer; Worry-Free Remote Manager considers an infection to have occurred whenever the antivirus scanner detects a virus/malware and is unable to clean, delete, or quarantine the threat. A spyware/grayware infection occurs when the computer cannot be completely cleaned unless it is restarted.
- **Messaging Security Agent (MSA):** The Agent that resides on Microsoft Exchange Servers and reports to CSM and WFBS-A servers. This Agent protects against virus/malware, Trojans, worms and other email born threats. It also provides spam blocking, content filtering, and attachment blocking.
- **Resellers:** Generic term to refer to organizations that directly provide security monitoring and management services to customers in Worry-Free Remote Manager.
- **Reseller administrators:** Administrators in the reseller side that perform service-related tasks using Worry-Free Remote Manager.
- **Trend Micro Data Center:** The Trend Micro monitoring and management center that hosts Worry-Free Remote Manager (and Hosted Email Security) servers and provides support to reseller administrators.
- **Security Server:** The WFBS(ALL) server computer.
- **Virus alert:** A state of vigilance that is declared by TrendLabs to prepare customer networks for a virus outbreak; TrendLabs alerts different Trend Micro products and delivers preventive solutions that IT administrators can implement as a first line of defense before a pattern becomes available.
- **Virus outbreak:** The rapid propagation of a virus threat to different computers and networks; depending on the prevalence of the threat, an outbreak can be internal, regional, or global.

# About this Getting Started Guide for Resellers

This manual guides the Worry-Free Remote Manager administrator when providing monitoring and management services for customers. This guide covers the following tasks:

- Setting up the service infrastructure
- Monitoring network security and system health
- Managing networks using supported commands
- Event tracking and notifications management
- Report generation and license maintenance

Trend Micro also provides the following documentation with this service:

- **Online Help:** Covers concepts, tasks, and interface items; accessible through the WFRM console
- **Quick Start Guide:** Quick overview of Worry-Free Remote Manager and reseller tasks
- **Agent Installation Guide:** Agent installation, management, and troubleshooting
- **Agent Readme:** Includes late breaking news, installation instructions, and known issues

# About Trend Micro

Trend Micro™, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway, gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impact of threats to information by offering centrally controlled, server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro enables companies and service providers worldwide to stop virus/malware and other malicious code from a central point, before they ever reach the desktop.

To make this possible, TrendLabs, a global network of antivirus research and product support centers, provides continuous 24 x 7 coverage to Trend Micro customers around the world. TrendLabs' modern headquarters has earned ISO 9002 certification for its quality management procedures, one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia, a global organization with more than 3,000 employees in 25 countries. For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

http://www.trendmicro.com

## TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

TrendLabs monitors potential security risks around the world to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support 24x7.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000, one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

# Chapter 2

# Getting Started

Before you start using Trend Micro™ Worry-Free™ Remote Manager, ensure that you can access it without problems. Also, ensure that your customers understand the capabilities of the console and how you can use it to monitor and manage their networks.

This chapter discusses the following topics:

# Web Browser Requirements

To access the console, ensure that you have a supported and properly configured Web browser as follows:

- Your Web browser is Internet Explorer 6, 7, or 8 with the latest service pack.
- You have added the console URL to your list of trusted sites in Internet Explorer. See *Adding the WFRM Console URL to Trusted Sites* on page 2-2 for instructions.
- Your Internet Explorer security level for **Trusted** sites is set to **Medium** or a lower level. A more restrictive security level may prevent the console from displaying correctly.
- Pop-up blockers on your Web browser have been disabled or set to allow pop-ups from the WFRM URL.

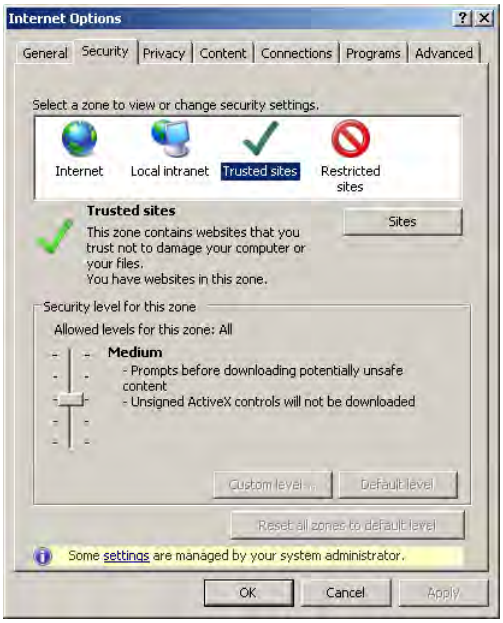



**FIGURE 2-1. Internet Explorer 8.0 security settings**

## Adding the WFRM Console URL to Trusted Sites

Add the console URL to your list of trusted sites in Internet Explorer to ensure that you can access all the console screens and features properly.

**To add the console URL as a trusted site in Internet Explorer:**

1. Open Internet Explorer.
2. Click **Tools > Internet Options > Security** (tab).
3. Select the **Trusted sites** zone.
4. Click **Sites**. The **Trusted Sites** window opens.

5. In **Add this website to the zone**, type the console URL and click **Add**.

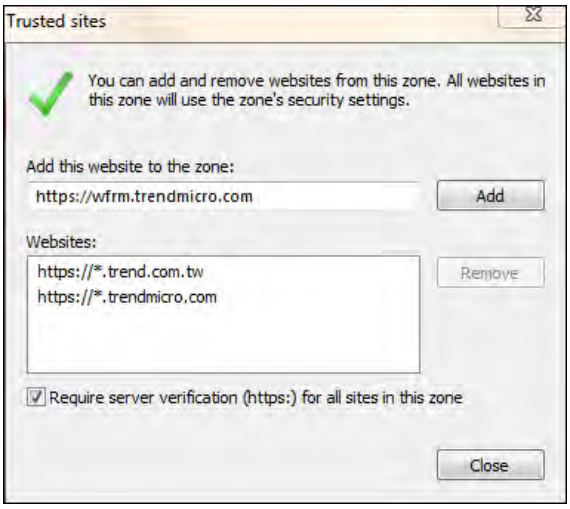



**FIGURE 2-2. Internet Explorer 8.0 Trusted sites**

6. Click **OK**.

# Accessing the Console

You access the Worry-Free Remote Manager console using a Web browser. The console URL varies between regions, but you can access all the regional consoles through the central landing page at:

http://wfrm.trendmicro.com/

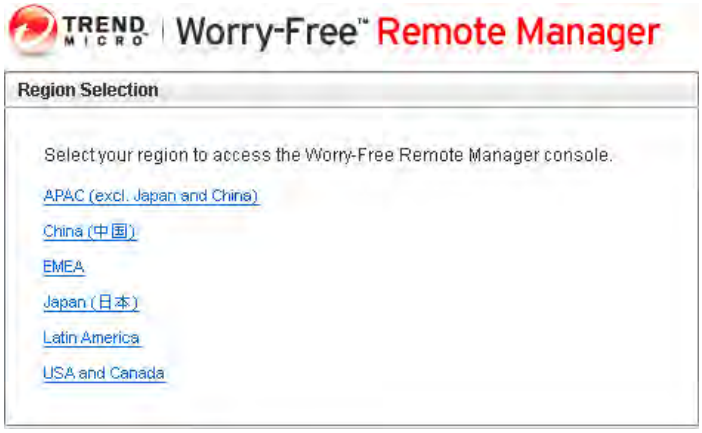



**FIGURE 2-3. Worry-Free Remote Manager central landing page**

After selecting the appropriate region, use the logon credentials that Trend Micro provides with the signing of a reseller agreement.

# Updating Your Account

From the console, click **Administration > Account Information** to modify the following details of your account:

- **Logon Name**
- **Logon Password**

- **Full name**
- **Address**
- **Zip code**
- **Telephone**
- **Mobile phone**
- **Email:** WFRM will send event notifications and reports to this address.
- **MSN Messenger**
- **Notifications via other applications:** WFRM enables linked applications (Kaseya and Autotask) to send event notifications.
- **Note**

Click **Save** when finished.

# Updating Your Reseller Profile

The console uses your reseller profile to customize customer-facing material which can include reports and notifications. The following items can be changed:

- **Name:** Name of your organization; type up to 32 characters without the following invalid characters: <&"\?
- **Description:** Relevant information about your organization; type up to 256 characters without the following invalid characters: <&"\?
- **Company Logo:** Your organization's logo; this logo may be used in interface screens, reports, notifications, and other customer-facing material. Click the current logo to modify it (use a supported format within the specified pixel size).

**To update your company profile:**

1. Click **Administration > Reseller Profile**.
2. Modify the name and description.
3. To change the logo, type the path of the image file or click **Browse** to navigate local folders. The logo image should be a .png, .jpg, .jpeg, .gif or .bmp image with dimensions of 600x55 (width x height) pixels or less. Click **Upload** (To reset to the default logo, click **Reset**).
4. A message prompts you to log off to implement the logo change. Do either of the following:
   - Click **OK** to log off.
   - Click **Cancel** to stay logged on. The banner logo will update on your next logon.

# Personal Settings

Modify the following settings:

- **Language:** Your preferred language; whenever possible, Worry-Free Remote Manager will display text and send reports and notifications in this language.
- **Records Displayed Per Page:** Number of rows to display in tables by default.
- **Total Number of Saved Reports per Profile:** Total number of saved reports can be limited based on types: daily, weekly, or monthly.

# Coordinating with the Customer

Monitoring and managing your customer's network through Worry-Free Remote Manager provides many benefits for your customer. However, just like other remote management activities, actions made on the console can drastically affect the managed network.

Before you start providing services, make sure that you have your customer's consent to do the following remote management and monitoring activities:

- View the list of computers on their network
- View the following security information:
  - Virus/malware, spyware/grayware, and network virus detections
  - Names and the number of infected computers
  - File names of infected files
  - Email addresses that have received infected files
  - Patch information for known vulnerabilities
  - License and system information on WFBS(ALL)[1] and Hosted Email Security[2]
- Send notifications to individuals within the customer organization
- Run the following actions:
  - Deploying security components
  - Starting Vulnerability Assessment scans
  - Starting or stopping Damage Cleanup Services
  - Starting or stopping manual scan
  - Updating the WFBS-S/WFBS-A server
  - Starting or stopping Outbreak Defense
- Configure the following settings:
  - Automatic deployment of Outbreak Defense
  - Real-time scan settings
  - Firewall settings
  - Location Awareness
  - Behavior Monitoring
  - Web Reputation

1. WFBS(A), WFBS(S), and WFBS-SVC are collectively referred to as WFBS(ALL) where appropriate.
2. InterScan Messaging Hosted Security was changed to Hosted Email Security in WFRM 2.2 SP1.

# Chapter 3

# Preparing the Service Infrastructure

To provide Worry-Free Remote Manager services to customer networks, you need to prepare the service infrastructure. This chapter presents the following:

# Infrastructure Installation Overview

In general, preparing the service infrastructure involves:

**If the product is WFBS-S/WFBS-A:**

**Step 1.** Add a new customer to the WFRM console.

**Step 2.** Add the main customer contact.

**Step 3.** Add at least one product to that customer.

**Step 4.** Install the Agent on the customer's server.

**Step 5.** Enter the GUID on the Agent.

**If the product is Hosted Email Security or WFBS-SVC:**

**Step 1.** Add a new customer to the WFRM console.

**Step 2.** Add the main customer contact.

**Step 3.** Add at least one service to that customer.

**Step 4.** Enter the Authorization Key on the customer's service console.

**If the product is Kaseya:**

**Step 1.** Link Kaseya and add Kaseya user email to the **Administration > Account Information** screen on the WFRM console.

**Step 2.** Add the notification recipient to the recipient list on the Customer > {customer} > Notification tab on the WFRM console.

**Step 3.** Add several fields to the Kaseya console.

**If the product is Autotask:**

**Step 1.** Link Autotask and add the Autotask logon credentials to the **Administration > Account Information** screen on the WFRM console.

**Step 2.** Add the notification recipient to the recipient list on the **Customer > {customer} > Notification** tab on the WFRM console.

**Step 3.** Add several fields to the Autotask console.

# Installing All Managed Products

This section contains information for setting up both WFBS-S/WFBS-A and Hosted Email Security.

## Adding Customers

You should identify basic customer information before you create the customer account. Fields to note are:

- **First and Last Name:** as it will appear on reports and notifications
- **Time Zone:** of the customer
- **Language:** in which the customer will receive reports and notifications

---

**Note:** Before you add a customer and install the Agent on the managed server, make sure you have written approval to perform tasks to access, monitor, and manage the customer's resources. See *Coordinating with the Customer* on page 2-4.

---

**To add a customer:**

1. Click **Customers** (tab) **>**  **Add customer** (icon at top of left pane).
   The Add Customer wizard appears.


**FIGURE 3-1. Add Customers > Step 1 > Company Information Screen**

2. Fill in the required information for the customer and click **Next**. Do not use the following characters: & " < ? \
The Step 2. Contact Info screen appears.

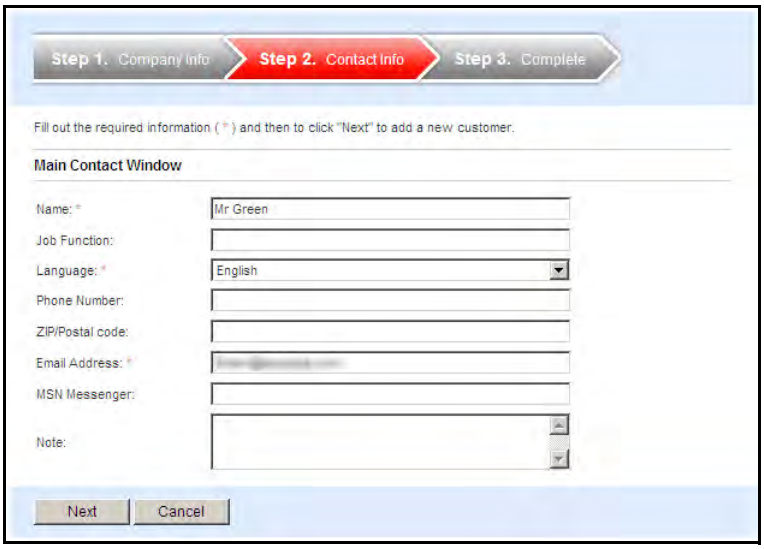



**FIGURE 3-2. Add Customer > Main Contact Window**

3. Fill in the required information for the main contact and click **Next**.
The Step 3 Complete screen appears, confirming that you added your customer. The Complete screen also includes a button for adding a product/service to the console.


**FIGURE 3-3. Add Customer > Complete Screen**

4. Click **Add Product/Service Now**.
The **Select Product/Service** screen appears.

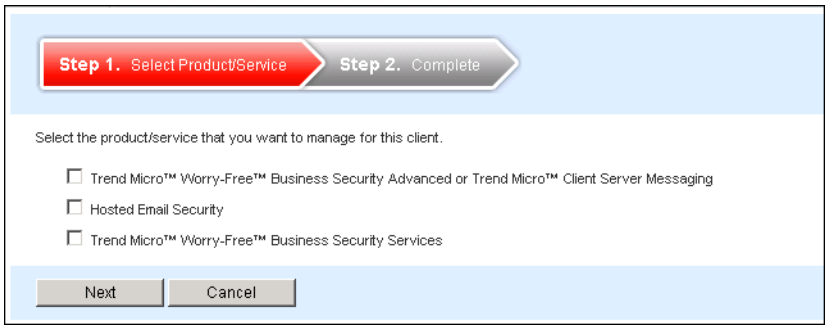



**FIGURE 3-4. Add Customer > Select Product/Service Screen**

5. Select the products or services to add, and click **Next**.

   WFRM presents you with the Globally Unique Identifier (GUID) for WFBS-S/WFBS-A and an Authorization Key for Hosted Email Security and WFBS-SVC.

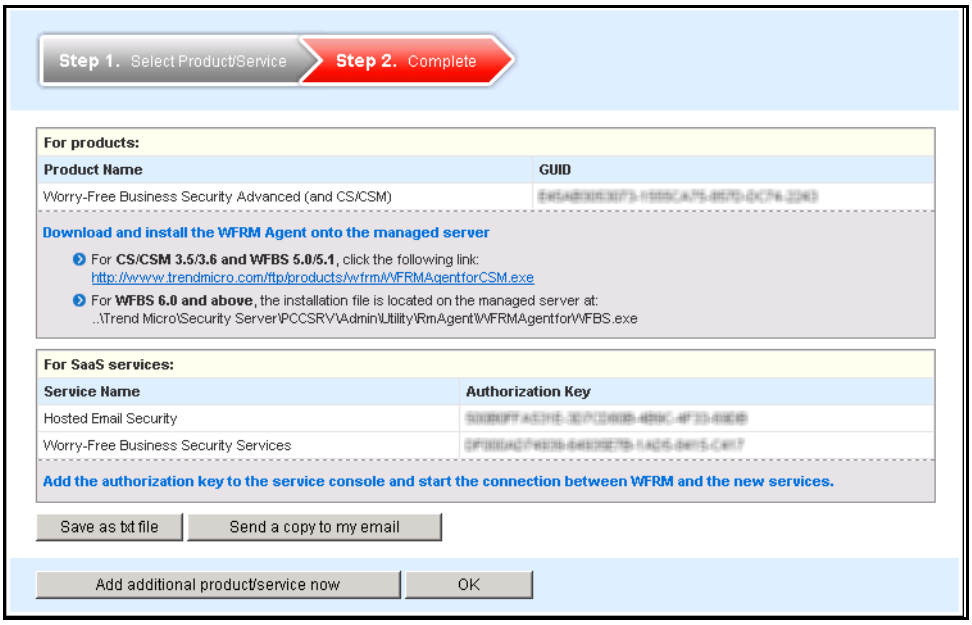



**FIGURE 3-5. GUID and Authorization Key for Selected Products/Services**

6. Save the GUID and the Authorization Key. You can save as a .txt file or send a copy to your email address of record.

---

**Note:** The globally unique identifier (GUID) is required during the installation of the WFRM Agent on the managed server. GUID is always available from **Customers > All Customers** (on the tree) **>** {customer} **> WFBS-A/CSM > Server/Agent Details** (right pane) **> WFRM Agent Details**.

The Authorization Key is required for connecting the Hosted Email Security and WFBS-SVC to the WFRM console. The Authorization Key is always available from **Customers > All Customers** (on the tree) **>** {customer} **> Hosted Email Security/WFBS-SVC > About** (right pane).

---

7. Use the displayed links and file paths to download and install the WFRM Agent for the selected products and services. For more information, see *Installing the WFRM Agent* on page 3-8.

## Obtaining the SSL Certificate

In order to use the Agent, the SSL certificate from Trend Micro must be added to the browser on the managed server.

### Using Internet Explorer 6 to Obtain the SSL Certificate

**To obtain the SSL certificate using Internet Explorer 6:**

1. Open Internet Explorer and go to http://wfrm.trendmicro.com/.
2. Click the relevant region.

3. Double-click the **padlock icon** on the status bar. This opens the **Certificate** window showing the certificate issued to `*.trendmicro.com`.
4. Click the **Certification Path** (tab) **> Equifax Secure Certificate Authority > View Certificate**.
5. When the **Certificate** window showing **Certificate Information Authority** opens, click the **Details** tab.
6. Click **Copy to File > Next** and then select DER encoded binary X.509 (.CER).
7. Click **Next**, and then type the path and filename of the certificate (example: `wfrmcert.cer`).
8. Click **Next > Finish**.

## Using Internet Explorer 7 or 8 to Obtain the SSL Certificate

**To obtain the SSL certificate using Internet Explorer 7 or 8:**

1. Open Internet Explorer, then go to http://wfrm.trendmicro.com/.
2. Click the relevant region.
3. Click the **padlock icon** to the right of the address bar. You will see the Web site identification menu.
4. Click **View Certificates**. This opens the **Certificate** window showing the certificate issued to *.trendmicro.com.
5. Click the **Certification Path** (tab) > **Geotrust** or **Equifax Secure Certificate Authority** > **View Certificate**.
6. When the **Certificate** window showing **Certificate Information Authority** opens, click the **Details** tab.
7. Click **Copy to File** > **Next** and then select **DER encoded binary X.509 (.CER)**.
8. Click **Next**, and then type the path and filename of the certificate (example: wfrmcert.cer).
9. Click **Next > Finish**.

# Registering WFBS-S/WFBS-A to WFRM

Worry-Free Remote Manager monitors and manages protected networks. It does this by communicating with an Agent that is installed on servers on the managed network. The performance of WFRM depends highly on the proper installation of the Agent.

This section contains information for setting up WFBS-S/WFBS-A. *Installing All Managed Products* on page 3-3, should also be referred to.

## Agent GUID

To distinguish between products and services, WFRM assigns a globally unique identifier (GUID) to each product and service. Every time you add a product or service to the console, WFRM generates a new GUID. The person who installs the Agent on the managed server or adds the service to the WFRM console must input the GUID during installation to allow the product to register to WFRM.

The GUID is always available from:

**WFBS-S/WFBS-A:** under **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > **WFBS-A** > **Server/Agent Details** (right pane) > **WFRM Agent Details**.

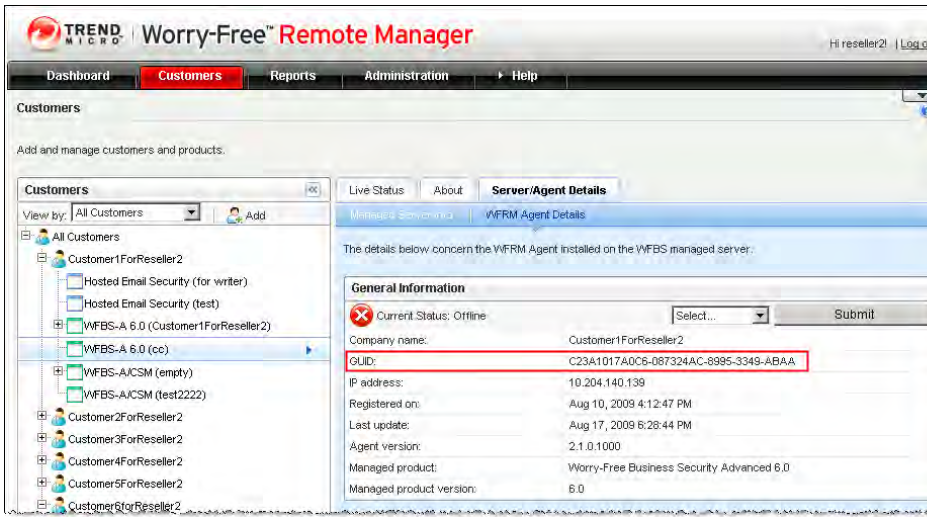



**FIGURE 3-6. The Agent GUID is always available (WFBS-S/WFBS-A)**

**Example of a WFRM Agent GUID:**

```
4F6F0F8697C9-A1FFCF63-D833-84D9-1C35
```

## Installing the WFRM Agent

The WFRM Agent allows Worry Free Remote Manager to provide monitoring services for customer environments. There are two different Agent installation procedures for different versions of WFBS-S/WFBS-A:

- WFBS-S/WFBS-A version 6.0 and above
- WFBS-S/WFBS-A 5.0/5.1

There are two different WFRM Agents. See the following table:

| WFBS VERSION | AGENT LOCATION |
|---|---|
| WFBS-S/WFBS-A 5.0/5.1 | http://www.trendmicro.com/ftp/products/wfrm/WFRMAgentforCSM.exe |
| WFBS 6.0 and above | On the managed server at: `..\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\WFRMAgentforWFBS.exe` |

For WFBS 6.0 and above, refer to the *WFBS Installation Guide* for WFRM Agent installation procedures.

### Agent Installation for WFBS-S/WFBS-A 5.0/5.1

**Overall installation consists of:**

**Step 1.** Adding the customer to the WFRM console (see *Adding Customers* on page 3-3).

**Step 2.** Adding the managed server to the WFRM console.

**Step 3.** Installing the Agent program.

**Prerequisites:**

- The customer and managed server must be added on the WFRM console (see *Adding Customers* on page 3-3) .
- WFRM Agent GUID

  (available under **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > **WFBS-A** > **Server/Agent Details** (right pane) > **WFRM Agent Details** on the WFRM console)
- Agent installer (`WFRMAgentforCSM.exe`)
- The fully qualified domain name (FQDN) of the Worry-Free Remote Manager communication server (see below)

**Requirements:**

- WFBS-S/WFBS-A 5.0/5.1
- Active Internet connection
- 50MB available hard disk space

Trend Micro also recommends that the latest service pack be applied to the server.

**To install the Agent on WFBS-S/WFBS-A 5.0/5.1:**

1. Copy the Agent installation file (`WFRMAgentforCSM.exe`) to the managed server (you should have received a link to this file when you signed up to use the WFRM service).

   **Note:** The Agent for WFBS-S/WFBS-A 5.0/5.1 is `WFRMAgentforCSM.exe`.
   The Agent for WFBS-S/WFBS-A 6.0 and above is `WFRMAgentforWFBS.exe`.

2. Open `WFRMAgentforCSM.exe`.
3. Select the installation language.
4. The **InstallShield Wizard Welcome** screen opens. Click **Next**.

5. The **License Agreement** screen opens. Read the license agreement carefully. If you disagree with the terms of the license agreement, click **Cancel** to exit the installation. If you agree with the terms, click **I accept the terms of the license agreement** and click **Next**.
6. Provide your name and the name of your company and click **Next**.
7. The **Installation Location** screen opens. To use the default location, click **Next**.
8. Provide the FQDN of the Worry-Free Remote Manager server that corresponds to your region in the **Server address** field:
   - **Asia Pacific:** `wfrm-apaca.trendmicro.com`
   - **Europe and the Middle East:** `wfrm-emeaa.trendmicro.com`
   - **Japan:** `wfrm-jpa.trendmicro.com`
   - **Latin America:** `wfrm-lara.trendmicro.com`
   - **North America:** `wfrm-usa.trendmicro.com`
9. Select a communication protocol and port:

   HTTPS. Use port 443. Type the path and filename of the SSL certificate or click **Browse** to locate the SSL certificate (see *Using Internet Explorer 6 to Obtain the SSL Certificate* on page 3-5 or *Using Internet Explorer 7 or 8 to Obtain the SSL Certificate* on page 3-6). Click **Next**.

   **WARNING! Do not click User authentication; it is not being used at this time.**

10. If the managed server uses a proxy server to connect to the Internet, specify the necessary settings. Click **Next**.
11. Type the GUID (see *Agent GUID* on page 3-7). Click **Next**.
12. Review the installation settings and click **Next**.
13. Click **Finish**.

If the installation is successful and settings are correct, the Agent should automatically register to the Worry-Free Remote Manager server. The Agent should show as Online on the WFRM console.

See *Verifying WFRM Agent Installation* on page 3-9 and *Verifying Agent / Server Connectivity* on page 3-10 for further information.

**Note:** For information on managing Agents, see the chapter *Managing Worry-Free Remote Manager Agents* on page 8-1.

### Agent Installation for WFBS-S/WFBS-A 6.0 and Above

**To install the Agent on WFBS-S/WFBS-A 6.0 and Above:**

Refer to the *WFBS Installation Guide* for WFRM agent installation procedures.

## Verifying WFRM Agent Installation

There are three methods for verifying that the WFRM Agent has been installed correctly and is operating properly. Check:

- Agent service
- Start menu shortcuts
- System tray icon

### Agent Service

On the computer where the WFRM Agent is installed, check if "Trend Micro Information Center for CSM" is started.

1. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. Look for **Trend Micro Worry-Free Remote Manager Agent**.
3. Check if the Status is **Started**.

### Start Menu Shortcuts

On the computer where the WFRM Agent is installed, check the Program Group in the Start Menu.

1. Click **Start > Programs > Worry-Free Remote Manager Agent**.
2. Verify that the Program Group contains the following items:
   - Agent Configuration Tool
   - Readme

### System Tray Icon

On the computer where the WFRM Agent is installed, check for the WFRM Agent icon in the system tray. If for any reason the icon is not visible, you can start it by clicking **Start > Programs > Worry-Free Remote Manager Agent > Agent Configuration Tool**.

Exiting the tool does not stop the WFRM service. It only closes the Configuration Tool and removes the icon from the task bar. The tool can be restarted at any time.

Suspend the mouse over the icon for status information:

**TABLE 3-1. System Tray Icons**

| ICON | MEANING |
|---|---|
|  | A green icon indicates that the Agent is connected to WFRMs communication server. The Agent is working normally. |
|  | A red icon indicates that the Agent isn't connected to WFRMs communication server or the version of the Agent is mismatched with the server and needs to be updated. |
|  | An icon with a red arrow indicates that the Agent has logged off from WFRM. |
|  | An icon with a red "X" means that the Agent has been disabled. |

## Verifying Agent / Server Connectivity

To ensure that the Worry-Free Remote Manager service is running smoothly, make sure that Agents have a status of "online" on the WFRM console.

**To view the status of Agents:**

Click **Customers** (tab) **> All Customers** (on the tree) **> All Agents** (right pane).

The tab lists the status of each Agent in the **Status** column. For details on each status, see *Agent Status* on page 8-2.

---

**Note:** In addition to the current chapter/section, see *Troubleshooting and FAQ* on page A-1 for more issues dealing with Server/Agent connectivity.

