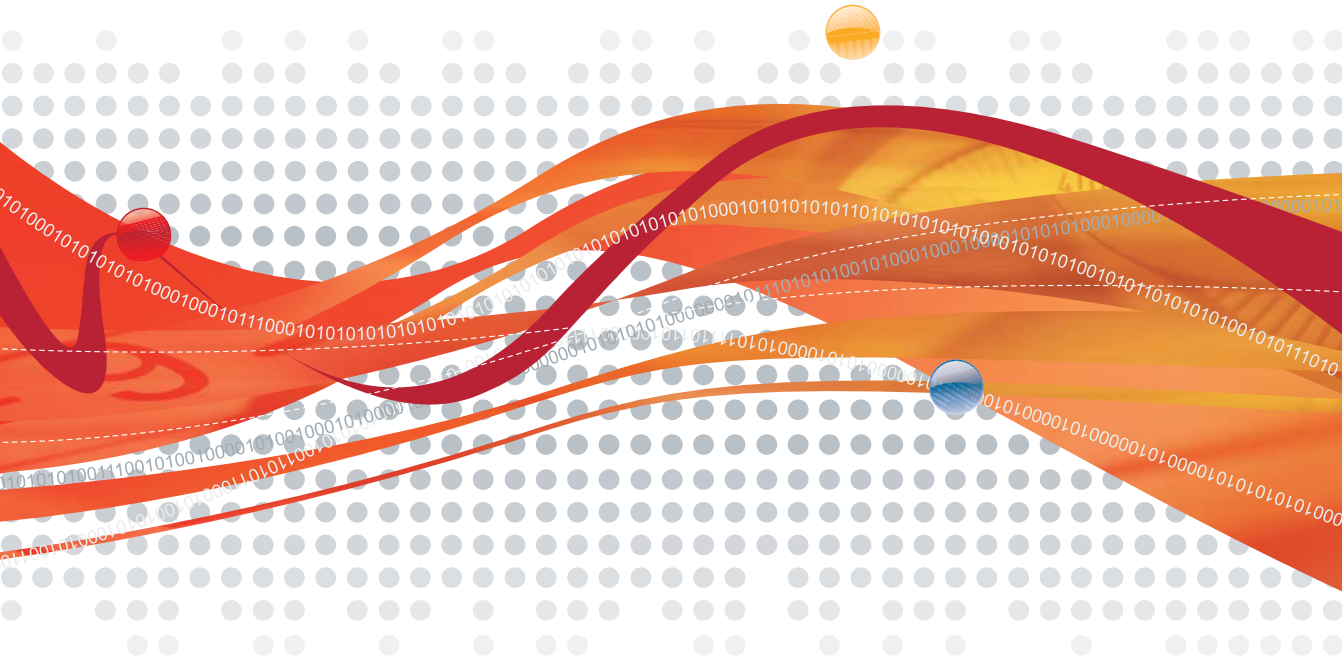
TREND MICRO

Trend Micro SecureSite1

for Small and Medium Business



Administrator's Guide

Document Part No.: MMEM13840/80908

Release Date: December 2008

Document Version No.: 1.1

Service Name and Version No.: Trend Micro™ SecureSite 1.5

The user documentation for Trend Micro™ SecureSite 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:

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

Contents

Chapter 1: Introducing Trend Micro SecureSite

Chapter 2: Getting Started

Chapter 3: Monitoring and Managing Sites

Chapter 4: Managing Reports

Chapter 5: Administering Trend Micro SecureSite

Appendix A: Troubleshooting and FAQs

Appendix B: Getting Help

Glossary

Index

Chapter 1

Introducing Trend Micro SecureSite

About Trend Micro SecureSite

Trend Micro™ SecureSite is a hosted solution that helps assure consumers of the safety and integrity of small business online retailers. The service tests Web sites daily for vulnerabilities, validates, and provides a mark (certificate) on sites that meet security policies. Included remediation tips help Trend Micro channel partners or other IT professionals you engage to fix vulnerabilities. By helping to protect online shoppers, SecureSite safeguards both your business reputation and your revenue.

