3.2 TREND MICRO™ SafeSync for Enterprise
Administrator’s Guide
Securely Share, Distribute, and Control Enterprise Information Within Your Private Cloud
Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:


Trend Micro, the Trend Micro t-ball logo, and SafeSync for Enterprise 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 © 2016. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM37323/160217

Release Date: March 2016

Protected by U.S. Patent No.: Patents pending.
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks 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.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
# Table of Contents

## Preface

Preface ........................................................................................................................................ vii  
SafeSync Documentation ........................................................................................................ viii  
Audience .................................................................................................................................. viii  
Document Conventions ............................................................................................................ ix  
Terminology ............................................................................................................................ x  

## Chapter 1: Introducing SafeSync

About SafeSync ...................................................................................................................... 1-2  
What’s New ........................................................................................................................... 1-2  
What’s New in This Version .................................................................................................. 1-2  
Features and Benefits .......................................................................................................... 1-8  
System Requirements ............................................................................................................ 1-10

## Chapter 2: Users, Policies, and Plans

SafeSync Users, Policies, and Plans ..................................................................................... 2-2  
Policy and Plan Priority of Domain Accounts .................................................................... 2-2  
Policy and Plan Priority of Manual Accounts ..................................................................... 2-5  
SafeSync Policy and Plan Features ..................................................................................... 2-5  
Managing Users .................................................................................................................... 2-6  
SafeSync User Accounts ...................................................................................................... 2-7  
Searching for a User Account or Group ............................................................................... 2-16  
Viewing Individual User Details ......................................................................................... 2-16  
Inviting Users to Share Files ............................................................................................... 2-17  
Configuring Policies ............................................................................................................ 2-17  
The Default Policy ............................................................................................................... 2-18  
Adding Policies .................................................................................................................... 2-20
Editing Policies ................................................................. 2-21
Deleting Policies ................................................................. 2-21
Reviewing Policy Assignments .......................................... 2-22
Configuring Plans ............................................................... 2-22
The Default Plan ............................................................... 2-23
Adding Plans ................................................................. 2-23
Editing Plans ................................................................. 2-24
Deleting Plans ................................................................. 2-24
Reviewing Plan Assignments ........................................... 2-25

Chapter 3: Monitoring SafeSync

SafeSync Dashboard ......................................................... 3-2
Working with Widgets ..................................................... 3-2
Threat Detections ............................................................. 3-3
Usage Overview ............................................................. 3-9
System Status ................................................................. 3-11
Reports ................................................................. 3-14
Generating Reports ......................................................... 3-15
Logs ................................................................. 3-15
Querying Logs ................................................................. 3-16
Deleting Logs ................................................................. 3-16
Forwarding Logs to a Syslog Server .................................. 3-16

Chapter 4: Administering SafeSync

Account Settings ............................................................. 4-3
Changing the Administrator Account Settings .................. 4-3
Administrator Accounts .................................................... 4-4
Adding Administrator Accounts ...................................... 4-4
Editing Administrator Accounts ...................................... 4-4
Deleting Administrator Accounts .................................... 4-5
Enabling or Disabling Administrator Accounts ................ 4-5
System Notifications ....................................................... 4-6
Configuring System Notification Settings ....................... 4-6
Active Directory Integration ............................................ 4-7
Configuring Active Directory Integration ....................... 4-7
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding Additional Active Directory Servers ................................. 4-8</td>
</tr>
<tr>
<td>Antivirus Settings .................................................................................. 4-9</td>
</tr>
<tr>
<td>Configuring Antivirus Settings .......................................................... 4-9</td>
</tr>
<tr>
<td>Configuring Smart Protection Server Settings ................................. 4-14</td>
</tr>
<tr>
<td>Performing a Manual Scan ................................................................. 4-15</td>
</tr>
<tr>
<td>Updating Components ........................................................................ 4-15</td>
</tr>
<tr>
<td>System Settings .................................................................................... 4-19</td>
</tr>
<tr>
<td>Configuring SafeSync Web Console Settings ...................................... 4-19</td>
</tr>
<tr>
<td>Configuring Proxy Server Settings ..................................................... 4-20</td>
</tr>
<tr>
<td>Configuring SMTP Server Settings ..................................................... 4-21</td>
</tr>
<tr>
<td>Updating SSL Certificate Information ................................................. 4-22</td>
</tr>
<tr>
<td>Understanding SafeSync Add-Ins .......................................................... 4-22</td>
</tr>
<tr>
<td>Configuring the Web Console Language .............................................. 4-27</td>
</tr>
<tr>
<td>High Availability ................................................................................... 4-28</td>
</tr>
<tr>
<td>Database Replication .......................................................................... 4-29</td>
</tr>
<tr>
<td>File Replication .................................................................................. 4-29</td>
</tr>
<tr>
<td>Load Balancing .................................................................................... 4-30</td>
</tr>
<tr>
<td>Configuring High Availability - Primary Server .................................. 4-31</td>
</tr>
<tr>
<td>Configuring High Availability - Secondary Server .............................. 4-31</td>
</tr>
<tr>
<td>Verifying MySQL HA ........................................................................... 4-32</td>
</tr>
<tr>
<td>Verifying File Replication .................................................................. 4-37</td>
</tr>
<tr>
<td>Security Control ................................................................................... 4-39</td>
</tr>
<tr>
<td>Enabling or Disabling Shareable Links ............................................... 4-39</td>
</tr>
<tr>
<td>Managing User Sessions ...................................................................... 4-40</td>
</tr>
<tr>
<td>Cache Servers ....................................................................................... 4-41</td>
</tr>
<tr>
<td>Adding Cache Servers ......................................................................... 4-42</td>
</tr>
<tr>
<td>Editing Cache Servers ......................................................................... 4-42</td>
</tr>
<tr>
<td>Deleting Cache Servers ....................................................................... 4-43</td>
</tr>
<tr>
<td>Storage Management ............................................................................ 4-44</td>
</tr>
<tr>
<td>Managing Storage ................................................................................ 4-44</td>
</tr>
<tr>
<td>Managing Team Folders ....................................................................... 4-48</td>
</tr>
<tr>
<td>Managing Files Left by Deleted Users ............................................... 4-49</td>
</tr>
<tr>
<td>System Maintenance .............................................................................. 4-51</td>
</tr>
<tr>
<td>System Updates ..................................................................................... 4-52</td>
</tr>
<tr>
<td>Downloading Update Files .................................................................. 4-52</td>
</tr>
</tbody>
</table>
Chapter 5: Frequently Asked Questions (FAQs)

Files ................................................................. 5-2
   How can I upload files that are more than 3 GB in size? .......... 5-2
   Why am I unable to view some thumbnail images? .............. 5-2
   Why am I unable to upload files to a team folder? .......... 5-3

Services ................................................................. 5-4
   What services should be installed after a successful SafeSync
   installation? ................................................................. 5-4
   How can I verify if all SafeSync services are working properly? .... 5-4

Storage ................................................................. 5-5
   How does SafeSync determine the storage limit for each user? .... 5-5

SSL Certificates ................................................................. 5-5
   Does SafeSync support PKCS7 certificates? .................... 5-6
   Does SafeSync support wildcard certificates? .................... 5-7

Chapter 6: Contacting Technical Support

   Contacting Trend Micro ................................................................. 6-2
   Speeding Up the Support Call ................................................................. 6-2

Appendix A: Understanding Threats

   Viruses and Malware ................................................................. A-2
   Trend Micro Smart Protection Network ................................................................. A-4

Appendix B: Understanding Components

   Smart Scan Agent Pattern ................................................................. B-2
   Virus Scan Engine ................................................................. B-2
Appendix C: Deploying SafeSync to End Users

Deploying SafeSync to Desktops and Laptops ........................................ C-2
Deploying SafeSync to Mobile Devices ..................................................... C-3

Appendix D: SafeSync Cache Server Program

System Requirements ..................................................................................... D-2
Installation Methods ..................................................................................... D-2
Installing the SafeSync Cache Server Program ........................................... D-2

Appendix E: Glossary

Index

Index .............................................................................................................. IN-1
Preface

Welcome to the Trend Micro™ SafeSync for Enterprise™ Administrator’s Guide. This document discusses SafeSync for Enterprise™ management and monitoring tasks.

Topics in this chapter include:

- SafeSync Documentation on page viii
- Audience on page viii
- Document Conventions on page ix
- Terminology on page x
SafeSync Documentation

SafeSync documentation includes the following.

**TABLE 1. SafeSync Documentation**

<table>
<thead>
<tr>
<th><strong>DOCUMENTATION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Guide</td>
<td>A PDF document that discusses requirements and procedures for installing SafeSync.</td>
</tr>
<tr>
<td>Administrator's Guide</td>
<td>A PDF document that provides &quot;how to's&quot;, advice, usage and field-specific information.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides the basic requirements and procedures for installing SafeSync.</td>
</tr>
<tr>
<td>Readme file</td>
<td>Text-based documentation that 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.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

Download the latest version of the PDF documents and readme at:


**Audience**

SafeSync documentation is intended for administrators responsible for installing and managing SafeSync. These administrators are expected to have advanced networking and server management knowledge.
Document Conventions

The documentation uses the following conventions.

**TABLE 2. Document Conventions**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documents</td>
</tr>
<tr>
<td>Monospace</td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>
Terminology

The following table provides the official terminology used throughout the SafeSync documentation.

**TABLE 3. SafeSync Terminology**

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator (or SafeSync administrator)</td>
<td>The person managing the SafeSync server</td>
</tr>
<tr>
<td>Console</td>
<td>The user interface for configuring and managing SafeSync</td>
</tr>
<tr>
<td></td>
<td>The console for the SafeSync server program is called &quot;web console&quot;.</td>
</tr>
<tr>
<td>End user</td>
<td>Users that share content using SafeSync</td>
</tr>
<tr>
<td>Portal</td>
<td>The end-user web console for managing SafeSync files</td>
</tr>
</tbody>
</table>
Chapter 1

Introducing SafeSync

This chapter introduces SafeSync and provides an overview of its features and benefits.

Topics in this chapter include:

- About SafeSync on page 1-2
- What's New on page 1-2
- Features and Benefits on page 1-8
- System Requirements on page 1-10
About SafeSync

Trend Micro™ SafeSync for Enterprise™ allows enterprises to securely synchronize, share, and manage corporate data. Deployed on premise and in a private cloud, SafeSync provides file encryption and document tagging to prevent unauthorized access to sensitive data. SafeSync also supports file version control and redundant file backup.

Businesses benefit from reduced infrastructure resource usage by using file sharing links instead of sending files through email servers. The web-based administrator console makes it easy to manage users, set coordinated policies and plans, and review logs and reports. SafeSync provides administrators the visibility required to control data misuse, compliance violations, and security risks.

What's New

What's New in This Version

The following new features and enhancements are available in version 3.2.

<table>
<thead>
<tr>
<th>TABLE 1-1. New Features and Enhancements for SafeSync for Enterprise 3.2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE</strong></td>
</tr>
<tr>
<td>Cache servers</td>
</tr>
<tr>
<td>Storage management</td>
</tr>
<tr>
<td>SSL certificate import</td>
</tr>
</tbody>
</table>
Introducing SafeSync

**Feature Description**

**Platform support**

This version supports the following:

- Windows Server 2008 R2 and 2012 R2 - Active Directory server
- Mac 10.11
- Android 6.x
- iOS 9.1, 9.2
- Outlook 2016

---

**What's New in Version 3.1**

The following new features and enhancements are available in version 3.1.

**Table 1-2. New Features and Enhancements for SafeSync for Enterprise 3.1**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Side</strong></td>
<td></td>
</tr>
<tr>
<td>Server installation</td>
<td>There are two ways to install SafeSync, either from an ISO image file or an Open Virtualization Format (OVF) installation package. Both methods allow you to set up a high availability deployment and add additional hard disks for storage expansion.</td>
</tr>
<tr>
<td></td>
<td>• ISO image file: can be installed on a bare metal server or a virtual machine.</td>
</tr>
<tr>
<td></td>
<td>• OVF installation package: can only be installed on a virtual machine. The installation process is fast (about 10 minutes). This method is suitable for proof of concept evaluation.</td>
</tr>
<tr>
<td>Administrator accounts</td>
<td>Set up multiple administrator accounts to manage SafeSync.</td>
</tr>
<tr>
<td>Active Directory integration</td>
<td>Integrate SafeSync with multiple Active Directory structures. Administrators can selectively choose the users or groups to synchronize with SafeSync.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web consoles settings</td>
<td>Set up web console settings using single-level domain and access SafeSync using the configured domain name.</td>
</tr>
<tr>
<td>High availability deployment</td>
<td>Set up a high availability deployment from the administrator web console.</td>
</tr>
<tr>
<td>Shareable links</td>
<td>Administrators can enforce security control on shareable links in policy settings. End users may be required to sign in or provide a password to access a link. End users can now exchange files through shareable links and set access permissions to the files they share.</td>
</tr>
<tr>
<td>User session control</td>
<td>Administrators can enforce strong security control on user sessions by requiring end users to sign in every time they access SafeSync. Administrators can also configure the security control setting to automatically sign out inactive users.</td>
</tr>
<tr>
<td>Storage management</td>
<td>Administrators can manage team folder storage and owners.</td>
</tr>
<tr>
<td>End-User Side</td>
<td></td>
</tr>
<tr>
<td>Online file preview</td>
<td>View files like PDFs, Microsoft Office files, images, and videos directly in the end-user portal. Users with permissions to open encrypted files can also view them in the end-user portal.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Notify users of important events in the end-user portal and Windows client, such as new team folders or malicious file detections.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Make files or folders as Favorites for easy access in the end-user portal.</td>
</tr>
<tr>
<td>Sub-folder level permission control</td>
<td>Control team folder permissions on the sub-folder level. Set permissions on each sub-level folder by different users or groups.</td>
</tr>
<tr>
<td>End-user portal interface</td>
<td>Brand new design and better user experience.</td>
</tr>
</tbody>
</table>
# Introducing SafeSync

## Feature Description

- **Diagnostic tool in Android and iOS apps**
  Collect SafeSync event logs that Support uses for troubleshooting purposes.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform support</td>
<td>• Administrator web console and end-user portal support Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>• Mac client supports Mac 10.10</td>
</tr>
<tr>
<td></td>
<td>• Windows client supports Windows 10</td>
</tr>
<tr>
<td></td>
<td>• Android app supports Android 5.x</td>
</tr>
<tr>
<td></td>
<td>• iOS app supports iOS 9.0</td>
</tr>
</tbody>
</table>

## What's New in Version 2.1 Service Pack 1

The following new features and enhancements are available in version 2.1 SP1.
## Table 1-3. New Features and Enhancements for SafeSync for Enterprise 2.1 SP1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus scan</td>
<td>Perform Antivirus scan when users upload or share files.</td>
</tr>
<tr>
<td></td>
<td>After installing this service pack, SafeSync for Enterprise can perform antivirus scan on files and quarantine files detected as malicious. SafeSync for Enterprise provides a configurable secure environment for data uploading, sharing, downloading, and synchronization.</td>
</tr>
<tr>
<td></td>
<td>Prevent malicious files from spreading.</td>
</tr>
<tr>
<td></td>
<td>Files detected as malicious are quarantined to prevent users from accidentally opening the files. The detected files are not synchronized, downloaded, or shared.</td>
</tr>
<tr>
<td></td>
<td>Analyze threat detection trends at a glance.</td>
</tr>
<tr>
<td></td>
<td>Administrators can easily manage the threat status using widgets. Threat detection widgets include threat statistics, top 10 detection and top 10 threats, and component status. Administrators have the option of exporting the data into CSV files.</td>
</tr>
<tr>
<td></td>
<td>Specify Active Update and Smart Protection Server sources.</td>
</tr>
<tr>
<td></td>
<td>Administrators can specify the Active Update and Smart Protection Server sources based on the network environment.</td>
</tr>
<tr>
<td>Multiple downloads</td>
<td>End users can download multiple files and folders as an archived file from the end-user portal.</td>
</tr>
</tbody>
</table>
Introducing SafeSync

More platform support

- SafeSync for Enterprise Windows client support for Windows 8.1.
- Active Directory integration now supports the Windows 2012 Active Directory server.