---

## Viewing Installation Errors

The Agent installation logs cover Agent installation activities. Collect these logs and send them to Trend Micro technical support if you encounter problems during installation. The Agent installation logs can be obtained from the following location on the managed server:

```
C:\WFRMAgentForCSM_Install.log
```

# Registering WFBS-SVC to WFRM

This section contains information for registering Worry-Free Business Security Services (WFBS-SVC) to the WFRM console. *Installing All Managed Products* on page 3-3 should also be referred to.

## Connect a WFBS-SVC Customer to the WFRM Console

In order to manage Worry-Free Business Security Services from the WFRM console, a customer's WFBS-SVC account must register with WFRM by carrying out the following:

1. Add the service to the WFRM console and save the Authorization Key (see *Adding Products/Services* on page 7-17).
2. Log on to the customer's WFBS-SVC account.
3. Click **Administration > Worry-Free Remote Manager**.
4. Type the Authorization Key and click **Connect**.


**FIGURE 3-7. WFRM Authorization Key entered on the WFBS-SVC console**

## Disconnect a WFBS-SVC Customer from the WFRM Console

WFBS-SVC can be disconnected from the WFRM console:

- By the reseller

  The reseller detaches the customer from the WFRM console
- By the WFBS-SVC customer

  Your customer simply opens the Remote Manager page on WFBS-SVC and clicks **Disconnect**.

  In either case, the customer is notified on the WFBS-SVC console.


**FIGURE 3-8. Disconnecting WFBS-SVC from WFRM**

# Registering Hosted Email Security to WFRM

This section contains information for registering Trend Micro™ Hosted Email Security to the WFRM console. *Installing All Managed Products* on page 3-3 should also be referred to.

WFRM enables the reseller to do certain management tasks regarding Hosted Email Security including:

1. Query information (like the managed domains, rules, approved senders) related with the customer.
2. Periodically transfer report data to the WFRM console.
3. Log on to the Hosted Email Security console and change rules, approved senders, etc.

## Connect a Hosted Email Security Customer to the WFRM Console

In order to manage Hosted Email Security from the WFRM console, a customer's Hosted Email Security account must register with WFRM by carrying out the following:

1. Add the service to the WFRM console and save the Authorization Key (see *Adding Products/Services* on page 7-17).
2. Log on to the customer's Hosted Email Security account.

3. Click **Administration > Remote Manager**.


**FIGURE 3-9. Hosted Email Security Administration menu**

4. Type the Authorization Key and click **Connect**.

**Note:** After entering the Authorization Key and clicking **Connect**, it can take **as long as ten minutes** in order for Hosted Email Security to complete the connection to the WFRM console.

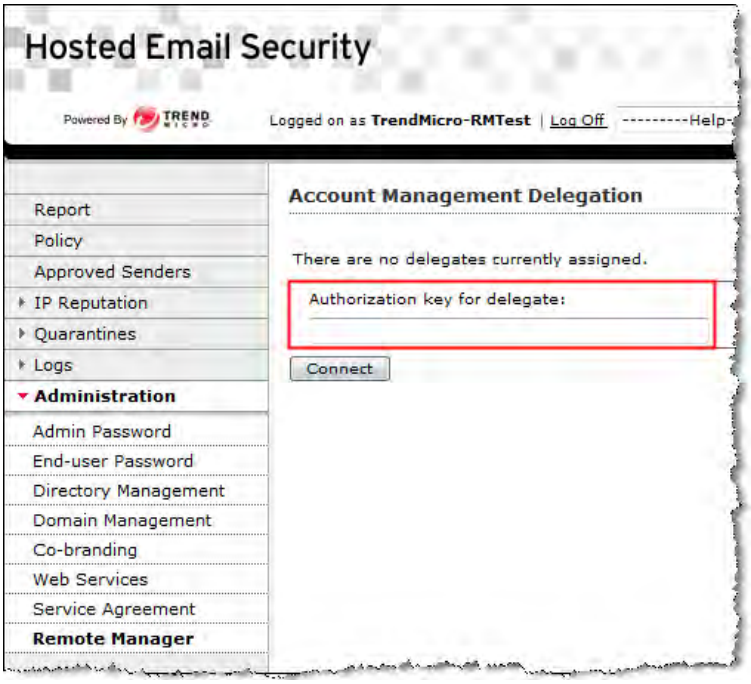



**FIGURE 3-10. Account Management Delegation: Authorization Key**

If the connection was successful, the following screen will appear:

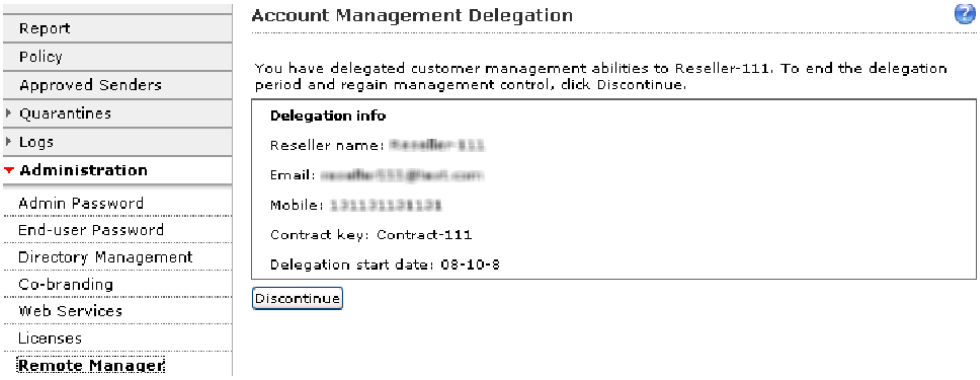



**FIGURE 3-11. Hosted Email Security Account Management Delegation**

**Note:** New Hosted Email Security data can take as long as three hours before it updates on the WFRM console. Hosted Email Security Customer information is updated once a day. See *Hosted Email Security Settings and Data Updates* on page 7-15.

If the connection fails, the error message will be displayed at the bottom of the page. Error messages can be one of the following:

- Unable to connect to remote manager server. Please check the network connection and remote manager status.
- Invalid authorization key
- Duplicate authorization key
- Server internal error

## Disconnect a Hosted Email Security Customer from the WFRM Console

Hosted Email Security can be disconnected from the WFRM console:

- By the reseller

  The reseller detaches the customer from the WFRM console
- By the Hosted Email Security customer

  Your customer simply opens the Remote Manager page on Hosted Email Security and clicks **Discontinue**.

In either case, the customer is notified on the Hosted Email Security console and clicks **OK**.

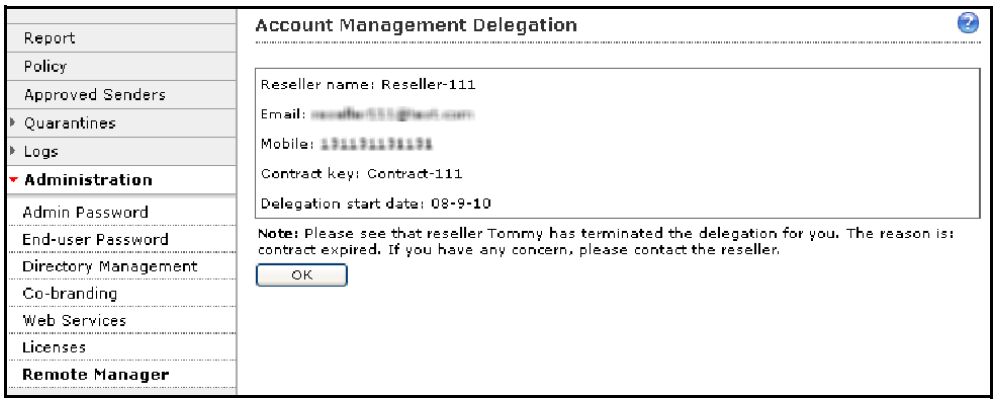



**FIGURE 3-12. Account Management Delegation - Account terminated**

If disconnecting fails, an error message will be displayed. It could be:

1. Unable to connect to remote manager server. Check the network connection and WFRM server status.
2. Server internal error.

# Integrating Kaseya with WFRM

## Kaseya Settings in WFRM

**To add Kaseya email accounts and notification recipient to the WFRM console:**

1. On the WFRM web console, click **Administration > Account Information**.

   The Account Information tab appears.

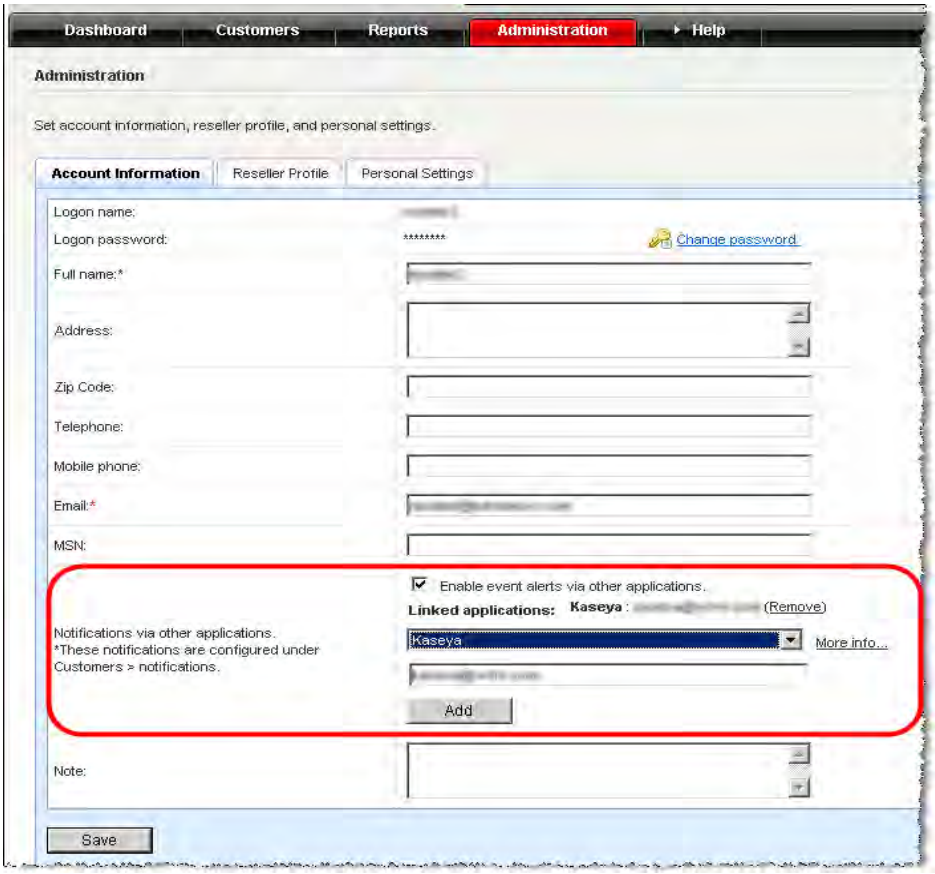



**FIGURE 3-13. Account Information Notifications Group Box**

2. Click **Enable event alerts via other applications** and select `Kaseya` from the **Linked applications** drop-down list.
3. Add the Kaseya user email and click **Add**.

   Kaseya appears as a linked application.
4. Click **Save**.

5. Add the notification recipient for the Kaseya user under **Customers > Notification > Notification Recipient (Edit)**.

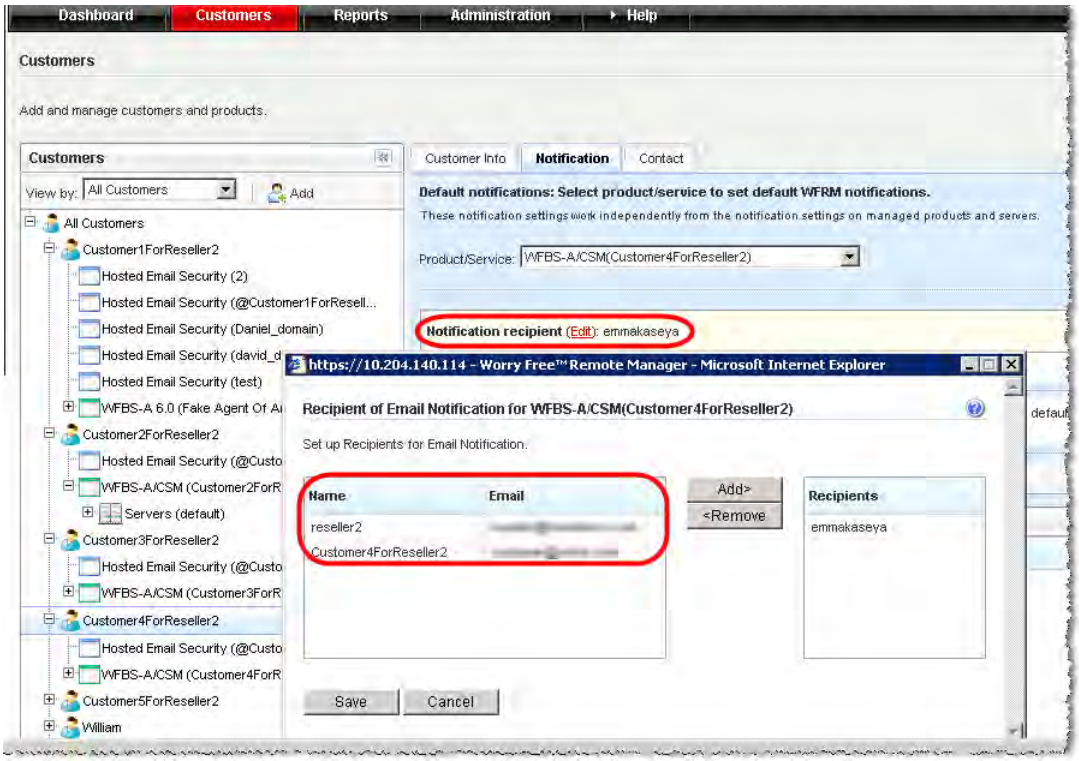



**FIGURE 3-14. Customers > Notification > Notification Recipient Screen**

## Settings in Kaseya

1. In Kaseya, add the following fields to the ticketing system in order to show WFRM notifications.

**TABLE 3-2. Kaseya ticketing fields**

| FIELD NAME | PURPOSE |
|---|---|
| TM_CreateTime | Event generation time |
| TM_ProductName | Product name |
| TM_AgentGUID | RM agent GUID |
| TM_CustomerName | Customer/Company name |
| TM_EventName | Event name |
| TM_MSAName | Exchange server name (only affects the Exchange Server Shutdown event) |
| TM_ServerName | WFBS server name (affect all events except Exchange Server Shutdown) |

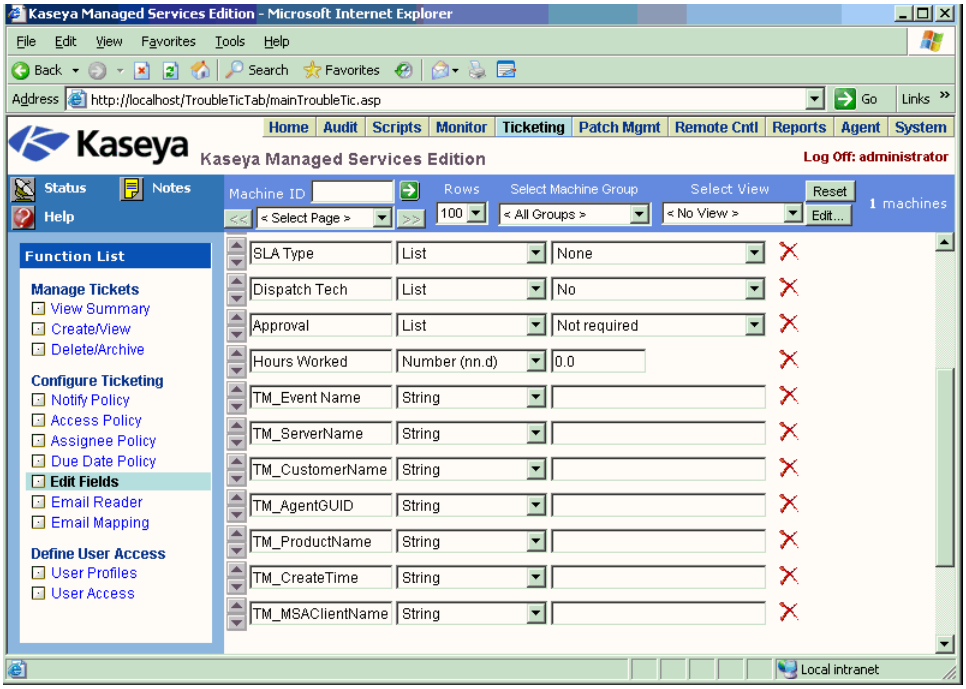



**FIGURE 3-15. Kaseya Ticketing Fields**

2. Ensure that the email setting is correct as on the following screen:

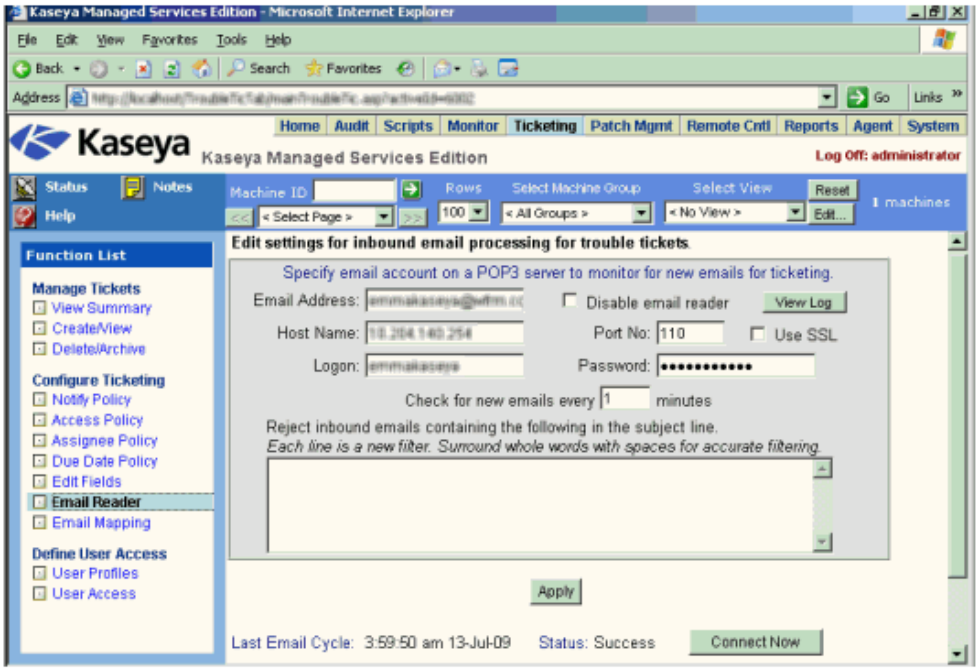



**FIGURE 3-16. Kaseya Email Settings**

When an event is triggered, Kaseya will receive the ticket as on the following screen:

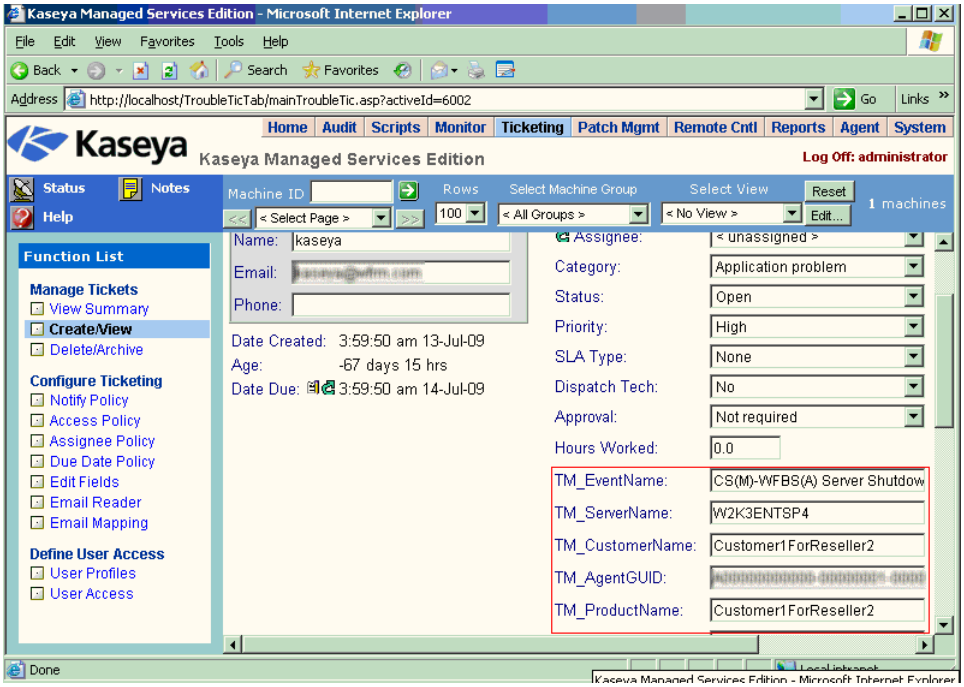



**FIGURE 3-17. Kaseya Event Ticket**

# Integrating Autotask with WFRM

## Autotask Settings in WFRM

**To add Autotask authentication to the WFRM console:**

1. Click the **Administration > Account Information** tab.

   The Account Information tab appears.

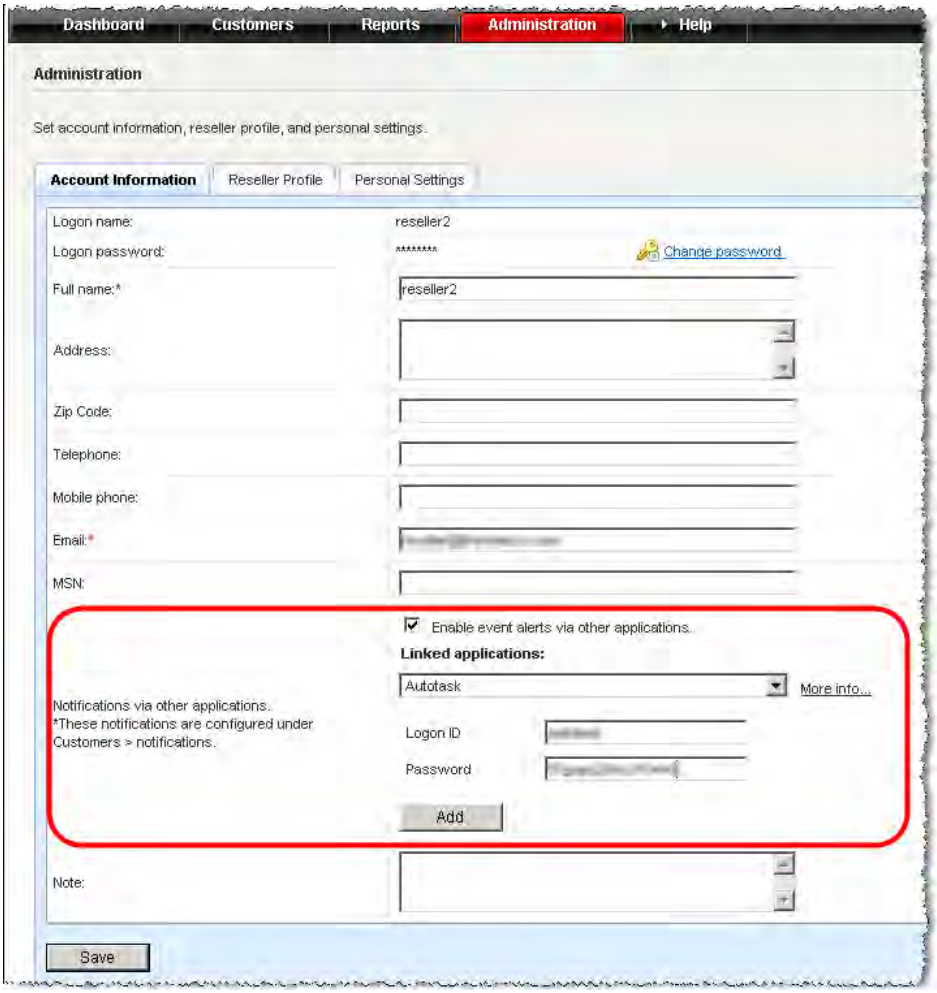



**FIGURE 3-18. Account Information > Notifications via other applications**

2. Click **Enable event alerts via other applications** and select `Autotask` from the **Linked applications** drop-down list.
3. Add the Autotask logon credentials and click **Add**.

---

**Note:** Find the Autotask account ID and password on the AutoTask UI (**Admin > AutotaskExtend > Tools > Add Ticket E-mail Service**).

---

   Autotask appears as a linked application.

4. Click **Save**.
5. Ensure that Autotask is added to the list of recipients on C**ustomers > Notification> Notification Recipient**.

6. Click **Customers > All Customers**.

   The All Customers tab appears with customer information and unique IDs.

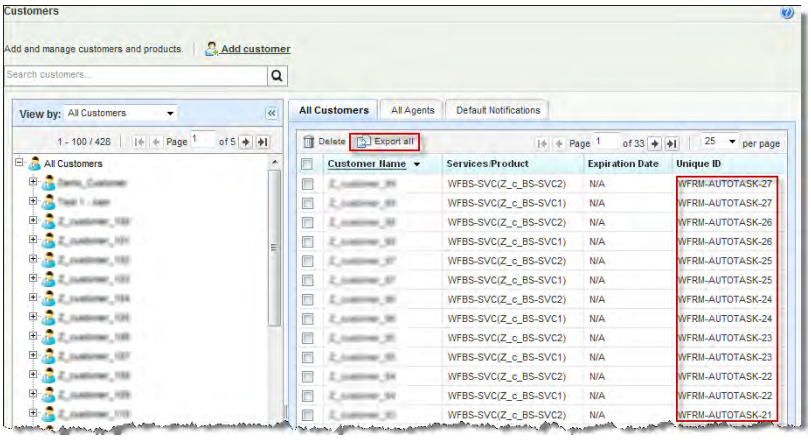



**FIGURE 3-19. Customers> All Customers Tab with Unique IDs**

7. Click **Export all** to download the customer unique IDs.

   The File Download screen appears asking if you want to save the `Exported-Customer-UniqueID.xls` file.

8. Save the export file. You will enter the unique ID in the Autotask Trend Micro Site ID field later.

---

**Note:** If you did not select E**nable event alerts via other applications** on the **Administration > Account Information** screen, the unique ID does not display on this page.

---

## Settings in Autotask

1. In Autotask, add the following fields to the ticketing system in order to show WFRM notifications (**Admin > Service Desk > Issue and Sub-Issue Types > Managed Services Alert**).