About Ranking

SecureSite assigns a numerical value to each detected vulnerability during a scan. These values determine the ranking of the vulnerability. The following table describes the relationship between the numerical value and the ranking.

TABLE 1-1. SecureSite Ranking

NUMERICAL VALUE OF THE VULNERABILITY	SECURESITE RANKING
0.0 to 3.9	Moderate
4.0 to 6.9	Severe
7.0 to 10.0	Critical

See *Scanning Capabilities* on page 1-5 for detailed information.

If Trend Micro SecureSite identifies

- 1 critical,
- 1000 or more severe, or
- 1000 or more moderate

vulnerabilities in a site, the site fails the scan.

About SecureSite Mark Certification

With Trend Micro SecureSite, assure customers that the site is safe and secure by displaying the Trend Micro SecureSite Mark (certificate).

FIGURE 1-1. Trend Micro SecureSite Mark

To display the certificate on your site, paste the `TREND MICRO SecureSite CODE` in the HTML code of your home page. This code dynamically changes the status of the site depending on the daily scan results. See *Configuring Site Settings* on page 3-6 for copying the code and *Certification Criteria* on page 1-4 for information on when the certificate is displayed.

FIGURE 1-2. Example of a site with the certificate

Certification Criteria

If the site fails three consecutive daily scans, the certificate will no longer appear on the site. The certificate will reappear once the site passes the next daily scan. See *Configuring Notifications* on page 3-7 for instructions to create notifications for these and other events. .

TABLE 1-2. Trend Micro SecureSite Mark Status

DISPLAYED IMAGE	CERTIFICATION STATUS	DESCRIPTION
	Certified	The site has passed the daily scan certification criteria. The site is certified.
Not Applicable <A transparent image>	Expired	The site is no longer certified.

Note: A site, though certified (passed the daily scan), could still have vulnerabilities. To fix the vulnerabilities and secure the site, follow the steps outlined in the latest Remediation Plan (see *Remediation Plan* on page 4-3).

Features

The main features of Trend Micro SecureSite are:

- Add sites to scan
- Manage added sites
- View summary information of sites
- View and download remediation plans to fix site vulnerabilities
- View and download executive summaries to update management about the site's health

Scanning Capabilities

SecureSite can scan a site for different types of vulnerabilities ranging from Cross-site Scripting to XPath Injection. The vulnerabilities are discussed in the section that follows.

Cross-Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications which allow code injection by malicious users into the Web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits. As of 2007, cross-site scripting carried out on Web sites were roughly 80% of all documented security vulnerabilities. Often during an attack "everything looks fine" to the end-user who may be subject to unauthorized access, theft of sensitive data, and financial loss.

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.

Predictable URLs

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. Normally, predictable URLs make a site vulnerable. 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, trade secrets, encryption keys and often much more could be vulnerable to theft. When an attacker is able to modify an SQL query, entire databases could fall into the wrong hands.

Insufficient Authentication

Insufficient authentication is 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. Depending on the specific online resource, these Web applications should not be directly accessible without the user required to properly verify their identity.

Insufficient Authorization

Insufficient authorization is 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.

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-release 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.

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^{SM}, 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, a global organization with more than 3,000 employees in 25 countries, is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia.

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

http://www.trendmicro.com

Chapter 2

Getting Started

System Requirements

To access Trend Micro SecureSite, the following are required:

- A compatible Web browser:
  - Microsoft™ Internet Explorer 7.0
  - Mozilla™ Firefox™ 2.0

Before you Begin

Before using Trend Micro SecureSite, registration is required. The following steps briefly describe the process:

Step 1. Go to the relevant link to register for Trend Micro SecureSite:

- USA and Canada: https://tmss-us.trendmicro.com/tmss_trial.php
- EMEA: https://tmss-emea.trendmicro.com/tmss_trial.php

Step 2. After a successful registration, Trend Micro will send a confirmation message with the user name and password.

Step 3. Next, log on to the console to confirm the details (see *Accessing the Console* on page 2-2).

