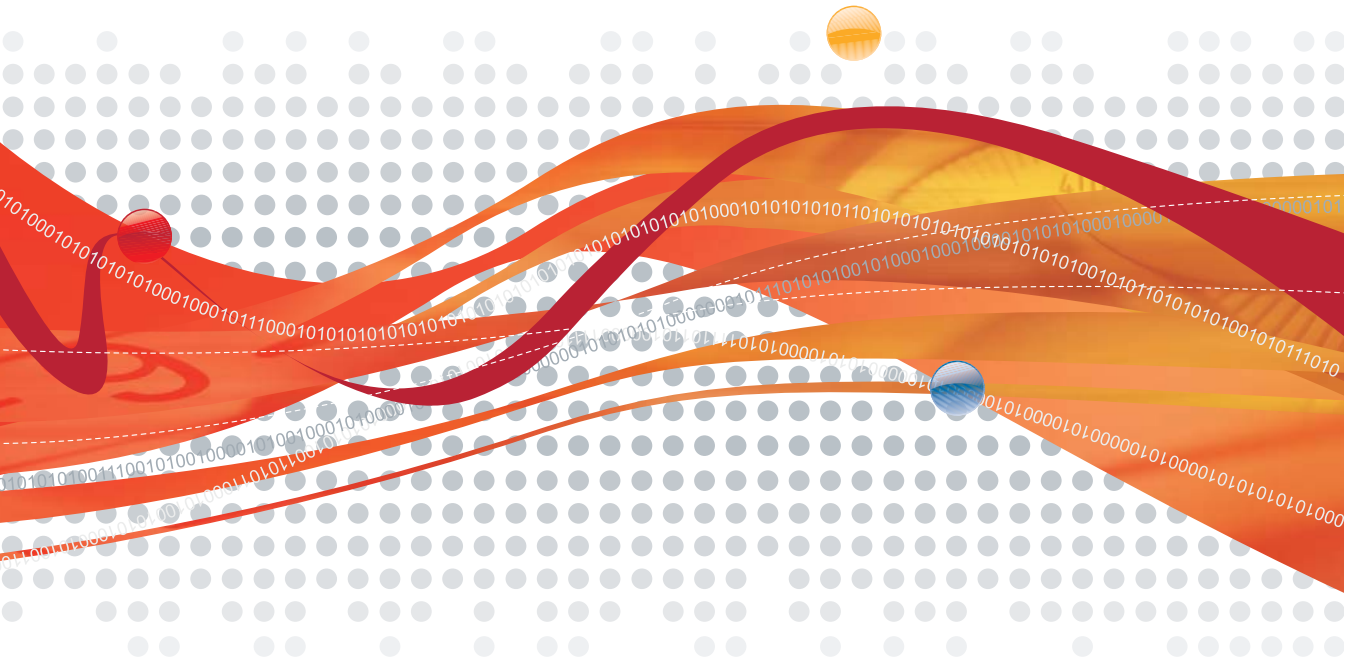




# Worry-Free™ SecureSite1

for Small and Medium Business



## Getting Started Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before using the software, please review the release notes and the latest version of the *Getting Started Guide*, which is available from the Trend Micro Web site at:

<http://www.trendmicro.com/download>

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

Copyright© 2008 Trend Micro Incorporated. All rights reserved.

Document Part No.: WSEM13550/80219

Release Date: March 2008

The Trend Micro™ Worry-Free™ SecureSite Getting Started Guide is intended to provide basic instructions on setting up Worry-Free SecureSite. Read it prior to installing the included products.