What's New in Version 2.1

The following new features and enhancements are available in version 2.1.

**Table 1-4. New Features and Enhancements for SafeSync for Enterprise 2.1**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory integration</td>
<td>- Enhanced Active Directory integration</td>
</tr>
<tr>
<td></td>
<td>- Select and assign Active Directory users and groups permission to use the</td>
</tr>
<tr>
<td></td>
<td>SafeSync service from the SafeSync web console</td>
</tr>
<tr>
<td>Shared Protection Extension add-in</td>
<td>- File encryption</td>
</tr>
<tr>
<td></td>
<td>- Secure file sharing</td>
</tr>
<tr>
<td></td>
<td>- Encrypt files under a folder automatically</td>
</tr>
<tr>
<td>Outlook Extension add-in</td>
<td>Enhanced with the Shared Protection Extension features</td>
</tr>
<tr>
<td>Dashboard widget</td>
<td>System Status Alert widget</td>
</tr>
<tr>
<td>Policy management</td>
<td>Control how end users share and upload files</td>
</tr>
<tr>
<td>Plan management</td>
<td>Assign plans to domain users based on plan priority or specify plans</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Logs</td>
<td>• Log query</td>
</tr>
<tr>
<td></td>
<td>• Log maintenance</td>
</tr>
<tr>
<td></td>
<td>• Syslog server settings</td>
</tr>
<tr>
<td>Administration</td>
<td>• System updates</td>
</tr>
<tr>
<td></td>
<td>• License management for SafeSync add-ins</td>
</tr>
<tr>
<td>End user mobile apps</td>
<td>User interface enhancements</td>
</tr>
</tbody>
</table>

### Features and Benefits

SafeSync provides the following features and benefits.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access files from anywhere</td>
<td>Anytime, anywhere file accessing, editing, and organizing from any device: PCs, Macs, and Android and iOS mobile devices.</td>
</tr>
</tbody>
</table>
| Sync files continuously and automatically | Data storage and synchronization with additional file copies held on your on-premise servers that can be easily restored or accessed, in case of a hardware loss, theft, or failure.  
Data storage and synchronization with additional file copies held on Trend Micro cloud servers.  
Continuous automatic file synchronization with 2 ways to synchronize files. End users can drag and drop files easily into the folder they wish to sync.  
Folder pairing enables automatic syncing of an entire folder without the need to drag and drop files into the SafeSync folder. |
### Introducing SafeSync

**Benefit** | **Description**
---|---
Share files easily and securely | Fast and secure file and folder sharing with the shareable link.  
Set links with passwords that expire for additional security.  
“Team Folders” for effective group collaboration that can be created on the fly by staff and administrators.  
View files like PDFs, Microsoft Office files, images, and videos directly in the end-user portal.

Easily create and control user accounts | SafeSync supports centralized administration for creating and controlling users.

Recover previous versions of files | Recover deleted files or previous file versions from the end user portal.

Protect files with encryption | Protect files with the same Advanced Encryption Standard (AES) 256-bit encryption used by the government and military.

Securely share email attachments sent from Microsoft Outlook | When the **SafeSync Outlook Extension** is enabled, users can either upload their attachments to SafeSync and send a shareable link in the email, or use the auto-encryption option to automatically encrypt file attachments.  
When the auto-encryption option is enabled, all attachments are automatically encrypted and the only people who can open the attachments are the SafeSync users who are the original recipients of the email.  
The **SafeSync Outlook Extension** helps to prevent unintentional data leakage through misdirected or forwarded emails, or device loss.

Automatically encrypt files using an auto-encryption folder | When the **Shared Protection Extension** is enabled, users can create an auto-encryption folder. All files added to this folder are encrypted automatically.  
When a user creates an auto-encryption folder, they are prompted to identify who can access the folder. An auto-encryption folder is essentially an encrypted team folder.  
Use the auto-encryption folder to securely share sensitive files, such as those used by Human Resources or Finance.
System Requirements

The following table provides the system requirements for using SafeSync.

**TABLE 1-5. System Requirements**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator web console</td>
<td>Chrome, latest version</td>
</tr>
<tr>
<td></td>
<td>Firefox, latest version</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>Safari 7.0 and later</td>
</tr>
</tbody>
</table>

**Benefit**

- **Convenient remote administration**: You have the ability to control user accounts and share or revoke access to your shared files at any time.
- **Prevent data loss**: Create policies to block specific file types and prevent the transmission of digital assets against accidental or deliberate leakage through the use of file encryption settings.
- **Scan files for virus/malware threats**: When the antivirus feature is enabled, SafeSync automatically scans uploaded and shared files for virus/malware threats. After detecting a potentially malicious file, SafeSync warns users before downloading the file.

**Description**

**Benefit**

- **Convenient remote administration**: You have the ability to control user accounts and share or revoke access to your shared files at any time.
- **Prevent data loss**: Create policies to block specific file types and prevent the transmission of digital assets against accidental or deliberate leakage through the use of file encryption settings.
- **Scan files for virus/malware threats**: When the antivirus feature is enabled, SafeSync automatically scans uploaded and shared files for virus/malware threats. After detecting a potentially malicious file, SafeSync warns users before downloading the file.
## Introducing SafeSync

### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user web portal</td>
<td>Chrome, latest version</td>
</tr>
<tr>
<td></td>
<td>Firefox, latest version</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td></td>
<td>Microsoft Edge</td>
</tr>
<tr>
<td></td>
<td>Safari 7.0 and later</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Recommended screen resolution for viewing the end-user web portal: 1366 x 768</td>
</tr>
<tr>
<td>End-user client</td>
<td>Mac 10.9, 10.10, 10.11</td>
</tr>
<tr>
<td></td>
<td>Windows 7, 8.x, 10</td>
</tr>
<tr>
<td></td>
<td>Android 4.x, 5.x, 6.x</td>
</tr>
<tr>
<td></td>
<td>iOS 7.x, 8.x, 9.0, 9.1, 9.2</td>
</tr>
</tbody>
</table>
Chapter 2

Users, Policies, and Plans

This chapter explains how to manage user accounts and configure the SafeSync plans and policies that apply to users.

Topics in this chapter include:

• SafeSync Users, Policies, and Plans on page 2-2
• Managing Users on page 2-6
• Searching for a User Account or Group on page 2-16
• Viewing Individual User Details on page 2-16
• Inviting Users to Share Files on page 2-17
• Configuring Policies on page 2-17
• Configuring Plans on page 2-22
SafeSync Users, Policies, and Plans

SafeSync allows you to create and assign specific policies and plans at a global or granular level to Active Directory user accounts, user groups, and manually created SafeSync accounts. When assigning policies and plans to users, consider the type of user account you are configuring.

Policy and Plan Priority of Domain Accounts

SafeSync allows you to prioritize your policies and plans to ensure that the highest priority policy or plan is always assigned to a domain account first.

You can assign Active Directory accounts policies and plans to specific user accounts or to entire groups.
If a domain account is part of an Active Directory group, the user inherits the policy and plan assigned to the group. However, if a specific policy or plan is assigned to a domain account, the specified policy or plan supersedes the policy or plan assigned to the group.

**Figure 2-1. Active Directory (AD) user policy and plan assignments**
When assigning policies and plans by priority, consider the example below.

**Figure 2-2. Active Directory (AD) user policy and plan priority**

Policy A has a higher priority than Policy B.
Plan A has a higher priority than Plan B.
### TABLE 2-1. User Policy and Plan Priority

<table>
<thead>
<tr>
<th>GROUP/USER</th>
<th>POLICY</th>
<th>PLAN</th>
<th>POLICY/PLAN ASSIGNMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>A</td>
<td>B</td>
<td>Assigned by administrator</td>
</tr>
<tr>
<td>Group B</td>
<td>B</td>
<td>A</td>
<td>Assigned by administrator</td>
</tr>
<tr>
<td>Group C</td>
<td>A</td>
<td>B</td>
<td>Inherited from Group A</td>
</tr>
<tr>
<td>User 1</td>
<td>A</td>
<td>B</td>
<td>Inherited from Group C</td>
</tr>
</tbody>
</table>
| User 2     | A      | A    | • Inherited higher priority Policy from Group A   
|            |        |      | • Inherited higher priority Plan from Group B     |

### Policy and Plan Priority of Manual Accounts

For manual accounts, you must individually specify the policy and plan to each account.

![Manual account policy and plan assignment](image-url)

**Figure 2-3. Manual account policy and plan assignment**

### SafeSync Policy and Plan Features

The following table describes the configurations related to policies and plans.
### Table 2-2. Policy and Plan Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td>“Permission Control” that allows you to:</td>
</tr>
<tr>
<td></td>
<td>• Define the maximum file size that a user can upload to the server</td>
</tr>
<tr>
<td></td>
<td>• Define the types of files that SafeSync blocks</td>
</tr>
<tr>
<td></td>
<td>• Grant users permissions to exchange files and create team folders</td>
</tr>
<tr>
<td></td>
<td>• Require users to sign in to exchange files and set passwords and expiration dates on shared files</td>
</tr>
<tr>
<td></td>
<td>• Allow users to download files detected as being malicious from the end-user portal</td>
</tr>
<tr>
<td><strong>Plan</strong></td>
<td>“Storage Control” that allows you to:</td>
</tr>
<tr>
<td></td>
<td>• Assign the maximum amount of storage users receive</td>
</tr>
<tr>
<td></td>
<td>• Limit the upload and download speeds for file transfers</td>
</tr>
<tr>
<td></td>
<td>• Define the level of version control assigned to users</td>
</tr>
</tbody>
</table>

### Managing Users

You can synchronize the preexisting Active Directory account structure and create manual accounts not managed by Active Directory to define SafeSync users.

Configure specific users or domains with customized SafeSync policies and plans to manage the access permitted to SafeSync users.

**Important**

You must configure the Active Directory and end-user portal connection settings before managing users, plans, or policies.

For more information, see Configuring Active Directory Integration on page 4-7 and Configuring SafeSync Web Console Settings on page 4-19.
SafeSync User Accounts

Define the following types of SafeSync user accounts:

- Domain Accounts on page 2-7
- Manual Accounts on page 2-10

Domain Accounts

Configure domain accounts after synchronizing SafeSync with your Active Directory. SafeSync uses the Active Directory structure to allow you to specify which SafeSync policies and plans to apply to users and domain groups.

**Important**

You cannot modify Active Directory domain user accounts or groups using the SafeSync web console.

Adding Active Directory Domain Groups to SafeSync

Grant selected domain accounts permission to use the SafeSync service.

For more information on manually creating SafeSync accounts, see *Adding Manual Accounts on page 2-10*.

**Note**

You must configure the Active Directory and end-user portal connection settings before managing users, plans, or policies.

For more information, see *Configuring Active Directory Integration on page 4-7* and *Configuring SafeSync Web Console Settings on page 4-19*.

**Procedure**

1. Go to Users.
2. From the left-hand users directory, click [ ].
The **Add Accounts** screen appears.

3. Select groups from the **Active Directory Groups** pane and click ➔.

   SafeSync adds the selected groups to the **SafeSync Groups** pane.

4. Click **OK**.

   SafeSync lists the users and groups in the left-hand Active Directory user directory. Click any user or group to view detailed information in the center pane.

---

### Removing Active Directory Domain Groups

---

**Note**

SafeSync automatically updates Active Directory account information after synchronizing with Active Directory. If you remove an account from Active Directory, SafeSync also removes the account information during the next scheduled Active Directory synchronization.

---

**Procedure**

1. Go to **Users**.

2. Click the gear icon (⚙️) beside the **Active Directory** domain list.

   The **Add Accounts** screen appears.

3. In the SafeSync Groups list, select the check box next to the group you want to remove from SafeSync.

4. Click the left arrow (↩️) to remove the selected groups from the SafeSync Groups list.

5. Click **OK**.
Changing Active Directory Account Plans and Policies

Procedure

1. Go to Users.

2. In the Active Directory domain list, select a domain group or specific user account.

   The selected account or group information appears in the center pane.

3. Change the policy or plan that SafeSync applies.

   • For domain groups:
     • To modify the settings for specific accounts, select the check boxes next to the user accounts to modify and then click Change Policy or Change Plan.
     • To modify the settings for the entire domain group, click change next to the policy or plan name above the list.
     • For specific accounts, click change next to the policy or plan name above the user account information.

   The Change Plan or Change Policy screen appears.

4. Specify how SafeSync applies the policy or plan to the selected user(s).

   • Assign by priority: SafeSync applies the highest priority policy or plan that matches the user account.

   • Specify: Select a policy or plan from the drop-down list.

5. Click Save.

Managing Disabled Domain Accounts

SafeSync temporarily disables domain accounts when the following occurs:
• Unsuccessful Active Directory synchronization due to connection issues
• Domain accounts have been deleted from the Active Directory structure

The **Disabled Accounts** screen allows administrators to remove disabled or deleted domain accounts from SafeSync.