Accessing the Console

Access the SecureSite console using a compatible browser.

To access the console:

1. Start a compatible Web browser.
2. Go to the following link to access Trend Micro SecureSite:

   http://securesite.trendmicro.com

FIGURE 2-3. Trend Micro SecureSite logon screen

3. On the **Logon** screen, type the user name and password.
4. Click **Log on**.

Tip: If you have forgotten your password, click **Forgot your password?** and follow the on-screen instructions.

Exploring the Console

After successfully logging on, the Trend Micro SecureSite console appears. There are two main parts to the Web console: the main menu and the configuration area.

The main menu, which is located along the top of the console, contains the following sections:

- **Summary:** View the summary of all the sites, detailed information about sites, and stop scans (see *Monitoring and Managing Sites* starting on page 3-1).
- **Report:** View, download, or maintain reports (see *Managing Reports* starting on page 4-1).
- **Administration:** Perform administration tasks (see *Administering Trend Micro SecureSite* starting on page 5-1).
- **Help:** View the complete online help, administrator's guide, support details, and more information about Trend Micro SecureSite.

Below the main menu items is the configuration area. Use this area to select or view options. This changes according to the item selected from the main menu.

FIGURE 2-4. Trend Micro SecureSite Console

Chapter 3

Monitoring and Managing Sites

Understanding Summary Information

The Summary screen of the Trend Micro™ SecureSite console provides all the information administrators need, at-a-glance, to easily monitor the status of all registered sites. The Summary screen contains the following:

- **Site listing:** Displays a list of sites that SecureSite will scan. To view additional details and edit the settings, click **More details**.
- **Scan details:** Displays the last scan, status of the scan, duration, and the next scheduled scan.

TABLE 3-3. Understanding Status Icons

ICON	DESCRIPTION
	The site is certified.
	The site is no longer certified.

Tip: To stop a current scan, click **Stop Scan**.

Adding Sites

Administrators can add sites to be scanned to SecureSite. To verify the site ownership, administrators are required to upload a unique file to the site. SecureSite checks for the file, and only after verifying the upload, starts scanning the site.

To add a site:

1. Click **Summary > Add New Site.**

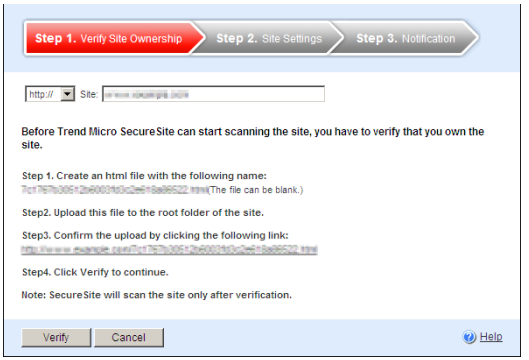


FIGURE 3-5. Step 1 of adding a site

2. On the **Verify Site Ownership** screen, type the domain name or IP address of the site and complete the verification process.
   a. Create a blank HTML file with the unique file name.
   b. Upload this file to the root folder of the server.
   c. Click the link to confirm the upload.
   d. Click **Verify** to continue.

Tip: Refer to *Site Verification Issues* starting on page A-2 for troubleshooting the verification process.

3. Click **Verify** to complete the site ownership verification process.

Note: You can proceed to the next step only after SecureSite verifies the upload.

4. On the **Site Settings** screen, update the certification mark, scan settings, and report format. See *Configuring Site Settings* on page 3-6 for more details. Click **Next**.
5. On the **Notifications** screen, update the details regarding the recipients and results. See *Configuring Notifications* on page 3-7 for more details.
6. Click **Finish**. The site will appear on the Summary screen.

Tip: Insert the certification mark code into the HTML code of the site. The certificate will appear after the site passes a daily scan.

Managing Sites

Administrators can view previous scan results, download corresponding reports and modify site and notification settings. In addition, administrators can modify the SecureSite Mark Certificate.

Site Overview

The Site Overview screen provides access to all the previous scan results and the corresponding site reports.