**TABLE 3-3. Autotask Ticketing Fields**

| FIELD NAME | PURPOSE |
|---|---|
| Trend Micro Threat Events | Managed services alerts for WFRM notification. There are four default event categories. |
| Trend Micro System Events | |
| Trend Micro License Events | |
| Trend Micro Other Events | |

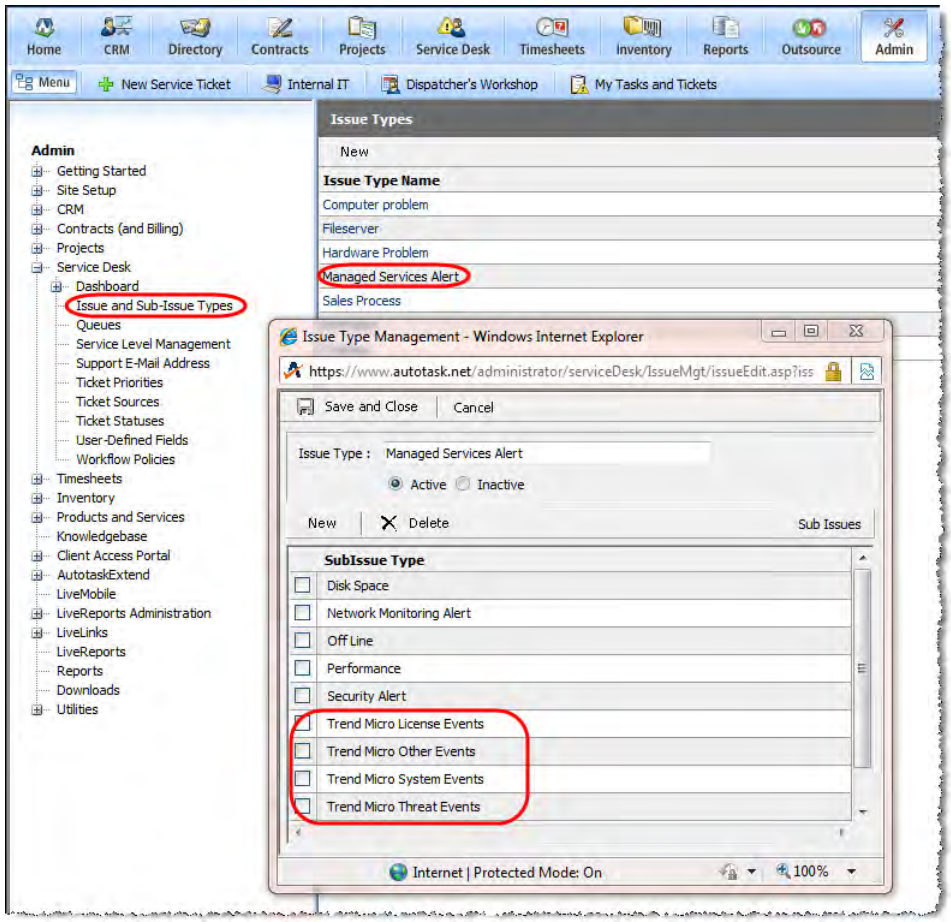



**FIGURE 3-20. Trend Micro Sub-issue Types**

2. Ensure that the email setting is correct (**Admin > AutotaskExtend > Tools > Add Ticket E-mail Service**):

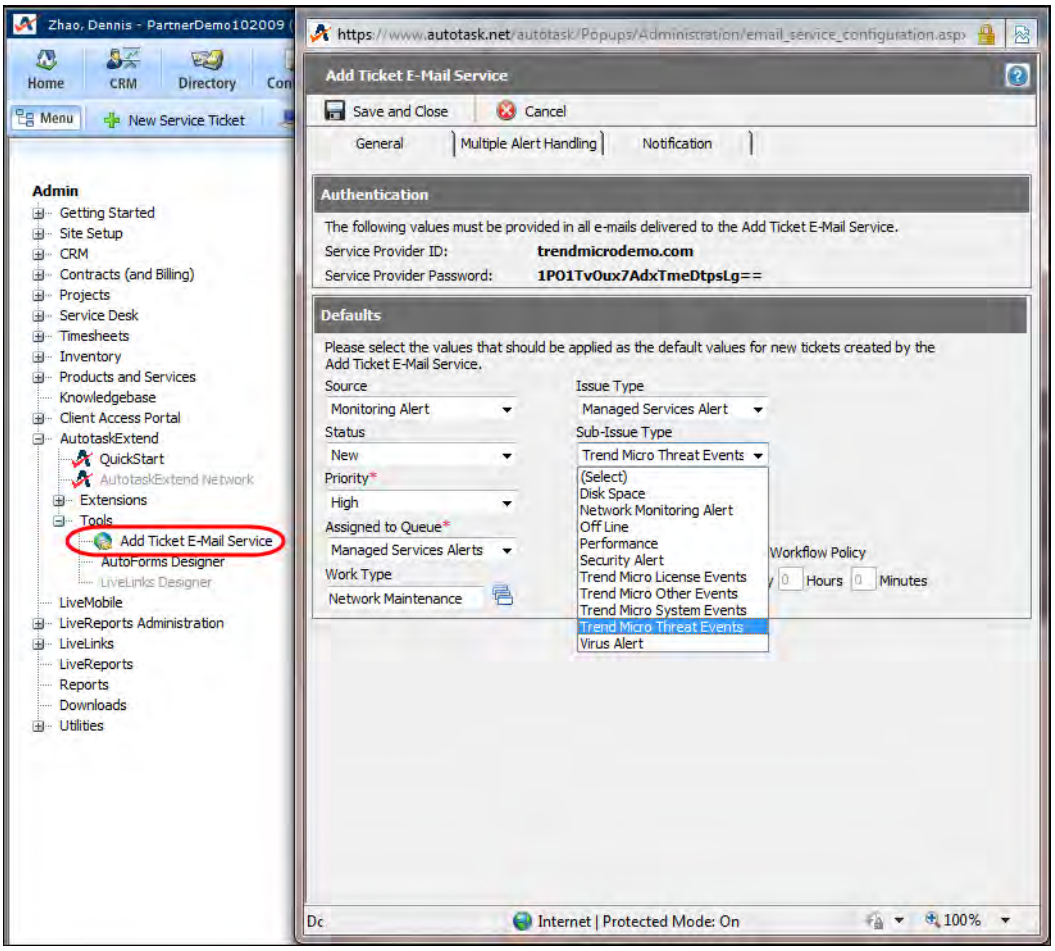



**FIGURE 3-21. Ticket Email Service Settings**

3. Create the Trend Micro Site ID field (**Admin > Site Setup > User-Defined Fields**):

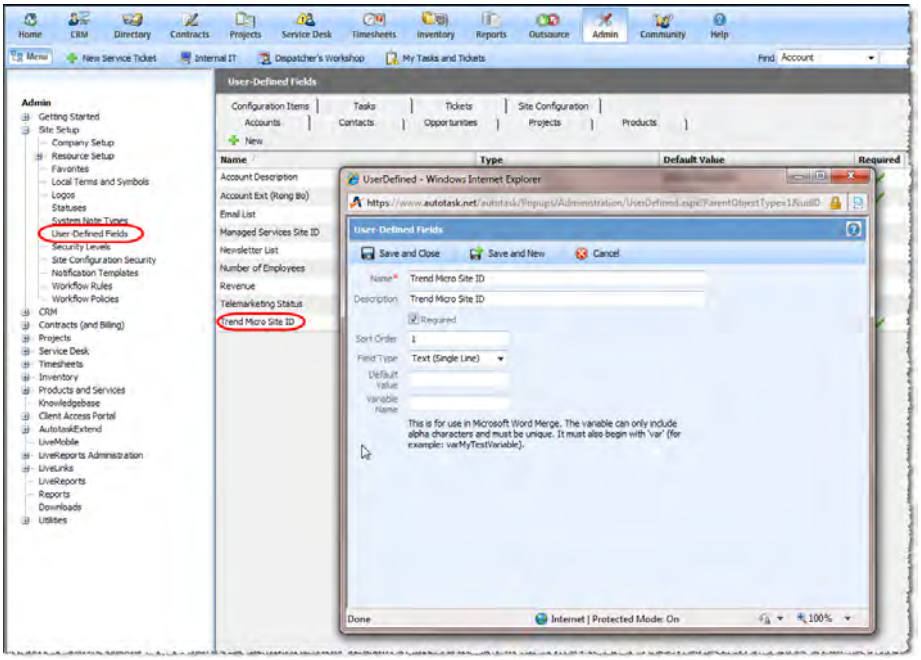



**FIGURE 3-22. Trend Micro Site ID Definition**

4. Input the WFRM unique ID in the new Trend Micro Site ID field (C**RM > Accounts > select Account > edit Account**).

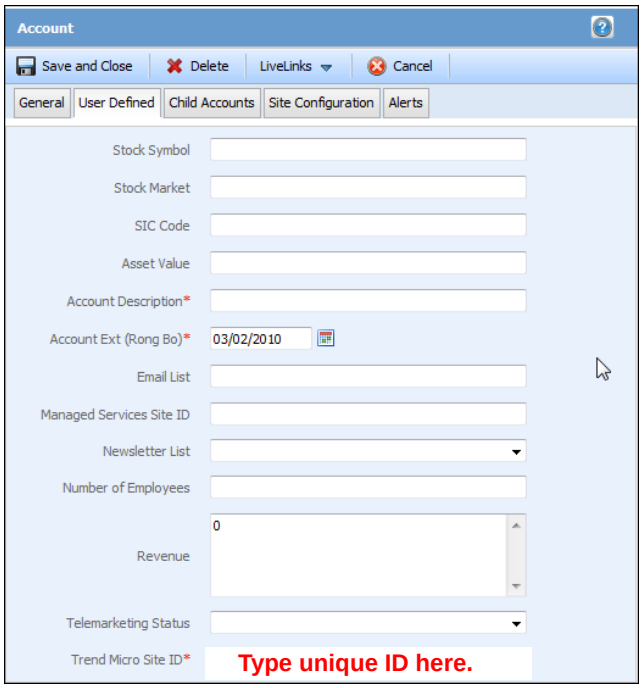



**FIGURE 3-23. Account Trend Micro Site ID Field**

**Note:** This is the unique ID exported from WFRM. See *Autotask Settings in WFRM* on page 3-21

When an event is triggered, Autotask will receive the ticket as on the following screen:

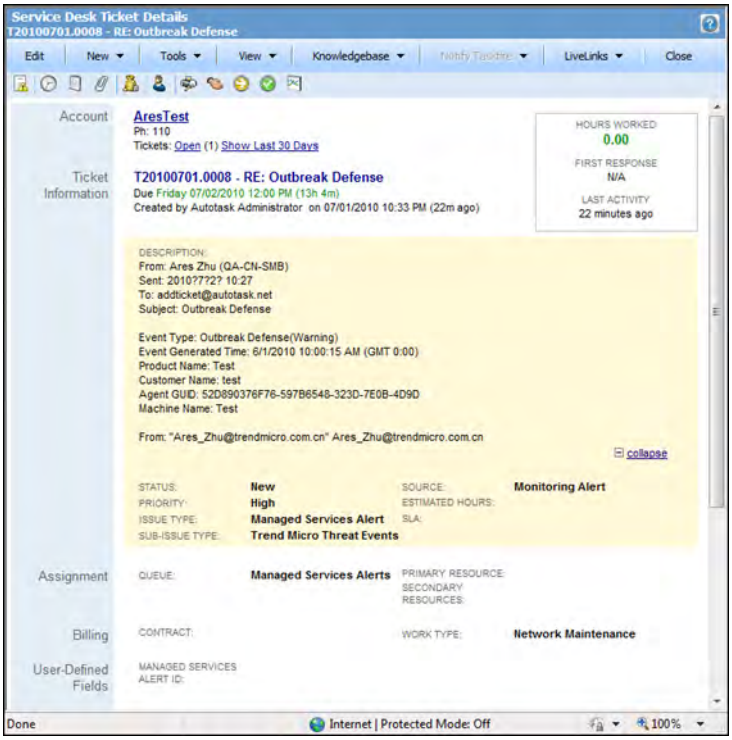



**FIGURE 3-24. Autotask Ticket Details**

# Chapter 4

# Understanding the Dashboard

# Dashboard Status Screens

The Dashboard is the central screen for reviewing the health of monitored networks. The Dashboard lists only the products whose statuses are not normal.

To access the Dashboard, open Microsoft™ Internet Explorer and log on to the Worry-Free Remote Manager site at http://wfrm.trendmicro.com/. From there, access the correct URL for your region.

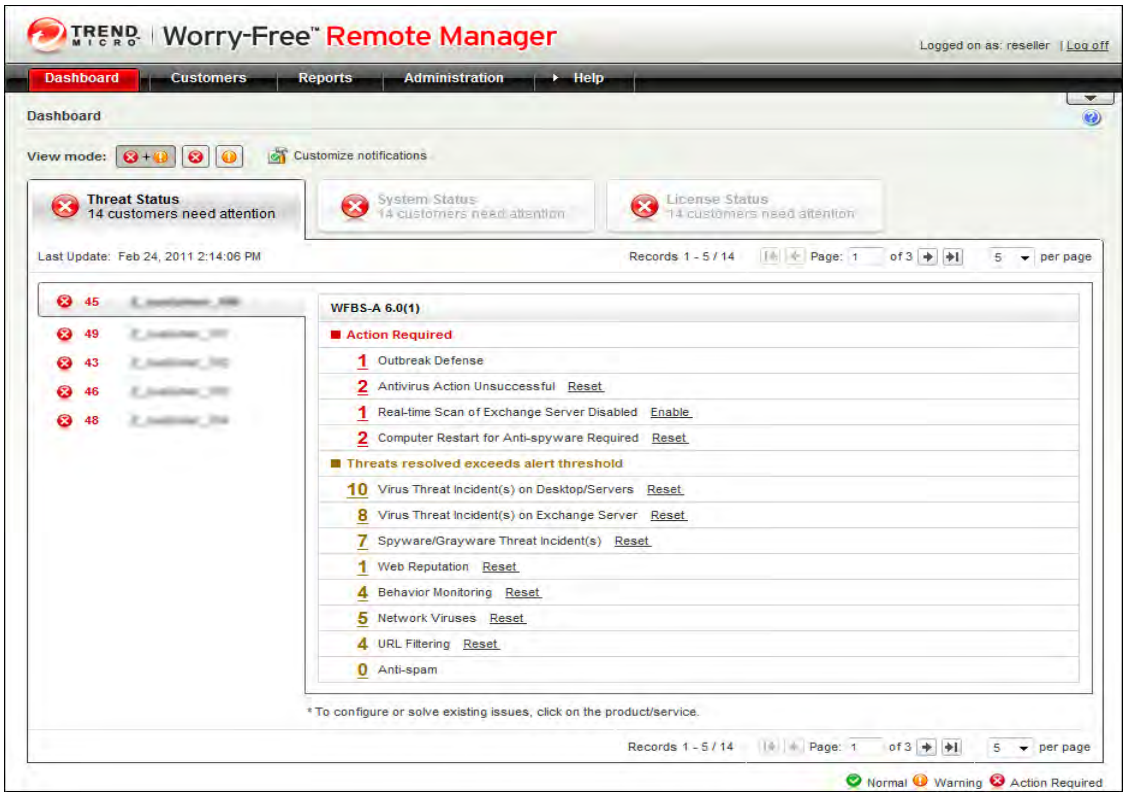



**FIGURE 4-1. Dashboard Threat Status Tab**

WFRM uses icons and color-coding to indicate if you need to take action. The table below describes the status icons:

**TABLE 4-1. Dashboard Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | **Normal condition**:<br>No action required for all customer networks. |
|  | **Warning**<br>Some action may be required for some customer networks. |
|  | **Action required**<br>Immediate action required; you need to check affected customer networks. |

For additional details about license icons and color-coding, see *License Status Icons and Color-coding* on page 4-4.

The left pane only displays customers whose products have a warning or action required status for one or more managed products. To check which products are affected, roll your mouse pointer over the customer name to see detailed threats (on the right panel).

The dashboard contains three tabs:

**TABLE 4-2. Dashboard Tabs**

| TAB | DESCRIPTION |
|---|---|
| Threat Status | Provides an overview of the threat and security status of customer products that require action or have events that exceed a pre-configured threshold. |
| System Status | Provides an overview of system-related risk situations of customer products, such as outdated security components (WFBS(ALL)). "Unusual system event" warns of potential risk situations due to inadequate disk space. |
| License Status | Provides an overview of the license status of customer products that have expired or are expiring (see *License Status Tab* on page 4-4). |

Products that display in the right pane are products that have the following warnings:

- **Action Required**
- **Threat resolved exceeds alert threshold**

Click the name of a service (Hosted Email Security or WFBS-SVC) to go to that service's console.

Click the product name (WFBS-S, WFBS-A) to go to the Live Status tab (on the Customer screen) for that product.

This table lists actions that you can take in response to Dashboard warnings.

**TABLE 4-3. Dashboard Product Warnings**

| TAB | ACTIONS TO TAKE |
|---|---|
| Threat Status | • For a detailed threat report, click the total count of the listed threats, such as the number of Antivirus Action Unsuccessful events.<br>• To re-enable scans that are disabled, click **enable**.<br>• To sync the report data with the latest information from the managed product, click **reset**. |
| System Status | • To go to the product's Live Status tab to update components, click the total count of the listed system warnings, such as the number of Outdated Managed Servers.<br>• Click **Dashboard > Threat Status >** {customer} > {product} to display the Live Status tab with a list of all red, yellow, or green system statuses for the product. |
| License Status | • Click "License expired..." and "License will expire..." hyperlinks to go to the **About** tab of the product. From the About tab, you can view license details and jump to the online registration site.<br>• Click **Dashboard > Threat Status >** {customer} > {product} to display the Live Status tab with a list of all red, yellow, or green license statuses for the product.<br>• To address license usage issues, you can contact the administrator of the affected domain. |

## License Status Icons and Color-coding

The table below shows license usage problems associated with the status icons.

**TABLE 4-4. WFBS(ALL) License Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal |
|  | Warning. This status icon appears if any of the following conditions occur:<br>- Customer exceeded 80-100% of the maximum seat count (depends on product).<br>- the managed product is running on a trial license that expires in 14 days.<br>- the managed product is running on a full license that expires in 60 days. |
|  | Action required. This status icon appears if either of the following conditions occurs:<br>- Customer has exceeded the maximum seat count.<br>- The managed product license has expired. |

## System Status Tab

This is the System Status tab. See the *Dashboard Status Screens* on page 4-2 for more information.

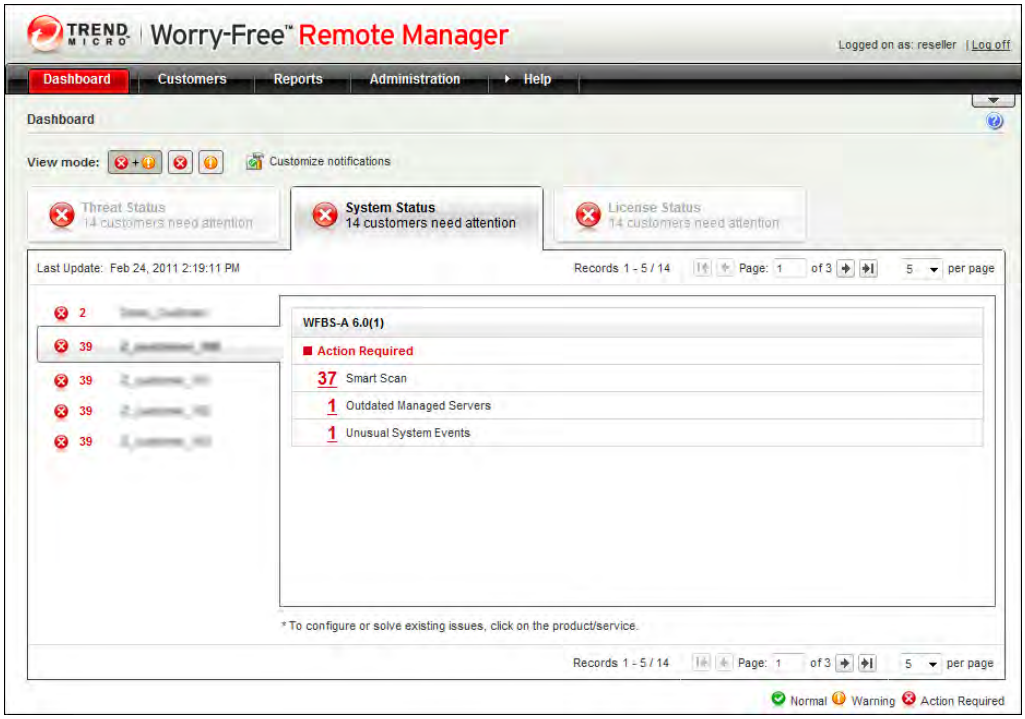



**FIGURE 4-2. Dashboard System Status Tab**

## License Status Tab

This is the **License Status** tab. See the *Dashboard Status Screens* on page 4-2 for more information.

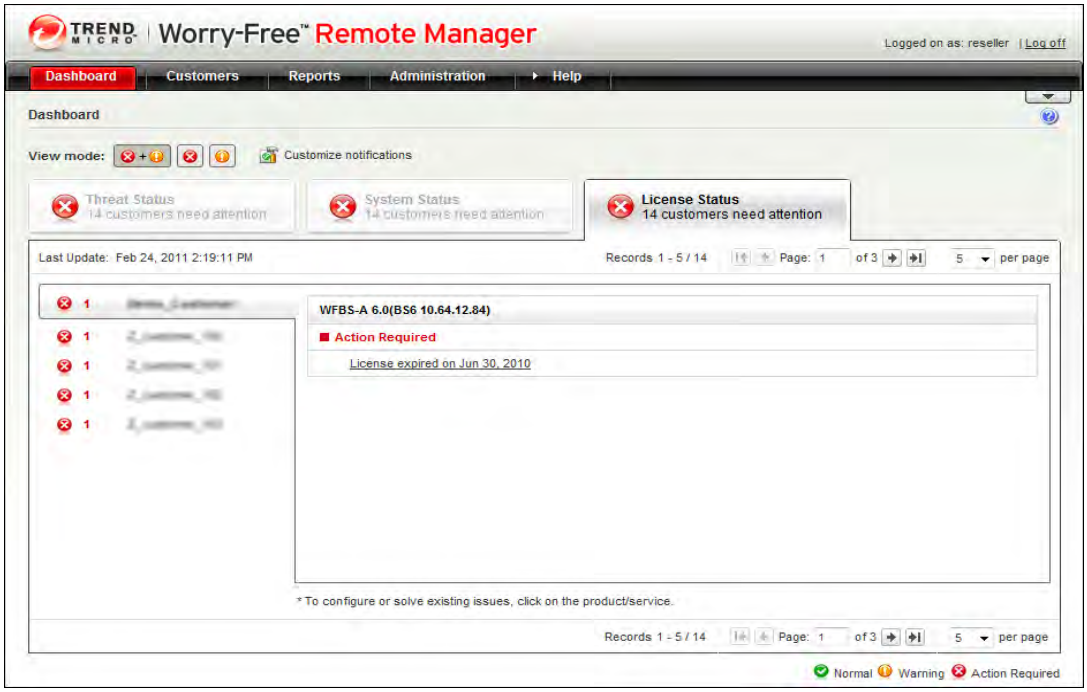



**FIGURE 4-3. Dashboard License Status Tab**

# Normal/Live Status Information

The dashboard lists only customers that are not in normal status. To get threat and system status details for any product, including those that are not listed on the dashboard, go to the **Customers** tab and access the product on the customer tree.

**To use the customer tree to get status details:**

Click **Customers** (tab) **> All Customers** (on the tree) >{customer} > {product} > **Live Status**.

The Live Status screen appears.

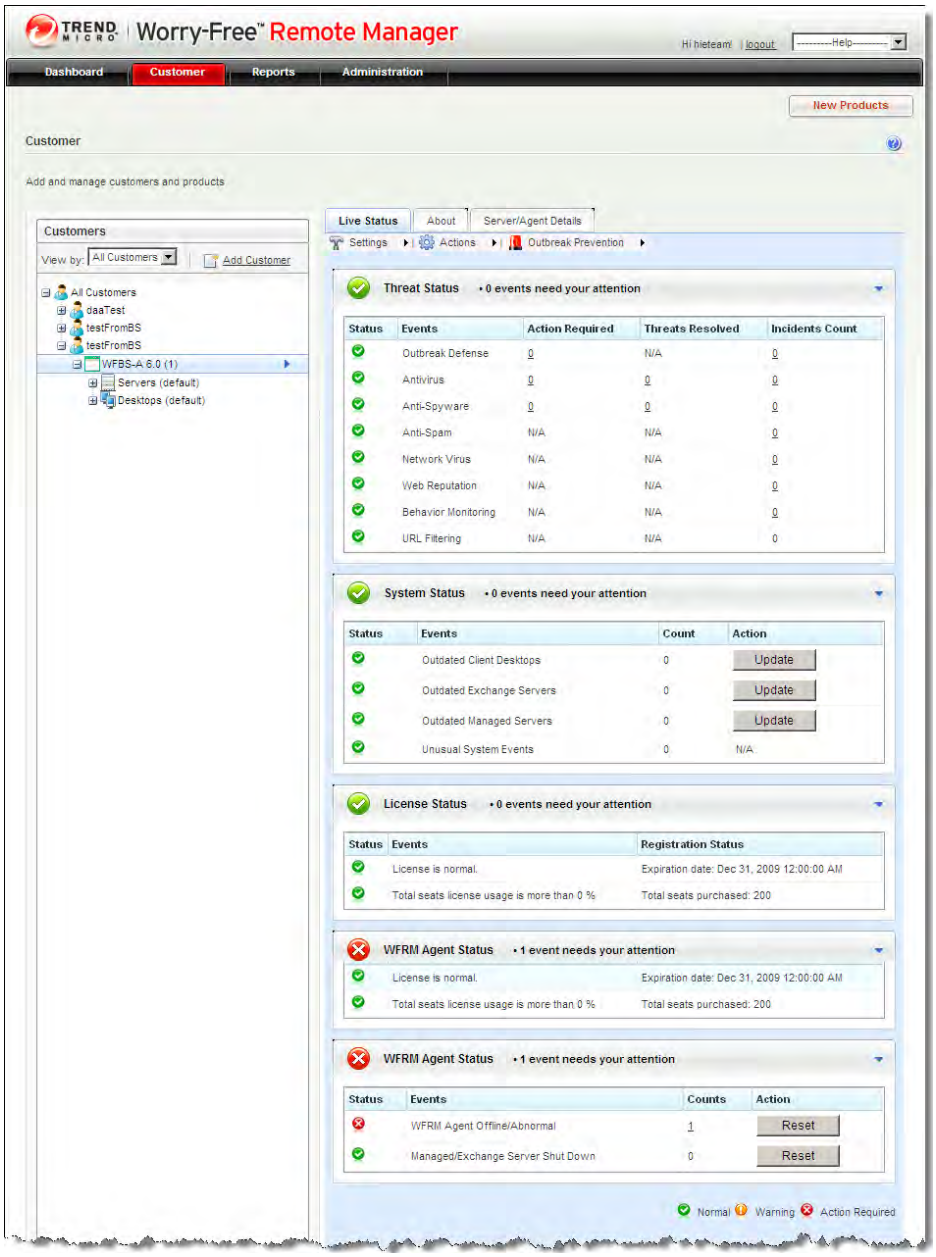



**FIGURE 4-4. Live Status**

These are the sections of the Live Status tab:

**TABLE 4-5. Live Status Sections**

| SECTION | DESCRIPTION |
|---|---|
| Threat Status | Summarizes the security status of the managed product. |
| System Status | Summarizes system status of the managed product, such as outdated components or unusual system events. |
| License Status | Summarizes the license status of the managed product. |
| WFRM Agent Status | Summarizes the status of the WFRM agent, such as WFRM agent being offline or the Exchange server being shutdown. |

# Chapter 5

# Monitoring Threat Status

This chapter covers the following topics:

# Threat Status Overview

WFRM offers two screens for viewing product threat statuses:

- The Dashboard **Threat Status** tab provides an overview of current threats. The dashboard lists only those products whose statuses are not normal for WFBS products and services.
- The customer product **Live Status** tab (on the Customer screen) provides an overview of red, yellow, and green statuses for a product.

---

**Note:** Hosted Email Security threats (except for license expiration warnings) do not display in the Dashboard Threat Status tab. You must view Hosted Email Security threats on the product Live Status tab of the Customer screen.

---

### To view the threat status of managed products from the Dashboard:

Click **Dashboard > Threat Status >** {customer}.

The Dashboard Threat Status tab appears, listing only those customers and products with warnings. Products and event categories for the customer appear in the right pane when you scroll over customer names.

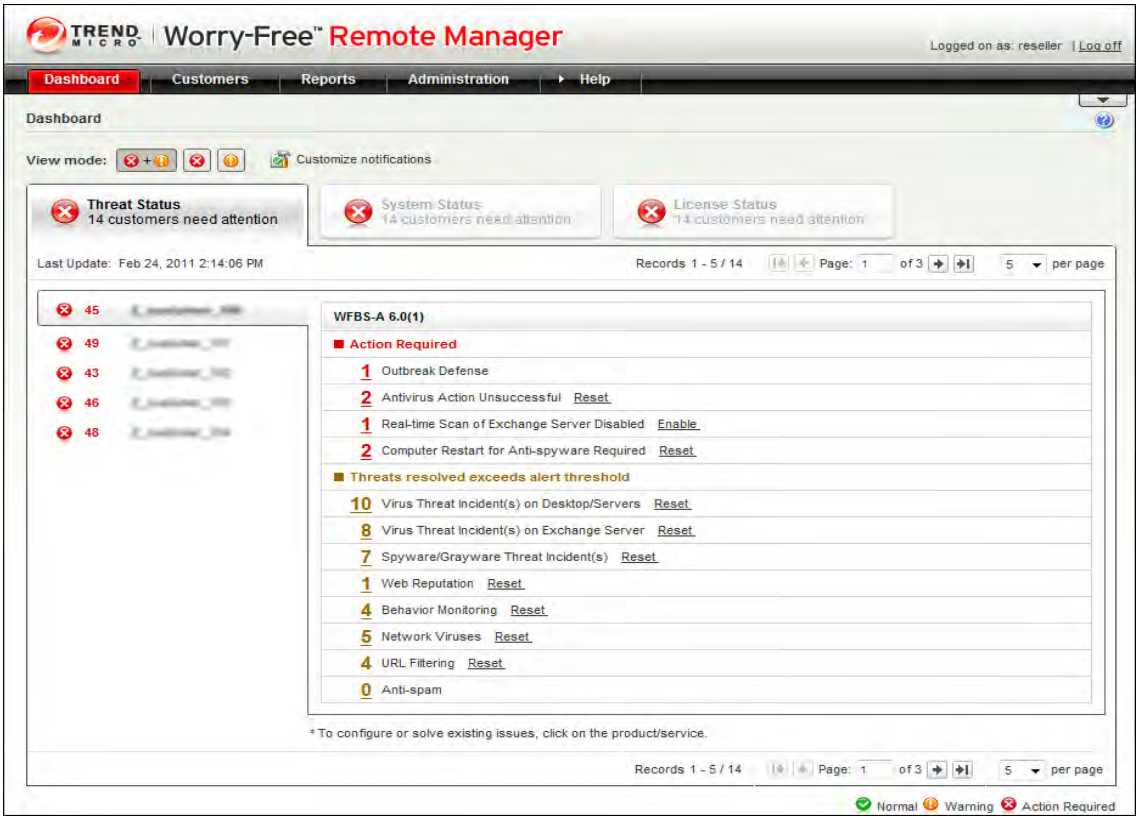



**FIGURE 5-1. Threat Status on the dashboard**

WFRM displays the following threat summary for each customer product that has experienced abnormal events.

- **Action Required:** Lists threats that require an action. Click the number of threats to view a detailed report.
- **Threats resolved exceeds alert threshold:** Lists threats that exceeded notification thresholds that you set up for the managed products. Click the number of threats to view the detailed report.

For WFBS-A/WFBS-S, clicking the number of events opens a detailed report pulled from data in the WFRM database.