---

**Procedure**

1. Go to **Users**.
2. Click the number next to **Disabled** at the top right corner of the table.
   
   The **Disabled Accounts** screen appears.
3. Select the check box next to the user account you want to manage.
4. Click **Delete** to remove disabled domain accounts.

---

**Manual Accounts**

SafeSync allows you to create custom user accounts for individuals that do not have an Active Directory account.

**Adding Manual Accounts**

---

**Procedure**

1. Go to **Users**.
2. Add a new account by:
   
   • Clicking the add icon (➕) in the **Manual Accounts** list.
   • Clicking **Manual Accounts** and then clicking the **Add** button above the table that appears.

   The **Add User** screen appears.
3. Specify the new account details and which plan and policy to apply.
   a. Specify the user name, email address, description, and password.
   b. Select a policy or plan from the drop-down lists.

4. Click Add.

SafeSync adds the account to the **Manual Accounts** list.

---

**Note**
SafeSync automatically enables all newly-created accounts.

---

**Editing Manual Accounts**

**Procedure**

1. Go to **Users**.

2. View an existing user account.
   - Click a user account under **Manual Accounts**.
   - Click **Manual Accounts** and then click an account name in the table that appears.

The selected user account's details display.

3. Click the **edit** link above the user account details.

   The **Edit User** screen appears.

4. Modify the description, password, policy, and plan as required.

5. Select **Disable** if you want to temporarily restrict access to this account.

6. Click **Save**.
Deleting Manual Accounts

You can delete a manual user account at any time. Delete manual user accounts through the SafeSync web console when you no longer want to allow a user access to the SafeSync service.

**WARNING!**
Deleting a manual user account also deletes all personal files that the user uploaded to SafeSync. SafeSync does not delete data uploaded to team folders.

**Procedure**

1. Go to **Users**.
2. Click **Manual Accounts**.
   
   The **Manual Accounts** list appears.
3. Select the check box next to the user account that you want to delete.
4. Click **Delete**.
5. Click **Yes** in the confirmation dialog that appears.
   
   SafeSync deletes the account and all personal data related to the account.

Enabling/Disabling Manual Accounts

You can disable manual user accounts to temporarily restrict a user's access to the SafeSync service. Disabling a user account does not delete any personal or team folder data associated with the user account.

**Procedure**

- Enable or disable an existing account from the account details screen:
  
  a. Go to **Users**.
  
  b. View an existing user account.
• Click a user account under Manual Accounts.

• Click Manual Accounts and then click an account name in the table that appears.

The selected user account's details display.

c. Click the edit link above the user account details.

The Edit User screen appears.

d. Select Enable or Disable.

e. Click Save.

• Enable or disable an existing account from the Manual Accounts table:

  a. Go to Users.

  b. Click Manual Accounts.

  c. Select the check box next to the user account you want to enable or disable.

  d. Click Enable or Disable.

---

Managing Disabled Manual Accounts

The Disabled Accounts screen allows administrators to decide whether to enable or remove disabled manual accounts from SafeSync.

Procedure

1. Go to Users.

2. Click the number next to Disabled at the top right corner of the table.

   The Disabled Accounts screen appears.

3. Select the check box next to the user account you want to manage.

4. Use the Enable and Delete buttons to manage the disabled manual accounts.
Changing Manual Account Policies and Plans

Procedure

• To change policies or plans from the Edit User screen:
  a. Go to Users.
  b. View an existing user account.
     • Click a user account under Manual Accounts.
     • Click Manual Accounts and then click an account name in the table that appears.
     The selected user account's details display.
  c. Click the edit link above the user account details.
     The Edit User screen appears.
  d. Select a policy or plan from the drop-down lists.
  e. Click Save.

• To change policies or plans from the Manual Accounts table:
  a. Go to Users.
  b. Click Manual Accounts.
  c. Select the check box next to the user account you want to change.
  d. Click Change Policy or Change Plan.
  e. Select a policy or plan from the drop-down lists.
  f. Click Save.
Managing the Manual Accounts Table

Procedure

1. Go to Users.

2. Click Manual Accounts.

3. Perform any of the following tasks.

<table>
<thead>
<tr>
<th>TABLE 2-3. Manual Account Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPTION</strong></td>
</tr>
<tr>
<td>Add</td>
</tr>
<tr>
<td>Delete</td>
</tr>
<tr>
<td>Change Policy</td>
</tr>
<tr>
<td>Change Plan</td>
</tr>
<tr>
<td>Enable</td>
</tr>
<tr>
<td>Disable</td>
</tr>
</tbody>
</table>

4. Depending on the selected option, follow the instructions on the screen that appears.
Searching for a User Account or Group

Procedure

1. Go to Users.
2. In the search bar, type any user name or group.
3. Click the magnifying glass icon or press the ENTER key.

   The search results display in the table.

Viewing Individual User Details

The individual user view shows all information about a user account, including email address, account type, status, policy and plan assignment, modified date, and storage used.

Procedure

1. Select the user account to view.
   • Expand the Active Directory or Manual Accounts lists and click the user account.
   • Click Active Directory or Manual Accounts and click the user account in the table.

   The individual user details appear.

2. Review the account details in the table and optionally edit accounts details.
   • To make changes to a manual account, click edit.
   • To make changes to a domain account, click change.
Inviting Users to Share Files

After adding user accounts and assigning policies and plans, notify the users about how to access SafeSync.

**Procedure**

1. View the user's account details.
   For more information, see *Viewing Individual User Details on page 2-16*.

2. Click the **send invitation** link above the account details.
   The default mail program opens with a new message containing a template invitation.

3. Modify the template invitation email message with the user logon information and click **Send**.

---

**Note**

If there are only domain accounts, then update the message instructing the users to log on with their domain account and send the message to the distribution list associated with the security group that was used for Active Directory integration.

---

Configuring Policies

SafeSync uses a first match rule when processing policies and plans. For user accounts that match multiple policies and plans, SafeSync applies the policy or plan with the highest priority to the account.

For example, Tom Smith belongs to both the HR and Recruitment domains in Active Directory. The administrator assigns the HR domain with policy “A” and assigns the Recruitment domain with policy “B”. Policy “A” has a higher priority than policy “B”. Since the administrator selected **Assign by priority** under policy for Tom's personal account, the highest priority policy is assigned. As a result, Tom inherits policy “A”.

Use policies to restrict the following settings.
### Table 2-4. Policy Settings

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload control</strong></td>
<td>• Maximum upload size in MB</td>
</tr>
<tr>
<td></td>
<td>• Blocked file types</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>SafeSync identifies files based on the file extensions, not the true-file type. If a blocked file’s file extension is changed, the blocked file will be unblocked.</td>
</tr>
<tr>
<td><strong>Team folder control</strong></td>
<td>• Creation of team folders</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Disabling this option only prevents end users from creating new team folders. Users can still access all existing team folders.</td>
</tr>
<tr>
<td><strong>Sharing control</strong></td>
<td>• Usage of shareable links</td>
</tr>
<tr>
<td></td>
<td>• File exchange through shareable links</td>
</tr>
<tr>
<td></td>
<td>• Security control of shareable links</td>
</tr>
<tr>
<td><strong>Download control</strong></td>
<td>• Download of malicious files</td>
</tr>
</tbody>
</table>

### The Default Policy

SafeSync provides a “Default Policy” that applies to all user accounts not assigned with a specific policy. Customize the “Default Policy” settings to best match your company's file sharing and network bandwidth policies.

**Note**

You cannot delete the “Default Policy”.

The default settings of the “Default Policy” are as follows:
### TABLE 2-5. Default Policy Settings

<table>
<thead>
<tr>
<th>SETTING</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Default Policy</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
</tr>
<tr>
<td><strong>Upload Control</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum upload size</td>
<td>None</td>
</tr>
<tr>
<td>Blocked file types</td>
<td>None</td>
</tr>
<tr>
<td><strong>Team Folders</strong></td>
<td></td>
</tr>
<tr>
<td>Allow users to create team folders</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Shareable Links</strong></td>
<td></td>
</tr>
<tr>
<td>Allow users to create shareable links</td>
<td>Enabled</td>
</tr>
<tr>
<td>Require users to sign in before accessing shareable links</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allow users to upload files to folders with shareable links</td>
<td>Disabled</td>
</tr>
<tr>
<td>Require users to sign in before uploading files to shared folders</td>
<td>Disabled</td>
</tr>
<tr>
<td>Security Requirements</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Antivirus Exception</strong></td>
<td></td>
</tr>
<tr>
<td>Allow users to download files detected as being malicious</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Tip**

Trend Micro recommends setting a **Maximum upload size** if network bandwidth is a concern.
Adding Policies

Procedure

1. Go to Policies.

2. Click Add.

   The Add Policy screen appears.

3. Specify the name and description for the new policy.

4. Specify the maximum upload size in MB.

5. Specify the types of files to block.

   Click the common audio files and common video files links to automatically populate the Blocked file types field with common media extensions.

6. Select Allow users to create team folders to allow end users to create new team folders.

   SafeSync provides team folders to allow groups of SafeSync users to access and modify shared files.

7. Configure the shareable link settings.

   • Select Allow users to create shareable links to allow end users to share files using shareable links.

     SafeSync uses shareable links to allow users to share files uploaded to SafeSync. A user creates a shareable link to a file and then sends the link to another person who can then download the file directly from SafeSync.

   • Select Require users to sign in before accessing shareable links to restrict file access to SafeSync users.

   • Select Allow users to upload files to folders with shareable links to allow end users to upload files to shared folders within shareable links. End users can use shareable links to exchange files with people who are not SafeSync users.
• Select **Require users to sign in before uploading files to shared folders** to restrict file exchange among SafeSync users.

• Select **Password** to enforce end users to set a password for shareable links.

• Select **Expires on** and specify the longest expiration date for shareable links. End users must set an expiration date within the days you specify.

8. Select **Allow users to download files detected as being malicious** to allow users to download files that SafeSync detected as containing malware threats.

---

**WARNING!**

Enabling this feature may open your network up to a malware outbreak or a targeted attack. Only enable this feature for specific users who are aware of the possible security risks that could occur.

9. Click **Save**.

SafeSync adds the new policy at the top of the list. Reorder the policies as required.

---

**Editing Policies**

**Procedure**

1. Go to **Policies**.

2. In the **Name** column, click the policy you want to modify.

3. Specify any changes to the policy.

4. Click **Save**.

---

**Deleting Policies**

When deleting an assigned policy, SafeSync automatically switches all user accounts with the deleted policy to the “Default Policy”. Review the affected accounts carefully before deleting an active policy and reassign new policies to the affected users as required.
Procedure

1. Go to Policies.
2. Select the check boxes next to the policies that you want to delete.
3. Click Delete.
   A confirmation dialog appears.
4. Review all users and groups affected by the change and then click OK.

Reviewing Policy Assignments

For more information about changing policy assignments, see Managing Users on page 2-6.

Procedure

1. Go to Policies.
2. Click any user or Active Directory group in the Groups/Users column.
3. Review the users and group assignment.

Configuring Plans

Each department, business unit, and project in an organization might all have different storage requirements. Plans allow administrators to set different storage privileges for different SafeSync users. Plans control the maximum allowed storage, upload or download speeds, and number of version backups.

SafeSync uses a first match rule when processing policies and plans. For user accounts that match multiple policies and plans, SafeSync applies the policy or plan with the highest priority to the account.

For example, Tom Smith belongs to both the HR and Recruitment domains in Active Directory. The administrator assigns the HR domain with plan “A” and assigns the
Recruitment domain with plan “B”. Plan “A” has a higher priority than plan “B”. Since the administrator selected Assign by priority under plan for Tom's personal account, the highest priority plan is assigned. As a result, Tom inherits plan “A”.

The Default Plan

SafeSync provides a “Default Plan” that applies to all user accounts and groups not assigned with a specific plan. Customize the default plan settings to best match your company's file sharing and network bandwidth policies.

---

**Note**

You cannot delete the “Default Plan”.

SafeSync applies the default plan to all user accounts and groups that have not been assigned a specific plan.

---

The default settings of the “Default Plan” are as follows:

- **Name**: Default Plan
- **Storage**: 1 GB
- **Version backups**: 10

---

**Note**

Trend Micro recommends setting a Download speed if network bandwidth is a concern.

---

Adding Plans

---

**Procedure**

1. Go to Plans.
2. Click Add.
3. Specify the name and description for the new plan.
4. Specify the storage limit in **MB**, **GB**, or **TB**.

5. Specify the maximum upload and download speeds.

6. Select the number of version backups to keep.

---

**Tip**

Saving more versions requires more storage space. Trend Micro recommends setting this to the lowest number required by your organization.

---

SafeSync allows you to save version backup copies of files for version control purposes. Use the SafeSync End-User Portal to restore a file to a previous version.

7. Click **Save**.

   SafeSync adds the new plan at the top of the list. Reorder the plans as required.

---

**Editing Plans**

---

**Procedure**

1. Go to **Plans**.

2. Click any plan name in the **Name** column.

3. Specify any changes to the plan.

4. Click **Save**.

---

**Deleting Plans**

When deleting an assigned plan, SafeSync automatically switches all user accounts with the deleted plan to the “Default Plan”. Review the affected accounts carefully before deleting an active plan and reassign new plans to the affected users as required.
Procedure

1. Go to Plans.
2. Select the check boxes next to the plans that you want to delete.
3. Click Delete.
   A confirmation dialog appears.
4. Review all users and groups affected by the change and then click OK.

Reviewing Plan Assignments

For more information about changing plan assignments, see Managing Users on page 2-6.

Procedure

1. Go to Plans.
2. Click any user or Active Directory group in the Groups/Users column.
3. Review the users and group assignment.
Chapter 3

Monitoring SafeSync

This chapter explains how to monitor SafeSync using widgets, reports, and logs.

Topics in this chapter include:

- SafeSync Dashboard on page 3-2
- Reports on page 3-14
- Logs on page 3-15
SafeSync Dashboard

SafeSync provides widgets on the Dashboard that serve as quick visual references to help manage SafeSync resources and users.

The Dashboard appears when you open the SafeSync web console or click Dashboard in the main menu.