To view previous scan results and download corresponding reports:

1. Click **Summary >** {the required site} **> More details > Overview**.

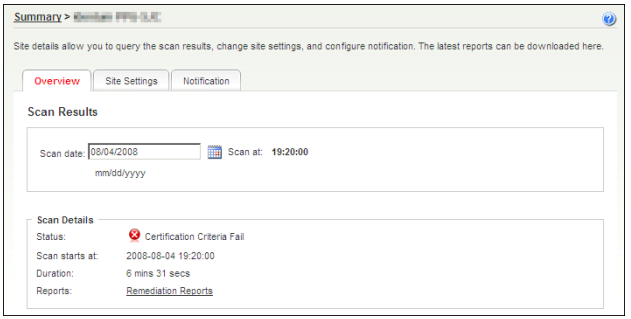


FIGURE 3-6. Overview tab of a site

2. On the **Overview** tab, type the scan date in mm/dd/yyyy format or select a date using the calendar control.

   The following scan results for the selected date and time appear:

   - Status of the certification criteria
   - Starting time of the scan
   - Duration of the scan
   - Links to relevant reports

Tip: To download a report, right-click the link corresponding to the report and select the required option to save the file.

Configuring Site Settings

SecureSite allows administrators to configure site settings. These include: the site name, report format, and the start time of the scan. From here, copy the HTML code to display the certificate on the site.

To configure site settings:

1. Click **Summary >** {the required site} **> More details > Site Settings**.

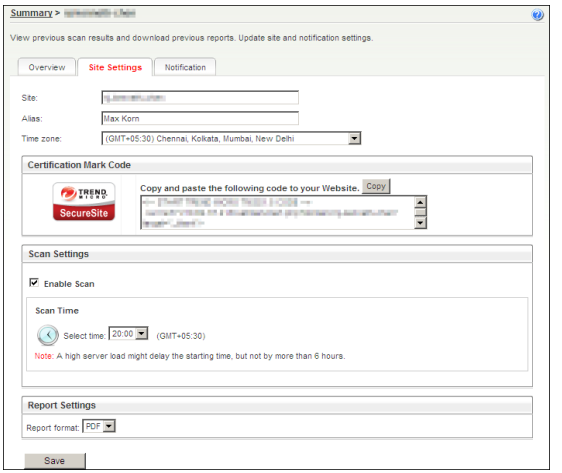


FIGURE 3-7. Site Settings tab of a site

2. On the **Site Settings** tab, update the following settings as required:
   - **Domain:** The URL of the site. If modified, the site will have to be reverified (see *Adding Sites* on page 3-3).
   - **Alias:** The name of the site as it appears on the **Summary** screen.
   - **Time zone:** The time zone of the site. This affects the scan time and the time displayed on reports.
   - **Certification Mark Code:** Paste this code on the Web site. This code dynamically changes the status of the site depending on the daily scan results.

- **Enable scan:** Enables or disables the daily scan.

  WARNING! **If the site skips three consecutive daily scans, the SecureSite Certificate Mark will not appear (see *Certification Criteria* on page 1-4).**

- **Scan time:** The required daily scan time.

  Note: A high server load might delay the starting time, but not by more than 6 hours.

- **Report format:** Select the format of the reports that SecureSite should send to the scan notification recipients (see *Configuring Notifications* on page 3-7).

3. Click **Save**.

Configuring Notifications

At the end of a scan, SecureSite can notify administrators or other recipients about the results of the scan. SecureSite also attaches a copy of the reports to the email notification. See *Configuring Site Settings* on page 3-6 to change the format of the notification.