For technical support, please see *Trend Micro Support on page 3-3*.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at [docs@trendmicro.com](mailto:docs@trendmicro.com). Your feedback is always welcome. Please evaluate this document at the following site:

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

---

# Contents

## Preface

### Chapter 1: About Worry-Free SecureSite

Introducing Worry-Free SecureSite .....	1-2
What Does Worry-Free SecureSite Scan? .....	1-2
Cross-Site Scripting .....	1-2
Information Leakage .....	1-2
Content Spoofing .....	1-3
Predictable URL .....	1-3
SQL Injection .....	1-3
Insufficient Authentication .....	1-3
Insufficient Authorization .....	1-4
Abuse of Functionality .....	1-4
Directory Traversal .....	1-4
XPath Injection .....	1-4
What You Can Do with SecureSite .....	1-4
Before You Begin .....	1-5
Check the Confirmation Email Message from Trend Micro .....	1-5
Ensure Your Web Server Can Accept Traffic From WFSS .....	1-6

### Chapter 2: Using Worry-Free SecureSite

Accessing Your SecureSite Account .....	2-2
Understanding Summary Information .....	2-3
Available Reports .....	2-4
Executive Summary .....	2-5
Remediation Plan .....	2-6
Viewing Reports .....	2-8
In Case of a Domain Name or IP Address Change .....	2-8

### Chapter 3: Getting Support

About Trend Micro .....	3-2
Contacting Trend Micro .....	3-3
Trend Micro Support .....	3-3

Knowledge Base .....	3-3
Contacting Technical Support .....	3-4

## **Appendix A: Unsupported Features**

### **Index**

---

# Preface

Welcome to the Trend Micro™ Worry-Free™ SecureSite Getting Started Guide. This book contains information about product settings and service levels.

This preface discusses the following topics:

- *What's New in Worry-Free SecureSite* on page 2
- *Worry-Free SecureSite Documentation* on page 2
- *Audience* on page 3
- *Document Conventions* on page 3

## What's New in Worry-Free SecureSite


Trend Micro™ Worry-Free™ SecureSite (WFSS) is an enterprise-class vulnerability assessment solution. SecureSite scans Web applications, databases, network devices, operating systems and other applications to identify and eliminate security vulnerabilities and ensure compliance with mandatory regulations.

This version of Worry-Free SecureSite includes the following features:

- Site summary information
- Executive Summary report
- Remediation Plan report

## Worry-Free SecureSite Documentation

The Trend Micro™ Worry-Free™ SecureSite documentation consists of the following:

**Online Help**—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon ()

**Getting Started Guide**—Helps you plan for deployment and configure all product settings.

**Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The Getting Started Guide and readme are available at:

<http://www.trendmicro.com/download>

---

## Audience

The WFSS documentation is written for IT managers. The documentation assumes that the reader has in-depth knowledge of firewall configuration and Web site operation.

## Document Conventions

To help you locate and interpret information easily, the WFSS documentation uses the following conventions.

**TABLE P-1. Document conventions and their descriptions**

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
<i>Italics</i>	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
<b>Note</b>	Configuration notes
<b>Tip</b>	Recommendations
<b>WARNING!</b>	Reminders on actions or configurations that should be avoided



# About Worry-Free SecureSite

This chapter discusses the features of Trend Micro™ Worry-Free™ SecureSite:

- *Introducing Worry-Free SecureSite* on page 1-2
- *What You Can Do with SecureSite* on page 1-4
- *Before You Begin* on page 1-5

## Introducing Worry-Free SecureSite

Trend Micro™ Worry-Free™ SecureSite (WFSS) is a hosted, enterprise-class vulnerability assessment and management service. SecureSite identifies security weaknesses in all layers of a network computing environment and provides vulnerability information, risk assessment, and remediation information.

Using the network to scan specific network components based on IP addresses or host names, SecureSite provides reports that show vulnerabilities on the target network and how to fix these security holes with the minimum set of resources. If site vulnerabilities are not patched, they could be used by hackers to compromise the network devices.

SecureSite scans Web servers, applications, databases and operating systems to find vulnerabilities. When provided with administrative credentials, SecureSite can perform deep inspection checks of system files to detect unauthorized programs and validate updates.

## What Does Worry-Free SecureSite Scan?

When SecureSite scans your Web site, it checks for the following ten key vulnerabilities.