**TABLE 3-1. Dashboard Screen Tabs**

<table>
<thead>
<tr>
<th>TAB</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detections</td>
<td>Displays real-time malware detection statistics and component status updates</td>
</tr>
<tr>
<td></td>
<td>For more information, see Threat Detections on page 3-3.</td>
</tr>
<tr>
<td>Usage Overview</td>
<td>Displays usage statistics and trends over a specified period</td>
</tr>
<tr>
<td></td>
<td>For more information, see Usage Overview on page 3-9.</td>
</tr>
<tr>
<td>System Status</td>
<td>Displays system usage statistics and receive system status alerts</td>
</tr>
<tr>
<td></td>
<td>For more information, see System Status on page 3-11.</td>
</tr>
</tbody>
</table>

**Working with Widgets**

The following table lists widget-related tasks:

**TABLE 3-2. Widget Tasks**

<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh widget data</td>
<td>Click the refresh icon ( ).</td>
</tr>
<tr>
<td>Export widget data to CSV file</td>
<td>Click the export to CSV icon ( ).</td>
</tr>
<tr>
<td>Change time range</td>
<td>If available, click the drop-down list on the left-hand corner of the widget to change the time range.</td>
</tr>
<tr>
<td>Change displayed data</td>
<td>If available, click the drop-down list on the left-hand corner of the widget to change the displayed information.</td>
</tr>
</tbody>
</table>
**Task** | **Steps**
---|---
View logs | If available, click the link to view the related virus/malware detection log.
View hourly or daily statistics | Hover over the graph line to view the widget data for a specific hour or day.

**Threat Detections**

The **Threat Detections** tab allows you to monitor widgets that provide malware-related information detected by SafeSync.

The **Threat Detections** tab contains the following widgets:

- **Threat Statistics Widget on page 3-3**
- **Top 10 Users with Virus/Malware Detections Widget on page 3-5**
- **Top 10 Threats Widget on page 3-7**
- **Component Status Widget on page 3-8**

**Threat Statistics Widget**

The **Threat Statistics** widget displays an overview of the number of potentially malicious files detected by SafeSync during a specific period. You can use this
information as a basis for determining if an outbreak is occurring or if you need to update the company security policy.

**Figure 3-1. Threat Statistics Widget**

The following table describes the information available on the widget.

**Table 3-3. Threat Statistics Widget**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>Displays the specified time range</td>
</tr>
<tr>
<td></td>
<td>Displays data from the <strong>Last 7 days</strong>, <strong>Last 14 days</strong>, <strong>Last 30 days</strong>, <strong>Last 60 days</strong>, or <strong>Last 90 days</strong>.</td>
</tr>
<tr>
<td>Period</td>
<td>Displays the dates of the specified time range</td>
</tr>
<tr>
<td>Interval</td>
<td>Displays the time interval used in the graph</td>
</tr>
<tr>
<td></td>
<td>Displays either <strong>Daily</strong> or <strong>Weekly</strong>.</td>
</tr>
<tr>
<td>Total detections</td>
<td>Displays the total number of virus/malware detections during the specified time range</td>
</tr>
<tr>
<td></td>
<td>Click the link to view the virus/malware detection log for all detections.</td>
</tr>
<tr>
<td><strong>ITEM</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Users</td>
<td>Displays the total number of users with detected files</td>
</tr>
<tr>
<td></td>
<td>Click the link to view the virus/malware detection log for all users with detected files.</td>
</tr>
<tr>
<td>Daily/Weekly statistics</td>
<td>Displays the daily or weekly summary for each interval</td>
</tr>
<tr>
<td></td>
<td>Hover over the graph line to view the daily or weekly totals.</td>
</tr>
</tbody>
</table>

**Top 10 Users with Virus/Malware Detections Widget**

The **Top 10 Users with Virus/Malware Detections** widget displays the top 10 users with files detected as being malicious over a period of time. You can use this information to warn and educate top violators about exposing the organization to security risks.

![Top 10 Users with Virus/Malware Detections Widget](image)

**FIGURE 3-2. Top 10 Users with Virus/Malware Detections Widget**

The following table describes the information available on the widget.
### TABLE 3-4. Top 10 Users with Virus/Malware Detections Widget

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>Displays the specified time range</td>
</tr>
<tr>
<td></td>
<td>Displays data from the <strong>Last 7 days</strong>, <strong>Last 14 days</strong>, <strong>Last 30 days</strong>, <strong>Last 60 days</strong>, or <strong>Last 90 days</strong>.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the names of users with files detected as being malicious Click the link to view the virus/malware detection log for each user with detected files.</td>
</tr>
<tr>
<td>Detections</td>
<td>Displays the total number of virus/malware detections for each user on the list during the specified time range.</td>
</tr>
<tr>
<td>Last Detected</td>
<td>Displays the timestamp of the last virus/malware detection</td>
</tr>
<tr>
<td>Total users</td>
<td>Displays the total number of users with detected files Click the link to view the virus/malware detection log for all users with detected files.</td>
</tr>
</tbody>
</table>
Top 10 Threats Widget

The **Top 10 Threats** widget displays the top 10 virus/malware threats detected during the specified period. You can use this information to identify and mitigate the top malware threats in your company.

![Top 10 Threats Widget](image)

**FIGURE 3-3. Top 10 Threats Widget**

The following table describes the information available on the widget.

**TABLE 3-5. Top 10 Threats Widget**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>Displays the specified time range</td>
</tr>
<tr>
<td></td>
<td>Displays data from the <strong>Last 7 days</strong>, <strong>Last 14 days</strong>, <strong>Last 30 days</strong>, <strong>Last 60 days</strong>, or <strong>Last 90 days</strong>.</td>
</tr>
<tr>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virus/Malware</td>
<td>Displays the name of the malware detected</td>
</tr>
<tr>
<td></td>
<td>Click the link to view the virus/malware detection log for each user detection.</td>
</tr>
<tr>
<td>Detections</td>
<td>Displays the total number of virus/malware detections for each user on the list during the specified time range.</td>
</tr>
<tr>
<td>Total threats</td>
<td>Displays the total number of unique malware threat types detected</td>
</tr>
<tr>
<td></td>
<td>Click the link to view the virus/malware detection log for all detections.</td>
</tr>
</tbody>
</table>

**Component Status Widget**

The **Component Status** widget displays information about the antivirus components currently used by SafeSync.

![Component Status Widget](image)

**FIGURE 3-4. Component Status Widget**

The following table describes the information available on the widget:
### TABLE 3-6. Threat Statistics Widget

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Displays the component names</td>
</tr>
<tr>
<td>Current Version</td>
<td>Displays the version number of the current pattern or engine</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Displays the timestamp of the last update</td>
</tr>
</tbody>
</table>

**Note**

Click **Update pattern** to go to the **Update** screen.

For more information on updating components, see *Updating Components on page 4-15*.

### Usage Overview

View usage statistics and trends over a specified period.
Usage Trends Widget

The **Usage Trends** widget displays usage statistics and trends during a specific period. You can view information about user activity, device usage, file sharing statistics, and storage usage.

![Usage Trends Widget](image)

**FIGURE 3-5. Usage Trends widget displaying active user statistics**

The following table describes the information available on the widget.
### Table 3-7. Usage Trends Widget

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Displays the usage trend information for the specified time range</td>
</tr>
<tr>
<td></td>
<td>Displays the total number of “Active users”, “Connected devices”, “Total files”, “Shared files”, “System storage used”, and “Average storage used”.</td>
</tr>
<tr>
<td></td>
<td>Displays data from the <strong>Last 7 days</strong>, <strong>Last 14 days</strong>, or <strong>Last 30 days</strong>.</td>
</tr>
</tbody>
</table>

**Note**

You can also generate reports about SafeSync usage statistics.

For more information, see *Reports on page 3-14*.

<table>
<thead>
<tr>
<th>Period</th>
<th>Displays the dates of the specified time range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily average</td>
<td>Displays the daily average for the requested information</td>
</tr>
<tr>
<td>Daily statistics</td>
<td>Displays the daily summary for each interval</td>
</tr>
<tr>
<td></td>
<td>Hover over the graph line to view the daily totals.</td>
</tr>
</tbody>
</table>

### System Status

View system usage statistics and review information regarding the SafeSync system status.

The **System Status** tab contains the following:

- *System Status Widget on page 3-12*
- *System Status Alert Widget on page 3-13*
System Status Widget

The **System Status** widget displays system usage statistics and averages over a specified period. Use this widget to get an overview of the CPU, memory, and disk usage in your SafeSync environment.

![System Status Widget](image)

**Figure 3-6. System Status widget displaying disk usage statistics**

The following table describes the information available on the widget.

**Table 3-8. System Status Widget**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Display | Displays the system status information for the specified time range  
| | Displays percentages for “CPU usage”, “Memory usage”, or “Disk usage”.  
| | Displays data from the **Last 24 hours**, **Last 7 days**, **Last 14 days**, or **Last 30 days**.  |
| Period | Displays either **Last 24 hours** or the dates of the specified time range |
### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly/Daily average</td>
<td>Displays the hourly or daily average for the requested information</td>
</tr>
<tr>
<td></td>
<td>The displayed average depends on the selected time range.</td>
</tr>
<tr>
<td>Hourly/Daily</td>
<td>Displays the hourly or daily summary for each interval</td>
</tr>
<tr>
<td>statistics</td>
<td>Hover over the graph line to view the hourly or daily totals.</td>
</tr>
</tbody>
</table>

### System Status Alert Widget

The **System Status Alert** widget displays information regarding the SafeSync system status and any available details about errors that occur. There is a separate **System Status Alert** widget for each installed server.

**Note**

The **System Status Alert** widget refreshes every 10 minutes.

![System Status Alert widget displaying primary and secondary server status](image)

**Figure 3-7. System Status Alert widget displaying primary and secondary server status**

The **System Status Alert** widget uses the following icons to indicate the system status.

- ![ NORMAL ]: Normal
- ![ WARNING ]: Warning

The following table describes the information available on the widget:
TABLE 3-9. System Status Alert Widget

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Version</td>
<td>Displays a warning when the current SafeSync product version is not working properly.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Displays a warning when the disk space is insufficient.</td>
</tr>
<tr>
<td>Storage</td>
<td>Displays a warning when the storage and backup features are not working properly.</td>
</tr>
<tr>
<td>System Service</td>
<td>Displays a warning when a system service is not working properly.</td>
</tr>
<tr>
<td>Database HA</td>
<td>Displays a warning when the database replication function is not working properly.</td>
</tr>
<tr>
<td>Shared Protection Extension</td>
<td>Displays a warning when the encryption function is not working properly.</td>
</tr>
</tbody>
</table>

Reports

Administrators can generate different types of reports about SafeSync usage statistics. The following table describes the types of reports available.

TABLE 3-10. Usage Trend Types

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active users</td>
<td>The number of users that logged on to the SafeSync end-user portal</td>
</tr>
<tr>
<td>Connected devices</td>
<td>The number of devices that connected to the SafeSync end-user portal</td>
</tr>
<tr>
<td>Total files</td>
<td>The total number of files stored on SafeSync</td>
</tr>
<tr>
<td>Shared files</td>
<td>The total number of files being shared by users</td>
</tr>
<tr>
<td>System storage used</td>
<td>The amount of storage used by files</td>
</tr>
<tr>
<td>Average storage used</td>
<td>The average amount of storage used per user</td>
</tr>
</tbody>
</table>
Generating Reports

Procedure

1. Go to Reports.
2. Select or specify a time range.
3. Select the type of report to generate.
4. Click Export to CSV.
   A Save As... dialog appears.
5. Specify the folder location and file name and click Save.

Logs

SafeSync uses logs to record events and detections. Use the Log Query screen to look up the following log types:

- **Administrator event**: Activities about managing the SafeSync server web console
- **End-user event**: Activities about SafeSync usage (for example, uploading files, creating folders)
- **System event**: Activities about Active Directory synchronization, system updates, and system status
- **Virus/malware detection**: Information about virus/malware detections (virus/malware name, location, the user that uploaded the file)

Use the Log Settings screen to delete old logs and forward logs to a syslog server.
Querying Logs

Procedure

1. Go to Logs > Log Query.

   The Log Query screen appears.

2. Select a log type to query.

3. Specify the time range for the query.

4. To filter data for a specific user or file name, specify the information in the User or File field.

5. Click Start Query.

Deleting Logs

Use the Log Settings screen to configure automatic log deletion based on time.

Procedure

1. Go to Logs > Log Settings.

   The Log Maintenance tab appears.

2. Select Enable scheduled maintenance and specify the age of logs to delete automatically.

3. Click Save.

Forwarding Logs to a Syslog Server

Use the Log Settings screen to configure automatic log deletion based on time.
Procedure

1. Go to Logs > Log Settings > Syslog Server.
   The Syslog Server tab appears.

2. Select Forward all logs to the following syslog server.

3. Type the IP address or fully qualified domain name (FQDN) in the Server field.

4. Type the port number.

5. Specify the following:
   • Severity level
   • Event format

6. Click Save.
This chapter explains how to perform SafeSync administrative tasks.

Topics in this chapter include:

- *Account Settings on page 4-3*
- *Administrator Accounts on page 4-4*
- *System Notifications on page 4-6*
- *Active Directory Integration on page 4-7*
- *Antivirus Settings on page 4-9*
- *System Settings on page 4-19*
- *High Availability on page 4-28*
- *Cache Servers on page 4-41*
- *Security Control on page 4-39*
- *Storage Management on page 4-44*
- *System Maintenance on page 4-51*
- *System Updates on page 4-52*
License Information on page 4-54
Account Settings

Use the **Account Settings** screen to update the SafeSync administrator information:

- **Email address**: Specify an email address to which SafeSync sends system notifications.
- **Password**: Change the account password.

---

**Tip**
Trend Micro recommends changing the logon password every 30 to 90 days.

---

Changing the Administrator Account Settings

---

**Procedure**

1. Go to **Administration > Account Settings**.
   
   The **Account Settings** screen appears.

2. Type a new email address for the administrator account.

3. To change the administrator password:
   
   a. Type a new password in the **New password** field.
   
   b. Type the same password in the **Confirm password** field.

---

**Tip**
Leave the password fields blank to keep using the old password.

---

4. Click **Save**.
Administrator Accounts

Use the Administrator Accounts screen to add and manage additional administrator accounts. Administrators can manage SafeSync from the administrator web console and manage team folders from the end-user portal.

Adding Administrator Accounts

Procedure

1. Go to Administration > Administrator Accounts.
   
   The Administrator Accounts screen appears.

2. Click Add.
   
   The Add Administrator screen appears.

3. Specify a user name for the new account.

   Note
   
   The user name must start with a letter and can only contain alphanumeric characters, dots, @, and underscores.