To configure notification recipients:

1. Click **Summary >** {the required site} **> More details > Notification**.

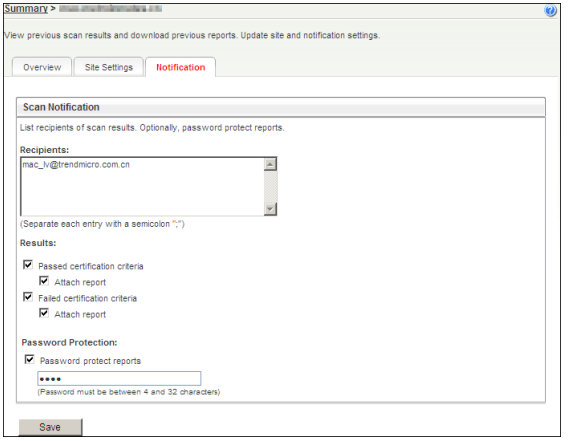


FIGURE 3-8. Notification tab of a site

2. On the **Notification** tab, update the following settings as required:
   - **Recipients:** Type the email addresses of the recipients. Separate multiple entries with semicolons ";".
   - **Results:** SecureSite notifies recipients of the following results:
     - **Passed certification criteria:** The scan is complete and the site passes the certification criteria (see *Certification Criteria* on page 1-4).

     Note: SecureSite generates a Remediation Plan for a site only if a scan detects vulnerabilities.

     - **Failed certification criteria:** The scan is complete and the site did not pass the certification criteria. Refer to the Remediation Plan to fix vulnerabilities.

     Select **Attach Report** to attach the reports of the scan along with the notification. Files will be compressed and sent as a single ZIP file.

- **Password Protection:** This password is required to open the ZIP file. Clear **Password protect reports** to not secure reports with a password.

3. Click **Save**.

Deleting Sites

Currently, Trend Micro SecureSite does not support deleting sites.

Handling Events

If a site has not passed the daily scan's certification, it could mean the site is not fully secure and could be vulnerable to threats. To fix the reported vulnerabilities, Trend Micro recommends following all steps described in the Remediation Plan (see *Remediation Plan* on page 4-3).

Chapter 4

Managing Reports

About Reports

In SecureSite, the following report types are available:

- **Executive Summary:** high-level information on the vulnerability status of the sites. See *Executive Summary* on page 4-2.
- **Remediation Plan:** information about patching detected vulnerabilities. See *Remediation Plan* on page 4-3.

Each of these reports are available in PDF formats. SecureSite stores these reports for a period of three months.

Executive Summary

The Executive Summary provides a high-level status report for all registered and scanned sites. 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.

The Executive Summary provides the following information:

- Name of the site, the start, end, and total time taken for the scan, and the status of the scan.
- Graphs displaying:
  - **Vulnerabilities by severity:** This graph categorizes the vulnerabilities for three different categories (critical, severe, and moderate) along with the number of incidents in each category.
  - **Most common vulnerabilities:** This graph names the most common vulnerabilities on the site and also displays the number of incidents for each vulnerability. The solutions to fix these vulnerabilities are available in the Discovered and Potential Vulnerabilities section of the generated report.
  - **Most common vulnerability categories:** In SecureSite, vulnerabilities are categorized based on its type. This graph names the most common vulnerability categories on the network along with the proportion for each category.
  - **Highest risk vulnerabilities:** Lists the vulnerabilities on the site that have the highest risk.

- **Most common services:** Lists the most common protocols served by the site.
- **Vulnerabilities by service:** Lists the vulnerabilities affecting each protocol.

For an example of an Executive Summary report, see Figure 4-9.