### Cross-Site Scripting

Most industry experts and researchers agree that cross-site scripting (XSS) continues to be the most prevalent Web site vulnerability. Depending on the Web site, XSS can be especially hazardous to businesses and consumers. New attack vectors employed are responsible for highly effective phishing scams and Web worms that are resistant to commonly accepted safeguards. The evolution of cutting-edge JavaScript malware as a payload has made finding and fixing this vulnerability more vital than ever.

### Information Leakage

Information leakage occurs when a Web site mistakenly reveals or is manipulated to reveal sensitive information such as developer comments, user information, internal IP addresses, source code, revision numbers, error messages/codes, etc., which may all aid an attacker.

## Content Spoofing

Content spoofing is used in phishing scams as a method of forcing a legitimate Web site to deliver or redirect users to bogus content. For example, users often receive a suspicious link that instructs them to confirm their user name and password information. Typically, phishing Web sites are hosted on look-alike domain names mimicking the content of the real site. In the case of Content spoofing phishing scams, fake content is injected into the real Web site, making it very difficult, if not impossible, for users to detect the difference and therefore protect themselves.

## Predictable URL

Over time, many pages on a Web site become unlinked, orphaned, and forgotten. These Web pages often contain payment logs, software backups, future press releases, debug messages, source code – nothing, or everything. Normally, the only mechanism protecting the sensitive information within is the predictability of the URL. Automated scanners have become adept at uncovering these files by generating thousands of guesses. Also, through a process called “Google Hacking,” attackers use search engines to discover sensitive information via forgotten links on a Web site.

## SQL Injection

SQL injection has been at the center of some of the largest credit card and identity theft incidents. Today’s backend Web site databases store highly sensitive information, making them a natural, attractive target for malicious hackers. Names, addresses, phone numbers, passwords, birth dates, intellectual property, trade secrets, encryption keys and often much more could be vulnerable to theft. With a few well-placed quotes, semi-colons and commands, entire databases could fall into the wrong hands.

## Insufficient Authentication

Insufficient authentication flaws are typically found within the business logic of an application. Successful exploitation leads to an attacker gaining unauthorized access to protected sections of a Web site. For example, while logged-in as a normal user, an attacker could impersonate another user on the system.

## Insufficient Authorization

Insufficient authorization flaws are also typically found within the business logic of an application. Successful exploitation leads to an attacker being able to escalate his or her privileges or exercise unauthorized access. For example, while logged-in as a normal user, an attacker could gain access to another user's data while still being logged-in under their current account.

## Abuse of Functionality

As stated by the WASC Threat Classification, "Abuse of functionality is an attack technique that uses a Web site's own features and functionality to consume, defraud, or circumvent access controls mechanisms. Some functionality of a Web site, possibly even security features, may be abused to cause unexpected behavior. When a piece of functionality is open to abuse, an attacker could potentially annoy other users or perhaps defraud the system entirely."

## Directory Traversal

As a feature of most popular Web servers, directory traversal lists the contents of a directory if no specific file name is given and no index file is present (example: index.html). Directory listings provided in this way could reveal sensitive information that was not intended for public viewing, such as pre-released Web pages, log files, temporary files, backup files, etc.

## XPath Injection

XPath Injection is an attack technique, similar to SQL injection, used to exploit Web sites that construct XPath queries from user-supplied input. When an attacker is able to modify an XPath query, they may be able to obtain sensitive information from an XML document that would otherwise be out of reach.

## What You Can Do with SecureSite

In this version of SecureSite, only two user tasks are supported:

- **Viewing site summary** – Check the Home page of your SecureSite account to learn about vulnerabilities that have been detected for the last four-month period. You can also view a list of all your Web sites that are configured for scanning by SecureSite. For more information, see [Understanding Summary Information](#) on page 2-3.
- **Viewing reports** – Two types of reports are available in SecureSite: Executive Summary and Remediation Plan. Reports are generated immediately after a vulnerability scan is completed. For more information, see [Available Reports](#) and [Viewing Reports](#) on page 2-8.