4. Specify an email address to which Trend Micro sends system notifications.

5. Specify a password for the new account.

6. Confirm the password.

7. Click Save.

Editing Administrator Accounts

Each administrator can change individual email addresses and passwords on the Account Settings screen. See Account Settings on page 4-3 for more information.
Deleting Administrator Accounts

When an administrator account is no longer in use, you can remove the account from the administrator account list. If the deleted administrator used to upload files to the end-user portal, SafeSync moves these files to a team folder named 
<Deleted User> administrator account name. All administrators have access to this team folder and can take actions on the files within the folder.

**Note**
You can only disable but not delete the default administrator account.

**Procedure**

1. **Go to Administration > Administrator Accounts.**

   The **Administrator Accounts** screen appears.

2. **Select the accounts you want to delete.**

3. **Click Delete.**

   A confirmation dialog appears.

4. **Review the account names and click Yes.**

Enabling or Disabling Administrator Accounts

You can disable an administrator account to temporarily restrict an administrator from managing SafeSync.

**Procedure**

1. **Go to Administration > Administrator Accounts.**

   The **Administrator Accounts** screen appears.

2. **Select the accounts you want to enable or disable.**
3. Click **Enable** or **Disable**.

---

**System Notifications**

Use the **System Notifications** screen to set up license information updates and system status alerts.

SafeSync sends the following notifications.

**TABLE 4-1. System Notifications**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| License Information | SafeSync sends daily notification emails after the SafeSync for Enterprise license expires.  
For more information about expired licenses, see *Limitations of Expired Licenses on page 4-55*. |
| System Status Alert | SafeSync sends email notifications for all warning messages that appear on the **System Status Alert** widget.  
For more information about the widget, see *System Status Alert Widget on page 3-13*. |

**Note**

SafeSync sends notification emails based on the specified delivery frequency.

---

**Configuring System Notification Settings**

**Procedure**

1. Go to **Administration > System Notifications**.
   
   The **System Notifications** screen appears.

2. Under **License Information**, select one of the following:
• **Administrators**: SafeSync sends email notifications to all administrators. Each administrator can modify the email address on the **Account Settings** screen.

• **Other recipients**: SafeSync sends email notifications to the email accounts specified.

3. Under **System Status Alert**, select one of the following:
   - **Administrators**: SafeSync sends email notifications to all administrators. Each administrator can modify the email address on the **Account Settings** screen.
   - **Other recipients**: SafeSync sends email notifications to the email accounts specified.

4. Under **Delivery Frequency**, specify how often SafeSync sends notifications.

---

**Note**

SafeSync only sends email notifications after detecting problems with the SafeSync service. If all services are functioning properly, SafeSync does not send any notification messages.

5. Click **Save**.

---

**Active Directory Integration**

Integrate SafeSync with the Active Directory structure to efficiently manage user and group permissions.

**Configuring Active Directory Integration**

**Procedure**

1. Go to **Administration > Active Directory Integration**.

   The **Active Directory Integration** screen appears.
2. Select **Enable Active Directory synchronization**.

3. Type the Active Directory IP address or fully qualified domain name (FQDN) in the **Server** field.

4. Type the port number.

5. Type the user name and password to access the Active Directory server.

6. To set the root bind distinguished name (DN) for the LDAP server, type the information in the **Root DN** field.
   
   Example: OU=new_ou,DC=domain,DC=com

7. Click **Save**.
   
   SafeSync performs a test connection and saves the Active Directory settings.

---

**Adding Additional Active Directory Servers**

You can synchronize SafeSync with additional Active Directory servers to allow more domain user accounts or groups to use the service. Once you set up the Active Directory server information, you can select the users or groups to add on the **Users** screen.

**Procedure**

1. Go to **Administration > Active Directory Integration**.
   
   The **Active Directory Integration** screen appears.

2. Click the **Add another server** link.
   
   A new **Server Settings** section appears.

3. Configure the Active Directory server settings.

4. Click **Save**.
   
   SafeSync performs a test connection and saves the Active Directory settings.
Antivirus Settings

Use the Antivirus Settings screen to perform the following tasks.

**TABLE 4-2. Antivirus Settings Tabs**

<table>
<thead>
<tr>
<th>TAB</th>
<th>TASKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Configure the antivirus scan settings and provide exclusion lists.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Configuring Antivirus Settings on page 4-9.</td>
</tr>
<tr>
<td>Smart Protection Server</td>
<td>Integrate with a local Smart Protection Server or connect to the Smart Protection Network.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Configuring Smart Protection Server Settings on page 4-14</td>
</tr>
<tr>
<td>Manual Scan</td>
<td>Perform a manual scan.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Performing a Manual Scan on page 4-15</td>
</tr>
<tr>
<td>Update</td>
<td>Update antivirus components, schedule automatic updates, select an update source, and roll back components to their previous versions.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Updating Components on page 4-15</td>
</tr>
</tbody>
</table>

Configuring Antivirus Settings

Enable the antivirus feature to automatically scan files when users perform the following tasks.

- Create a shareable link
- Upload files

You can also use the Settings tab to specify file types to scan, provide exclusion lists, and configure advanced settings.
Procedure

1. Go to Administration > Antivirus Settings.

   The Antivirus Settings screen appears.

2. Select Enable antivirus.

3. Select Scan files after generating shareable links to prevent creating shared links to files that are malicious.

   **Note**
   SafeSync scans all files not previously scanned by the current pattern file and engine when a user attempts to create a shareable link.

4. Select scan targets.

   - **All scannable files**: Scans all files that are not password protected, encrypted, or exceed the user-defined scanning restrictions.
Note

This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

- **File types scanned by IntelliScan**: Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name.
  
  For more information, see *IntelliScan on page E-3*.

- **Files with specified extensions (separate entries with a ",",*)**: Only scan files whose extensions are included in the file extension list.

5. Specify scan exclusions.

![Exclusions](image)

- Enable or disable scan exclusions
- Exclude files with the specified names from malware scanning
- Exclude files with specific extensions from malware scanning
Note

Wildcard characters, such as "*", are not accepted for file extensions.


![Advanced Settings](image)

**Table 4-3. Advanced Scan Settings**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not scan files that exceed ___ MB</td>
<td>SafeSync does not scan files that exceed the value specified.</td>
</tr>
</tbody>
</table>
### Option: Scan compressed files

A compressed file has one layer for each time it has been compressed. If an infected file has been compressed to several layers, it must be scanned through the specified number of layers to detect the infection. Scanning through multiple layers, however, requires more time and resources.

Specify the following settings.

- **Maximum layers**: SafeSync scans up to the specified number of layers and does not scan any further.
- **Do not scan files in the compressed file if the size exceeds ___ MB**: SafeSync does not scan files in compressed files that exceed the value specified.
- **In a compressed file, scan only the first ___ files**: SafeSync scans only the first files specified. SafeSync does not scan other files.

### Option: Scan OLE objects

When a file contains multiple Object Linking and Embedding (OLE) layers, SafeSync scans up to the specified number of compression layers.

Specify the following settings.

- **Maximum layers**: SafeSync scans up to the specified number of OLE layers and does not scan any further.
- **Detect exploit code in OLE files**: OLE Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.

---

**Note**

The specified number of layers is applicable to both the **Maximum layers** and **Detect exploit code in OLE files** options.
Enable IntelliTrap | IntelliTrap detects malicious code, such as bots, in compressed files. For more information, see *IntelliTrap on page B-2.*

7. Click **Save**.

## Configuring Smart Protection Server Settings

Smart Protection Network is a cloud-based query process that makes use of two network-based technologies:

- **Trend Micro™ Smart Protection Network™:** A globally scaled, Internet-based, infrastructure that provides services to users who do not have immediate access to their corporate network.

- **Smart Protection Server:** Smart Protection Server exists in the local network. This is made available for users who have access to their local corporate network. These servers are designed to localize operations to the corporate network to optimize efficiency.

### Procedure

1. Go to **Administration > Antivirus Settings > Smart Protection Server.**

   The **Smart Protection Server** screen appears.

2. Select one of the following:
   - **Connect to Trend Micro Smart Protection Network:** SafeSync sends data about unknown and potentially malicious files to the Trend Micro Smart Protection Network.

     For more information, see *Trend Micro™ Smart Protection Network™ on page A-4.*

   - **Connect to local Smart Protection Server:** SafeSync sends data about unknown and potentially malicious files to the local Smart Protection Servers
on the network. Administrators can specify the priority of the Smart Protection Servers in the list.

3. Click Save.

Performing a Manual Scan

Manually scan files with shareable links. Manual Scan does not scan files that are not shared.

Tip
Trend Micro recommends performing Manual Scan after updating pattern files or scan engines.

Procedure

1. Go to Administration > Antivirus Settings > Manual Scan.
   The Manual Scan screen appears.
2. Click Scan Now.

Updating Components

SafeSync supports manual updates, automatic updates, and rolling back component updates.

Manually Updating Components

You can choose to manually download component updates at any time.

Procedure

1. Go to Administration > Antivirus Settings > Update.
The Update screen appears.

2. Click Update Now.

Configuring Scheduled Updates

Schedule component updates to ensure that users stay protected from the latest security risks.

Procedure

1. Go to Administration > Antivirus Settings > Update.

   The Update screen appears.

2. Expand the Scheduled Update section.

   The Scheduled Update section appears.

3. Select Enable scheduled updates.

4. Specify the update frequency.

5. Specify the start time.

6. Click Save.

Configuring the Update Source

Select a download source for the component updates.
Procedure

1. Go to Administration > Antivirus Settings > Update.

   The Update screen appears.

2. Expand the Update Source section.

   The Update Source section appears.

   ![Update Source](image)

   **Figure 4-2. Update Source section**

3. Select one of the following:

   - **Trend Micro ActiveUpdate Server**: The official source for Trend Micro component updates
   - **Alternate update source**: Specify a URL or IP address as an alternative update source

   __Note__

   Aside from the Trend Micro ActiveUpdate Server, you can specify an alternate update source. Alternate update sources help reduce update traffic directed to the SafeSync server.

4. Click Save.
Rolling Back Component Updates

Rollback refers to reverting to the previous version of the Smart Scan Agent Pattern, Virus Scan Engine, IntelliTrap Pattern, and IntelliTrap Exception Pattern. If there appears to be an issue after updating components, roll back the last component update to restore the patterns and engines to their previous version before the last update occurred.

Procedure

1. Go to Administration > Antivirus Settings > Update.

   The Update screen appears.

2. Expand the Rollback section.

   The Rollback section appears.

   ![Rollback section](image)

   **Figure 4-3. Rollback section**

3. Click Roll Back to Previous Version.

   **Note**

   SafeSync only rolls back components to their previous state before the last update. Components that did not change during the last update do not roll back to a previous version.
System Settings

Use the **System Settings** screen to perform the following tasks:

**TABLE 4-4. System Settings Tabs**

<table>
<thead>
<tr>
<th>TAB</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| Web Consoles   | Configure the network settings for the administrator web console and end-user portal.  
                  For more information, see *Configuring SafeSync Web Console Settings on page 4-19.* |
| Proxy Server   | Configure the proxy server settings.  
                  For more information, see *Configuring Proxy Server Settings on page 4-20* |
| SMTP Server    | Specify the SMTP server settings.  
                  For more information, see *Configuring SMTP Server Settings on page 4-21* |
| SSL Certificate| Paste the SSL certificate text and upload the private key file.  
                  For more information, see *Updating SSL Certificate Information on page 4-22* |
| Add-Ins        | Enable the add-ins and decrypt encrypted files.  
                  For more information, see *Understanding SafeSync Add-Ins on page 4-22* |
| Language       | Specify the administrator web console language.  
                  For more information, see *Configuring the Web Console Language on page 4-27* |

**Configuring SafeSync Web Console Settings**

Use the **Web Consoles** tab to configure the network settings of the end-user web portal and the SafeSync administrator’s web console.
Procedure

1. Go to Administration > System Settings.

   The System Settings screen appears.

2. On the Web Consoles tab, specify the network information for SafeSync end users to access the web console.

   Important
   • The administrator's web console also uses the same IP address with a different port, for example https://192.168.100.1:3443. Once administrators modify the IP address and click Save, SafeSync saves the changes and redirects to the logon screen.
   • SafeSync requires a fully qualified domain name (FQDN). For more information on domain mapping, refer to the SafeSync for Enterprise Installation Guide.

3. Click Save.

Configuring Proxy Server Settings

If the network requires that SafeSync uses a proxy server, configure the proxy settings to register and activate SafeSync.

Procedure

1. Go to Administration > System Settings > Proxy Server.

   The Proxy Server screen appears.

2. Select Use a proxy server for the connection.

3. Type the IP address or fully qualified domain name (FQDN) of the proxy server in the Server field.

4. Type the port number.

5. Select the protocol:
• HTTP
• SOCKS 4/5

6. If the proxy server requires authentication, select **Proxy server authentication**.
7. Provide the authentication credentials in the **User name** and **Password** fields.
8. Click **Save**.

SafeSync tests the connection and saves the proxy server settings.

---

**Configuring SMTP Server Settings**

Use the **SMTP Server** tab to set up an email server to send log reports.

**Procedure**

1. Go to **Administration > System Settings > SMTP Server**.

   The **SMTP Server** screen appears.

2. Select **Use an SMTP server to send logs**.

3. Type the IP address or fully qualified domain name (FQDN) of the SMTP server in the **Server** field.

4. Type the port number.

5. Type the sender’s email address in the **Sender** field.

   SafeSync uses this address as the sender address (a requirement for some SMTP servers).

6. If the SMTP server requires authentication, select **SMTP server authentication**.

7. Type the user name and password.

8. Click **Save**.

   SafeSync performs a test connection and saves the SMTP server settings.
Updating SSL Certificate Information

When importing certificates, the following must be considered:

- Certificates must use the **PEM** file format.
- Whenever available, intermediate certificates must be included when importing the certificate. The typical sequence of the certificate chain is:
  
- The certificate chain must be uploaded to the administrator console all at once and in the proper sequence.
- Whenever available, Certificate Attributes must be included.
- Third-party certificates must use the following format:
  
  *.<your_domain>.<top-level_domain>

Procedure

1. Go to **Administration > System Settings > SSL Certificate**.
   
   The **SSL Certificate** screen appears.
2. Click **Import Certificate**.
   
   The **Import SSL Certificate** screen appears.
3. Select the following files:
   
   - **Certificate**: .cer file
   - **Private key**: .pem file
   - **Certificate chain bundle**: .ca-bundle file
4. Click **Import**.

Understanding SafeSync Add-Ins

Licensed SafeSync users can enable the following add-ins:
• **Outlook Extension**: Users can prevent unintentional data leakage by securing their email file attachments. Users can either upload the files to SafeSync and include a shareable link in email messages, or use the auto-encryption option to automatically encrypt file attachments.