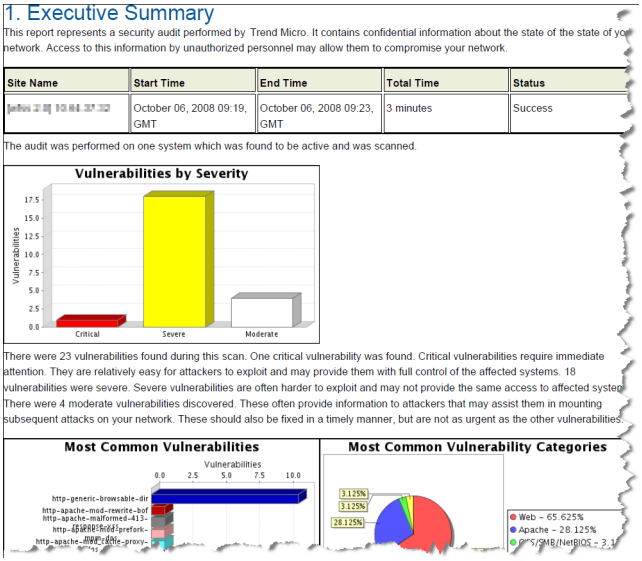


FIGURE 4-9. Sample Executive Summary

Remediation Plan

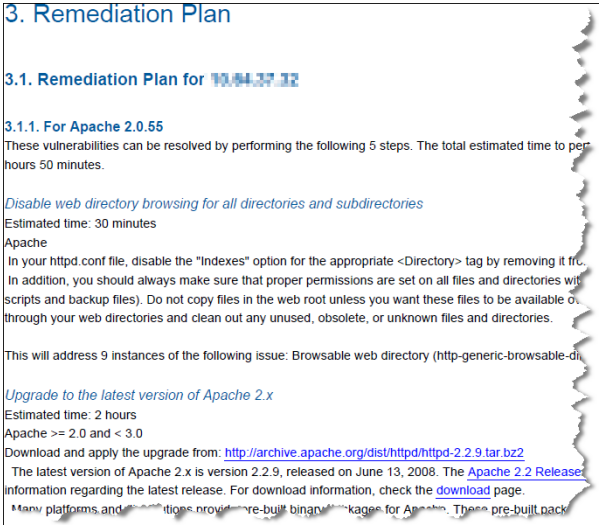
The Remediation Plan consolidates information about all vulnerabilities detected, risk assessment, and discovered systems of a site and provides an optimized plan for remediation.

Note: SecureSite generates a Remediation Plan for a site only if a scan detects vulnerabilities.

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 4-10.



3. Remediation Plan

3.1. Remediation Plan for [redacted]

3.1.1. For Apache 2.0.55

These vulnerabilities can be resolved by performing the following 5 steps. The total estimated time to per
hours 50 minutes.

Disable web directory browsing for all directories and subdirectories

Estimated time: 30 minutes

Apache

In your httpd.conf file, disable the "Indexes" option for the appropriate <Directory> tag by removing it fro
In addition, you should always make sure that proper permissions are set on all files and directories wit
scripts and backup files). Do not copy files in the web root unless you want these files to be available o
through your web directories and clean out any unused, obsolete, or unknown files and directories.

This will address 9 instances of the following issue: Browsable web directory (http-generic-browsable-di

Upgrade to the latest version of Apache 2.x

Estimated time: 2 hours

Apache >= 2.0 and < 3.0

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.bz2

The latest version of Apache 2.x is version 2.2.9, released on June 13, 2008. The Apache 2.2 Release
information regarding the latest release. For download information, check the download page.

Many platforms and [redacted]tions provide pre-built binary [redacted]kages for Apache. These pre-built pack

FIGURE 4-10. Sample Remediation Plan

Working With Reports

SecureSite stores all generated reports. Use search filters to narrow the results. From the Reports screen, administrators can view, download, or delete reports. SecureSite also allows downloading multiple reports as a single ZIP file.

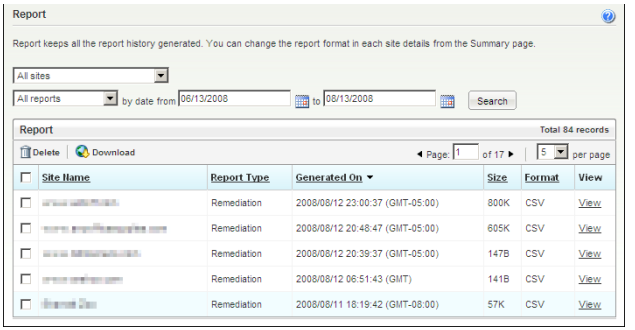


FIGURE 4-11. Reports screen

Searching for Reports

Administrators can search for a specific report on the **Reports** screen, using search criteria filters. The following filters are available:

- **Sites:** Select All sites or a specific site.
- **Report type:** Select All reports, Remediation plan, or Executive summary.
- **Date range:** Select the from and to date

Click **Search** to update the results.