For WFBS-SVS, clicking the number of events opens a detailed report on the managed product. Based on the information on the Threat Status screen, you may need to coordinate with the customer's system administrator or submit commands yourself. (See *WFBS-S/WFBS-A Commands* on page 7-12.)

**To view the threat status of WFBS products or services from the Live Status tab:**

**Note:** You can drill down to finer levels of detail about a customer product through the customer product Live Status tab.

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} > **Live Status**. Expand **Threat Status**.

   The Threat Status section appears.

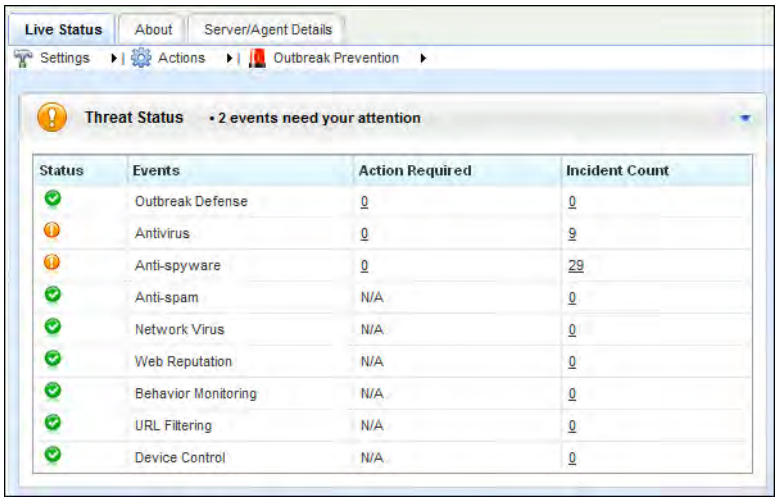



**FIGURE 5-2. Detailed Threat Status**

These are the WFBS event categories that may display on the Threat Status section, depending on the product:

**TABLE 5-1. WFBS Events**

| EVENT | DESCRIPTION |
|---|---|
| Outbreak Defense | The Outbreak Defense section indicates whether TrendLabs has declared an alert (see *Virus Alerts* on page 5-20), and displays the number of computers that require an action and the incident count. See *Outbreak Defense Status Detail* on page 5-7. |
| Antivirus | The Antivirus section indicates the number of antivirus incidents the require an action and the incident count. See *Antivirus Status Detail* on page 5-8. |
| Anti-spyware | The Anti-spyware section indicates the number of anti-spyware incidents the require an action and the incident count. See *Anti-spyware Status Detail* on page 5-11. |
| Anti-spam | The Anti-spam section indicates the number of anti-spam incidents that occurred. See *Anti-spam Status Detail* on page 5-12. |

**TABLE 5-1. WFBS Events (Continued)**

| EVENT | DESCRIPTION |
|---|---|
| Network Virus | The Network Virus section indicates the number of network viruses that were detected. See *Network Virus Status Detail* on page 5-15. |
| Web Reputation | The Web Reputation section indicates the number of URL violations that were attempted. See *Web Reputation Status Detail* on page 5-13. |
| Behavior Monitoring | The Behavior Monitoring section indicates the number of attempts that were made to modify the operating system and other programs. See *Behavior Monitoring Status Detail* on page 5-14. |
| URL Filtering | The URL Filtering section indicates the number of attempts that were made to access unauthorized websites. WFRM displays URL Filtering for WFBS-SVC and WFBS 6.0 and up only. See *URL Filtering Status Detail* on page 5-16. |
| Device Control | The Device Control section indicates the number of attempts that were made to access unauthorized devices. WFRM displays Device Control for WFBS 7.x only. See *Device Control Status Detail* on page 5-17. |

2. Click an {Incident Count} or {Action Required Count} on any threat category.
The Live Status screen displays detailed threat information for each category.

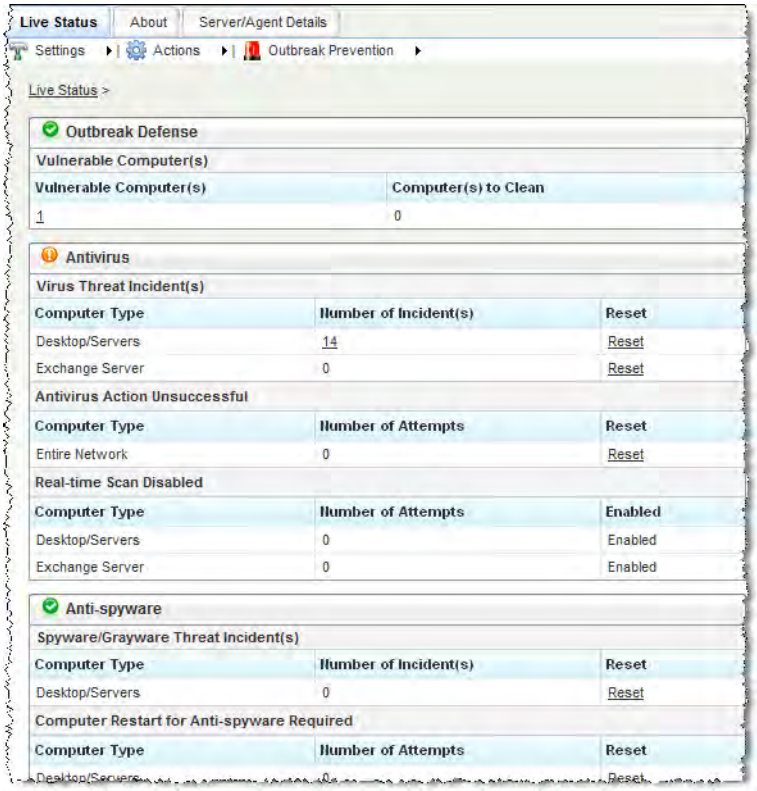



**FIGURE 5-3. Detailed Threat Status**

The table below describes the information that displays for WFBS event categories that may appear, depending on the product.

**TABLE 5-2. WFBS Events**

| EVENT | DESCRIPTION |
|---|---|
| Outbreak Defense | The Outbreak Defense section displays the number of vulnerable computers and the number of computers to clean for virus alerts that TrendLabs declares. See *Outbreak Defense Status Detail* on page 5-7. |
| Antivirus | The Antivirus section displays the following information:<br>**Virus Threat Incidents:** number of computers and Exchange servers with antivirus incidents.<br>**Antivirus Action Unsuccessful:** number of times the configured antivirus action failed. For example, the antivirus product on a computer may be configured to delete a certain type of virus upon detection. If the antivirus product fails to delete the virus, this counts as a failed action.<br>**Real-time Scan Disabled:** number of computers and Exchange servers with disabled real-time scanners. Computers without real-time scanners are highly susceptible to virus infection. Exchange servers with disabled real-time scanners will let all viruses in email messages pass, leaving the customer network susceptible to mass-mailing worms.<br>See *Antivirus Status Detail* on page 5-8. |
| Anti-spyware | The anti-spyware section displays the following information:<br>**Spyware/Grayware Threat Incident(s):** the number of spyware detections on all computers.<br>**Computer Restart Required:** the number of computers that need to be restarted to successfully complete a spyware cleanup process.<br>See *Anti-spyware Status Detail* on page 5-11. |
| Anti-spam | The anti-spam section displays the following information:<br>**Current Spam Threshold:** The spam detection rate as configured through WFBS-A.<br>**Spam Detected:** The number of messages found to be spam.<br>**Phish**: The number of messages found to be phishing messages.<br>**Reported False Positives:** The number of false spam detections reported by users.<br>**Total Messages Scanned:** The total number of messages scanned.<br>See *Anti-spam Status Detail* on page 5-12. |
| Network Virus | The Network Viruses section displays the following information:<br>**Network Threat Incident(s):** The number of network virus detections on all computers. See *Network Virus Status Detail* on page 5-15. |
| Web Reputation | The web reputation section displays the following information:<br>**Blocked URLs Detected:** The number of access attempts to URLs that have been blocked by Web Reputation.<br>See *Web Reputation Status Detail* on page 5-13. |

**TABLE 5-2. WFBS Events (Continued)**

| EVENT | DESCRIPTION |
|---|---|
| Behavior Monitoring | The Behavior Monitoring section displays the following information:<br>**Policy Violations Detected:** The number of attempts against unauthorized changes to the computer. See *Behavior Monitoring Status Detail* on page 5-14. |
| URL Filtering | The URL Filtering section displays the following information:<br>**Blocked URLs Detected:** The number of attempts to access URLs blocked by URL Filtering. See *URL Filtering Status Detail* on page 5-16.<br>**Note:** WFRM displays URL Filtering for WFBS-SVC and WFBS 6.0 and up only. |
| Device Control | The Device Control section displays the following information:<br>**Device Control:** The number of attempts to access devices blocked by Device Control. See *Device Control Status Detail* on page 5-17.<br>**Note:** WFRM displays Device Control for WFBS 7.x only. |

3. For Outbreak Defense, Antivirus, and Anti-spyware, click the number of incidents or attempts to view log details for each incident. For all others, click the number of incidents.

   Details about the event appear.

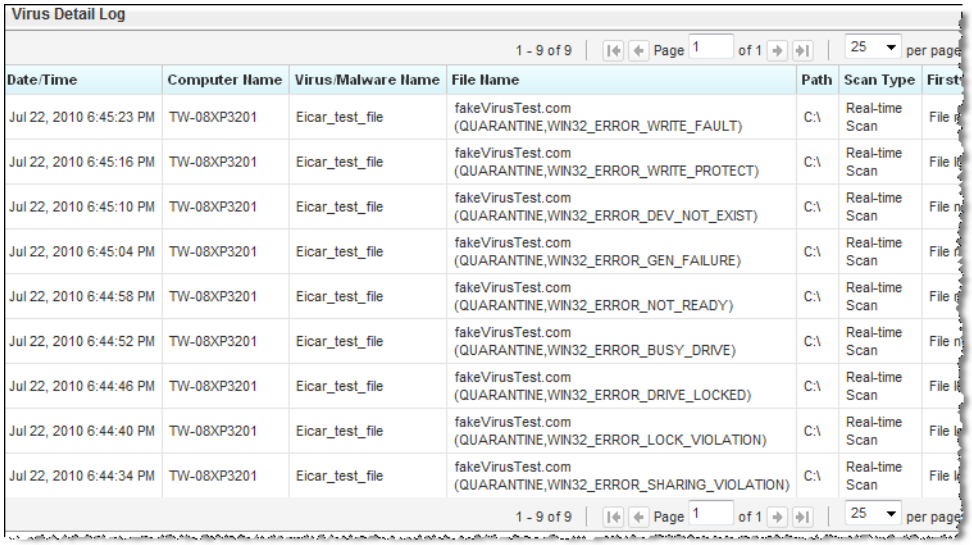



**FIGURE 5-4. Antivirus Log Details**

# WFBS-A and WFBS-SVC Status Alerts

**To see detailed threat status for any customer:**

Click **Dashboard > Threat Status >** {customer} > {product}.

WFRM monitors for the following WFBS(ALL) events:

# WFBS Detailed Status Alerts

## Outbreak Defense Status Detail

Outbreak Defense provides early warning for Internet threats and other world-wide outbreak conditions. Outbreak Defense automatically responds with preventive measures to keep computers and networks safe, followed by protective measures to identify the problem and repair the damage. While Outbreak Defense protects networks and clients, TrendLabs (see *TrendLabs* on page 1-9) creates solutions to the threat. After developing the solution, TrendLabs releases updated components, and WFBS(ALL) servers download and deploy the updated components to clients. Outbreak Defense then cleans any virus remnants and repairs files and directories damaged by the threat.

Outbreak Defense may take the following actions if an outbreak occurs:

- Block ports
- Write-protect certain files and directories
- Block certain attachments

To determine the outbreak defense status for managed networks, WFRM checks whether TrendLabs has declared a virus alert. An Outbreak Defense event only displays on the dashboard if one or more Outbreak Defense events have occurred.

The table below shows the possible outbreak defense status icons.

**TABLE 5-3. Outbreak Defense status icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | No virus alert |
|  | TrendLabs has declared a Yellow Alert |
|  | TrendLabs has declared a Red Alert |

**To view detailed Outbreak Defense statuses from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Outbreak Defense** row, click the {Incident Count} or {Outbreak Defense - Action Required count}.

   The Outbreak Defense section displays details about the number of vulnerable computers and computers to clean.

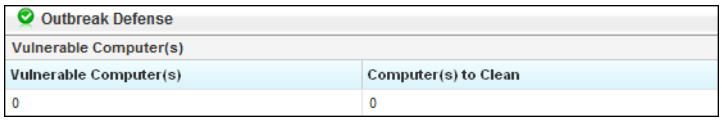



**FIGURE 5-5. Outbreak Defense Status Details**

**To enable Outbreak Defense or set Outbreak Defense to automatically deploy during alerts for all computers in a domain:**

Click **Customers** (tab) > {customer (on the tree)} > **WFBS-S/WFBS-A >** Live Status > **Outbreak Prevention** (right pane toolbar) > **Automatic Outbreak Defense**. For detailed instructions, see *WFBS-S/WFBS-A Commands* on page 7-12.

### Alert Status

Alert status information displays whenever there is a red or yellow alert. Enable Outbreak Defense to ensure that preventive measures deploy automatically and protect the network before a pattern becomes available.

### Vulnerable Computers

Vulnerable computers have not been patched for known software vulnerabilities. To handle vulnerable computers, contact the administrator of the affected domain and provide the names of the vulnerable computers and the vulnerabilities affecting them. To get this information, click the number of vulnerable computers.

To ensure that the list of vulnerable computers is current, run a Vulnerability Assessment (VA) scan. or detailed instructions, see *WFBS-S/WFBS-A Commands* on page 7-12.

### Computers to Clean

**Computers to Clean** are infected computers with a virus or malware that the security client did not successfully clean, delete, or quarantine upon detection. Typically, an infected computer contains a running copy of the virus or malware that configured the computer to allow the virus or malware to automatically start and stay running.

To view a list of the infected computers and the names of the viruses, click the number of computers to clean. To address infected computers, deploy Damage Cleanup Services (DCS) to the domain. or detailed instructions, see *WFBS-S/WFBS-A Commands* on page 7-12.

## Antivirus Status Detail

If one or more antivirus events occurs, an antivirus event displays on the dashboard. The table below shows the possible antivirus status icons and color-coding.

**TABLE 5-4. Antivirus Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. No significant virus/malware threats. |
|  | This status icon displays if any of the following conditions occur:<br>- 15 or more spyware/grayware incidents within 1 hour have been found (WFBS(ALL) default). Administrators can modify the threshold on the managed server. The one-hour interval is the 60-minute period before the point of assessment.<br>- WFBS-S/WFBS-A 5.0 only:<br>The real-time scanner is disabled in at least one computer. |
|  | This status icon displays if any of the following conditions occur:<br>- The real-time scanner on the Exchange server is disabled.<br>- A security client is unable to clean or quarantine a malware.<br>- For WFBS-S/WFBS-A 5.1 or later:<br>The real-time scanner is disabled in at least one computer. |

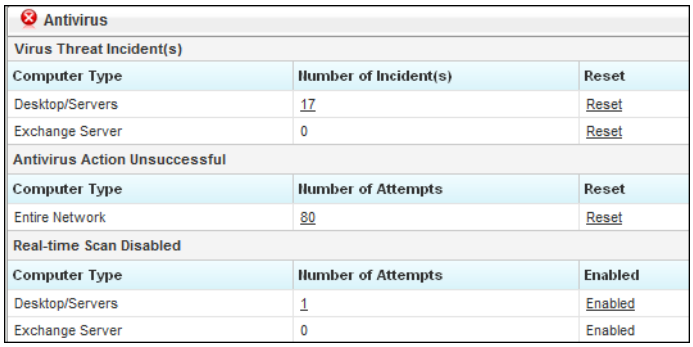
**To view detailed Antivirus status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Antivirus** row, click the {Incident Count} or {Antivirus - Action Required count}.

   The Antivirus section displays details about the computer type and number of incidents related to virus threat incidents, unsuccessful antivirus actions, and disabled real-time scans.



Antivirus

| Virus Threat Incident(s) | | |
|---|---|---|
| **Computer Type** | **Number of Incident(s)** | **Reset** |
| Desktop/Servers | 17 | Reset |
| Exchange Server | 0 | Reset |
| **Antivirus Action Unsuccessful** | | |
| **Computer Type** | **Number of Attempts** | **Reset** |
| Entire Network | 80 | Reset |
| **Real-time Scan Disabled** | | |
| **Computer Type** | **Number of Attempts** | **Enabled** |
| Desktop/Servers | 1 | Enabled |
| Exchange Server | 0 | Enabled |

**FIGURE 5-6. Antivirus Status Details**

## Virus Threat Incidents

Virus threat incidents are the number of virus/malware detections in the domain. The console groups this statistical information into the following groups:

- **Desktop/Servers:** virus/malware detected during manual scans or when files are accessed on desktop and server computers
- **Exchange servers:** virus/malware detected in email messages that are processed by an Exchange server

To view the list of affected computers, affected email addresses (for viruses found in email messages), and the names of the malware, click the number of incidents. To reset the current count, click **Reset**.

**WARNING!** **Do not click Reset unless you are sure that the incidents have been addressed and contained. To determine whether there are unresolved incidents, see the next topic,** *Antivirus Action Unsucessful.*

## Antivirus Action Unsuccessful

Antivirus scanners clean, quarantine, or delete files found with malware or viruses. Typically, the scanner performs an initial action. If the scanner cannot perform this action, the scanner performs a secondary action.

Unsuccessful actions indicate that a malware/virus has successfully circumvented antivirus defenses and has infected the computer. WFRM assumes that computers with an unsuccessfully cleaned, quarantined, or deleted virus or malware are infected.

To view a list of the infected computers and the names of the viruses, click the number of incidents.

To address computers that were infected due to unsuccessful antivirus actions, deploy Damage Cleanup Services (DCS) to the domain. For detailed instructions, see *WFBS-S/WFBS-A Commands* on page 7-12.

## Real-time Scan Disabled

Computers with disabled real-time scanners cannot scan files in real time (scheduled scans will continue). These computers are highly susceptible to virus or malware infection. Exchange servers with disabled real-time scanners let all viruses in email messages pass, leaving the customer network susceptible to mass-mailing worms.

To view the list of computers with disabled real-time scanners, click the number of computers. This number is clickable only when there is at least one affected computer.

To enable the real-time scanner on all computers and Exchange servers in the domain, click the corresponding Enable link.

## Anti-spyware Status Detail

To show the anti-spyware status, the dashboard displays status icons and color-coding that indicate a relatively high spyware/grayware incident rate and the presence of computers that are infected with spyware/grayware.

The table below shows the possible anti-spyware status icons.

**TABLE 5-5. Anti-spyware Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. Few spyware/grayware threats found. |
|  | 15 or more spyware/grayware incidents within 1 hour have been found (WFBS(ALL) default). Administrators can modify the threshold on the managed server. The one-hour interval is the 60-minute period before the point of assessment. |
|  | Action required. At least one computer needs to be restarted to completely remove a spyware/grayware infection. |

**To view detailed Antivirus status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Anti-spyware** row, click the {Incident Count} or {Anti-spyware - Action Required count}.

   The Anti-spyware section displays details about the number spyware and grayware threat incidents and required computer restarts.

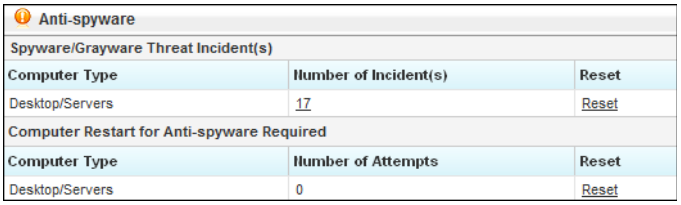



**FIGURE 5-7. Anti-spyware Status Details**

## Spyware/Grayware Threat Incidents

Spyware/Grayware threat incidents are the number of spyware/grayware detections in the domain. To view the list of affected computers and the names of the spyware/grayware threats, click the number of incidents. To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the incidents have been addressed and contained.**

### Computer Restart for Anti-spyware Required

**Computers restart for anti-spyware required** displays the number of computers infected with spyware/grayware that were partially cleaned. These computers remain infected because the spyware/grayware affecting them cannot be removed completely until after a restart. To complete the cleanup process on these computers, contact an administrator on the customer's side to restart the computers manually.

To view the list of affected computers and the names of the spyware/grayware threats, click the number of incomplete cleanup attempts. To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the affected computers have been restarted.**

## Anti-spam Status Detail

The Anti-spam Status Detail section warns of the increasing number of spam messages that the Exchange server processes. The dashboard displays status icons to show whether the percentage of spam messages (out of all messages that the Exchange server processes) has reached a certain threshold. An anti-spam event only displays on the dashboard if one or more anti-spam events occurs.

The table below shows the possible Anti-spam status icons.

**TABLE 5-6. Anti-spam Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. Spam messages comprise less than 10% of the total messages processed by the Exchange server. Note that administrators can modify the 10% threshold on managed servers. |
|  | Warning. Spam messages comprise 10% or more of the total messages processed by the Exchange server (CSM/WFBS-A default). Administrators can modify the threshold on the managed server. |

**To view detailed Anti-spam status on the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Anti-spam** row, click the number of incidents.

   The console displays the following Anti-spam activity details:

   - **Current Spam Threshold:** The spam detection rate as configured through WFBS-A.
   - **Spam Detected:** The number of messages found to be spam.
   - **Phish**: The number of messages found to be phishing messages.
   - **Reported False Positives:** The number of false spam detections reported by users.
   - **Total Messages Scanned:** The total number of messages scanned.

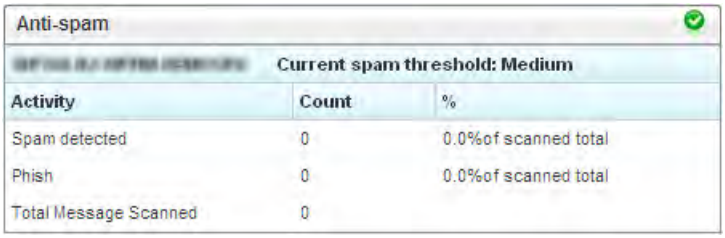



**FIGURE 5-8. Anti-spam Status Details Section**

## Web Reputation Status Detail

Web Reputation evaluates the potential security risk of requested Web pages before displaying them. Depending on the rating that the database returns and the configured security level, the Client/Server Security Agent located on computers managed by WFBS(ALL) either block or approve the request. The Web Reputation Services section indicates the number of attempts to retrieve web pages evaluated as a security risk. A Web Reputation event only displays on the dashboard if one or more Web Reputation events occur.

The table below shows the possible Web Reputation status icons.

**TABLE 5-7. Web Reputation Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
| | No action required. |
| | The clients are reporting numerous or frequent URL violations. More than 200 violations have been found within 1 hour (WFBS(ALL) default). Administrators can modify the threshold on the managed server. The one-hour interval is the 60-minute period before the point of assessment. |

**To view detailed Web Reputation status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Web Reputation** row, click the {Incident Count}.

   The Web Reputation section displays details about the blocked URLs detected, including computer type and the number of attempts to retrieve web pages that Web Reputation determines is a security risk.

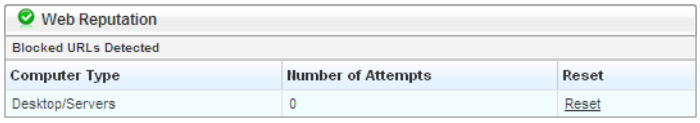



**FIGURE 5-9. Web Reputation Status Details**

To view the list of affected computers and additional details, click the number of attempts. To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the affected computers have been restarted.**

## Behavior Monitoring Status Detail

Behavior Monitoring constantly monitors the client for attempts to modify the operating system and other programs. When a Client/Server Security Agent located on computers managed by WFBS (ALL) detects an attempt, Security Agent notifies the user of the change. The user can allow or block the request. WFBS (ALL) administrators (or users) can create exception lists that allow certain programs to run while violating a monitored change or completely block certain programs. When the violations count exceeds the threshold, the status icon changes and the number of incidents is listed on the Dashboard and Live Status tab.

**To view detailed Behavior Monitoring status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Behavior Monitoring** row, click the {Incident Count}.

   The Behavior Monitoring section displays details about detected policy violations, including computer type and the number of attempts to make unauthorized changes to the computer.

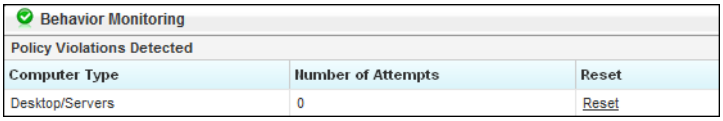



**FIGURE 5-10. Behavior Monitoring Status Details**

To view the list of affected computers and additional details, click the number of attempts. To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the affected computers have been restarted.**

## Network Virus Status Detail

The network virus status detail section warns of any significant network virus activity on the network. The dashboard displays status icons and color-coding to indicate whether network virus activity in customer domains has reached a certain threshold. A network virus event only displays on the dashboard if one or more network virus events occurs.

The table below shows the possible Network Virus status icons.

**TABLE 5-8. Network Virus Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. Few network virus threats found. |
|  | Warning. Ten or more network virus incidents within 1 hour have been found (WFBS(ALL) default). Administrators can modify the threshold on the managed server. The one-hour interval is the 60-minute period before the point of assessment. |
|  | This icon is not used to show the network virus protection status. |

To view the list of affected computers, IP addresses, and the names of the network virus threats, click the number of incidents.

To address network virus incidents, contact the administrator from the customer network to ensure that the machine sending out the viruses is isolated and cleaned. Most network viruses are removed by restarting the affected computer. To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the incidents have been addressed and contained.**

### To view detailed Network Virus status from the Customer screen:

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Network Virus** row, click the {Incident Count}.

   The Network Virus section displays details about network threat incidents, including computer type and the number of network virus attempts.

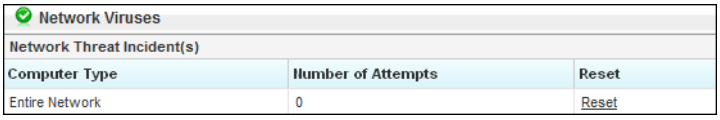



**FIGURE 5-11. Network Viruses Status Details**

To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the incidents have been addressed and contained.**

## URL Filtering Status Detail

The Trend Micro URL Filtering module delivers powerful, effective tools to manage employee Internet access and block offensive or non-work-related Web sites. URL Filtering filters content through a database with millions of categorized URLs and employs dynamic rating technology to classify new Web pages in real time or in the background. IT managers can set URL policies by group or user, category, file type, time, day, bandwidth, and other variables.

**Note:** URL Filtering pertains to WFBS-SVC and WFBS-S/WFBS-A version 6.0 and up only.

**TABLE 5-9. URL Filtering Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. URL Filtering incidents number less than 300 incidents in the last hour. Note that administrators can modify this threshold on managed servers. |
|  | Warning. URL Filtering incidents exceed 300 in the last hour. |

**To view detailed URL Filtering status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **URL Filtering** row, click the {Incident Count}.

   The console displays the following detailed information related to URL Filtering incidents:

   - **Blocked URLs Detected:** The number of access attempts to URLs that were blocked by URL Filtering.

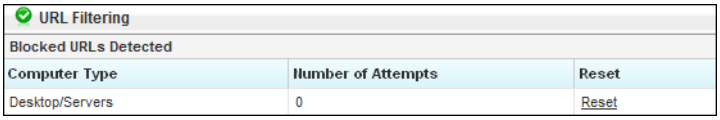



**FIGURE 5-12. URL Filtering Status Details**

To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the incidents have been addressed and contained.**

## Device Control Status Detail

The Trend Micro Device Control module delivers powerful, effective tools to regulate access to external storage devices and network resources.

**Note:** Device Control pertains to WFBS-S/WFBS-A version 7.x and up only.

**TABLE 5-10. Device Control status icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. Unauthorized device access incidents number less than 300 incidents in the last hour. Note that administrators can modify this threshold on managed servers. |
|  | Warning. Unauthorized device access incidents exceed 300 in the last hour. |

**To view detailed Device Control status from the Customer screen:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} **> Live Status > Threat Status.**

   A list of threats categories appear.

2. In the **Device Control** row, click the {Incident Count}.

   The console displays the following detailed information related to device control attempts:

   - **Device Control:** The number attempts to access unauthorized devices.

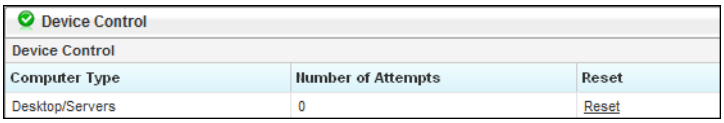



**FIGURE 5-13. Device Control Status Details**

To reset the current count, click **Reset**.

**WARNING! Do not click Reset unless you are sure that the incidents have been addressed and contained.**

# Hosted Email Security Live Status

WFRM monitors the following Hosted Email Security events:

- Total Email Message Traffic
- Accepted Email Message Size
- Threat Summary
- Top Spam Recipients
- Top Virus Recipients

WFRM can take up to three hours to update New Hosted Email Security data on the WFRM console. WFRM updates Hosted Email Security Customer information once a day. See *Hosted Email Security Settings and Data Updates* **on page 7-15**.**To see the detailed threat status for each customer:**

Click **Customers** (tab) **>** {customer} **> Hosted Email Security > Live Status** (right pane).

The Hosted Email Security Live Status tab appears.