---

**Note:** There are currently no user configurable settings from within the SecureSite Web interface. All SecureSite settings (site IP addresses or domain names and scan schedules) were configured during the SecureSite registration process which you or your company representative completed.

---

## Before You Begin

Before you start using your SecureSite account, there are a couple of items that Trend Micro recommends you check:

- The confirmation email message from Trend Micro
- Your Web server and firewall settings

## Check the Confirmation Email Message from Trend Micro

After your SecureSite account is set up and confirmed, Trend Micro sends out a confirmation email message to the email address you used to sign up. This confirmation email message contains, among others, the *user name* and *password* for your SecureSite account. Make sure you have this information before attempting to access the SecureSite login page.

The confirmation email message also contains information on the domain name or IP address that has been set up for scanning by SecureSite.

## Ensure Your Web Server Can Accept Traffic From WFSS

To scan your Web site, SecureSite servers will connect to your Web server and perform vulnerability tests. Traffic from the SecureSite servers must therefore be allowed for the vulnerability tests to be initiated.

- If your Web site is hosted by a third party, contact your Web hosting company and ask them to allow traffic from the following IP address range: **216.99.131.1 - 216.99.131.126**. These are the IP addresses of the Trend Micro SecureSite servers.
- If your Web site is hosted in-house, configure your firewall to accept traffic from the following IP address range: **216.99.131.1 - 216.99.131.126**.

---

# Using Worry-Free SecureSite

This chapter discusses the usage details of Trend Micro™ Worry-Free™ SecureSite. Topics include:

- *Accessing Your SecureSite Account* on page 2-2
- *Understanding Summary Information* on page 2-3
- *Viewing Reports* on page 2-8
- *In Case of a Domain Name or IP Address Change* on page 2-8

## Accessing Your SecureSite Account

You can access your Worry-Free SecureSite account using a Web browser. The SecureSite Web interface contains some Asynchronous JavaScript and XML (AJAX) elements, which require compatible Web browsers to display properly.

To ensure proper operation of the Web interface, Trend Micro recommends using the following browsers when accessing your SecureSite account:

- Microsoft® Internet Explorer® 6 or later
- Mozilla® Firefox® 1.5.x or later



**FIGURE 2-1.** Worry-Free SecureSite Login Page

**To access your SecureSite account:**

1. Start your Web browser.
2. In the address or location bar, type  
<https://us.WFSS.trendmicro.com/>.  
The Worry-Free SecureSite login page appears.
3. Enter the login credentials (user name and password) that Trend Micro sent to you via email when your SecureSite account was confirmed.
4. Click **Login**.

The Home page of the SecureSite Web interface appears.

## Understanding Summary Information

The Home page of the SecureSite interface is designed to provide all the information you need, at-a-glance, to easily monitor the status of your sites. The Home page contains the following sections:

- **Most Vulnerable Asset Groups** - Includes a bar graph that shows the number of vulnerabilities detected on your Web sites within the group. This section is useful if you have multiple Asset Groups configured to be scanned by SecureSite and you want a snapshot of the vulnerabilities detected on each group.
- **Asset Group Listing** - Shows a list of your Asset Groups that are configured to be scanned by SecureSite. To view the summary information on all devices defined in this Asset Group, click the group name.



FIGURE 2-2. SecureSite Home Page

## Available Reports

Two types of reports are available in SecureSite:

- Executive Summary, which provides high-level information on the vulnerability status of your sites
- Remediation Plan, which provides information on how to patch the vulnerabilities that SecureSite detected on your sites

---

**Note:** Reports in SecureSite are available in Portable Document Format (PDF). Therefore, you need a PDF viewer, such as Adobe Acrobat Reader, installed on your computer to view these reports.

---

## Executive Summary

The Executive Summary provides a high-level status report on the systems tested. It does not provide technical details of the test results. Executive summary reports can be distributed to management to demonstrate the current vulnerability status of a network.