Downloading Reports

SecureSite allows administrators to download a single report in its native format or a collection of reports as a single ZIP file.

To download a single report:

1. Click **Reports**.
2. After searching (see *Searching for Reports* on page 4-5) for the required report, right-click the corresponding **View** link.
3. Select the required option to save the file.

To download a collection of reports:

1. Click **Reports**.
2. Select the checkboxes corresponding to the reports to download.
3. Click **Download**.

   SecureSite creates a single ZIP file that can be saved.

Creating/Generating Reports

Trend Micro SecureSite automatically generates reports based on daily scan results. Since administrators cannot manually start a scan, reports cannot be explicitly created

Deleting Reports

SecureSite stores all generated reports for a period of three months or until manually deleted.

WARNING! A deleted report cannot be recovered or regenerated.

To delete reports:

1. Click **Reports**.
2. Select the checkboxes corresponding to the reports to delete.
3. Click **Delete**.

Chapter 5

Administering Trend Micro SecureSite

Site License

Administrators can view and renew the validity of site licenses on the Site License screen. If required, resellers can also renew a site's license.

To view or update license information:

1. Click **Administration > License Information**.

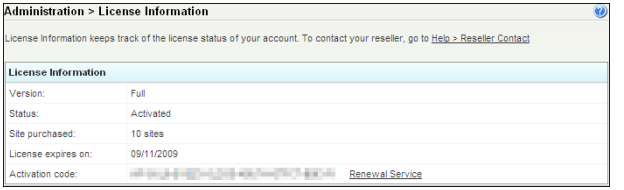


FIGURE 5-12. License Information screen

2. The Site License screen displays the following:
   - **Version:** Full or Trial.
   - **Status:** Activated or Expired.
   - **Packages purchased**
   - **Expiration date:** The date the Trend Micro SecureSite license expires.
   - **Activation Code**: The Activation Code.

   Note: Trial versions do not have an Activation Code.

3. To renew the license or view additional license details of a site, click **Renewal Service**.
   a. Trend Micro's Online Registration site opens in a new window.
   b. Log on with the appropriate credentials.
   c. Follow the on-screen instructions.

Changing the Console Password

Trend Micro recommends changing the password periodically and using strong passwords to ensure security. A strong password is at least eight characters long, has one or more uppercase letters (A-Z), one or more lowercase letters (a-z), one or more numerals (0-9), and one or more special characters or punctuation marks (!@#$%^&,.:;?). Strong passwords should not be similar to the user name, in part or whole. They should not consist of the user's given or family name, birth dates, or any other item that is easily identified with the user. In addition, avoid using dictionary words as passwords.

To change the Web console password:

1. Click **Administration > Password**. SecureSite opens the Trend Micro Online Registration (OLR) site in a new window.
2. Log on with OLR site credentials.
3. Follow the on-screen instructions to change the password.

Note: Trial users can change the password directly on the console.

Appendix A

Troubleshooting and FAQs

Troubleshooting

This section helps troubleshoot issues that may arise while using Trend Micro SecureSite.

Logon Issues

Issue: When I type my user name and password on the console and click Logon, nothing happens.

Resolution: The cookies and temporary files stored on your computer could be outdated. Clear the cookies and temporary files and try logging on again.

Issue: I cleared my cookies and temporary files. I still cannot logon.

Resolution: Ensure you are using the correct logon credentials.

Issue: The user name and password I use to logon are correct. I still cannot logon.

Resolution: Contact support for further assistance (see *Technical Support* on page B-3).

Site Verification Issues

Issue: SecureSite is unable to find the domain name/IP address of the site.

Resolution: The following reasons could be the cause of the issue:

- The server hosting the site is not accessible or extremely busy. Retry the verification process after confirming the server is accessible.
- The domain name is not resolving correctly. Contact the hosting service to help resolve the issue.

Issue: A DNS or server time-out occurs during the verification process.

Resolution: The following reasons could be the cause of the issue:

- The server hosting the site is not accessible or extremely busy. Retry the verification process after confirming the server is accessible.
- The domain name is not resolving correctly. Contact the hosting service to help resolve the issue.