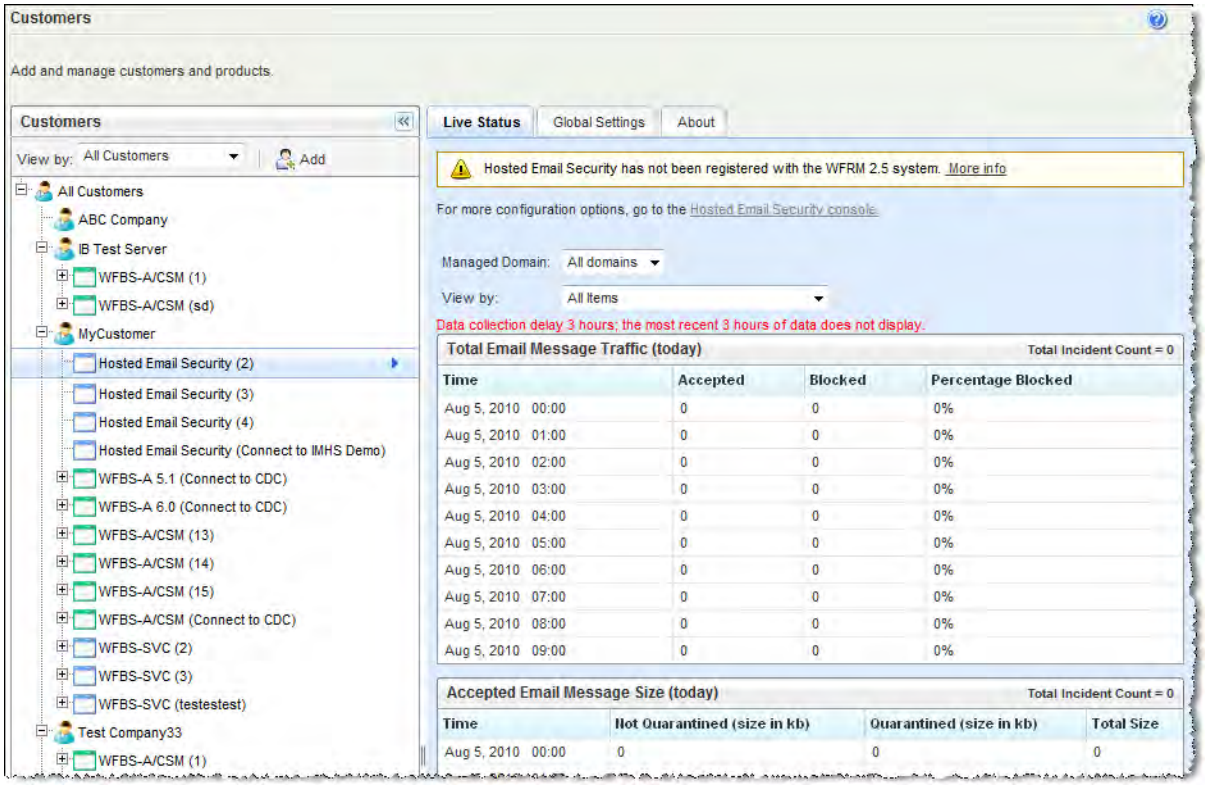



**FIGURE 5-14. Hosted Email Security Live Status Tab**

The table below describes the sections on the Hosted Email Security Live Status tab:

**TABLE 5-11. Hosted Email Security Live Status Details**

| SECTION | DESCRIPTION |
|---|---|
| Total Email Message Traffic | This section displays total email message traffic information from Hosted Email Security for the selected domain. The reporting period is the current day. The following columns are displayed:<br>**Accepted:** The number of messages that the Trend Micro Email Reputation Services (ERS) filter passes and accepts for further processing by Hosted Email Security.<br>**Blocked:** The number of "bad" message attempts to send to the selected domain. "Bad" message traffic includes connections that the ERS filter blocks.<br>**Percentage Blocked:** The percentage of message traffic that the ERS filter blocks for the selected mail domain. |
| Accepted Email Message Size | This section displays accepted email message size information from Hosted Email Security for the selected domain. The reporting period is the current day. This section shows the total size (in KB) of accepted email traffic.<br>The following columns are displayed:<br>**Not Quarantined:** The size of accepted messages, which were not quarantined, for the selected mail domain.<br>**Quarantined:** The size of quarantined messages for the selected mail domain. If quarantine is not configured in policies for this mail domain (on the Hosted Email Security server), no quarantined mail is shown.<br>**Total Size:** The total size of accepted messages for the selected mail domain. This is the sum of non-quarantined and quarantined messages. |
| Threat Summary | This section displays summary information from Hosted Email Security. This section summarizes the entire selected domain for blocked and cleaned email messages, phishing attempts, spam, virus, and other malware/grayware. The reporting period is the current week. |
| Top Spam Recipients | This section displays summary information from Hosted Email Security. This section shows the top spam recipients for the selected mail domain. The reporting period is the current week. Top spam recipient reports are displayed according to the customer's time zone settings. See *Modifying Customers* on page 7-7. |
| Top Virus Recipients | This section displays virus recipient information from Hosted Email Security. This section shows the top virus recipients for the selected mail domain. The reporting period is the current week. Top virus recipient reports are displayed according to the customer's time zone settings. See *Modifying Customers* on page 7-7. |

# Virus Alerts

Trend Micro's global antivirus research center, TrendLabs (*TrendLabs* on page 1-9), declares virus alerts whenever a malware is found to be rapidly spreading to different locations. TrendLabs categorizes alerts into the following levels based on the severity of the outbreak:

- Red alert
- Yellow alert

Once TrendLabs declares an alert, Trend Micro products are typically able to receive this warning. Certain products may initiate active responses, including the display of alerts or the implementation of certain policies. Worry-Free Remote Manager automatically obtains information on the alert malware to assist monitoring.

# Virus Outbreak

When the same malware is found on several computers, a virus outbreak is considered to have occurred. Depending on the distribution of a malware, a virus outbreak can be one of the following:

- Internal outbreak
- Regional outbreak
- Global outbreak

## Internal outbreak

An internal outbreak occurs when a malware is found in several computers in a network. Worry-Free Remote Manager uses the settings defined on the managed server to determine whether there is an internal outbreak. By default, the managed server considers an outbreak to be occurring if:

- More than 5 incidents due to the same malware have been detected in desktop or server computers in one hour
- More than 10 malware incidents have been detected in email messages in the Exchange Server in one hour

**Note:** You cannot use Worry-Free Remote Manager to configure how the managed server determines when internal outbreaks occur.

## Regional outbreak

A regional outbreak is an outbreak that involves several networks but is still limited in distribution to a specific geographical region. For example, a malware program may be spreading rapidly in a country or several countries on the same continent, but it has not spread in other locations. In such cases, TrendLabs (see *TrendLabs* on page 1-9) declares that a regional outbreak has occurred. However, depending on the severity of a regional outbreak and its potential to affect more locations, TrendLabs can declare a global outbreak.

## Global outbreak

Global outbreaks involve the rapid spread of a malware that requires global attention. This means that a malware has or will likely spread to several geographical regions.

# Chapter 6

# Monitoring System Status

This chapter covers the following topics:

# System Status Overview

The System Status section of the dashboard provides an overview of the managed domains system status, including update status of security components and disk usage on managed servers. The dashboard lists only those products whose statuses are not normal. (To view the status of domains whose statuses are normal, see *Normal/Live Status Information* on page 4-6.)

**To view the system status of managed products that require an action:**

Click **Dashboard > System Status** >{customer}.

The System Status screen for the customer appears with a list of events by product. Only events with a Warning or Action Required status are displayed.

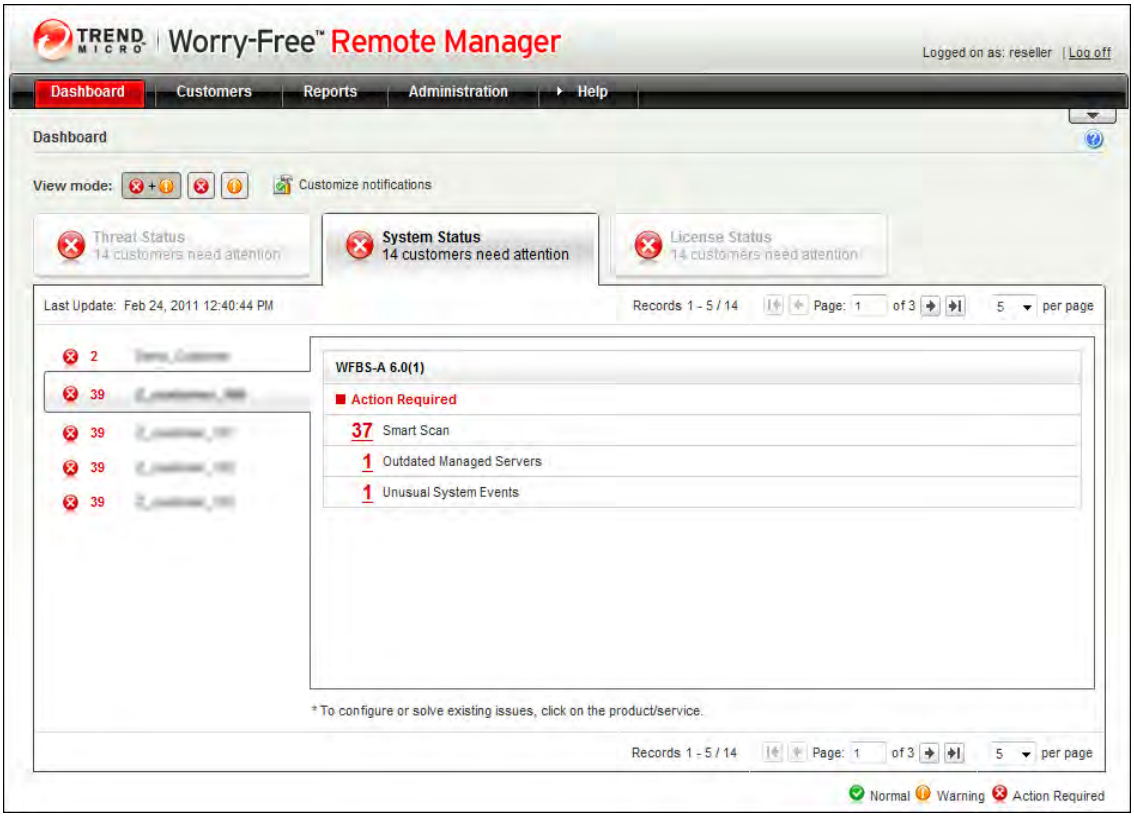



**FIGURE 6-1. WFBS(ALL) Live System Status**

**Note:** In the current version of WFRM, Threat Status and System Status only display abnormal information for WFBS(ALL)[1]. License Status displays for both WFBS(ALL) and Hosted Email Security[2].

Clicking the count for the event type opens the Customer Live Status tab for more detailed information.

1. WFBS(A), WFBS(S), and WFBS-SVC are collectively referred to as WFBS(ALL) where appropriate.
2. InterScan Messaging Hosted Security was renamed to Hosted Email Security in WFRM 2.2 SP1.

## WFBS(ALL) System Status

WFBS-S/WFBS-A System Status has five possible events:

**Outdated Client Desktops:** In WFBS(ALL), the CSA pattern on the desktop is older than the pattern on the server.

**Outdated Exchange Servers:** In CSM WFBS-S/WFBS-A, the MSA pattern on the Exchange server is older than the pattern on the CSM WFBS-A server.

**Outdated Managed Servers:** In WFBS-S/WFBS-A, WFBS-S/WFBS-A server's pattern is older than the Trend Micro official pattern.

**Unusual System Events:** WFRM defines one type of system event, "Unusual system events", which means the available free disk space has decreased to less than x%.

**Smart Scan:** In WFBS(ALL), the Smart Scan Service is not currently available.

**To view the Live System Status of a customer's domain:**

Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > {product} > **Live Status**.

The System Status appears in the right pane.


**FIGURE 6-2. WFBS Live System Status**

# Component Update

The table below shows how the dashboard displays icons to indicate any update problems.

**TABLE 6-1. Update status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal |
|  | Warning. This status icon appears if either of the following conditions occurs:<br>- The managed product has not updated successfully for more than seven days.<br>- The pattern and engine deploy rate on desktop and server computers is less than 90%. |
|  | Action required. This status icon appears if any of the following conditions occur:<br>- The managed product has not updated successfully for more than 14 days.<br>- The pattern and engine deploy rate on desktop and server computers is less than 70%.<br>- At least one Exchange server is running with outdated security components. |

To address update problems, you can run the following commands from the menu bar on the **Customers** tab. Click **Customers** (tab) **> All Customers** (on the tree) **> Customer >** {product} **> Live Status** (right pane) **> Actions**:

- **Update Client Server Security Agent:** Deploys the latest security components, including the scan engine and pattern files, to all Client Server Security Agents in the domain.
- **Update Managed Server:** Deploys the latest security components, including the scan engine and pattern files, to the managed server.

**Note:** Because **Update Client Server Security Agent** uses components already on the managed server, the effectiveness of this command relies on whether the managed server has updated successfully (which can be done by **Update Managed Server**).

Once you have successfully updated the managed server and have deployed the latest components, Trend Micro recommends running a **Manual Scan** (under the **Actions** menu). A scan can find threats that outdated components missed. For detailed instructions on running commands, see *WFBS-S/WFBS-A Commands* on page 7-12.

The dashboard lists only those products whose statuses are not normal. (To view the status of domains whose statuses are normal, see *Normal/Live Status Information* on page 4-6.)

# Disk Usage

The dashboard lets you monitor disk usage on computers in the domain by displaying icons to indicate potential and current disk space problems. To understand what these icons mean, see the table below.

**TABLE 6-2. Disk Usage Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. |
|  | This icon is not used to indicate the disk usage status. |
|  | Action required. This status icon appears if more than one computer has less than 1% disk space (1% is the WFBS-S/WFBS-A default which can be changed on the WFBS-S/WFBS-A console). |

To address disk usage issues, contact the administrator of the affected domain.

The dashboard lists only those products whose statuses are not normal. (To view the status of domains whose statuses are normal, see *Normal/Live Status Information* on page 4-6).

# Smart Scan

Trend Micro™ Worry-Free™ Business Security uses a new technology called Smart Scan. In the past, WFBS-SVC clients only used Conventional Scan, which involved each client downloading scan-related components to perform scans. With Smart Scan, the client uses the pattern file on the Smart Scan server instead. Only the Scan Server's resources are used for scanning files.

**Note:** Smart Scan technology is used by WFBS-S/WFBS-A 6.x and 7.x and WFBS-SVC 3.x and above only.

**TABLE 6-3. Smart Scan Status Icons**

| STATUS ICON | DESCRIPTION |
|---|---|
|  | Normal. |
|  | The Smart Scan service has been interrupted. |
|  | This icon is not used to indicate Smart Scan status. |

If the Smart Scan service is not running, wait 30 minutes to give the Agent time to sync with the Global scan server. If the Agent still does not connect to Global scan server, check the Agent's internet connection. Finally, contact Trend Micro Support for more help.

# Chapter 7

# Managing Networks

This chapter covers the following aspects of managing networks in Worry-Free Remote Manager:

# Customers Tab

The **Customers** tab provides a representation of the customers and their products that you manage. By default, the tab displays a tree view of all customers and their products in the left pane and detailed information, settings, and control possibilities in the right pane.

The **Customers** tab has two panes:

- *Network Tree* on page 7-3
- *Information Pane* on page 7-3

**Note:** For detailed information on Hosted Email Security[1] and WFBS(ALL)[2], see the documentation for those products.

**To view a product on the network tree:**

Click **Customers > All Customers** (on the tree) > {customer} > {product}.

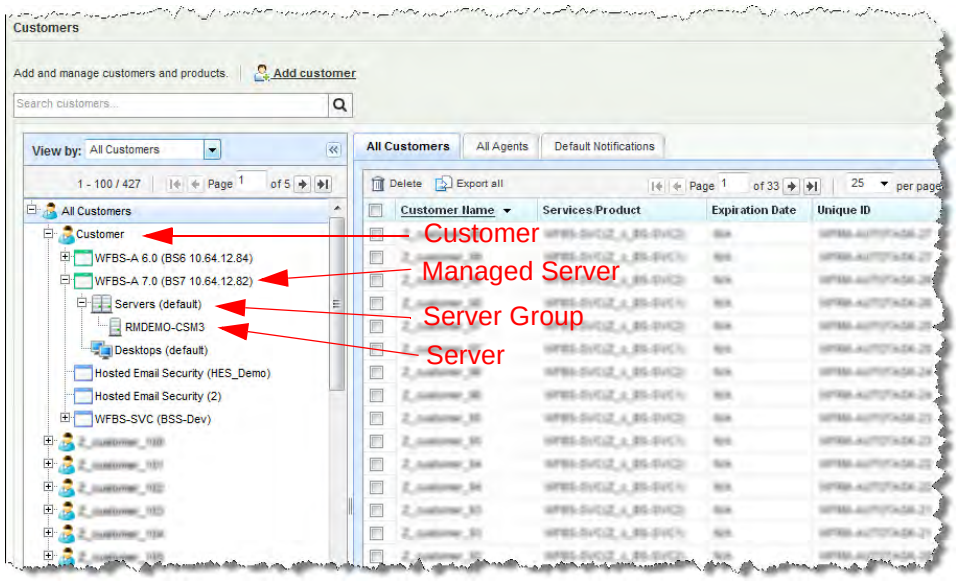



**FIGURE 7-1. Customer Tree**

# Viewing Managed Products

To view managed products, click the **Customers** tab. This tab displays a tree view of all customers and their managed products on the left pane and detailed information, settings, and control possibilities on the right pane.

**Note:** For detailed information on Hosted Email Security and WFBS(ALL), see the documentation for those products.

**To view a product on the network tree:**

Click **Customers > All Customers** (on the tree) > {customer} > {product}.

1. InterScan Messaging Hosted Security was renamed to Hosted Email Security in WFRM 2.2 SP1.
2. WFBS(A), WFBS(S), and WFBS-SVC are collectively referred to as WFBS(ALL) where appropriate.

## Network Tree

On the left side of the **Customers** tab, the screen displays a tree representation of your customers' networks. You can search for a customer, view all products at once or only WFBS-S/WFBS-A, WFBS-SVC, or Hosted Email Security under the **View by** drop down list, or browse through all the customers using the pagination arrows. You can also add a customer here and right click on most nodes of the tree to perform specific commands. The table below describes the objects in the network tree.

**TABLE 7-1. Network tree objects**

| ICON | NETWORK OBJECT | DESCRIPTION |
|---|---|---|
|  | Customer | Customer |
|  | Product | WFBS-S/WFBS-A |
|  | Product | Hosted Email Security and WFBS-SVC |
|  | Group | Server Group; this group manages many Client Security Agents (CSAs). |
|  | Group | Desktop Group |
|  | Server | A server computer; this computer runs the Client Security Agent (CSA). |
|  | Exchange server | Exchange Server computer; this computer runs the Messaging Security Agent (MSA). |
|  | Desktop | A desktop computer; this computer runs the Client Security Agent (CSA). |

## Information Pane

The information pane is the right pane of the **Customers** tab. It displays tabs related to the selected network tree object. See the table below for the tabs displayed for each network object.

**TABLE 7-2. Network tree objects and their information pane tabs**

| TREE OBJECT | INFORMATION PANE TABS | TAB DESCRIPTION |
|---|---|---|
| All Customers | All Products | Lists all your customers and their products. Here you can remove customers and products and send commands by right clicking the nodes. See *All Products* on page 7-6. |
| | All Agents | Lists all Agents for all customers. It lets you view Agents according to various states: 1) Online 2) Offline 3) Abnormal 4) Version mismatch 5) Disabled 6) Unregistered 7) Plugin-errors found. See *Agent Status* on page 8-2 and *All Agents* on page 7-11. |
| | Notifications | Lists event types and allows you to customize what events will trigger a notification. See *Notifications* on page 7-9. |

**TABLE 7-2. Network tree objects and their information pane tabs (Continued)**

| TREE OBJECT | INFORMATION PANE TABS | TAB DESCRIPTION |
|---|---|---|
| Customer | Customer Info | Lets you modify customer information. This tab also allows you to add Trend Micro products and services you wish to monitor via WFRM to this customer. See *Adding Products/Services* on page 7-17. |
| | Notification | Allows you to select who and what kinds of notifications contacts will receive. Recipient names come from contacts for this company. See *Notifications* on page 7-9. |
| | Contact | Lists all the customer's contacts and lets you add or delete contacts. Clicking the name of a contact lets you edit the contact's details. See *Adding Contacts* on page 7-7. |
| Product - Hosted Email Security | Live Status | Displays the Hosted Email Security status details. Allows you to view statistics from any of the customer's domains protected by Hosted Email Security. Displays a link that allows you to log into the Hosted Email Security console. See *Normal/Live Status Information* on page 4-6. |
| | Global Settings | Allows you to view Hosted Email Security policy settings for different groups. |
| | About | Displays the Authorization Key and Expiration date. See *Checking Product License* on page 7-16. |
| WFBS-S/WFBS-A | Live Status | Displays the WFBS-S/WFBS-A status details. Allows you to view Live Status and drill down for more detailed information by clicking on incident numbers. This page also lets you submit commands via the menu bar. See *Normal/Live Status Information* on page 4-6, *Menu Bar* on page 7-6 and *WFBS-S/WFBS-A Commands* on page 7-12. |
| | About | Displays licensing information about the managed product. See *Checking Product License* on page 7-16. |
| | Server/Agent Details | Displays basic information including pattern and version numbers concerning the server and Agent. |
| WFBS-SVC | Live Status | Displays the WFBS-SVC status details. Allows you to view Live Status and drill down for more detailed information by clicking on incident numbers. Displays a link that allows you to log into the WFBS-SVC console. See *Normal/Live Status Information* on page 4-6. |
| | About | Displays licensing information about the managed product. See *Checking Product License* on page 7-16. |
| Group | Security Settings | Group settings are not configurable in this version of WFRM. |
| Server / Desktop Computer | Basic Information | Displays basic system information and a summary of virus/malware, spyware/grayware, network virus incidents, Behavior Monitoring, and Web Reputation Services incidents on the selected computer. |

## Security Settings Status

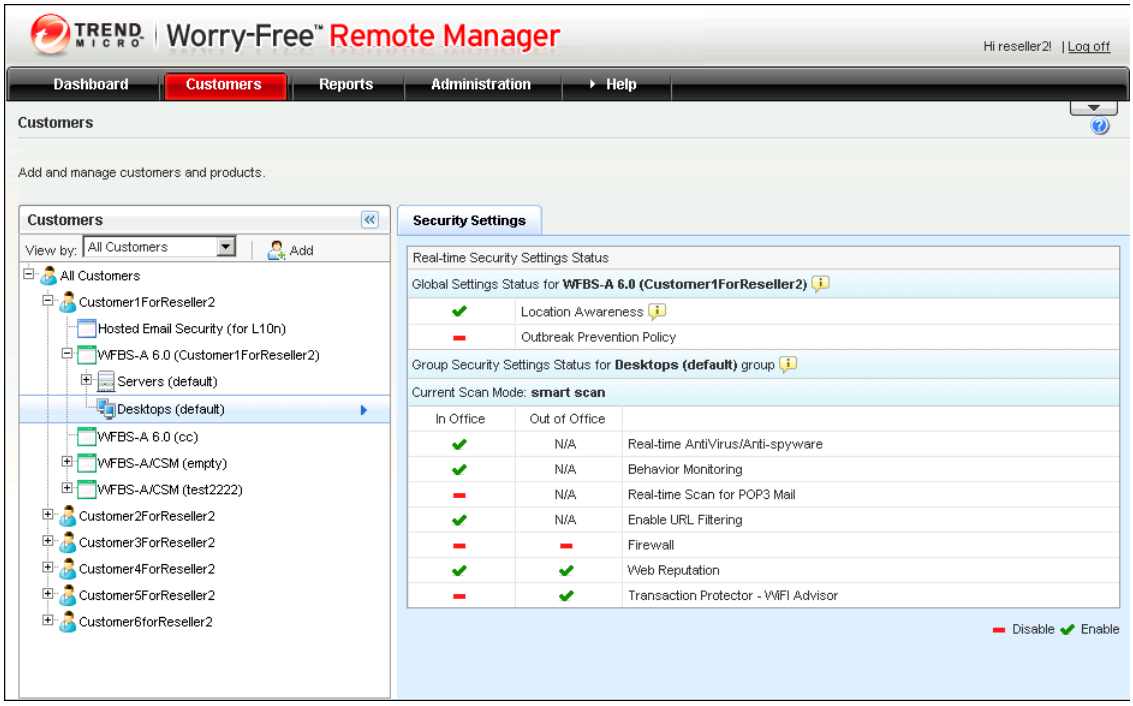



**FIGURE 7-2. Real Time Security Settings Status**

**Real Time Security Settings Status** can be viewed by clicking **Customers > All Customers** (on the tree) **>** {customer} **> WFBS-S/WFBS-A >** {group} **> Security Settings** (right pane).

Both In Office and Out Of Office settings are viewable (applies to WFBS-S/WFBS-A only). Settings are controlled through the **Settings** drop down menu (see *Menu Bar* on page 7-6 and *WFBS-S/WFBS-A Commands* on page 7-12). Out of Office settings are relevant only when **Location Awareness** is turned on.

### Location Awareness

With Location Awareness (applies to WFBS-S/WFBS-A only), administrators can control security settings depending on how the Client is connected to the network. WFBS-S/WFBS-A automatically identifies the location of the client and controls the Web sites users can access. The restrictions differ based on the user's location. Worry-Free Business Security classifies Clients as:

- **Normal Clients**: computers that are stationary and maintain a continuous network connection with the Security Server.
- **Roaming Clients**: computers that do not always maintain a constant network connection with the Security Server, such as portable computers. These Clients' Client/Server Security Agents continue to provide virus protection, but have delays in sending their status to the Security Server.

Location Awareness controls the In Office/Out of Office connection settings.

## Menu Bar

The menu bar (applies to WFBS-S/WFBS-A only) on the right pane (Settings, Action, Outbreak Prevention Services) only displays when WFBS(ALL) is selected on the network tree. These commands enable you to manage critical aspects of network security including real-time scan settings and the deployment of component updates. For a list of the network commands on the menu bar and instructions on how to use these commands, see *WFBS-S/WFBS-A Commands* on page 7-12.

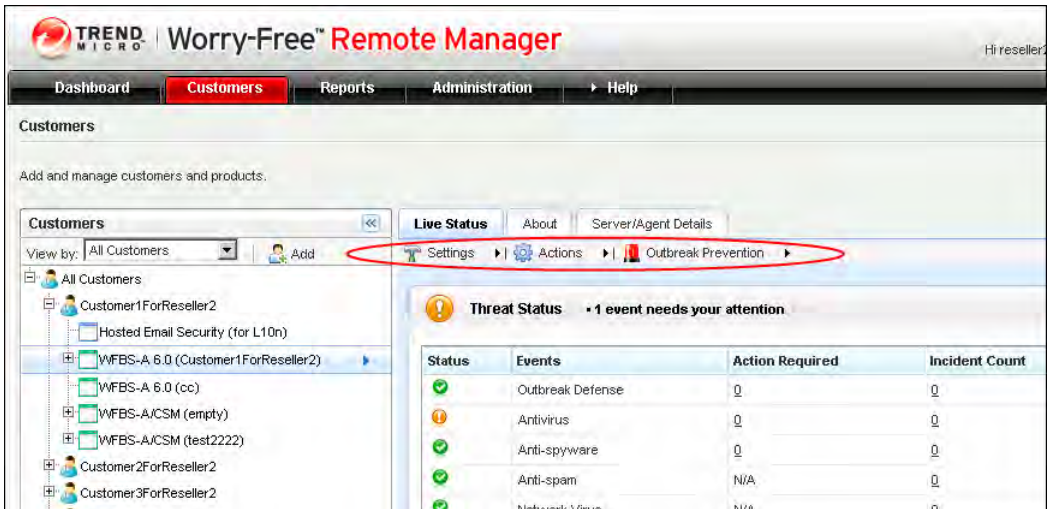



**FIGURE 7-3. Menu Bar**

---

**Note:** Items in the menu bar are disabled and will not respond to mouse clicks if the selected network object cannot receive commands.

---

# All Products

The **All Products** tab on the right pane lists all products of all customers and allows you to delete those products.

To view **All Products**, click **Customers** (tab) **> All Customers** (on the tree) > **All Products** (right pane).

To delete a customer, check the box to the left of the customer and click **Delete**.

Interface items in the **All Products** tab follow:

- **Company Name**
- **Services/Product**
- **Expiration Date**

---

**Note:** New Hosted Email Security data can take as long as three hours before it updates on the WFRM console. Hosted Email Security Customer information is updated once a day. See *Hosted Email Security Settings and Data Updates* on page 7-15.

---

# Managing Customers

The following sections describe how to add, modify and delete customers.

## Adding Customers

See *Adding Customers* on page 3-3

## Modifying Customers

The **Customer Info** tab lets you edit a customer's information.

**To modify a customer's information:**

- Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Customer Info** (tab-right pane) **> Customer Information > Edit**.
- Click the **Customers** (tab) > **All Customers** (on the tree) > right-click {customer} > **Edit Information**.

A pop-up window appears where you can modify information.