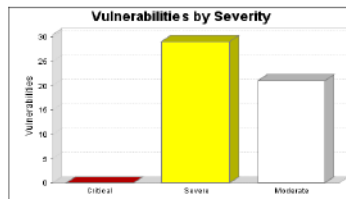
For an example of an Executive Summary report, see Figure 2-3.

### 1. Executive Summary

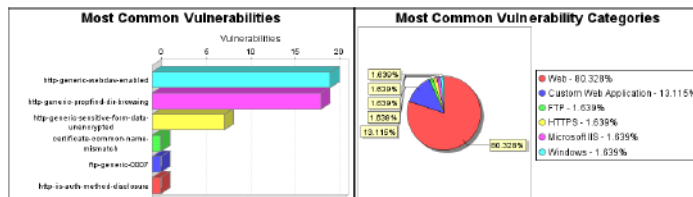
This report represents a security audit performed by WFSS from Trend Micro. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
www.company.com	March 04, 2008 11:00, GMT	March 04, 2008 11:17, GMT	17 minutes	Success

The audit was performed on one system which was found to be active and was scanned.



There were 50 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 29 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 21 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



There were 20 occurrences of the http-generic-webdav-enabled vulnerability, making it the most common vulnerability. There were 49 vulnerabilities in the Web category, making it the most common vulnerability category.

FIGURE 2-3. Executive Summary (Sample)

For instructions on how to view reports, see [Viewing Reports](#) on page 2-8.

## Remediation Plan

The Remediation Plan consolidates information about all vulnerabilities detected on the site and provides an optimized plan for remediation.

The SecureSite internal database of vulnerabilities maintains an index of patches together with the specific vulnerabilities that each one fixes. In many cases, a single service pack can fix dozens of vulnerabilities. Using this information, SecureSite optimizes the fix plan for remediation, allowing vulnerabilities to be fixed within the shortest time frame.

For each solution that SecureSite recommends, there is a time estimate for fixing the problem and a consolidated list of vulnerabilities that are fixed by implementing the solution.

For an example of a Remediation Plan report, see Figure 2-4.

## 3. Remediation Plan

### 3.1. Remediation Plan for xxx.xxx.xxx.xxx

#### 3.1.1. For Microsoft IIS 6.0

These vulnerabilities can be resolved by performing the following 4 steps. The total estimated time to perform all of these steps is 3 hours 35 minutes.

##### *Disable HTTP PROPFIND Method for Microsoft IIS*

Estimated time: 2 hours

IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS  
For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at <http://www.microsoft.com/technet/security/tools/urlscan.mspx>

This will address 19 instances of the following issue: WebDAV PROPFIND Method Allows Web Directory Browsing ([http-generic-propfind-dir-browsing](#)).

##### *Disable WebDAV for IIS*

Estimated time: 30 minutes

IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS  
For Microsoft IIS, follow [Microsoft's instructions](#) to disable WebDAV for the entire server.

This will address 20 instances of the following issue: WebDAV Extensions are Enabled ([http-generic-webdav-enabled](#)).

##### *Use the HTTPS (HTTP over SSL) protocol to submit sensitive form data*

Estimated time: 45 minutes

Enable the HTTPS protocol on the server. Change the "action" URL of the form tag to use the HTTPS protocol ("https://...") instead of just the HTTP protocol ("http://..."). All sensitive data should be sent over HTTPS instead of over HTTP.

This will address the following issue: Form action submits sensitive data in the clear ([http-generic-sensitive-form-data-unencrypted](#)).

##### *Fix Microsoft IIS Authentication Method Disclosure*

Estimated time: 20 minutes

If the server is intended for public use then it may be possible to simply disable both basic and integrated Windows authentication.

Sites that use form-based logins when users are authenticated against a database and track logged in users with cookies will be able to disable these authentication methods. Doing this will prevent such attacks.