---

**Note**

The encryption feature is only available after enabling **Shared Protection Extension**.

---

When the auto-encryption option is enabled, all attachments are automatically encrypted and the only people who can open the attachments are the SafeSync users who are the original recipients of the email.
**Note**

Encrypted attachments have the file extension .spt.

- **Shared Protection Extension**: Users can create auto-encryption folders. All files added to these folders are encrypted automatically. When users create an auto-encrypted team folder, SafeSync prompts the users to identify who can access the folder. Users can also create auto-encrypted personal folders which are only accessible by users who created them.

Auto-encryption folders help protect confidential documents, such as those created by Human Resources or Finance professionals, from being accessed by unauthorized users.

**Note**

Encrypted files have the file extension .spt.

---

### Configuring SafeSync Add-Ins

**Note**

Activate SafeSync add-ins on the **License Information** screen.

For more information, see *Activating SafeSync Add-Ins on page 4-56.*
Procedure

1. Go to Administration > System Settings > Add-Ins.

2. To enable or disable an add-in, select Enable [add-in name] from the add-in section.

3. To specify how frequently authentication is required for files encrypted using Shared Protection Extension:
   - Drag the slider from Low to High to indicate how frequently users have to authenticate themselves in order to open and use encrypted files
   - Turn on Force authentication to require users to provide authentication credentials in order to access encrypted files.
The number of days before users must provide authentication credentials automatically changes based on the selected protection level. Manually changing the number of days automatically sets the protection level to Custom.

Administrators can also choose to turn off authentication. After turning off authentication, SafeSync does not require users to provide authentication credentials to access encrypted files.

### Decrypting all Encrypted Files

If the file encryption license expires or the organization simply wants to stop using file encryption, administrators can use the Decryption Utility to decrypt all encrypted files and disable file encryption.

**Tip**

Decrypting all SafeSync files may take some time to complete. Trend Micro recommends starting the decryption process after work hours. If necessary, cancel the decryption process and restart it at a more convenient time.

**Procedure**

1. Go to Administration > System Settings > Add-Ins.
2. Click the Decrypt all encrypted SafeSync files link.
3. Click **OK** to begin the decryption process.

Confirguring the Web Console Language

SafeSync allows you to change the display language of the web console at any time for users in different regions.

**Procedure**

1. Go to **Administration > System Settings > Language**.
   
   The **Language** screen appears.

2. Select the preferred language from the list.

3. Click **Save**.

   The SafeSync web console automatically refreshes in the new language. You do not need to log on to the SafeSync server again.
High Availability

The high availability (HA) feature of SafeSync requires two appliances to avoid having a single point of failure. The secondary server acts as a backup and failover for increased reliability. High availability deployments help reduce system downtime and data loss.

In a high availability deployment, a virtual IP address is required for SafeSync to synchronize data between the primary and secondary server. The two servers must exist within the same network and be able to connect to the virtual IP address.

**Table 4-5. Primary and Secondary Servers**

<table>
<thead>
<tr>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary server</td>
<td>• Always configured first</td>
</tr>
<tr>
<td></td>
<td>• Configuration of the primary server must be completed before setting up the secondary server</td>
</tr>
<tr>
<td>Secondary server</td>
<td>• Installed after configuring and verifying the primary server</td>
</tr>
<tr>
<td></td>
<td>• Primary server settings are replicated while setting up the secondary server</td>
</tr>
</tbody>
</table>
You may use either database replication or load balancing to achieve high availability in SafeSync.

For more information, see *Database Replication on page 4-29* and *Load Balancing on page 4-30*.

**Database Replication**

SafeSync leverages existing MySQL Master-Master Replication to achieve database replication high availability. The MySQL Master-Master Replication means that both primary and secondary servers function as a Master MySQL server. Any SQL statement executed in one server is pulled and executed on the other server. From an application point of view, both servers’ databases are fully replicated.

**File Replication**

SafeSync supports file replication for local and iSCSI storage. The default file replication number is 2. This means that all files uploaded by users are stored on two disks.
File replication has two main benefits:

- Prevents having a single point of failure by using two servers
- Increases service performance by providing access to two different physical locations

SafeSync automatically generates streaming and thumbnail files when users upload certain file types. The auto-generated files' replication number is 1.

---

**Note**

File replication is not supported in NFS storage.

---

- Local and iSCSI storage uses balanced percentages to store files. This means newly added storage is used first.
- NFS storage does not use balanced percentages.

---

### Load Balancing

There are two ways to achieve load balancing high availability. The first method uses a Network Load Balancer (NLB). The second method implements a Domain Name System (DNS) load balance.

The NLB requires third-party hardware and/or software and the configuration will depend on the type of NLB used. The required DNS records for SafeSync needs to point to the NLB’s IP address.

DNS load balance means setting up the required DNS records for SafeSync and pointing them to the production IP address of both the primary and secondary servers. This means each fully qualified domain name (FQDN) resolves two IP addresses.
Configuring High Availability - Primary Server

**Procedure**

1. Log on to the SafeSync server you want to configure as the primary server.

2. Go to Administration > High Availability.

   The High Availability screen appears.

3. Select Primary server.

4. Click Continue.

   The High Availability - Primary Server Configuration screen appears.

5. Specify the virtual IP address.

   SafeSync uses the virtual IP address to synchronize data between the primary and the secondary server. The primary and secondary SafeSync servers must exist within the same network and be able to connect to the virtual IP address.

6. Click Continue.

7. Click Enable.

   The configuration process begins and SafeSync becomes temporarily unavailable.

---

**Note**

The configuration process may take up to several minutes to complete. Trend Micro recommends starting the process during off-peak hours.

---

Configuring High Availability - Secondary Server

You must configure the primary server first before proceeding with this task.

---

**WARNING!**

Any existing data or partitions are removed during the configuration process. Ensure that you back up any existing data on the server before continuing.
Procedure

1. Log on to the SafeSync server you want to configure as the secondary server.

2. Go to Administration > High Availability.

   The High Availability screen appears.

3. Click Continue.

   The High Availability - Secondary Server Configuration screen appears.

4. Specify the IP address and system account password for the primary server.

5. Click Continue.

6. Click Enable.

   The configuration process begins and SafeSync becomes temporarily unavailable.

---

Note

The configuration process may take up to several minutes to complete. Trend Micro recommends starting the process during off-peak hours.

---

Verifying MySQL HA

Verify the high availability deployment of your MySQL database.

Procedure

1. On the primary server, log on to the MySQL console and create a test database.
   a. Log on to the MySQL console by typing the following command:
      
      \texttt{mysql -u root -p}

   b. Type the MySQL password.

      Default password: \texttt{safesync}
c. Create a test database by typing the following command:

```sql
create database new1;
```

---

**Note**
This procedure uses “new1” as the test database name.

---

The following result appears:

```
Query OK, 1 row affected (0.00 sec)
```

2. On the secondary server, log on to the MySQL console and verify that “new1” also exists in the database.

a. Log on to the MySQL console by typing the following command:

```bash
mysql -u root -p
```

b. Type the MySQL password.

Default password: **safesync**

c. Verify that “new1” is in the database list by typing the following command:

```sql
show databases;
```
The following result appears:

```
<table>
<thead>
<tr>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>information_schema</td>
</tr>
<tr>
<td>au</td>
</tr>
<tr>
<td>auth</td>
</tr>
<tr>
<td>data</td>
</tr>
<tr>
<td>gearman</td>
</tr>
<tr>
<td>lost+found</td>
</tr>
<tr>
<td>mogilefs</td>
</tr>
<tr>
<td>mysql</td>
</tr>
<tr>
<td>new1</td>
</tr>
<tr>
<td>osdp</td>
</tr>
<tr>
<td>performance_schema</td>
</tr>
<tr>
<td>shard_1</td>
</tr>
<tr>
<td>test</td>
</tr>
<tr>
<td>tmsb_db</td>
</tr>
</tbody>
</table>
```

14 rows in set (0.00 sec)

d. After verifying that “new1” exists in the database, remove it from the secondary server by typing the following command.

`drop database new1;`

The following result appears:

`Query OK, 0 rows affected (0.00 sec)`

3. Go back to the primary server and verify that “new1” has also been removed.
a. Log on to the MySQL console by typing the following command:

   `mysql -u root -p`

b. Type the MySQL password.

   Default password: `safesync`

c. Verify that “new1” is not in the database list by typing the following command:

   `show databases;`
The following result appears:

```
+-----------------+  
| Database        |  
+-----------------+  
| information_schema |  
| au              |  
| auth            |  
| data            |  
| gearman         |  
| lost+found      |  
| mogilefs        |  
| mysql           |  
| osdp            |  
| performance_schema |  
| shard_1         |  
| test            |  
| tmsb_db         |  
+-----------------+  
13 rows in set (0.00 sec)
```

**Failover**

SafeSync provides a failover if two servers are deployed. Administrators must correctly deploy the servers and in some cases configure other areas of their network. For example, there are two required criteria for SafeSync failover to work correctly:

1. The Primary and Secondary servers must be configured and running correctly.
2. The administrator must setup name services to provide for failover in DNS.
Internal Failover

The SafeSync failover mechanisms rely on Keepalived (a third-party program) and high availability. Keepalived uses the Virtual Router Redundancy Protocol (VRRP) to provide and manage a virtual IP address. The virtual IP address fails over to the secondary server when any of the following events occurs:

• The primary server shuts down
• Connection to the primary server becomes unavailable

Verifying File Replication

Check the file replication status of your high availability deployment.
Note
This procedure only applies to local and iSCSI storage. NFS storage is not supported.

Procedure

1. Upload a test file (test.txt) to SafeSync.
2. Log on to the server shell.
3. Log on to the MySQL console by typing the following command:
   
   mysql -u root -p shard_1

4. Type the MySQL password.
   Default password: safesync

5. Find the data ID of the test file by typing the following command:
   
   select data_id from objects where name= 'test.txt';

   The following result appears:

   +--------+
   | data_id |
   +--------+
   | 5      |
   +--------+

   1 row in set (0.00 sec)

   Note
   This procedure uses “5” as the data ID example.

6. Verify that two file paths exist in MogileFS by typing the following command:
   
   mogtool --trackers=tracker1:6001 --domain=osdp locate 5
The following result appears:

```
http://0.1.195.37:4751/dev11/0/000/000/000000039.fid
http://0.1.195.37:4751/dev21/0/000/000/000000039.fid
#2 paths found
```

## Security Control

Use the **Security Control** screen to enforce extra security control on shareable links and user sessions.

- **Shareable links**: Enable or disable shareable link usage. See [*Enabling or Disabling Shareable Links* on page 4-39](#) for more information.

- **User sessions**: Require users to start a new session every time SafeSync starts and automatically end a user session after being inactive for a certain time. See [*Managing User Sessions* on page 4-40](#) for more information.

## Enabling or Disabling Shareable Links

You can disable shareable links to stop file sharing. All of the previously shared links become temporarily unavailable and users cannot create new links until you enable shareable links again.

### Procedure

1. Go to **Administration > Security Control**.

   The **Security Control** screen appears.

2. Click **Disable Shareable Links** or **Enable Shareable Links**.

   A confirmation dialog appears.

3. Click **Disable** or **Enable**.
Managing User Sessions

You can require users to start a new SafeSync session in the following scenarios:

- Every time the SafeSync program starts
- After users have been inactive for a certain time

Once you configure the user session settings, the following actions will require users to sign in again to access SafeSync.

**TABLE 4-6. Managing User Sessions**

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>USER ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user web portal</td>
<td>• Close and reopen the browser</td>
</tr>
<tr>
<td></td>
<td>• Sign out from the end-user portal</td>
</tr>
<tr>
<td></td>
<td>• End the computer session</td>
</tr>
<tr>
<td></td>
<td>• Restart the computer</td>
</tr>
<tr>
<td>Windows/Mac client</td>
<td>• End the computer session</td>
</tr>
<tr>
<td></td>
<td>• Restart the computer</td>
</tr>
<tr>
<td></td>
<td>• Shut down the SafeSync program</td>
</tr>
<tr>
<td>Mobile apps</td>
<td>• Sign out from the app</td>
</tr>
<tr>
<td></td>
<td>• End the app process</td>
</tr>
</tbody>
</table>

**Procedure**

1. Go to Administration > Security Control.
   
   The Security Control screen appears.

2. Select Require users to sign in every time SafeSync starts to disable the Stay signed in option on the end user sign-in screen.

3. Specify when to automatically end a user session.
   
   For example, set the time to 3 hours to automatically sign out users from SafeSync when there is no activity for 3 hours.
Note

The Windows client connects to the SafeSync server regularly for status updates. The setting of this option does not affect the Windows client because the update frequency is less than 30 minutes.

4. Click Save.

Cache Servers

Use the **Cache Servers** screen to add and manage cache servers. Cache servers can help speed up access to SafeSync files and reduce the amount of network traffic on the SafeSync server. When users with access to cache servers open or download SafeSync files, cache servers keep a copy of the requested files for future access from the same users.

Setting up cache servers require the following actions:

- Add the cache server information to the SafeSync server and obtain a pairing code. See *Adding Cache Servers on page 4-42* for more information.

- Install the cache server program on the cache server and provide the pairing code during installation.

Note

You can get the SafeSync cache server program from the Trend Micro Download Center.

See *SafeSync Cache Server Program on page D-1* for more information.

- Use the URL listed in **Test URL** to test the connection between the cache server and the end user's computer.

- Check the detailed cache server information and status by selecting the row containing the cache server you just added. The server information appears on the right of the cache servers list.
Adding Cache Servers

Procedure

1. Go to Administration > Cache Servers.
   The Cache Servers screen appears.

2. Click Add.
   The Add Server screen appears.

3. Specify the server information.

4. Click Add in the User IP Address section to assign users to access SafeSync from the cache server.
   The Add IP Address screen appears.

5. Specify the user's IP address or specify an IP range.

6. Click Add.
   SafeSync adds the user information to the User IP Address list.

7. Repeat steps 4 to 6 to add additional user IP addresses.

8. Click Save.
   SafeSync adds the server information to the Cache Servers list and the Server Pairing screen appears.

9. Provide the pairing code during the cache server program installation to pair the cache server with the SafeSync server.

Editing Cache Servers

Use the Edit Server screen to update the server information and manage users that connect to the cache server.
Administering SafeSync

Procedure

1. Go to Administration > Cache Servers.

   The Cache Servers screen appears.

2. Click the display name of the server you want to modify.

   The Edit Server screen appears.