## Deleting Customers

**Note:** If you delete a product or service, all the records for this product or service will be deleted. If you wish to re-register the product or service to the WFRM Server, you have to create a Globally Unique Identifier (GUID) for this customer. You also need to reinstall the WFRM Agent on the managed product and use the new GUID.

**To delete a customer from the WFRM Server:**

- Delete all associated products/services from the customer.

  Click the **Customers** (tab) **> All Customers** (on the tree) **>** {customer} > right-click {product/service} **> Delete this Product/Service**.
- Delete the customer from the customer tree.

  Click the **Customers** (tab) > **All Customers** (on the tree) > right-click {customer} > **Delete this Customer**.

# Managing Contacts

The following sections describe how to add, modify and delete contacts.

## Adding Contacts

To subscribe to event notifications and reports, users in your customer's organization first need to be added as contacts.

**To add a contact for a customer:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Contact** (right pane) **> Add**.
2. In **New Contact**, provide the requested information. Note the following fields:
   - **Language:** Whenever possible, WFRM will display text and send reports and notifications in this language.
   - **Email Address:** WFRM will send event notifications and reports to this address.
3. Click **Add**.

## Modifying Contacts

Customers can subscribe to notifications and reports as contacts.

**To modify a customer's contacts:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Contact** (right pane).
2. Check the box next to the contact. Click **Edit**.
3. Edit details as necessary.
4. Click **Save**.

## Deleting Contacts

**To delete a customer's contact:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Contact** (tab-right pane).
2. Check the name next to the contact. Click **Delete**.

# Notifications

Customer notifications for red alerts are sent by email. In addition to the reseller and primary customer contact (from the **Customer Info** tab), contacts must be on the customer contact list (from the **Contact** tab; see *Adding Contacts* on page 7-7) in order to receive notifications.

To add a contact to the notification list, click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Notification** (right pane).

Click the check boxes to determine whether to receive notifications for individual alerts.

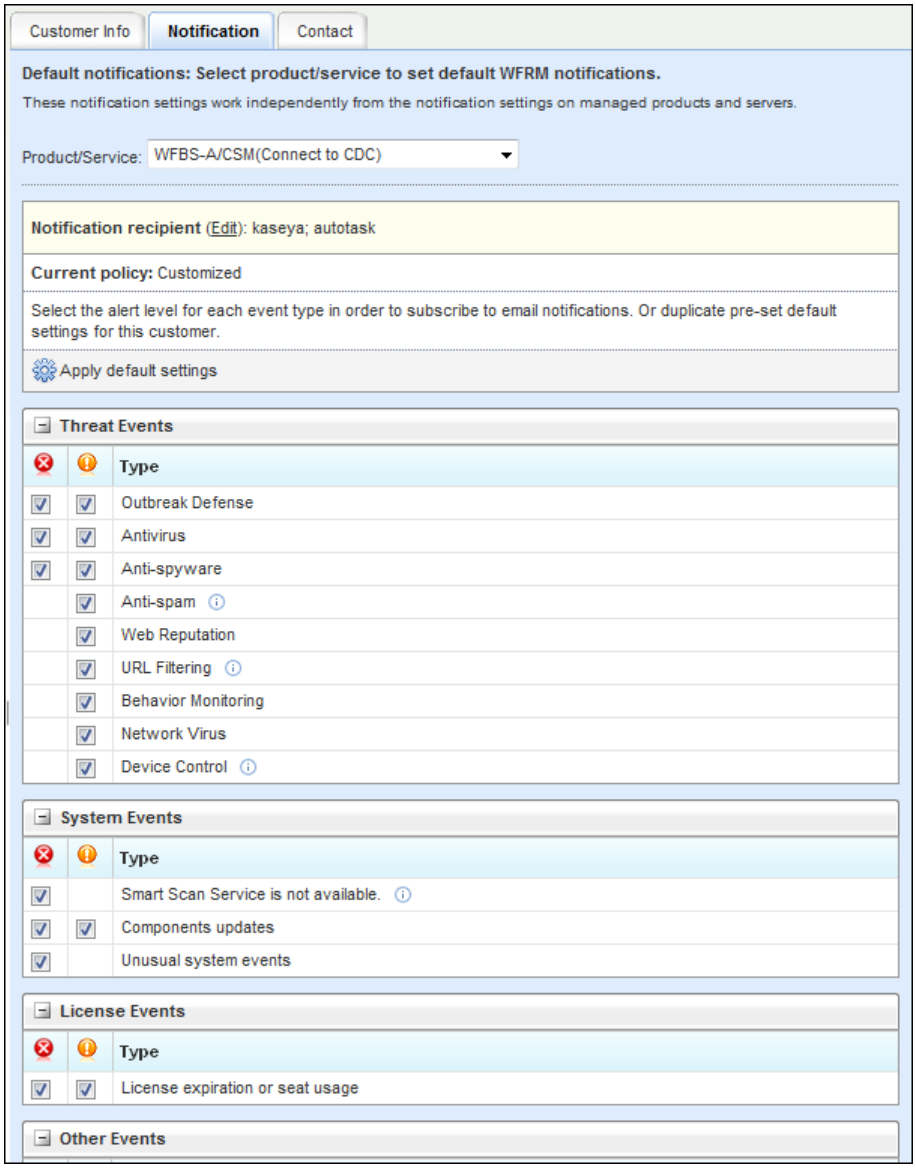



**FIGURE 7-4. Notification Settings**

**To set notifications:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Notifications** (right pane).
2. Select the product or service from the drop-down list.
3. Check the notifications you want to receive.
4. Click **Save**.

Notifications can be any of the following:

**TABLE 7-3. Possible notifications**

| ISSUE | EXPLANATION |
|---|---|
| Agent abnormal | The WFBS(ALL) Agent status is abnormal. |
| Outbreak Defense | Outbreak Defense issue in WFBS(ALL). |
| Antivirus | Antivirus issue in WFBS(ALL). |
| Anti-Spyware | Anti-spyware issue in WFBS(ALL). |
| Web Reputation | Web Reputation issue in WFBS(ALL). |
| Behavior Monitoring | Behavior Monitoring issue in WFBS(ALL). |
| Network Virus | Network virus issue in WFBS(ALL). |
| Anti-Spam | Anti-spam issue in WFBS(ALL). |
| URL Filtering | Unauthorized website access attempt in WFBS 6.0 and 7.0. |
| Device Control | Unauthorized device access attempt in WFBS 7.0. |
| Components Update | The WFBS-S/WFBS-A server and its managed CSA/MSA servers are out of pattern. |
| Unusual System Events | Disk space usage for related WFBS-S/WFBS-A server is above its threshold. |
| License Expiration | The WFBS(ALL) server has license expiration issue (seats issue and license issue). |
| Hosted Email Security Service License Expiration | The Hosted Email Security server has license expiration issue. |
| Client Server Messaging for SMB Shutdown | WFBS-S/WFBS-A server shut-down issue. |
| Exchange Server Shutdown | Exchange server shut-down issue. |
| Report Disk Is About to Run Out | The disk used to store report history is about to run out. |
| Report Disk Full | The disk used to store the report history is full. |

**To edit the notification recipient list:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Notifications** (right pane) **> Edit** (link).

   The Email recipient screen appears.

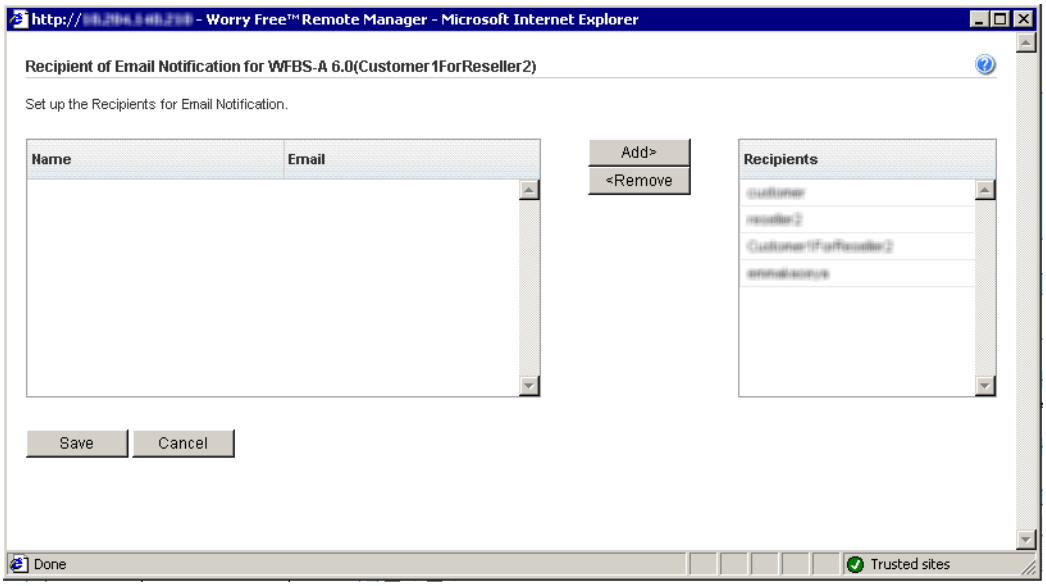



**FIGURE 7-5. Notification Recipient List**

2. Select the recipients you wish to add or remove.
3. Click **Add** or **Remove**.
4. Click **Save**.

# All Agents

Agents allow Worry Free Remote Manager to provide monitoring services to managed products.

To view **All Agents**, click **Customers** (tab) **> All Customers** (on the tree) **> All Agents** (right pane).

Interface items in the **All Agents** tab follow:

- **Customer**
- **Managed Product**
- **Status:** See *Agent Status* on page 8-2
- **Action:** Click **Submit** to send the following commands to Agents:
  - Uninstall
  - Disable
- **Registered:** Date and time the Agent registered to the server

After clicking the **Submit** link, the pop-up will show an additional button called **Purge**. The **Purge** button will delete all information and settings from the Agent and change the Agent back to the "Unregistered" status.

Purge will not work and will be grayed out when the status is "Online".

**Tip:** To sort Agents by status, use the "View by" drop-down list.

# WFBS-S/WFBS-A Commands

The menu bar contains WFBS-S/WFBS-A commands grouped into menus. These commands let you manage critical aspects of security including deploying security components, scanning computers for viruses and known vulnerabilities, and upgrading managed servers.

**Note:** Items in the menu bar disable if you select a tree object that cannot receive commands. You need to select a domain to use any item in the menu bar. Also see *Grayed out menus* on page A-15.

**Note:** The commands in this section are only available for WFBS-S/WFBS-A. For WFBS-SVC and Hosted Email Security, you need to log on to the consoles for those products.

### To submit a command from the Settings menu:

Click **Customers** (tab) > {customer} > {WFBS-S/WFBS-A} **> Live Status** (right pane) > **Settings** > {command}.

For some commands, you may need to specify options through a pop-up window.

**Note:** Before you submit a command, make sure that there is a prior agreement between you and your customer that allows you to do so.

The table below lists the commands of the WFBS-S/WFBS-A Settings menu.

**TABLE 7-4. Settings Menu**

| COMMAND | ACTION | EFFECTS |
|---|---|---|
| Real-time Antivirus/ Anti-spyware | Enable/Disable the real-time Antivirus and Anti-spyware scanners on all computers in the domain. | Real-time scan automatically scans accessed files. Disabling real-time scan will leave the domain at risk. |
| Real-time Scan for POP3 Mail | Enable/Disable Real-time Scan for POP3 Mail for the entire domain. | POP3 Mail Scan (using the Trend Micro Anti-Spam toolbar plug-in) protects computers in real-time against security risks and spam transmitted through POP3 email messages. |
| Behavior Monitoring | Enable/Disable Behavior Monitoring for the entire domain. | Behavior Monitoring protects computers from unauthorized changes to the operating system, registry entries, other software, or files and folders. |
| Location Awareness | Enable/Disable Location Awareness for the entire domain. | With Location Awareness, administrators can control security settings depending on how the Client is connected to the network.<br>This affects "In Office/Out of Office" settings of the Firewall, Web Reputation and TrendSecure toolbars: Anti-Key Loggers, Keystroke Encryption, Page Ratings.)<br>In Office Settings work as the default settings if Location Awareness is disabled.<br>Out of Office Settings are available only if Location Awareness is enabled. |

**TABLE 7-4. Settings Menu (Continued)**

| COMMAND | ACTION | EFFECTS |
|---|---|---|
| Firewall | Enable/Disable the personal firewall for the entire domain. | Depending on existing firewall rules, enabling the firewall can limit the ability of computers to communicate with the network. Disabling can expose computers to unwanted network traffic. |
| Web Reputation | Configure Web Reputation for the entire domain. | Web Reputation helps prevent access to URLs that pose potential security risks by checking any requested URL against the Trend Micro Web Security database. |
| Trend Secure Toolbars | Configure Trend Secure Toolbars for the entire domain. | TrendSecure helps safeguard Internet transactions by determining the safety of wireless connections and the Web page you are visiting. To prevent information theft, TrendSecure can also encrypt information typed into Web pages, including personal information, passwords, and credit card numbers. |
| URL Filtering | Enable/Disable URL Filtering for the entire domain. | Enabling URL Filtering will monitor attempts to access unauthorized websites. This is only available for WFBS-SVC and WFBS-A 6.0 andabove. |
| Device Control | Enable/Disable Device Control for the entire domain. | Enabling Device Control will monitor unauthorized attempts to access devices. This is only available for WFBS-A 7.0. |

**To submit a command from the Actions menu:**

Click **Customers** (tab) > {customer} > **WFBS-S/WFBS-A/WFBS-A 7.0 > Live Status** (right pane) > **Actions** > {command}.

The table below lists the commands of the WFBS-S/WFBS-A Actions menu.

**TABLE 7-5. Actions Menu**

| COMMAND | ACTION | EFFECTS |
|---|---|---|
| Update Client Server Security Agent | Deploy the latest security components, including the scan engine and pattern files, to all Client Server Security Agents (CSA) in the domain. | Ensures that computers are running the latest security components.<br>The deployment can increase traffic between computers and the managed server. |
| Update Managed Server | Deploy the latest security components, including the scan engine and pattern files, only to the Managed Server. | Ensures that computers are running the latest security components.<br>The deployment can increase traffic between computers and the managed server. |
| Sync with Managed Server | Force the WFRM Agent on the Managed Server to resend its data to WFRM Server. | If a domain node in the client tree is clicked but the node does not expand, issue this command to synchronize the servers. |
| Manual Scan | Start or stop a scan for an entire domain or group. | Allows for an on-demand, manual scan. |

The table below lists the commands of the WFBS-S/WFBS-A Outbreak Prevention menu.

**TABLE 7-6. Outbreak Prevention Menu**

| COMMAND | ACTION | EFFECTS |
|---|---|---|
| Automatic Outbreak Defense | Enable or disable automatic deployment of Outbreak Prevention Services (OPS) from TrendLabs. | If automatic deployment is enabled, the behavior of security solutions will automatically change during outbreaks. For example, the spam filter may automatically block certain messages based on general rules provided by TrendLabs.<br>If automatic deployment is disabled, security solutions will not automatically enforce preventive measures during outbreaks, leaving the network without outbreak protection until TrendLabs releases a pattern file. |

**TABLE 7-6. Outbreak Prevention Menu**

| COMMAND | ACTION | EFFECTS |
|---|---|---|
| Current Outbreak Defense Policies | Enable or disable OPS (Outbreak Prevention Services) for ongoing alerts. | Stopping the OPS during an outbreak will stop the deployment of the prevention policy. During an alert, stopping the OPS could leave the network vulnerable to the outbreak malware unless TrendLabs has released a pattern and network administrators have deployed this pattern to the network. |
| Start Vulnerability Assessment | Initiate Vulnerability Assessment (VA) to scan computers in the domain for known vulnerabilities. | Consumes some resources on computers and slightly increases traffic between the managed server and the computers. |
| Start Damage Cleanup Service | Deploy Damage Cleanup Services (DCS) to clean infected computers. | Consumes some resources on computers and can add some traffic between the managed server and the computers. |

# Hosted Email Security Settings and Data Updates

To view Hosted Email Security settings and data including Live Status, Global Settings, and About, click **Customers** (tab) > {customer} > Hosted Email Security.

Hosted Email Security Customer information is updated once a day. This includes:

- All the information under the **Live Status** and **Global Settings** tab.
- **Policy Settings** under the **Global Settings** tab.
- **Approved Senders** under the **Global Settings** tab.
- The **Expiration Date** under the **About** tab (the Expiration Date is the Hosted Email Security AC Expiration Date).

To immediately update Hosted Email Security customer settings on the WFRM console, right-click the Hosted Email Security icon on the Network Tree and click **Sync with Server**.

New Hosted Email Security data can take as long as three hours before it updates on the WFRM console.

# WFBS-SVC Status and Data Updates

To view WFBS-SVC settings and data including Live Status and About, click **Customers** (tab) > {customer} > **WFBS-SVC**.

WFBS-SVC information is updated once a day. This includes:

- All the information under the **Live Status**.
- The **Expiration Date** under the **About** tab (the Expiration Date is the WFBS-SVC AC Expiration Date).

To immediately update WFBS-SVC customer settings on the WFRM console, right-click the Hosted Email Security icon on the Network Tree and click **Sync with Server**.

New WFBS-SVC data can take as long as three hours before it updates on the WFRM console.

# Managed Server / Computer Info

If you select a server or desktop computer on the network tree, WFRM displays information about the computer. The information it displays varies depending on whether the computer is a server/desktop or an Exchange server.

## Server/Desktop

**To see server information:**

Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **>** {product} **>** {group} **>** {Server/Desktop} **> Basic Information** (right pane).

Worry-Free Remote Manager displays the following information when you select a regular desktop or server computer:

- **Basic information:** Computer Name, Status, IP Address, Platform, Platform Version, Managed Product Version, Virus Pattern, Virus Scan Engine, Disk Capacity, Free Disk Space, Minimum Disk Space, Processor Architecture
- **Threat Incidents:**
  - Viruses
  - Spyware
  - Network Viruses
  - Behavior Monitoring
  - Web Reputation
  - URL Filtering
  - Device Control

## Exchange server

**To see exchange server information:**

Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **>** {product} **>** {exchange server} **> Basic Information** (right pane).

Worry-Free Remote Manager displays the following information when you select an Exchange server:

- **Basic Information:** Computer Name, Status, IP Address, Platform, Platform Version, Managed Product Version, Virus Pattern, Virus Scan Engine, Disk Capacity, Free Disk Space, Minimum Disk Space, Exchange Server version
- **Threat Incidents:**
  - Viruses
  - Spam

# Checking Product License

Check your customers' managed server product licenses regularly to ensure continuous protection.

**To check a managed server license:**

Click **Customers** (tab) **>** {customer (on the tree)} **>** {product} **> License Status** (right pane).

# Adding Products/Services

**To add a product or service to an existing customer:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Customer Info** (right pane) **> Add**.
2. Click **Add Product** or **Add Service** and select the product or service to be added.
3. Click **Next**.

   After adding the product, WFRM presents you with the Globally Unique Identifier.

---

**Note:** Save the globally unique identifier (GUID). The GUID is required during the installation of the Agent on the managed server. The GUID is always available. See *Agent GUID* on page 3-7.

---

# Chapter 8

# Managing Worry-Free Remote Manager Agents

This chapter provides information concerning managing Worry-Free Remote Manager Agents installed on WFBS-S/WFBS-A.

**Managing Agents from the WFRM Console:**



**Managing Agents from the Managed Server:**



**Removing Agents:**

# Managing Agents from the WFRM Console

The following sections concern managing WFRM Agents installed on WFBS-S/WFBS-A from the WFRM console.



For information on installing the WFRM Agent, see *Registering WFBS-S/WFBS-A to WFRM* on page 3-7.

## Verifying Agent/Server Connectivity

To ensure that the Worry-Free Remote Manager service is running smoothly, make sure that Agents have a status of "online".

**To view the status of Agents:**

Click the **Customers** (tab) **> All Customers** (on the tree) **> All Agents** (right pane).

The tab lists the status of each Agent in the **Status** column. For details on each status, see *Agent Status* on page 8-2.

Also see *Verifying WFRM Agent Installation* on page 3-9.

---

**Note:** In addition to the current chapter/section, see *Troubleshooting and FAQ* on page A-1 for more issues dealing with Server/Agent connectivity.

---

## Agent Status

The status of a WFBS-S/WFBS-A Agent indicates whether the Agent is able to collect data and receive commands from the WFRM server. The status also indicates the reason why the Agent cannot function properly and how you can handle the situation. The table below describes the different Agent status types.

**TABLE 8-1. Agent status types**

| STATUS | DESCRIPTION | RESOLUTION |
|---|---|---|
| Online | The Agent is running normally. | NA |
| Abnormal | The Agent appears offline and is not responding to the Worry-Free Remote Manager server, but has not sent a logoff request. | This status can occur if the managed server did not shut down properly. Ensure that the managed server administrator is aware of this situation. Contact the administrator if necessary. |
| Disabled | This status is set manually via the console. When an Agent in disabled status, the Agent queries commands from the server every 10 minutes. | Submit a command to enable the Agent (See *Submitting Agent Commands* on page 8-3). |
| Offline | The Agent closed normally after having sent a logoff request to the Worry-Free Remote Manager server. Typically, an Agent is in this status if a user has shut down the Agent service or the managed server has shut down. | Ensure that the managed server administrator is aware that the server has shut down. Contact the managed server administrator if necessary. |

**TABLE 8-1. Agent status types (Continued)**

| STATUS | DESCRIPTION | RESOLUTION |
|---|---|---|
| Unknown | The Agent is not working normally. | Remove the Agent and have the managed server administrator reinstall the Agent. Contact Trend Micro Technical Support if this problem persists. |
| Plug-in errors | The console has detected errors in the Agent's service plug-in component. | Remove the Agent and ask the managed server administrator to re-install the Agent. Contact Trend Micro Customer if this problem persists. |
| Unregistered | The Agent has not registered to the WFRM server. | The Agent may have not been installed or has not been able to communicate successfully with the Worry-Free Remote Manager server. Contact the managed server administrator. |
| Version mismatch | Incompatibility between the versions of any of the following components has been detected:<br>- Agent<br>- WFRM<br>- WFBS-S/WFBS-A | Upgrade the Agent and the managed server. If this does not work, report this problem to the Trend Micro Data Center administrator. |

## Submitting Agent Commands

Agent commands allow you to remotely resolve issues affecting the WFBS-S/WFBS-A Agent. The following commands can be submitted to an Agent depending on the service that the Agent supports and the status of the Agent:

- **Enable:** Restores the Agent from disabled status to normal functionality.
- **Disable:** Agent stops collecting information but continues to query the server for commands every 10 minutes.
- **Uninstall:** Agent removes itself from the managed server.
- **Upgrade plugin:** Agent downloads and installs updates.

**Note:** Commands in this section are for WFBS-S/WFBS-A only. To issue commands for WFBS-SVC, you must log on to the WFBS-SVC console.

**Note:** If an Agent is in abnormal/unregistered status, you cannot submit a command to it.

**To submit a command to an Agent:**

1. Click **Customers** (tab) **> All Customers** (on the tree) **> All Agents** (right pane).
2. Click **Submit** under the **Action** column.
3. In the pop-up window, select a command from the drop-down list and click **Submit**.

## Viewing Agent Details

**To view Agent details:**

Click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> WFBS-S/WFBS-A > Server/Agent Details** (right pane) **> WFRM Agent Details**.

The following can be viewed:

- **Company Name**
- **GUID:** Globally unique identifier; Worry-Free Remote Manager generates this string automatically. Provide the GUID to the administrator who will install the Agent program.
- **IP Address:** IP address of the server where the Agent is installed
- **Registered On**
- **Last Update:** Date and time the Agent was last updated
- **Agent Version**
- **Managed Product:** Product managed through the Agent
- **Managed Product Version:** Version of the product managed through the Agent

# Managing Agents from the Managed Server

The following sections concern managing Agents from the managed server.


- *Agent Status Messages* on page 8-4
- *Changing the Agent GUID on the Managed Server* on page 8-6
- *Agent Configuration* on page 8-6


## Agent Status Messages

On the managed server, the Agent displays one of the following system tray icons:

**TABLE 8-2. System tray icons**

| ICON | DESCRIPTION |
|---|---|
|  | A green icon indicates that the Agent is connected to WFRM's communication server. The Agent is working normally. |
|  | A red icon indicates that the Agent isn't connected to WFRM's communication server or the version of the Agent is mismatched with the server and needs to be updated. |
|  | An icon with a red arrow indicates that the Agent has logged off from WFRM. |
|  | An icon with a red "X" means that the Agent has been disabled. |

Whenever you move your mouse over the system tray icon, it displays a status message that indicates whether the Agent is functioning normally. These are listed in the table below:

**TABLE 8-3. Status messages displayed by the Agent's system tray icon**

| | |
|---|---|
| Message | Unknown error encountered. Check the system or restart the Agent. |
| Description | Unexpected errors, typically system errors, are preventing the Agent from functioning properly. |
| Resolution | Check the managed server for low memory or other system problems. |
| Message | Unable to register with the remote server. |
| Description | The GUID you provided may be incorrect or there may be a network issue. |
| Resolution | There are two situations that may cause this:<br>1) Verify that you have used the correct GUID. See *Agent GUID* on page 3-7 to find the correct GUID on the WFRM console, and see *Unable to Register with the Remote Server* on page A-7 to check (and possibly change) the GUID on the Agent.<br>2) If the network has an issue, the Agent cannot connect to the server. Check the network connection between WFBS-S/WFBS-A server and the WFRM server. |
| Message | Unable to connect to the remote server. |
| Description | The managed server may be experiencing Internet connectivity problems. |
| Resolution | Check Internet connectivity on the managed server. Also, check the Agent's proxy settings and the specified server address and port. |
| Message | Agent disabled by Worry-Free Remote Manager. |
| Description | The Agent has been temporarily disabled through the Worry-Free Remote Manager console. |
| Resolution | Enable the Agent through the Worry-Free Remote Manager console. |
| Message | Agent does not match the Client Server Messaging Security (CSM). |
| Description | The CS/CSM and Agent versions do not match. |
| Resolution | Upgrade the CS/CSM server to the latest version and install the latest Agent. |
| Message | Agent service stopped. |
| Description | Agent has logged off from WFRM. |
| Resolution | Start the Agent service by right-clicking the Agent system tray icon and clicking **Start Service**. |
| Message | Unable to load components. You may need to reinstall the Agent. |
| Description | The Agent encountered problems while loading some components. |
| Resolution | First try restarting the Agent service by right-clicking the Agent system tray icon and clicking **Restart Service** or **Start Service**. If this does not work, uninstall and then reinstall the Agent. Make sure you use the same GUID. |

## Changing the Agent GUID on the Managed Server

Use this procedure only if you entered an incorrect Globally Unique Identifier (GUID) during WFRM Agent installation:

1. Go to `"C:\Program Files\Trend Micro\WFRMAgentForCSM"`.
2. Open the `AgentSysConfig.xml` file using a text editor.
3. Look for the GUID between the parameters `<AgentGUID>` and `</AgentGUID>`.
4. Edit the GUID and then save the file.
5. In the same folder, open the `csmSysConfig.xml` file using a text editor.
6. Look for the GUID between the parameters `<ProductGUID>` and `</ProductGUID>`.
7. Edit the GUID and then save the file.
8. Right-click the Worry-Free Remote Manager Agent icon on the task bar and then click Restart Service.

## Agent Configuration

The Agent Configuration Tool allows changes to be made to WFRM Agent configuration settings.

**To start the Agent configuration tool:**

Click **Start > Programs > Worry-Free Remote Manager Agent > Agent Configuration Tool**.

### Agent Configuration Menu

To configure the Agent, right click on the tray icon to open the following menu:

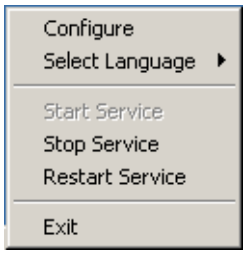



**FIGURE 8-1. Agent Configuration Tool pop-up menu**

The following items appear:

- **Configure:** Opens the Agent configuration screen (see *Configuration Tool Main Dialog* on page 8-7).
- **Select Language:** In addition to other possible languages, the "English" language always exists.
- **Service:** Start, Stop, Restart.
- **Exit:** Exiting the tool does not stop the WFRM service. It only closes the Configuration Tool and removes the icon from the task bar. The tool can be restarted at any time (See *Agent Configuration* on page 8-6).

## Configuration Tool Main Dialog

Right click on the tray icon and click **Configure** on the Agent configuration menu to open the Agent configuration tool **General** screen.

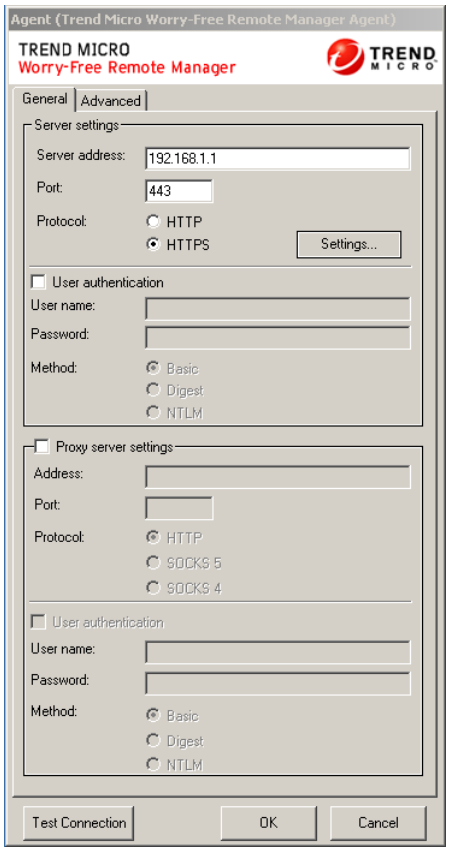



**FIGURE 8-2. Agent Configuration Tool "General" tab**

## Configuration Tool General Panel

The following sections of the Agent configuration screen are the only presently relevant sections of this tool.