Issue: SecureSite cannot locate the verification file.

Resolution: The following reasons could be the cause of the issue:

- Incorrect file name: Check to see if the file name is the same as the one generated.
- Incorrect file extension: SecureSite requires the file extension to be `*.html`. Some editors could change the extension to `*.htm` or even `*.html.txt`. Check to see if the file extension is `*.html`.
- Incorrect location: Check to see if the file is uploaded to the root folder of the site.

Issue: The site does not return a 4xx HTML status code for non-existing URLs.

Resolution: If the site is using HTML verification, it's required for non-existing URLs to return a 4xx status code. SecureSite cannot verify sites configured to return other status codes (2xx or 5xx) for non-existing URLs. Try changing the server's configuration.

SecureSite Certification Mark Issues

Issue: My SecureSite Certification Mark is not appearing on my site.

Resolution: There could be a number of reasons why your certificate is not appearing. They are:

1. Your site has not met the required certification criteria (see *Certification Criteria* on page 1-4).
2. You have pasted the incorrect code on the Web site. See *Configuring Site Settings* on page 3-6 to get the correct code.
3. Your site license could have expired. See *Site License* on page 5-2 to view the site license.

Frequently Asked Questions (FAQs)

The following is a list of frequently asked questions and answers.

Question: What is Trend Micro SecureSite?

Answer: Trend Micro SecureSite is a hosted solution that helps assure consumers of the safety and integrity of small business online retail Web sites.

Question: How do I retain my certification?

Answer: You retain your certification by passing a daily scan at least once in the previous 72 hours.

Question: Can I choose a different Trend Micro SecureSite certificate for my site?

Answer: This version provides only one certificate type. Future versions could support multiple certificate types.

Question: The URL of my site has changed. What do I do?

Answer: You can change the URL or IP address of your site (see *Configuring Site Settings* on page 3-6). However, after making the change, you would need to reverify the site.

Question: Why am I not getting any Remediation Plans?

Answer: SecureSite generates a Remediation Plan for a site only if it detects vulnerabilities. However, you should still receive Executive Summaries. If not, check if you have enabled this option (see *Configuring Notifications* on page 3-7).

Question: Why can't I see the Welcome screen when I logon?

Answer: The Welcome screen is only visible to Trial Users who haven't migrated their account. After migration, you cannot see this screen.

Question: Why did my settings disappear after migration?

Answer: After migration, your account will use the new profile. Your old settings will no longer be available.

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 *Technical Support* on page B-3 for more information).

Product Documentation

Trend Micro SecureSite documentation includes Online Help and an Administrator's Guide.

- **Online Help:** Click the help icon () to open context-sensitive help.
- **Administrator's Guide:** Download the latest Administrator's Guide from the Trend Micro Update Center:

  http://www.trendmicro.com/download

Note: Trend Micro is always seeking to improve its documentation. For questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. You can also evaluate this documentation on the following site:
www.trendmicro.com/download/documentation/rating.asp

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 a trial version of a product.

http://esupport.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

To contact Trend Micro Technical Support:

- Visit the following URL:

  http://esupport.trendmicro.com

  Click the link for the required segment. Follow the instructions for contacting support in your region.
- If you prefer to communicate by email, send a query to the following address:

  tmss_support@trendmicro.com
- In the United States, you can also call the following toll-free telephone number:

  `(877) TRENDAV, or 877-873-6328`

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

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

Glossary

TABLE G-4. Glossary of Terms

TERM	DEFINITION
Certificate	The image (Trend Micro SecureSite Mark) that certifies the site is safe and secure.
Console	The Web console from where administrators can view and configure site settings and download reports.
Executive Summary	Provides high-level information on the vulnerability status of the sites.
Remediation Plan	Provides information about patching detected vulnerabilities.
SecureSite	Trend Micro SecureSite
Site Alias	The name of the site as it appears on the Summary screen. A nickname.
Time Zone	The time zone of the site. This affects the scan time and the time displayed on reports.

Index

S (cont.)

T

V

X