3. Modify the server information.

4. Modify the user IP address information.

   • Add: Add additional IP addresses.

   • Edit: Select a user IP address from the list and click Edit to modify the information.

   • Remove: Select a user IP address from the list and click Remove to stop the selected users from connecting to the cache servers.

5. Click Save.

Deleting Cache Servers

Procedure

1. Go to Administration > Cache Servers.

   The Cache Servers screen appears.

2. Select the row you want to remove.

3. Click Remove.

   A confirmation screen appears.

4. Click Remove.
Storage Management

Use the **Storage Management** screen to manage the following items:

- **Storage**: Add and manage SafeSync storage. See *Managing Storage on page 4-44* for more information.

- **Team folders**: View how each team folder is used and change the storage owner. See *Managing Team Folders on page 4-48* for more information.

- **Deleted users**: Manage the files remaining in the personal folders of deleted users. See *Managing Files Left by Deleted Users on page 4-49* for more information.

Managing Storage

Use the **Storage** tab to add and manage SafeSync storage. SafeSync supports the following types of storage:

- **Local disk**: hard disks attached to the SafeSync server
  
  See *Adding Local Disks on page 4-45* for more information.

- **iSCSI (Internet Small Computer Systems Interface)**: network storage
  
  See *Adding iSCSI Storage on page 4-45* for more information.

- **NFS (Network File System)**: network storage
  
  See *Adding NFS Storage on page 4-47* for more information.

---

**Important**

The storage must be greater than 10 GB in size and enable write access for the SafeSync server.

---

**WARNING!**

SafeSync removes any existing data after adding the storage. Back up any existing data before you add any storage.
Adding Local Disks

Important
The storage must be greater than 10 GB in size and enable write access for the SafeSync server.

Procedure

1. Go to Administration > Storage Management.
   The Storage Management screen appears.
2. Click Add in the Storage tab.
   The Add Storage screen appears.
3. Select Local disk and click Next.
   The Add Storage - Local Disk screen appears.

   Note
   SafeSync only supports disks that are greater than 10 GB.

4. Select the disks you want to add and click Add.
   SafeSync adds the storage and returns to the storage list.
5. Select the row containing the storage you just added to check the detailed storage information and status.
   The storage information appears on the right of the storage list.

Adding iSCSI Storage

Important
The storage must be greater than 10 GB in size and enable write access for the SafeSync server.
Procedure

1. Go to Administration > Storage Management.
   The Storage Management screen appears.

2. Click Add in the Storage tab.
   The Add Storage screen appears.

3. Select iSCSI and click Next.
   The Add Storage - iSCSI screen appears.

4. Specify the server information in the iSCSI Server section.

5. Select the SafeSync server and the network card to connect to the storage in the SafeSync Server section.

6. Click Next.
   The Available Storage list and CHAP Account section appear.

7. Select the IQN (iSCSI Qualified Name) you want to use from the Available Storage list.

8. If the iSCSI storage uses CHAP (Challenge Handshake Authentication Protocol) authentication, specify the CHAP account information in the CHAP Account section.

9. Click Add.
   SafeSync adds the storage and returns to the storage list.

10. Select the row containing the storage you just added to check the detailed storage information and status.
   The storage information appears on the right of the storage list.
Adding NFS Storage

**Important**

The storage must be greater than 10 GB in size and enable write access for the SafeSync server.

**Procedure**

1. Go to Administration > Storage Management.

   The Storage Management screen appears.

2. Click Add in the Storage tab.

   The Add Storage screen appears.

3. Select NFS and click Next.

   The Add Storage - NFS screen appears.

4. Specify the NFS server information.

5. Click Add.

   SafeSync adds the storage and returns to the storage list.

6. Select the row containing the storage you just added to check the detailed storage information and status.

   The storage information appears on the right of the storage list.

Editing Storage

**Procedure**

1. Go to Administration > Storage Management.

   The Storage Management screen appears.
2. Click the display name of the storage you want to modify.
3. Modify the storage information.

---

**Tip**

Modifying the **Display name** helps you better identify the storage.

---

**Managing Team Folders**

When users create new team folders, SafeSync automatically assigns the storage owner role to these users. Any files uploaded to the team folders take up the storage space assigned to the storage owners. When the storage owner uses up all the assigned storage space, SafeSync does not allow users to upload new files to the team folder and the storage owner's personal folders. SafeSync does not delete any previously uploaded files to accommodate new files.

For example, Tom Smith created a team folder named HR for the Human Resources department and became the storage owner. The HR team members then uploaded 1GB of files to the team folder. Tom currently has 150MB of files in his personal folders. In this case, Tom has used up (1GB + 150MB) of his SafeSync storage space.

When a storage owner's account is deleted, SafeSync automatically assigns the Default Plan to the affected team folders. You can assign a new owner to these folders.

---

**Procedure**

1. Go to **Administration > Storage Management**.

   The **Storage Management** screen appears.

2. Click a link in the **Size** column to check the types of uploaded files and the amount of storage used in a team folder.
3. Click **Change storage owner** to assign a different owner. You can also click **Change Plan** to assign a different plan to the storage owner.

**Managing Files Left by Deleted Users**

When a SafeSync user is deleted, SafeSync still keeps the user's personal files. You can delete the files or transfer the file ownership to another SafeSync user.
Procedure

1. Go to Administration > Storage Management.

   The Storage Management screen appears.

2. Select the Deleted Users tab.

3. Select a user and click Delete to delete the files uploaded by the user.

4. Click Transfer folder and select a new file owner to transfer the file ownership to another SafeSync user.
System Maintenance

System Maintenance allows you to restart, shut down, or restart the SafeSync server and services.

**Note**

Shutting down or restarting SafeSync services prevents all end users from accessing SafeSync until you restart the server.

**Procedure**

1. Go to Administration > System Maintenance.

   The System Maintenance screen appears.

2. Select one of the following:

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart SafeSync Services</td>
<td>Restarts the following SafeSync services</td>
</tr>
<tr>
<td></td>
<td>• mysql</td>
</tr>
<tr>
<td></td>
<td>• memcached</td>
</tr>
<tr>
<td></td>
<td>• gearman</td>
</tr>
<tr>
<td></td>
<td>• lighttpd</td>
</tr>
<tr>
<td></td>
<td>• mogstored</td>
</tr>
<tr>
<td></td>
<td>• mogilefsd</td>
</tr>
<tr>
<td></td>
<td>• apache</td>
</tr>
<tr>
<td>Restart SafeSync Server</td>
<td>Restarts the SafeSync server</td>
</tr>
<tr>
<td>Shut Down</td>
<td>Shuts down the SafeSync server</td>
</tr>
</tbody>
</table>

3. Click OK.
System Updates

Use the System Updates screen to keep SafeSync up-to-date for optimal system performance and functionality.

---

**Important**
Performing an update restarts the SafeSync server and disconnect all end users. Choose a time that has the minimal impact on end users to perform the task.

---

Downloading Update Files

For official patches or services packs, you can download the update file from the Trend Micro Software Download Center.

**Procedure**

1. Go to the following website:
   

2. Under Mobile Protection, click SafeSync for Enterprise.

3. Click the Product Download/Update or Product Patch tab.

4. Click the appropriate download package.

5. In the confirmation window that appears, select whether you want to use the Download Manager or HTTP download.

---

Performing System Updates

**Procedure**

1. Go to Administration > System Updates.

   The System Updates screen appears.
2. Click **Browse**... and select the update file.
3. Click **Update** and then click **Yes**.
   SafeSync starts the update process and applies the changes.

---

**Note**
If the update requires a system restart, the page redirects to the **Logon** screen when the process completes.

If the update does not require a restart, the page reloads and SafeSync updates the **Update history** table.

---

**Rolling Back System Updates**

Rollback refers to reverting to the previous version of the SafeSync update file. If there appears to be an issue after updating SafeSync, roll back the last update to restore the system to the previous version before the last update occurred.

---

**Procedure**

1. Go to **Administration > System Updates**.
   The **System Updates** screen appears.

2. Click **Roll Back to <Last update timestamp>**.
   SafeSync starts the rollback process and applies the changes.

---

**Note**
If the rollback requires a system restart, the page redirects to the **Logon** screen when the process completes.

If the rollback does not require a restart, the page reloads and SafeSync updates the **Update history** table.
License Information

Use the License Information screen to manage activation codes for the following:

- SafeSync for Enterprise
- SafeSync for Enterprise: Outlook Extension
- SafeSync for Enterprise: Shared Protection Extension

Viewing Product License Information

Procedure

1. Go to Administration > License Information.

   The License Information screen appears.

2. View the following information:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Displays either &quot;Full&quot; or &quot;Trial&quot; version</td>
</tr>
<tr>
<td>Seats</td>
<td>Displays the total number of seats and the number of seats in use</td>
</tr>
<tr>
<td>Activation Code</td>
<td>Displays the Activation Code</td>
</tr>
<tr>
<td>Status</td>
<td>Displays either &quot;Activated&quot;, &quot;Not Activated&quot; or &quot;Expired&quot;</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Displays the expiration date</td>
</tr>
</tbody>
</table>

**Note**

The version and expiration date of licenses that have not been activated are "N/A".
Limitations of Expired Licenses

The following table describes the limitations of the different license types and versions after expiration.

**TABLE 4-7. Limitations of Expired Licenses**

<table>
<thead>
<tr>
<th>LICENSE</th>
<th>VERSION</th>
<th>LIMITATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeSync</td>
<td>Full</td>
<td>End users can continue accessing the SafeSync server and web console. However, Trend Micro no longer provides technical support.</td>
</tr>
<tr>
<td>Trial</td>
<td></td>
<td>The SafeSync server and web console are no longer accessible.</td>
</tr>
<tr>
<td>SafeSync for Enterprise: Outlook Extension</td>
<td>Full</td>
<td>End users can continue accessing the Outlook Extension and the SafeSync server. However, Trend Micro no longer provides technical support.</td>
</tr>
<tr>
<td>Trial</td>
<td></td>
<td>The Outlook Extension is no longer accessible.</td>
</tr>
<tr>
<td>SafeSync for Enterprise: Shared Protection Extension</td>
<td>Full</td>
<td>End users can still encrypt or decrypt files. However, Trend Micro no longer provides technical support.</td>
</tr>
<tr>
<td>Trial</td>
<td></td>
<td>End users can no longer encrypt new files but they may still decrypt previously encrypted files.</td>
</tr>
</tbody>
</table>

Activating or Renewing SafeSync

SafeSync needs to be activated after installation.

**Procedure**

1. Go to Administration > License Information.

   The License Information screen appears.
2. Under **SafeSync for Enterprise**, click **Specify New Activation Code**.

   The **New Activation Code** screen appears.

   ![New Activation Code](image)

   3. Type the Activation Code.

   4. Click **OK**.

---

**Activating SafeSync Add-Ins**

**Important**

You must first activate SafeSync for Enterprise before activating the add-ins.

---

**Procedure**

1. Go to **Administration > License Information**.

   The **License Information** screen appears.

2. In the purchased add-in section, click **Specify Activation Code**.

   The **New Activation Code** screen appears.
3. Type the Activation Code for the add-in.

4. Click **OK**.

SafeSync activates and enables the feature.

For more information on managing add-ins, see *Configuring SafeSync Add-Ins on page 4-24.*
Frequently Asked Questions (FAQs)

This chapter answers various Frequently Asked Questions.

Topics in this chapter include:

- Files on page 5-2
- Services on page 5-4
- Storage on page 5-5
- SSL Certificates on page 5-5
Files

How can I upload files that are more than 3 GB in size?

When users upload files more than 3 GB using a web browser, they may encounter the following issues:

• The progress bar displays but there is no progress shown. The bar stays at 0%.
• The following error messages appear:
  • Storage not available
  • You have tried to store too many files

These issues occur because most modern browsers have a maximum file size limit of 2-3 GB for uploads. As a workaround, use a SafeSync client such as Windows or Mac OSX to upload large files.

Why am I unable to view some thumbnail images?

The broken thumbnail image appears on the end-user portal when users upload files that are more than 20 MB in size. By default, SafeSync only creates thumbnail images for files that are 20 MB or less.

To resolve this issue, increase the thumbnail size limitation.

Procedure

1. Log on to the SafeSync server shell.
2. Use a text editor to edit the file /etc/osdp/OSDP.cfg.
3. Add the following line to the file:

   MAX_IMAGE_THUMB_BUILD_SIZE => 26 * 1024 * 1024,
4. Save and close the file.

5. Restart the “grunjobs” service using the following command.

   `/etc/init.d/grunjobs restart`

6. Double-click the broken thumbnail image.
   The thumbnail images display correctly.

**Why am I unable to upload files to a team folder?**

Team folder capacity is affected by the storage owner's storage space. When the storage owner uses up all the assigned storage space, SafeSync does not allow users to upload new files to the team folder.

To resolve the issue, have the storage owner clean up his storage space or assign a storage plan with a larger storage size to the storage owner.

**Procedure**

1. Go to Administration > Storage Management.
   The Storage Management screen appears.

2. Locate the team folder and click Change storage owner in the same row.
   The Change Storage Owner screen appears.

3. Click Change Plan.

4. Select a plan with a larger storage size for the owner and click Save.

5. Click Save.
Services

What services should be installed after a successful SafeSync installation?

The following services should be installed after a successful SafeSync installation.

- apache2
- appache2-store
- avscand
- bov1d
- gearmand
- grunjobs
- healthcheck
- keepalived
- kmsd
- libreoffice
- lighttpd
- memcached
- mgmtui
- mogilefsd
- mogstored
- mysql
- nginx
- perlbal81
- perlbal82
- perlbal83
- perlbal84
- tmsyslog
- sshd
- thin
- safesync-fusedav

How can I verify if all SafeSync services are working properly?

Procedure

1. Log on to the server shell.
2. Run the following command to go to the specific directory:

   `cd /opt/SingleInstaller/nodeControl/bin/`
3. Run the following command to check the service status:

   ./check_all_service_status.sh

   If there are no problems, the command line editor displays the following message:

   All SafeSync services are working properly

---

**Storage**

**How does SafeSync determine the storage limit for each user?**

SafeSync uses plans to assign storage limits for each user. Plans control the maximum allowed storage, upload or download speeds, and number of version backups.

After users exceed the assigned storage limit, subsequent uploads are no longer allowed. To resolve the issue, users must delete files and then empty the **Recycle Bin** to free up storage space.

**SSL Certificates**
Does SafeSync support PKCS7 certificates?

SafeSync does not support PKCS7 certificates. The following error message appears when uploading a PKCS7 certificate to the SafeSync server.