If basic or integrated Windows authentication is required on the server, these steps should be considered:

- Set the account lockout threshold to help minimize the risk of successful brute force attacks. Using the "passprop" utility it is possible to enable account lockout for the default "administrator" account.
- Rename the administrator account if this has not already been done.

## FIGURE 2-4. Remediation Plan (Sample)

For instructions on how to view reports, see [Viewing Reports](#) on page 2-8.

## Viewing Reports

Reports are generated immediately after a scan is completed and scan schedules are configured during the SecureSite registration process. Therefore, the frequency by which SecureSite will generate vulnerability reports for your sites depend on the frequency of your site scans.

### To view the latest version of a report:

1. Click the **Reports** tab. The Report page displays the latest versions of the Executive Summary and Remediation Plan.
2. Under the **Report Name** column, click the name of the report that you want to view. Your Web browser refreshes and displays a PDF version of the report that you selected.

### To view a history of previously generated reports:

1. Click the **Reports** tab.
2. Under the **History** column, click the document icon for the report type that you want to view. The related Report History page appears, listing previously generated reports that are available on the system. Reports are named based on the date when they were generated.
3. To view the report generated on a particular date, click the date link under the **Created On** column.

Your Web browser refreshes and displays a PDF version of the report that you selected.

## In Case of a Domain Name or IP Address Change

SecureSite servers scan the Web server that corresponds to the domain name or IP address that you provided when you registered for the SecureSite service. If the domain name or IP address for your Web site changes, contact Trend Micro immediately so we can update your SecureSite configuration.

Send an email message to [wfss\\_beta@trendmicro.com](mailto:wfss_beta@trendmicro.com) with the new domain name or IP address information.

# Getting Support

This chapter describes how to contact Trend Micro.

- *About Trend Micro* on page 3-2
- *Contacting Trend Micro* on page 3-3
- *Trend Micro Support* on page 3-3

## 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 viruses 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 over 30 countries.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

<http://www.trendmicro.com>

## 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://us.trendmicro.com/us/about/contact\\_us](http://us.trendmicro.com/us/about/contact_us)

---

**Note:** The information on this Web site is subject to change without notice.

---

## Trend Micro Support

Trend Micro Support can help you resolve queries relating to your Trend Micro products. Most queries have already been answered on the Knowledge Base (refer *Knowledge Base* on page 3-3 for more information). If you cannot find your answer on the Knowledge Base, you can contact Trend Micro Technical Support for further assistance (refer *Contacting Technical Support* on page 3-4 for more information).

## 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 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. Visit:

<http://esupport.trendmicro.com/support/smb/search.do>

## Contacting 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

### **To contact Trend Micro Technical Support:**

1. Visit the following URL:  
[http://us.trendmicro.com/us/about/contact\\_us/](http://us.trendmicro.com/us/about/contact_us/)
2. Click the link for the required region. Follow the instructions for contacting support in your region.

# Unsupported Features

In the current version of SecureSite, a number of Web interface elements that are unsupported are still visible when you log on. Although these interface elements appear to be functioning (for example, you can click them), these are unsupported and Trend Micro does not guarantee the accuracy of information that is generated by these features.

Table A-1 identifies the pages that contain these unsupported elements.

**TABLE A-1. Unsupported Features on the SecureSite Web Interface**

CONVENTION	DESCRIPTION
Common	Assets tab, Vulnerabilities tab, Search box
Home tab	Configure link, Site Listing section
Assets tab	All
Reports tab	New Report button, Generate link, Edit link, Copy link, Delete link
Vulnerabilities tab	All



# Index

## **A**

About

    Trend Micro 3-2

    Worry-Free SecureSite 1-2

## **C**

Contact information 3-3

Contacting Trend Micro 3-3

## **E**

Executive Summary 2-5

## **K**

Knowledge Base 3-3

## **R**

Remediation Plan 2-6

## **S**

Support 3-1

## **T**

Trend Micro, about 3-2

Troubleshooting 3-1

## **W**

Worry-Free SecureSite

    about 1-2