### Server Settings

Configure server communication by setting the following:

- **Server address:** The fully qualified domain name (FQDN) of the Worry-Free Remote Manager communication server. The FQDN varies in each region as follows:
  - **Asia Pacific:** `wfrm-apaca.trendmicro.com`
  - **Europe and the Middle East:** `wfrm-emeaa.trendmicro.com`
  - **Japan:** `wfrm-jpa.trendmicro.com`
  - **Latin America:** `wfrm-lara.trendmicro.com`
  - **North America:** `wfrm-usa.trendmicro.com`
- **Port:** The port that the WFRM server uses to communicate with the Agent. This should be 80 for HTTP and 443 for HTTPS.
- **Protocol:** The protocol used for communication between the server and the Agent.

### Proxy Server Settings

Enable this area by clicking the **Proxy server settings** checkbox if the user's network requires a proxy to communicate with the WFRM server.

- **Address:** The IP address of the proxy server
- **Port:** The port or the proxy server
- **Protocol**

### Test Connection button

The **Test Connection** button is used to test communication between the Agent and the WFRM server. Use this function to test if the basic connection to the communication server works well. If it fails (a popup dialog box will appear if the tool cannot connect to the server), there may be a basic issue such as the address of the communication server and its port, or the Proxy server address and its port.

# Removing Agents

A WFRM Agent can be removed either locally from the managed WFBS-S/WFBS-A server or remotely from the WFRM console.

## Removing Agents Locally

**WARNING!** **When removing Agents locally, the Agent will unregister from Worry-Free Remote Manager which automatically deletes all data associated with the Agent. To prevent the Agent from unregistering (and deleting its data), modify the Server address value on the Agent interface before removing the Agent.**

There are three ways to remove an Agent locally:

1. Directly uninstall the WFRM Agent.
2. Uninstall the WFRM Agent via the Control Panel.
3. Uninstall the WFRM Agent manually.

**Note:** Agents can also be removed remotely from the WFRM console.

**Note:** Also see *Backing Up and Restoring Agent Settings* on page A-8.

#### Option 1: Directly uninstall the WFRM Agent:

1. Open the WFRM Agent installation file (`WFRMAgentforCSM.exe` or `WFRMAgentforWFBS.exe`).
2. Click **Yes** to confirm the **Confirm Uninstall** dialogue box.

   **Note:** During removal, you will be prompted to close certain applications. Close these applications and click **Retry** to continue.

3. Click **Finish** to close the wizard after the uninstallation is complete.

### Option 2: Uninstall the WFRM Agent via the Control Panel:

1. Open the Control Panel's **Add or Remove Programs** applet (or **Programs and Settings** on Windows Vista™).
2. Select **Worry-Free Remote Manager Agent** and then click the **Change/Remove** button.

### Option 3: Uninstall the WFRM Agent manually:

If for any reason an Agent cannot be removed through standard ways, perform the following steps to manually remove it:

1. Stop the **Trend Micro Worry-Free Remote Manager Agent** service.
   a. Click **Start > Run**.
   b. Type `"cmd"` on the command line and then press the **Enter** key.
   c. Run the following command:

      ```
      net stop Trend Micro Worry-Free Remote Manager Agent
      ```
2. Remove the Trend Micro Worry-Free Remote Manager Agent service.
   a. On the command line, use the change directory (cd) command to go to the WFRM Agent directory.
   b. Run the following command:

      ```
      TMICAgent -u
      ```
3. Remove the program files.

   `Delete` {Agent install directory} `/ WFRMAgentForCSM`
4. Open the Registry Editor (`regedit.exe`) and remove the following registry keys:

---

**Note:** 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`.

---

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMIC4CSM\Agent\..
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products\
23FC8F347B51DD440AD13A73D13A73D22D58E6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Installer\UserData\S-1-5-18\Products\
23FC8F347B51DD440AD13A73D13A73D22D58E6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall\{43F8CF32-15B7-44DD-A01D-A3372DD2856E
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall\InstallShield Uninstall Information\
{43F8CF32-15B7-44DD-A01D-A3372DD2856E}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Uninstall\InstallShield_\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}
```

5. Remove the WFRM Agent shortcut from the Start menu.
   a. On the desktop, click **My Computer**.
   b. Change the current directory to `..\Documents and Settings\All Users\ Start Menu\Programs`.
   c. Delete the Worry-Free Remote Manager Agent folder.

## Removing Agents Remotely

Agents allow Worry Free Remote Manager to provide monitoring services in customer environments. To remove an Agent, remotely uninstall the Agent and then delete the product on the WFRM console associated with the Agent.

**Tip:** To temporarily stop an Agent from sending data and querying commands, submit the Disable command (see *Submitting Agent Commands* on page 8-3).

### To uninstall the WFRM Agent remotely:

1. Click the **Customers** (tab) **> All Customers** (on the tree) **> All Agents** (right pane).
2. Put a check by the Agent or Agents you wish to uninstall.
3. Select Uninstall on the dropdown.
4. Click the **Submit** link in the **Action** column.

# Chapter 9

# Managing Reports

This chapter covers the following topics:

# Reports Overview

Trend Micro™ Worry-Free™ Remote Manager lets you generate, download, and automatically send out reports. Reports provide an overview of license status, assessment results, security incidents, major threats, and the most affected computers, files and email addresses in your customers' networks.

Reports include a range of statistics from WFBS(ALL)[1] and Hosted Email Security[2]. WFRM allows for report profiles, one-time and periodic reports, date ranges, multiple formats, and multiple email recipients. WFRM enables you to save reports up to the present limit of 512MB. General reports are suitable for resellers and customers. Detailed reports are most suitable for resellers.

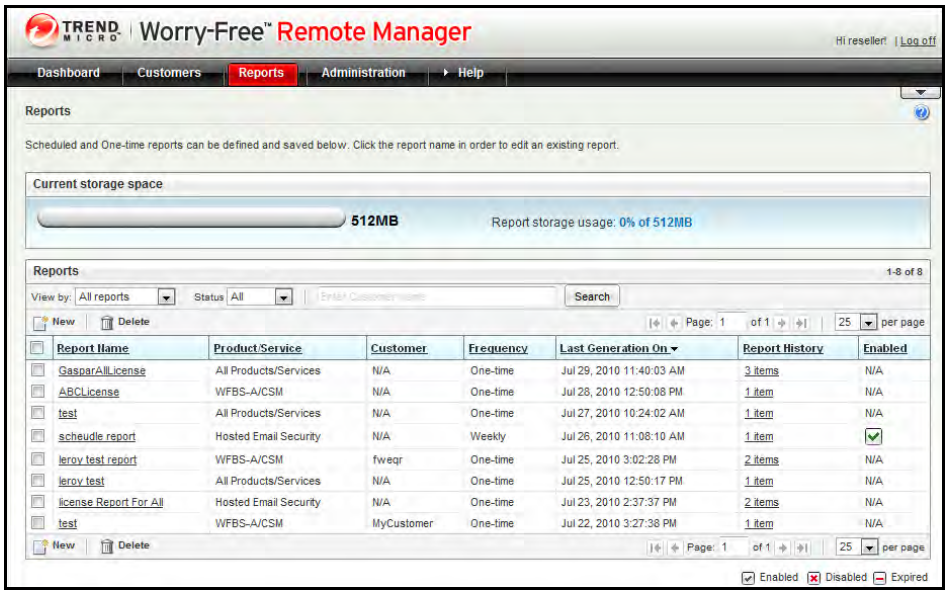



**FIGURE 9-1. Reports Page**

Report profiles enable you to create multiple reports from a single profile. For example, you can create a one-time report today, generate that report, and tomorrow, change some options and regenerate without having to recreate the entire report.

Worry-Free Remote Manager currently supports general and detailed reports.

**The General Report for WFBS provides the following information:**

- Spyware/Gateway action results summary
- Spam Daily/Weekly/Monthly detection summary
- Network Viruses
- Behavior Monitoring
- Vulnerability Assessment (daily report only)
- Outbreak Defense (daily report only)
- Managed product license information
- Managed product pattern file status

1. WFBS(A), WFBS(S), and WFBS-SVC are collectively referred to as WFBS(ALL) where appropriate.
2. InterScan Messaging Hosted Security was renamed to Hosted Email Security in WFRM 2.2 SP1.

**The Detailed Report for WFBS provides the following information:**

- Product/Service Summary
- Weekly Internal Virus/Malware Outbreak Summary
- Top 10 High Risk Computers Including 5 Most Prevalent Viruses/Malware
- Top 10 Virus/Malware and Top 5 Machines Infected by these Viruses/Malware.
- Top 10 Virus/Malware Infection Sources
- Spyware Detection Summary (monthly report only)
- Top 10 High Risk Computers Including 5 Most Prevalent Spyware/Grayware
- Top 10 Spyware/Grayware and Top 5 Machines Infected by this Spyware/Grayware
- Prohibited Web site URLs that Users Most Frequently Attempted to Access
- DAC Policy Detail

---

**Note:** For WFBS-SVC, there is only a General report.

---

**The General Report for WFBS-SVC provides the following information:**

- Desktop/Server Virus Summary
- Desktop/Server Spyware/Grayware Summary
- Top 5 Desktops with Virus Detections
- Top 5 Servers with Virus Detections
- Top 10 Network Viruses Detected
- Top 10 Computers Attacked
- Top 5 Desktops with Spyware/Grayware Detections
- Top 5 Servers with Spyware/Grayware Detections
- Top 10 Computers Violating Web Threat Protection Policies
- Top 5 Programs Violating Behavior Monitoring Policies
- Top 10 Computers Violating Behavior Monitoring Policies
- Top 5 URL Category Policies Violated
- Top 10 Computers Violating URL Category Policies

---

**Note:** For Hosted Email Security, there is only a General report.

---

**The General Report for Hosted Email Security provides the following information:**

- Top Virus Recipients
- Top Spam Recipients
- Threat Summary
- Total Email Traffic

**The Summary License Report for all products provides the following information:**

- Full and Trial License Distributions
  - Full Licenses expired and not renewed
  - Trial Licenses expired and not converted
  - Full Licenses expiring in 60 days
  - Full Licenses expiring in 30 days
  - Trial Licenses expiring in 14 days

- Companies with a seat count at 80% to 100% of available seats
- Worry-Free Business Security Advanced detailed license information for all customers
- Worry-Free Business Security Standard detailed license information for all customers
- Worry-Free Business Security Services detailed license information for all customers
- Hosted Email Security detailed license information for all customers

**The Summary License Report for one product provides the following information:**

- License summary for all products/services
  - License distribution
  - Full license expiration status
  - Trial license expiration status
  - Detail license information listed by expiration date
- Seats count summary for all products/services
  - Detail license information listed by seat count usage

Detail license information

# Report Settings

WFRM enables you to save reports up to a limit of 512MB. In order to more efficiently use this space, you can set the number of saved reports per profile.

To change the number of saved reports per profile, click **Administration** (tab) **> Personal Settings**. Set the number of saved reports for daily, weekly, and monthly reports.

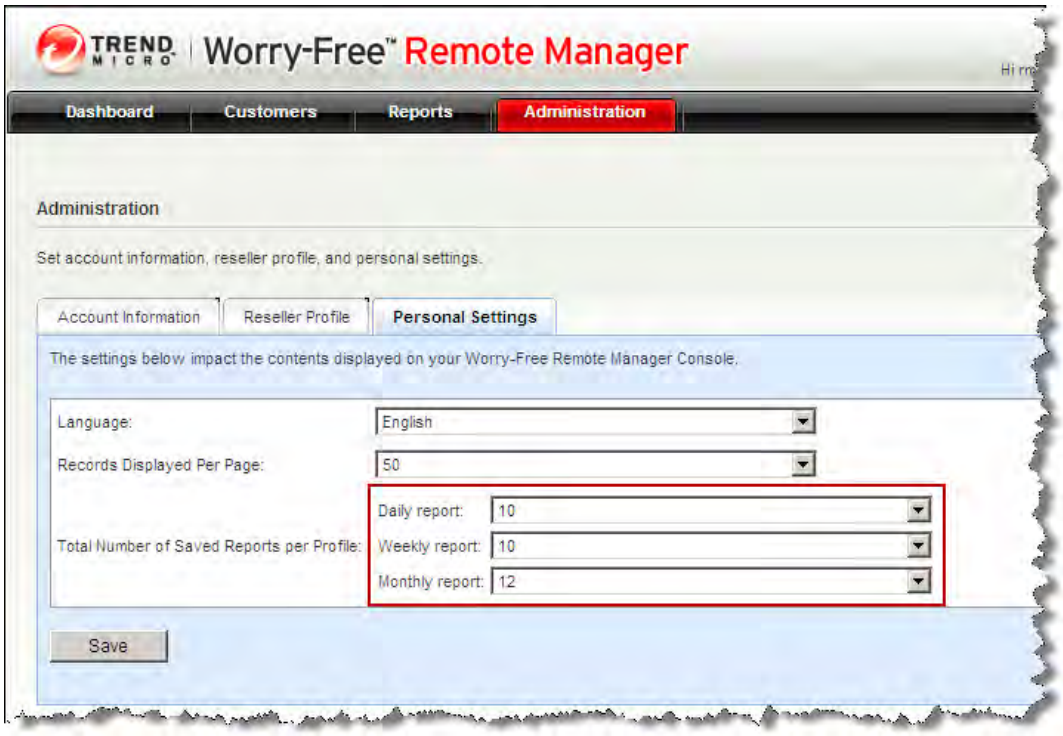



**FIGURE 9-2. Report Settings**

When the limit is reached and a new report is generated, the oldest report is replaced by the latest one.

# Creating Reports

WFRM offers the following ways to create a report template:

- Click an existing report, modify the report, and click **Save As** at the bottom of the screen.
- Create a new report template.
- Click the right-mouse button on a customer and select **New report**.

**To create a new report template:**

---

**Tip:** You can click the **Customers** (tab) > **All Customers** (on the tree) > right-click {customer} > **New report** to create a report for a particular customer.

---

1. Click **Reports** (tab) **> New**.

   The New Report screen appears.

2. Type the **Report Settings**:
   - **Name**
   - **Report Type**

   ---

   **Note:** General and detailed reports for Hosted Email Security are currently identical in this version of WFRM.

   ---

3. On the **Select report data** section, select data for your report. Select to filter the data by **Customer** or **Product/Service**.

   For example, if you select **Customer**, the drop-down list populates with all of your customer names. Clicking a customer name displays that customer's products in the first box. Selecting the customer product in the first box displays all products by version for the product name in the second box. Selecting a Hosted Email Security service displays a third box so you can select the Hosted Email Security domain.

   ---

   **Note:** If the reseller is not connected to the customer's server or there is no data, information does not display for the customer.

   ---

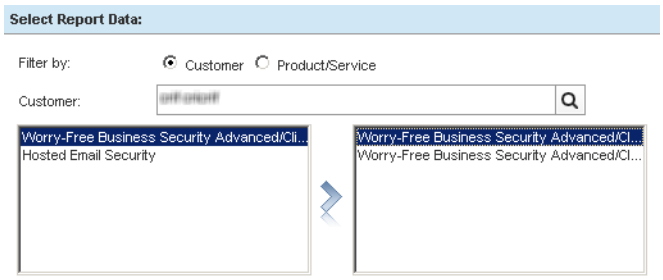



**FIGURE 9-3. Report Data Selections**

4. Select the **Report Timeframe**:

   **One-time report:**

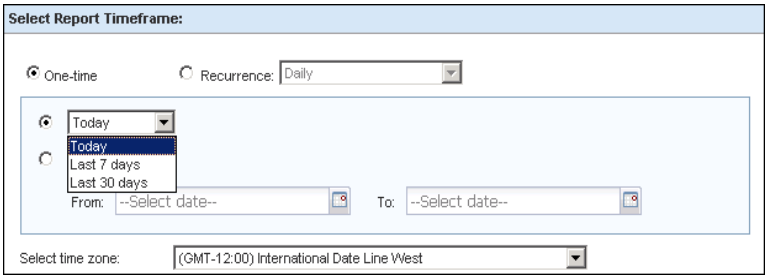



**FIGURE 9-4. Report Timeframe**

**TABLE 9-1. One-time Report Options**

| OPTION | DESCRIPTION |
|---|---|
| Today | Calculates the report with data received from 12 midnight up until the moment the report is generated (based on the selected time zone). |
| Last 7 days | Calculates the report with the last 7 days' data (excluding today's data). |
| Last 30 days | Calculates the report with the last 30 days' data (excluding today's data). |
| Specific range | The "From" date must be later than or equal to the first date of the last month (WFRM only stores the last and current month's data); the "To" date cannot be later than today. |

**Recurring report:**

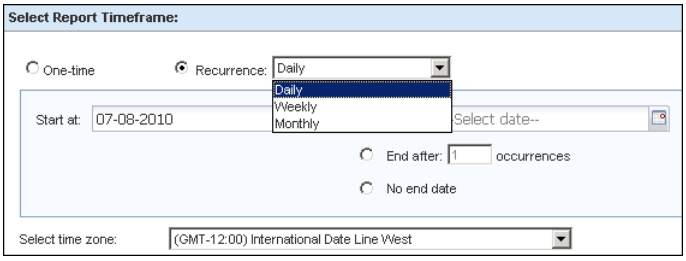



**FIGURE 9-5. Select Report Timeframe: Recurrence**

**TABLE 9-2. Recurring Report Options**

| OPTION | DESCRIPTION |
|---|---|
| Daily Report | The end date must be later than today. Then every day in the specified range generates a report based on the previous day's data.<br>For example, if the range is set from Jan-27-2009 to Jan-29-2009, then:<br>• On the 27th, WFRM generates a report based on the 26th<br>• On the 28th, WFRM generates a report based on the 27th<br>• On the 29th, WFRM generates a report based on the 28th |
| Weekly Report | WFRM generates the weekly report every Monday using the previous week's data. Therefore, to generate a report for this week, set the end date to at least Monday of the following week. |
| Monthly Report | WFRM generates the monthly report every second day of the month using the previous month's data. This means that to generate a report for this month, set the end date to at least the second day of the following month. |

5. Set the **Report Content**. This includes the following report format elements:
   - **Report format:** PDF, DOC, XLS, or XML
   - **Report language**
   - **Customer logo:** The customer logo is optional. Customer logo must be a .png, .jpg, .bmp, or .gif image with a suggested size of width 270 x height 40 pixels.
   - **Note:** The note field is for internal use and does not display on the report itself.

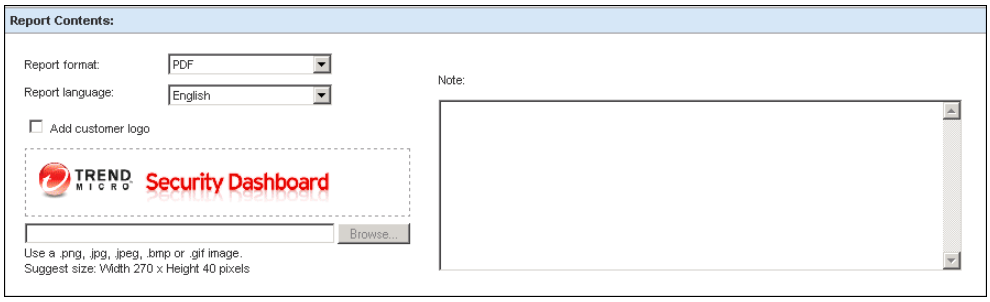



**FIGURE 9-6. New Report - Report Contents**

6. Specify **Notification** email. Recipients under Email options come from the companies contact list. See *Adding Contacts* on page 7-7.
7. Click **Save**.

   WFRM adds the report template to the list of report templates.
8. Click the report item in the Report History column to view the report.

# Editing Reports

To edit a report, click **Reports** (tab) **>** {report name}**.**

# Viewing Reports

To view a report that has already been generated, click **Reports** (tab) > {item or number of items under **Report History**} **>** {file under **View Report**}.

# Subscribing to Reports

**To subscribe contacts to reports:**

1. Click **Reports** (tab) **>** {report name} **> Email Options**:
2. Select the name of the contact.
3. Click **Add** to add the contact to the **Recipients** list, or manually type in a new email address.
4. Revise the subject line as desired.
5. Click **Save**.

---

**Note:** The list of possible email recipient when creating reports comes from **Customers** (tab) **>** {customer} **> Contact** (right pane)

---

# Sending and Downloading Reports

You can download and send reports to recipients. Although recipients were specified when you defined the report, the recipient list can be modified. See *Subscribing to Reports* on page 9-8.

**To download a report:**

1. Click **Reports** (tab) **>** {number under **Report History** column} **>** {report type under **View Report**}.
2. Save the report after it opens.

**To send a report:**

1. Click **Reports** (tab) **>** {number under **Report History** column}.
2. Check the box to the left of the report, and click **Send**.

# Appendix A

# Troubleshooting and FAQ

The following sections discuss issues you may encounter while working with Worry-Free Remote Manager and possible solutions you can try before calling technical support (although these are organized by server, Agent and other, they often cross lines):

**Troubleshooting**



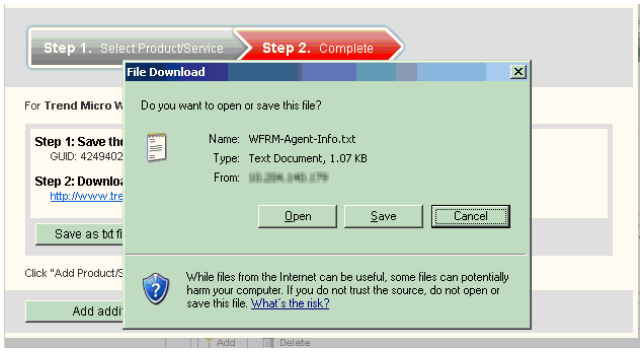
**FAQ**

# Troubleshooting Issues Dealing (largely) with the WFRM Console

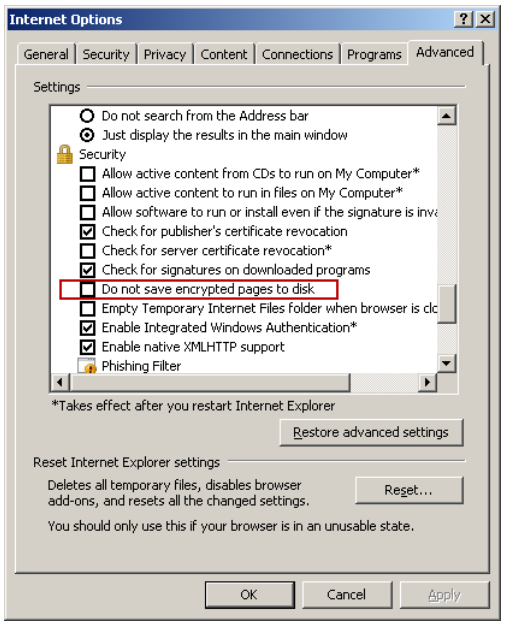
Issues in this section are seen from the WFRM console.

## "Save as txt file" doesn't work

When adding a product, then trying to "Open" the file after choosing "Save as txt file" in Internet Explorer 6, why doesn't it work?




The Internet Explorer 6 default setting doesn't support opening file downloads via HTTPS.




In order to fix this (IE 6.0 only), click **Tools > Internet Options > Advanced > Security** and uncheck, "Do not save encrypted pages to disk".

## Domain Tree not Visible after Installing the Agent

The domain tree does not appear on the console after you install the Worry-Free Remote Manager Agent on the managed server.

There are two possible reasons why this happened:

1. The Globally Unique Identifier (GUID) is incorrect.
2. The WFRM Agent cannot communicate with the Worry-Free Remote Manager Server.

**To fix the issue:**

Make sure that the GUID (steps 1 - 4) entry is correct:

1. On the Security Server, use a text editor like Notepad to open "C:\Program Files\Trend Micro\WFRMAgentForCSM\AgentSysConfig.xml".
2. Check the GUID right after the parameter.
3. If you corrected the GUID, save the file then restart the Trend Micro Worry-Free Remote Manager Agent service.
4. Check the status of the customer's domain from the Worry-Free Remote Manager Server after a couple of minutes.

   Check the Agent-Server connection using the Test Connection feature (steps 5 - 7):
5. Click **Start > Programs > Worry-Free Remote Manager Agent > Agent Configuration Tool**.
6. Click the Test Connection button.
7. If the test connection fails:
   a. Check if the managed server can connect to the Internet.
   b. Check if you entered the Worry-Free Remote Manager Server address correctly.
   c. If the Security Server uses a proxy to connect to the Internet, make sure that you also entered the proxy server settings.

## Node on Tree Cannot Be Expanded

If a node on the domain tree (under the **Customers** tab) does not expand when clicked, group and client information on the WFBS server and the WFRM server may be out of sync. To remedy this, right-click the node, then click **Action > Sync with Managed Server** to resend data from the Agent to the WFRM server.

## Page Cannot be Displayed

"Page cannot be displayed" shows up when trying to open the Worry-Free Remote Manager Server URL.

The error shows up in Microsoft Internet Explorer (MSIE) when you try to access

http://wfrm.trendmicro.com/

This happens if:

- The URL is incorrect.
- The WFRM Server's URL is not an MSIE Trusted Site.

**To fix the issue:**

Make sure that the WFRM Server's URL is an MSIE Trusted Site.

1. Open MSIE.
2. Click **Tools > Internet Options > Security > Trusted Sites > Sites**.
3. Check if the WFRM Server URL is in the list. If not, type it in and then click **OK**.

## Unable to Receive Notifications

If email notifications are not being received even though contacts are set to receive these notifications, check for the following:

- **Incorrect Notification Address** (for customer): To set the correct notification information, click **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> Contact >** {contact name} **> Email**
- **Incorrect Notification Address** (for reseller): To set the correct notification information, click **Administration > Account Information > Email**

## Incorrect Information on the Dashboard

If the dashboard seems to be giving you incorrect or incomplete information about a particular domain, check the following:

- Check if the managed server is started.
- Check if the Agent is started and running correctly.
  - Check the WFRM console at **Customers** (tab) **> All Customers** (on the tree) **>** {customer} **> WFBS-S/WFBS-A > Server/Agent Details** (right pane) **> WFRM Agent Details** (see *Agent Status* on page 8-2).
  - Check the status of the Agent on the managed server (see *Managing Agents from the Managed Server* on page 8-4) . Also see *Verifying WFRM Agent Installation* on page 3-9.
- Check if the customer re-installed the Agent. Also check if the customer re-installed the Agent and used a different or duplicate GUID. By default, the Agent should get up to the last three days of data from the managed server.
- You can try generating a new GUID and re-installing the Agent.

## Unable to Deploy Commands

If you are unable to deploy network commands to an Agent, check the following:

- WFBS-S/WFBS-A service is running.
- Client Agent is running. If not, to start the Agent, see *Agent Service* on page 3-10.
- Ports 80 and 443 are open. You can check this by telneting from the Worry-Free Remote Manager server to the Agents on ports 80 and 443 and vice versa. If the ports are not open, the customer administrator must open the ports on their firewall.

## Agent Status Is Abnormal

Several reasons can cause the Agent to be abnormal. To remedy this:

Agent status will be abnormal if the Agent did not send a logoff request to the Worry-Free Remote Manager server before the Agent shut down. To fix this, restart the Agent service (see *Agent Service* on page 3-10).

If this does not resolve the problem, open the Agent configuration tool by right-clicking the Agent icon and clicking **Configure**. Click the **Test Connection** button to test the network connection to the WFRM server.

If you receive an error, check your firewall policy.

If the connection is OK, inspect the Agent log (See *Agent logs and configuration files location* on page A-10).

If the problem is critical and can be reproduced after restarting the Agent service, enable the debug log (See *Enabling the Agent debug log* on page A-9) and contact Trend Micro support.

## WFRM reports a version mismatch

If this occurs, first wait about 5 to 10 minutes. The Agent should upgrade itself automatically. If the issue has existed for a long time, perform the following steps:

1. Check that the network and Internet Explorer are working normally.
2. Check that the disk where the WFRM Agent is installed is not full and that the size of directory "`<install path>\windows\temp\`" is not restricted.
3. Use Internet Explorer to download the Agent upgrade package from the URL provided by Trend Micro Support.
4. Unzip the download package. Double click `TMICPluginUpgrade.exe`. If you receive an error, check the upgrade log in `C:\TMpatch.log`.

5. Check the Agent status. If the icon turns green, the Agent is working normally. If it is still red, again, check the upgrade log.

   In addition to the preceding steps, perform the following steps to obtain more information about the Agent version:

   Open the Agent configuration file on the WFBS server called:

   `<Install Path>\Trend Micro\WFRMAgentForCSM\AgentSysConfig.xml`

   platform version (between `<Build>` and `</Build>`):

   ```
   <Version>2.5</Version>
   <ServicePackVersion>0</ServicePackVersion>
   <Build>1255</Build>
   <Language>0</Language>
   ```

   plugin version (between `<PluginHotfixVersion>` and `</PluginHotfixVersion>`:

   ```
   <PluginSPVersion>0</PluginSPVersion>
   <PluginHotfixVersion>1207</PluginHotfixVersion>
   <PluginType>256</PluginType>
   ```

6. Send the version information and GUID to Trend Micro support.

### Agent working abnormally using an existing GUID after ...

Why doesn't the Agent work normally using an existing GUID after reinstalling the operating system, reinstalling the WFRM Agent, changing the machine's network card, or installing an Agent on another machine?

Before performing any of the operations mentioned above, the Agent should first be uninstalled in order to delete existing information on the WFRM server. If this is not done, an Agent using an existing GUID will work abnormally.

## Troubleshooting Issues Dealing (largely) with the Agent

Issues in this section are seen from the managed WFBS-S/WFBS-A servers.


- *Unable to Connect to the Server* on page A-6
- *Unable to Register with the Remote Server* on page A-7


### Unable to Connect to the Server

The following error message shows up when you click the **Test Connection** button in the Agent Configuration Tool of WFRM:

"Unable to connect to the server. It may be invalid settings. Enter valid settings and try again."

There are three possible reasons for this:

1. The managed server cannot connect to the Internet. Make sure WFBS-WFBS-A can access the Internet.
2. The FQDN of the Worry-Free Remote Manager communication server address is incorrect.

   Use the FQDN that corresponds to your region:

   - **Asia Pacific:** `wfrm-apaca.trendmicro.com`
   - **Europe and the Middle East:** `wfrm-emeaa.trendmicro.com`
   - **Japan:** `wfrm-jpa.trendmicro.com`
   - **Latin America:** `wfrm-lara.trendmicro.com`

- **North America:** `wfrm-usa.trendmicro.com`

3. If the Security Server uses a proxy server to connect to the Internet, make sure the proxy and user authentication settings are correctly configured.

## Unable to Register with the Remote Server

"Unable to register with the remote server" shows up when the mouse is moved over the Worry-Free Remote Manager Agent icon.

This happens when the Globally Unique Identifier (GUID) is incorrect.

**To fix this issue:**

1. Go to `<install path>\Trend Micro\WFRMAgentForCSM`.
2. Open the `AgentSysConfig.xml` file using a text editor.
3. Look for the GUID between the parameters "`<AgentGUID>`" and "`</AgentGUID>`".
4. Edit the GUID and then save the file.
5. In the same folder, open the `csmSysConfig.xml` file using a text editor.
6. Look for the GUID between the parameters "`<ProductGUID>`" and "`</ProductGUID>`".
7. Edit the GUID and then save the file.
8. Right-click the Worry-Free Remote Manager Agent icon on the task bar and then click **Restart Service**.

# Other Troubleshooting Issues



## Resetting a Lost Password

If you forgot your WFRM password, click the **Forgot your password** link on the Worry-Free Remote Manager login page.

If you cannot reset your password because the system tells you that you are entering an invalid email address, send a password reset request to the email address corresponding to your region:

- **Asia Pacific:** wfrm_apacsupport@trendmicro.com
- **Europe/Middle East:** wfrm_emeasupport@trendmicro.com
- **Latin America:** wfrm_larsupport@trendmicro.com
- **North America:** wfrm_support@trendmicro.com

Include the following information in your email:

- User name
- Phone number
- Office address
- Primary distributor

## Backing Up and Restoring Agent Settings

If you need to uninstall and then reinstall the Agent using the same GUID within a span of three days, keep the Agent settings to avoid any overlapping data. To do this, back up the configuration files manually and then replace the configuration files with the backup after reinstalling the Agent.

**To back up the configuration files:**

1. On the managed server, right click the Agent system tray icon and click **Stop Service** to stop the Agent service.
2. Copy all the `.xml`, `.dat`, and `.ini` files from the installation folder `C:\Program Files\Trend Micro\WFRMAgentforCSM`. These files are listed below:

**TABLE A-1. Agent configuration files**

| .XML FILES | .DAT FILES | .INI FILES |
|---|---|---|
| csmSysConfig.xml | MSA.dat | csmStatusData.ini |
| csmLocalConfig.xml | logBuf.dat | |
| csmLogDef.xml | group.dat | |
| AgentWorkConfig.xml | CSA.dat | |
| AgentSysConfig.xml | CriticalVA.dat | |
| AgentStatus.xml | | |
| AgentLocalConfig.xml | | |

3. Copy all the files from the `\Cache` folder.
4. Restart the Agent service.

**To restore the settings from backup:**

1. Remove the Agent locally if you haven't already. For detailed instructions, see *Removing Agents Locally* on page 8-8.

> **Note:** When removing the Agent locally, the Agent will unregister from Worry-Free Remote Manager which automatically deletes all data associated with the Agent. To prevent the Agent from unregistering, modify the **Server address** value in Agent interface before removing the Agent.

2. Reinstall the Agent. Ensure that you use the same GUID which can be obtained from a`gentSysConfig.xml`.
3. On the managed server, right click the Agent system tray icon and click **Stop Service** to stop the Agent service.
4. Replace the configuration files with the backup files.
5. Right-click the Agent system tray icon and click **Start Service** to restart the Agent service.

## Finding the Agent Build Number

**To check the build number of the Agent:**

1. Go to the `C:\Program Files\Trend Micro\WFRMAgentForCSM` directory.
2. Right-click the `csmplugin.dll` file and then click **Properties > Version** (tab) to see the build number.

**To check the build number from the Worry-Free Remote Manager console:**

1. Click the **Customers** tab.
2. Select the target domain from the **View by** drop-down list in the left pane.

   The Customer tab appears.
3. Click **All Customers** > {customer} > {agent}.

   The **Live Status** tab appears.
4. Click the **Server/Agent Details** tab.
5. Click **WFRM Agent Details**.
6. Check the agent version in the **General Information** table.

## Enabling the Agent debug log

Normally the Agent will only log warning and error information. If more detail log information is required, enable the Agent's debug log:

Open the file AgentLocalConfig.xml in `<install path>\Trend Micro\WFRMAgentForCSM\` in a text editor, then:

1. Change `<DebugLogLevel>` from `LL_FOR_ERROR` to `LL_FOR_ALL`.
2. Restart the Agent service by right-clicking the WFRM Agent on the task bar, then clicking **Restart Service**.
3. The Agent log file is `<install path>\Trend Micro\WFRMAgentForCSM\log\TMICAgent.log`

### Agent logs and configuration files location

Agent configuration files are located in:

```
<install path>\Trend Micro\WFRMAgentForCSM\*.xml
<install path>\Trend Micro\WFRMAgentForCSM\*.ini
```

Log files are located in:

```
<install path>\Trend Micro\WFRMAgentForCSM\log\
```

## Known Server Issues

The following are known server issues in this release:

| | |
|---|---|
| **Issue** | **Inconsistent status icons.** |
| **Description** | During the initial stages of data gathering (right after the Agent registers with the server), Worry Free Remote Manager may display antivirus and anti-spam status icons that are inconsistent with the displayed number of virus and spam incidents.<br>Right after it registers with the server, the Agent transmits the current antivirus and anti-spam statuses from WFBS(ALL), but does not transmit the historical data on which these statuses are based. As a result, it may display, for example, a red status symbol but show no incidents. |
| **Resolution** | Worry Free Remote Manager will display the correct icon and data as soon as WFBS(ALL) detects an incident. |
| **Issue** | **Unable to uninstall Agent remotely.** |
| **Description** | Users cannot send the uninstall command to the Agent when there is a version mismatch. This occurs when the "automatic upgrade" option is enabled and the upgrades keep failing. |
| **Resolution** | Disable automatic upgrades and then uninstall the Agent. |
| **Issue** | **Spam data inconsistent with WFBS-S/WFBS-A.** |
| **Description** | Spam data may differ between WFBS-S/WFBS-A and Worry Free Remote Manager if the servers running both systems are in different time zones. |
| **Resolution** | Spam incidents in Worry Free Remote Manager console and reports may be dated earlier or later, depending on the time difference between the servers. |
| **Issue** | **Reinstalled Agents can provide overlapping data.** |
| **Description** | Agents automatically transmit three days worth of certain WFBS(ALL) data upon registration. If an Agent is uninstalled and then reinstalled within a three-day period, the Agent will likely pull data that will overlap with data that it pulled before it was uninstalled. |
| **Resolution** | Back up the Agent configuration files before removing the Agent and restore these files after reinstalling the Agent. See *Backing Up and Restoring Agent Settings* on page A-8. |

| | |
|---|---|
| **Issue** | **Result of scan command cannot be verified.** |
| **Description** | The Agent cannot verify whether WFBS-S/WFBS-A successfully deploys the "scan" command to the network. This prevents Worry Free Remote Manager from verifying the results of the "scan" command. |
| **Resolution** | You may need to verify the status of the scan command through your customer's IT administrator. |
| **Issue** | **Inconsistent console language.** |
| **Description** | If WFRM is set to use a language other than English but the operating system is set to use English as its default language, then the "OK" and "Cancel" buttons will be in English, not the other language. |
| **Resolution** | There is presently no known resolution for this issue. |
| **Issue** | **When using multiple tabs in Internet Explorer 7, two instances of the WFRM console should not be opened at the same time using different accounts.** |
| **Description** | When using multiple tabs in Internet Explorer 7, information from one tab may be incorrectly shown on the other tab if the reseller is signed into two different accounts at the same time. |
| **Resolution** | There is presently no known resolution for this issue. Therefore, only one instance of WFRM should be open at a time. |
| **Issue** | **When total seat usage is 90%, the license should be red, but is green instead.** |
| **Description** | The license light status and the number of the seats are sent by a WFBS-S/WFBS-A server to WFRM. But if the license light status is sent later than the number of seats, this issue can occur. |
| **Resolution** | When this issue occurs, wait a short time. The license light will turn to RED. |
| **Issue** | **Customer shows up twice on the network tree when adding a WFRM Agent to a WFBS 6.0 server.** |
| **Description** | If you install an Agent on WFBS 6.0 and generate the GUID from the Agent Installation program, the customer may show up twice on the WFRM network tree. |
| **Resolution** | Before installing the Agent, add the WFBS 6.0 managed server to the WFRM console, then install the WFRM Agent using the GUID generated on the WFRM console. |
| **Issue** | **Incorrect user name shows on WFBS-SVC console.** |
| **Description** | After signing on to WFBS-SVC through the WFRM console, the reseller name will show on the WFBS-SVC console instead of the WFBS-SVC customer name. |
| **Resolution** | There is presently no known resolution for this issue. |

# Known Agent Issues

The following are known Agent issues in this release:

| | |
|---|---|
| **Issue** | **Reinstalled Agents can provide overlapping data.** |
| **Description** | Agents automatically transmit three days worth of certain WFBS-S/WFBS-A data upon registration. If an Agent is uninstalled and then reinstalled within a three-day period, the Agent will likely pull data that will overlap with data that it pulled before it was uninstalled. |
| **Resolution** | Back up the Agent configuration files before removing the Agent and restore these files after reinstalling the Agent. See *Backing Up and Restoring Agent Settings* on page A-8. |
| **Issue** | **Result of scan command cannot be verified.** |
| **Description** | The Agent cannot verify whether WFBS-S/WFBS-A successfully deployed the "scan" command to the network. This prevents, Worry Free Remote Manager from verifying the results of the "scan" command. |
| **Resolution** | You may need to verify the status of the scan command through your customer's IT administrator. |
| **Issue** | **The Agent Configuration Tool is not visible after the Agent has been upgraded even though it is running.** |
| **Description** | The Agent Configuration Tool is not visible after upgrading the Agent on a Windows Vista™ or Windows Server 2008™ operating system. Before the upgrade, the user usually runs the Agent Configuration tool under the user's account. During the upgrade process, the tool is killed, then restarted by LocalSystem instead of the user's account. Therefore, even though it is running, the user cannot see it. |
| **Resolution** | The machine should be restarted in order to restart the Agent Configuration Tool under the user's account. |

# FAQ

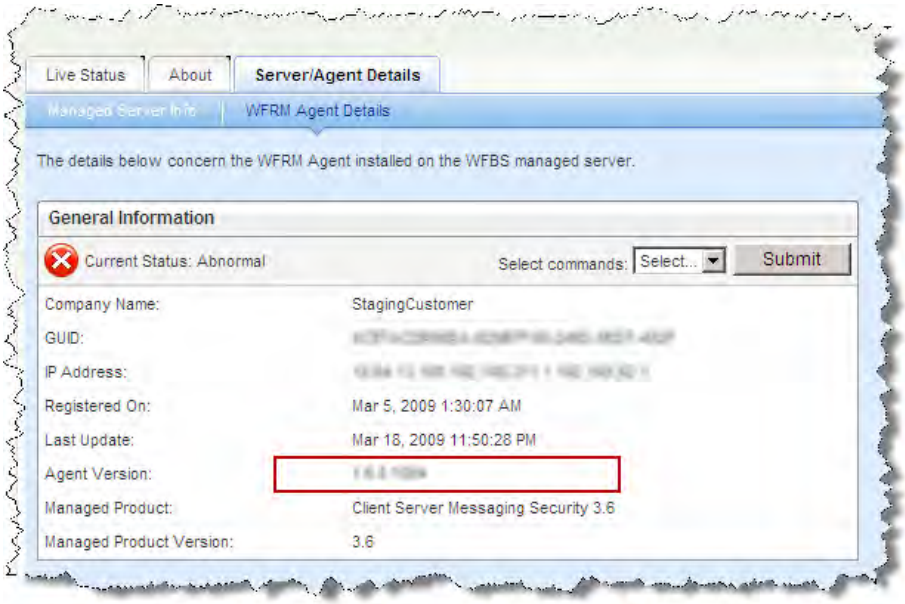
The FAQ is divided into the following sections:



## Web Console

### Why does the agent still show version 1.6 on the WFRM console when the WFRM server is version 2.6?

WFRM 2.6 still uses the 1.6 agent (on servers prior to WFBS 6.0); only the server is version 2.6.




### Is it possible to crack the login/password of WFRM?

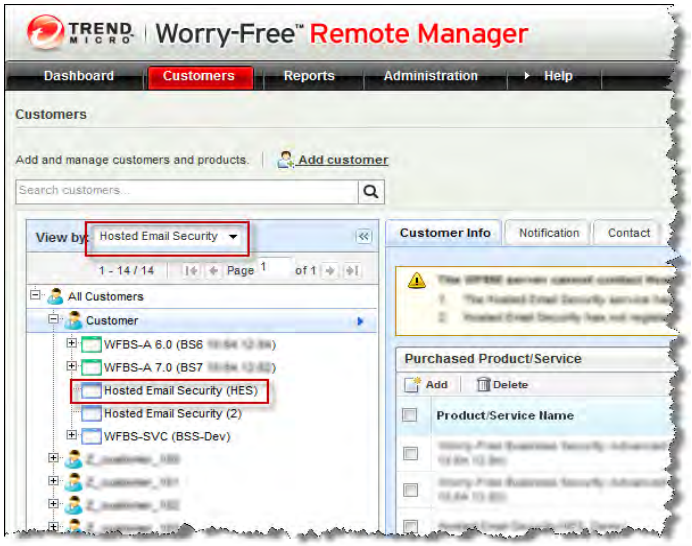
It is not easy for a hacker to crack a WFRM password if he/she uses a brute force crack method. If this is tried more than five times, the account will be disabled (If a password is forgotten, a reseller can receive their password by email or ask Trend Micro support for help. If a reseller receives the lost password by email, the account is re-enabled automatically).

### Can a reseller have more than one account on WFRM?

No. In WFRM 2.6, a reseller can have only one account.

### When selecting Hosted Email Security (or WFBS-S/WFBS-A) in the "View by" list above the customer tree, why is the tree still sorted by the customer name?

When selecting Hosted Email Security, this filters all Hosted Email Security customers; it does not sort by Hosted Email Security. In other words, when selecting Hosted Email Security in the drop down list, customers without Hosted Email Security will not be displayed.




Note that other products for this Hosted Email Security customer will also be displayed.

### Uploaded logo is cut.

On the **Reseller Profile** page and the **Add Customer** page, the entire logo may not display.

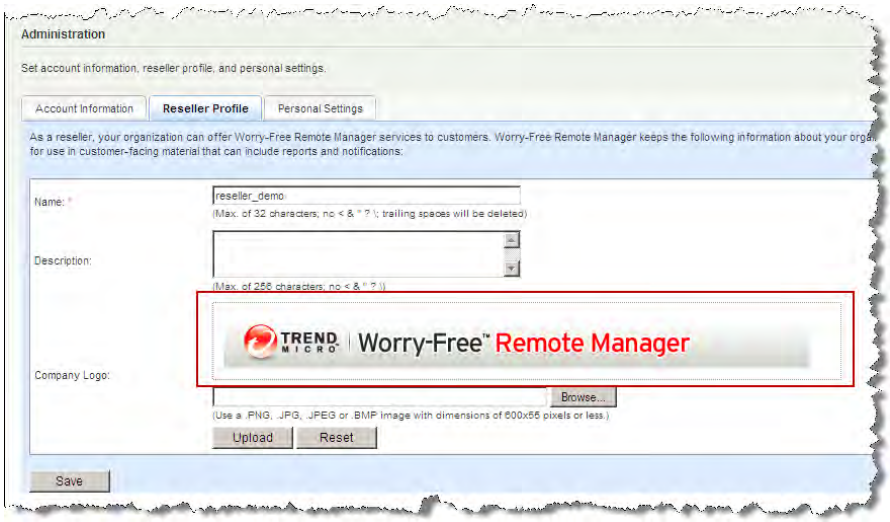



**FIGURE A-1. Reseller Profile page**

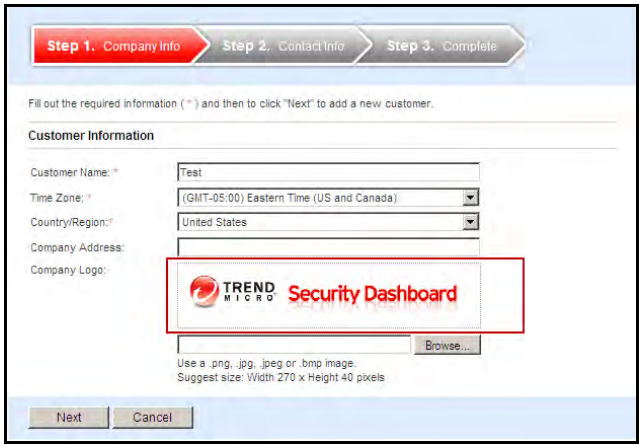


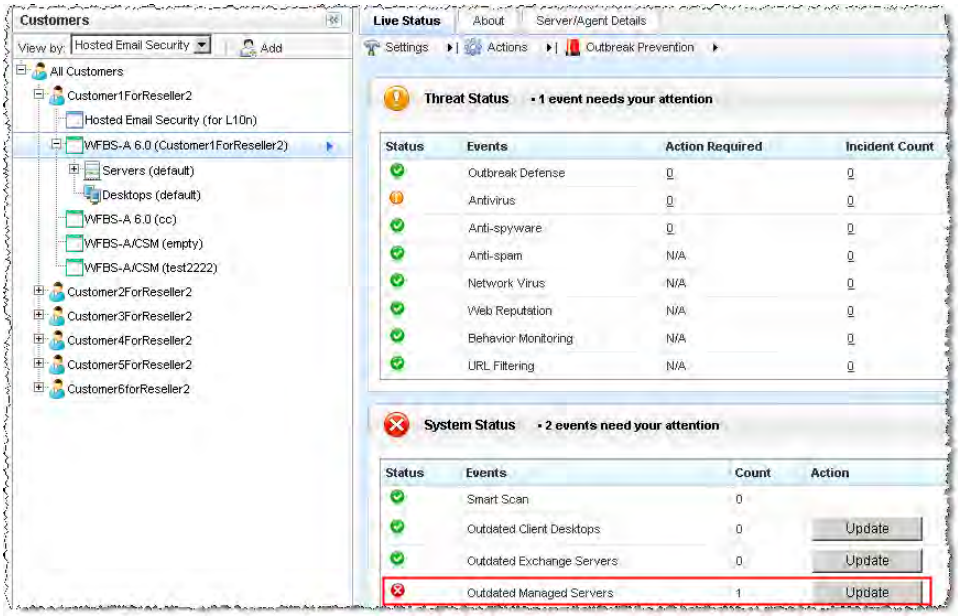

**FIGURE A-2. Add Customer page**

1. If the picture is uploaded using Internet Explorer 7 or 8, the picture may be cut in the preview window. But after the reseller actually uploads the picture, the entire picture will be displayed as a thumbnail.
2. If the picture is uploaded using Internet Explorer 6, the picture will be displayed as a thumbnail in the preview window if it is too large.

### Grayed out menus

Certain menu items used to send commands to an Agent may be grey. This can occur when the Agent hasn't yet registered to the WFRM server or relevant data has not yet been communicated (due to network time delay or other reasons).

### Why is the "Outdated Managed Servers" light still red even after clicking the Update button?




The **Update** button only sends commands to the WFBS-S/WFBS-A server. Any of the following can occur:

- The WFBS-S/WFBS-A server receives the update command, but due to configurations on the WFBS-S/WFBS-A server, the update operation cannot be executed.
- The WFBS-S/WFBS-A server has updated itself, but it hasn't updated most the CSAs which belong to it, so it continues to send a Red alert to WFRM. It may take some time for most of the CSAs to be updated.
- The live status page can't refresh itself (as opposed to the Dashboard, which can), so even though the WFBS-S/WFBS-A server has changed the Red alert to a Green light, the live status page may need to be refreshed manually in order to see the latest status.

## Hosted Email Security Integration

### Why is the latest 3 hours data not displayed on Live Status?

On the Hosted Email Security server, data collection takes places over a period of 2 hours. To be certain that the WFRM server will have integrated data from the Hosted Email Security server, data collection is delayed for 3 hours.

### Why are Sync with Server and Go to Customer Console grayed out when right-clicking on Hosted Email Security on the customer tree?

There are three possible reasons:

Hosted Email Security is not activated:

1. Hosted Email Security hasn't yet been connected to WFRM.
2. The customer terminated the connection.

   See "*Connect a Hosted Email Security Customer to the WFRM Console* on page 3-12".

   Hosted Email Security is activated.
3. The customer tree may need to be refreshed.

### Why do I get the error message "Your Hosted Email Security customer has not connected to WFRM or has been disconnected by Hosted Email Security. Contact your administrator" when I try to redirect to the customer's Hosted Email Security console after the customer connected Hosted Email Security to WFRM?

After entering the Authorization Key and clicking Connect, it can take as long as ten minutes in order for Hosted Email Security to complete the connection to the WFRM console. If the problem persists, contact Trend Micro Support.

### Why does an Hosted Email Security customer's Activation Code (AC) and Expiration Date show "N/A" on the WFRM console?

If an Hosted Email Security customer has not connected the Hosted Email Security service to WFRM or has disconnected, WFRM cannot retrieve data. The other reason is that Hosted Email Security cannot find a valid AC and Expiration Date for this customer. This is a rare occurrence.

## Reports

### Why is there no new report generated in the report history after creating a one-time report profile?

Wait for one or two minutes after creating the report profile. The report will show up in the report history. If the report still cannot be generated, open the report profile and save it again. If the issue persists, contact Trend Micro support.

### Why can't I receive daily/weekly/monthly reports via email when there are reports in report history?

Make sure the customer's email address is valid and is in the list of report profile recipients. If both are OK, it may be a network issue.

### On a generated report, why isn't the data time displayed according to my time zone?

The time zone that the report depends on is the one that the reseller selected when creating the profile. It is not determined by the customer's machine.

### What does the "N/A" means after creating a one-time report?

For a one-time report, the status column will always show "N/A". This happens because there is no status for the one-time report (can't disable, enable, suspend, etc.).

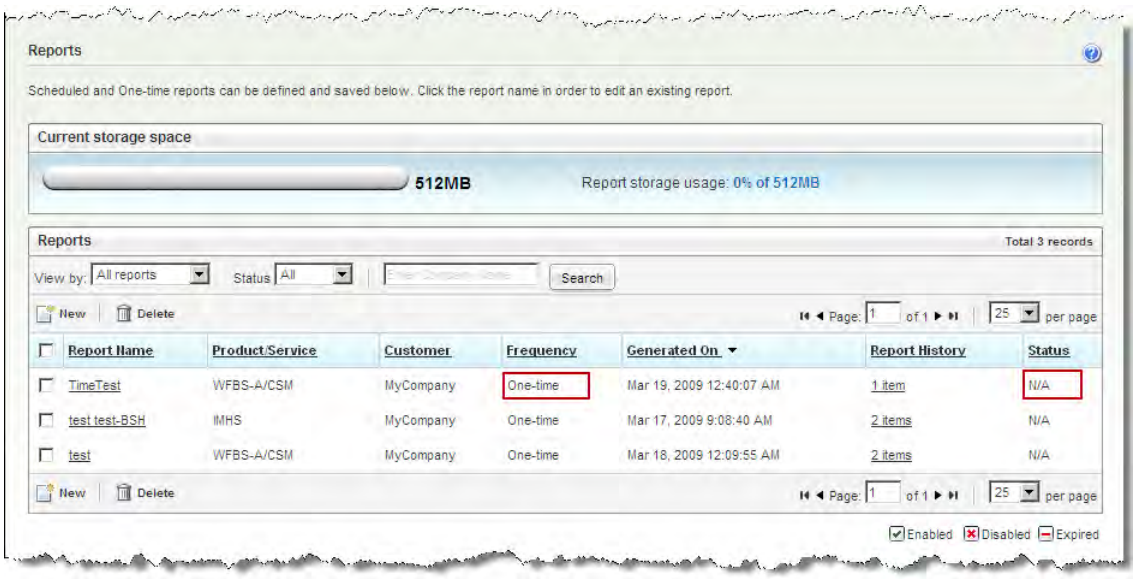



**FIGURE A-3. N/A on one-time reports**

### Cannot view reports when using SSL (HTTPS) connections.

"Do not save encrypted pages to disk" is a security setting for Internet Explorer 6.0/7.0/8.0 and comes into play when dealing with SSL (HTTPS) connections. If you check this setting, nothing will be saved to the cache, and you will not be able to open or download reports.

In order to fix this, in IE 6.0/7.0/8.0, click **Tools > Internet Options > Advanced > Security** and uncheck, "Do not save encrypted pages to disk".

# Appendix B

## Getting Help

Most questions have already been answered on the Knowledge Base (refer *Knowledge Base* on page B-2 for more information). If you cannot find your answer on the Knowledge Base, you can contact Trend Micro Technical Support for further assistance (refer to *Trend Community* on page B-2 for more information).

# Product Documentation

Worry-Free Remote Manager documentation includes Online Help and the Getting Started Guide for Resellers.

- **Online Help:** Click the help icon (  ) to open context-sensitive help.
- **Getting Started Guide:** Download the latest Getting Started Guide for Resellers from the Trend Micro Update Center:

  http://www.trendmicro.com/download

# Knowledge Base

The Trend Micro Knowledge Base is an online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use the Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in the Knowledge Base are product FAQs, tips, advice on preventing virus/malware infections, and regional contact information for support and sales.

The Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product.

http://esupport.trendmicro.com/smb/default.aspx

# Trend Community

Visit the Trend Community. Get help, share your experiences, ask questions, and discuss security concerns in the forums with fellow users, enthusiasts, and security experts.

http://community.trendmicro.com/

# Technical Support

When you contact Trend Micro Technical Support, to speed up your problem resolution, ensure that you have the following details available:

- Operating system
- Network type
- Brand and model of the computer and connected hardware
- Amount of memory and free hard disk space on your machine
- Detailed description of the installation environment
- Exact text of any error message
- Steps to reproduce the problem

**Go to the following URL for web support:**

http://esupport.trendmicro.com/support/srf/questionentry.do

**For email and telephone support:**

**APAC**

Australia:

Tel No: 1800 201 122

New Zealand:

Tel No: 0800 888 190

Hong Kong:

Email: hksupportcenter@trendmicro.com.hk

Tel No: +852 2866 4362

**USA**

Tel No: +1 (877) 873-6307

**LAR**

Spanish Support:

http://la.trendmicro.com/la/partners/program/

Portuguese Support:

http://br.trendmicro.com/br/partners/program/

Brazil:

email: smb@support.trendmicro.com.br

Mexico and other countries:

email: soporte_smb@trendmicro.com

**EMEA**

Registration Assistance:

Online technical support: http://smb.trendmicro.eu

(Use Category "Online Registration(OLR)/Renewal")

Coverage: 09:00-17:00 Monday - Friday

Technical Issues:

Online technical support: http://smb.trendmicro.eu

(Use Category "Configuration" or "New Installation/Uninstallation")

Coverage: 09:00-17:00 Monday – Friday

English Support:

Tel No: +353 21 7307 433

French Support:

Tel No: +353 21 7307 424

German Support:

Tel No: +353 21 7307 423

Italian Support:

Tel No: +353 21 7307 444

Spanish Support:

Tel No: +353 21 4710 229

See http://us.trendmicro.com/us/products/sb/worry-free-remote-manager/support-info/index.html for updated contact information.

# Contacting Trend Micro

Trend Micro has sales and corporate offices in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

http://uk.trendmicro.com/uk/about/contact_us/

**Note:** The information on this Web site is subject to change without notice.

# Sending Suspicious Files to Trend Micro

You can send your virus/malware, infected files, Trojans, suspected worms, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

Click the link under the type of submission you want to make.

**Note:** Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you submit your case, an acknowledgement screen displays. This screen also displays a case number. Make note of the case number for tracking purposes.

# Index