The error appears because SafeSync only supports PKCS12 certificates with file extensions such as `.pfx` and `.p12`.

To resolve the issue, contact the Certificate Authority (CA) company to request for a PKCS12 certificate and then perform the following steps:

**Procedure**

1. Using the PKCS12 certificate, convert the **PEM** file.
   a. Upload the `.pfx` file to the `/home/safesync` folder in the SafeSync server using an SFTP and FTP client.
   b. Log on to the SafeSync command console using the putty command line.
   c. Under `/home/safesync`, run the following command.
      ```
      openssl pkcs12 -in xxxxxx.pfx -out xxxxxx.pem -nodes
      ```

2. Open the **PEM** file.
   a. Copy the SSL certificate and save it as a text file.
      ```
      -----BEGIN CERTIFICATE-----
      xxxxxxxxxxxxxxxxx......
      ```
b. Copy the private key and save it as a text file.

-----BEGIN PRIVATE KEY-----
xxxxxxxxxxxxxxxxxxxxx.....
-----END PRIVATE KEY-----

3. Go to Administration > System Settings > SSL Certificate.
4. Click Import Certificate.
5. Click Choose File to select the certificate and private key files created from step 2.
6. Click Import.

Does SafeSync support wildcard certificates?

SafeSync supports wildcard certificates. However, only first-level sub-domains are supported. For example, if the domain name is ssfe.<your_domain>.com, a wildcard certificate for * ssfe.<your_domain>.com may be used.

If the wildcard certificate is for *.ssfe.<your_domain>.com, the certificate cannot be used because the address www.ssfe.<your_domain>.com is already a second-level sub-domain of the wildcard certificate. Only first-level sub-domains are supported because SSL wildcard certificates would not work for multiple levels.
Chapter 6

Contacting Technical Support

This chapter describes how to use the Support Portal and contact Trend Micro.

Topics in this chapter include:

• Contacting Trend Micro on page 6-2
• Speeding Up the Support Call on page 6-2
Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Toll free: +1 (800) 228-5651 (sales)</td>
</tr>
<tr>
<td></td>
<td>Voice: +1 (408) 257-1500 (main)</td>
</tr>
<tr>
<td>Fax</td>
<td>+1 (408) 257-2003</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:
- Trend Micro product documentation:
  [http://docs.trendmicro.com](http://docs.trendmicro.com)

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Activation code and license status
- Browser information and version
- Product version and system update history
- Steps to reproduce the problem
- Appliance or network information
- Computer/device brand, model, and any additional hardware connected to the endpoint
• Memory and disk or storage status
• Computer/device operating system and service pack version
• Detailed description of the installation environment
• Exact text or screenshot of any error message received
Appendix A

Understanding Threats

Organizations without dedicated security personnel and with lenient security policies are increasingly exposed to threats, even if they have basic security infrastructure in place. Once discovered, these threats may have already spread to many computing resources, taking considerable time and effort to eliminate completely. Unforeseen costs related to threat elimination can also be staggering.

Trend Micro network security intelligence and in-the-cloud servers that are part of Trend Micro Smart Protection Network identify and respond to next-generation threats.
Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Although once most common in DOS or Windows, endpoint viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

**TABLE A-1. Virus/Malware Types**

<table>
<thead>
<tr>
<th>Virus / Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joke program</td>
<td>Joke programs are virus-like programs that often manipulate the appearance of things on the endpoint's monitor.</td>
</tr>
<tr>
<td>Others</td>
<td>“Others” include viruses/malware not categorized under any of the other virus/malware types.</td>
</tr>
<tr>
<td>Packer</td>
<td>Packers are compressed and/or encrypted Windows or Linux™ executable programs, often a Trojan horse program. Compressing executables makes packers more difficult for antivirus products to detect.</td>
</tr>
<tr>
<td>Rootkit</td>
<td>Rootkits are programs (or collections of programs) that install and execute code on a system without end user consent or knowledge. They use stealth to maintain a persistent and undetectable presence on the machine. Rootkits do not infect machines, but rather, seek to provide an undetectable environment for malicious code to execute. Rootkits are installed on systems via social engineering, upon execution of malware, or simply by browsing a malicious website. Once installed, an attacker can perform virtually any function on the system to include remote access, eavesdropping, as well as hide processes, files, registry keys and communication channels.</td>
</tr>
<tr>
<td>Test virus</td>
<td>Test viruses are inert files that act like a real virus and are detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation scans properly.</td>
</tr>
<tr>
<td><strong>Virus / Malware Type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>Trojan horse programs often use ports to gain access to computers or executable programs. Trojan horse programs do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.</td>
</tr>
</tbody>
</table>
| Virus                  | Viruses are programs that replicate. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes, including:  
  - **ActiveX malicious code**: Code that resides on web pages that execute ActiveX™ controls.  
  - **Boot sector virus**: A virus that infects the boot sector of a partition or a disk.  
  - **COM and EXE file infector**: An executable program with .com or .exe extension.  
  - **Java malicious code**: Operating system-independent virus code written or embedded in Java™.  
  - **Macro virus**: A virus encoded as an application macro and often included in a document.  
  - **VBScript, JavaScript or HTML virus**: A virus that resides on web pages and downloaded through a browser.  
  - **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other endpoint systems, often through email. |
<table>
<thead>
<tr>
<th>Virus / Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Virus</td>
<td>A virus spreading over a network is not, strictly speaking, a network virus. Only some virus/malware types, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of agent endpoints, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.</td>
</tr>
<tr>
<td>Probable virus/ malware</td>
<td>Probable viruses/malware are suspicious files that have some of the characteristics of viruses/malware. For more information, see the Trend Micro Threat Encyclopedia: <a href="http://about-threats.trendmicro.com/us/threatencyclopedia#malware">http://about-threats.trendmicro.com/us/threatencyclopedia#malware</a></td>
</tr>
</tbody>
</table>

**Trend Micro™ Smart Protection Network™**

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight agents to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers’ protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

For more information on the Smart Protection Network, visit: [http://www.smartprotectionnetwork.com](http://www.smartprotectionnetwork.com)
Appendix B

Understanding Components

Antivirus components consist of the following engine and patterns:

- *Smart Scan Agent Pattern on page B-2*
- *Virus Scan Engine on page B-2*
- *IntelliTrap Pattern on page B-3*
- *IntelliTrap Exception Pattern on page B-3*
Smart Scan Agent Pattern

The Smart Scan Agent Pattern is updated daily and is downloaded by the SafeSync update source (the ActiveUpdate server or a custom update source).

Note

SafeSync uses the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged.

Virus Scan Engine

At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of Viruses and Malware on page A-2. The scan engine also detects controlled viruses that are developed and used for research.

Rather than scanning every byte of every file, the engine and pattern file work together to identify the following:

- Tell-tale characteristics of the virus code
- The precise location within a file where the virus resides

IntelliTrap

IntelliTrap is a Trend Micro heuristic technology used to discover threats that use real-time compression paired with other malware characteristics like Packers. This covers virus/malware, worms, trojans, backdoors and bots. Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider
quarantining (not deleting or cleaning) files when you enable IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the same scan engine as virus scanning. As a result, the file handling and scanning rules for IntelliTrap are the same as administrator-defined rules for virus scanning.

**Note**

IntelliTrap uses the following components when checking for bots and other malicious programs:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

---

**IntelliTrap Pattern**

The IntelliTrap pattern detects real-time compression files packed as executable files.

**IntelliTrap Exception Pattern**

The IntelliTrap Exception Pattern contains a list of "approved" compression files.
Appendix C

Deploying SafeSync to End Users

This chapter explains how to deploy SafeSync to end users.

Topics in this chapter include:

- Deploying SafeSync to Desktops and Laptops on page C-2
- Deploying SafeSync to Mobile Devices on page C-3
Deploying SafeSync to Desktops and Laptops

Administrators can deploy SafeSync to the desktops or laptops of their end users using an MSI file.

**Note**

The MSI file includes the SafeSync Windows client and the SafeSync for Outlook extension.

**Procedure**

1. Log on to the Active Directory server with an account with sufficient privileges. For example, a system administrator account.
2. Open the **Active Directory Users and Computers** management console.
3. Right-click the domain for the network’s Active Directory server.
4. Click **Properties**. The **Domain Properties** screen appears.
5. Click **Group Policies**.
6. Click **New** to create a new group policy.
7. Type a name for the group policy. For example, **SafeSync-Deploy**.
8. Select the new group policy.
9. Click **Edit**. The **Group Policy Object Editor** screen appears.
10. Expand **User Configuration > Software Settings** from the left-hand pane. The entry **Software Installation** appears under **Software Settings**.
11. Right-click **Software Installation**.

12. Select **New > Package**.

A dialog box appears.

13. Select the SafeSync MSI file.

14. Click **Open**.

The **Deploy Software** dialog appears.

15. Select **Assigned**.

Selecting **Assigned** means that SafeSync installs automatically the next time the end-user logs on to their laptop or desktop.

---

**Deploying SafeSync to Mobile Devices**

Administrators can deploy SafeSync to their end users by sending an email message.

---

**Tip**

Trend Micro recommends this deployment method for mobile devices (Android and iOS).

---

**Procedure**

1. Create an email template for deployment.

2. Insert the following URL into the email message:

   `https://<SafeSync domain name>/app#downloads`

3. Send the email to the end users who have SafeSync accounts.

4. End users should click the link in the email and follow the instructions included in the SafeSync installation package.
Appendix D

SafeSync Cache Server Program

This chapter explains how to install the SafeSync cache server program on endpoints assigned to connect to the cache servers.

Topics in this chapter include:

• *System Requirements on page D-2*
• *Installation Methods on page D-2*
• *Installing the SafeSync Cache Server Program on page D-2*
System Requirements

Ensure that end user's computers meet the following system requirements:

• Disk space: 100 GB
• Memory: 2 GB
• Network card: 1 Gb network interface card (NIC)

Installation Methods

There are two ways to install the SafeSync cache server program, either from an ISO image file or an Open Virtualization Format (OVF) installation package. The OVF installation package can only be installed on a virtual machine.

Note
You can get the SafeSync cache server program from the Trend Micro Download Center.

Installing the SafeSync Cache Server Program

Note
A pairing code is required to complete the installation. Obtain one by adding the storage information on the Administration > Cache Servers screen in the SafeSync administrator web console.

If the cache server is already set up on SafeSync, select the row containing the cache server and check the information appears on the right of the cache servers list. Click Get Pairing Code to obtain a pairing code.

Procedure

1. Run the SafeSync cache server program on the endpoint you want to install.
   The system requirements display if you install the program on a computer.
2. (Skip this step if you install the program on a virtual machine) Press the ENTER key to begin the installation.

The **Configure the network** screen appears.

3. Type the IP address for the cache server.

4. Select **Continue** or press the ENTER key.
The following screen appears.

5. Type the IP address for the subnet mask.

6. Select **Continue** or press the ENTER key.
The following screen appears.

7. Type the IP address for the gateway.

8. Select **Continue** or press the ENTER key.
The following screen appears.

9. Type the IP address for the DNS server.

10. Select **Continue** or press the ENTER key.
The **Set up users and passwords** screen appears.

11. Type a password for the system account.

   The user name for the account is **safesync**. Use this account to log on to the command line console of the SafeSync server and configure advanced server settings.

12. Select **Continue** or press the ENTER key.
The following screen appears.

13. Retype the password.

14. Select **Continue** or press the ENTER key.
The **Connect to SafeSync Server** screen appears.

15. Type the IP address or FQDN for the SafeSync server.
16. Select **Continue** or press the ENTER key.

The **Server Pairing** screen appears.

A pairing code is required to connect the cache server to SafeSync.

Note: Obtain the pairing code by adding the storage information on the Administration > Cache Servers screen in the SafeSync administrator web console.

<Continue>
17. Type the pairing code to connect the cache server to SafeSync.

18. Select **Continue** or press the ENTER key.

The installation completes and the following screen appears.

```
Installation completed successfully.
Use the following account information to log on to the command line console of the SafeSync server and configure advanced server settings:

User name: safesync
Password: ********

Hint: Num Lock on

ubuntu login: _
```
Appendix E

Glossary

The terms contained in this glossary provide further information about commonly referenced computer terms, as well as Trend Micro products and technologies.
ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of pattern files, scan engines, programs, and other Trend Micro component files through the Internet.

Compressed File

A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip.

End User License Agreement

An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product.

Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

False Positive

A false positive or false alarm occurs when a file is incorrectly detected by security software as infected.
**HTTP**

Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting web pages (including graphics and multimedia content) from a server to a client over the Internet.

**HTTPS**

Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.

**IntelliScan**

IntelliScan is a method of identifying files to scan. For executable files (for example, .exe), the true file type is determined based on the file content. For non-executable files (for example, .txt), the true file type is determined based on the file header.

Using IntelliScan provides the following benefits:

- **Performance optimization**: IntelliScan does not affect applications on the client because it uses minimal system resources.

- **Shorter scanning period**: Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

**True File Type**

In “true file type” scanning, the scan engine examines the file header, rather than the file name, to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named “family.gif,” it does not assume the file is a graphic file. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file or an executable that someone named to avoid detection.
True file type scanning works in conjunction with IntelliScan to scan only those file types known to be potentially dangerous. These technologies can reduce, by as much as two-thirds, the number of files the scan engine examines; this file-scanning reduction also creates some risk that a harmful file might be allowed onto the network.

For example, .gif files make up a large volume of all web traffic, but they are unlikely to harbor viruses/malware, launch executable code, or carry out any known or theoretical exploits. Therefore, does this mean they are safe? Not entirely. It is possible for a malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. This file could cause damage if someone renamed it and ran it.

---

**Tip**

For the highest level of security, Trend Micro recommends scanning all files.

---

**IntelliTrap**

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
**IP**

"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

**Proxy Server**

A proxy server is a World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

**SSL**

Secure Socket Layer (SSL) is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
Index

A
about SafeSync, 1-2
account password, 4-3
accounts
    disabled, 2-9, 2-13
activating, 4-55
    add-ins, 4-56
Activation Code, 4-54, 4-55
Active Directory integration, 4-7
    adding servers, 4-8
    enabling, 4-8
    root DN, 4-8
    selecting users, 2-7
ActiveX malicious code, A-3
adding
    Active Directory servers, 4-8
    administrator accounts, 4-4
    cache servers, 4-42
    iSCSI storage, 4-45
    local disks, 4-45
    NFS storage, 4-47
    policies, 2-20
    users, 2-7
add-ins, 4-22
    activating, 4-56
    configuring, 4-25
    Outlook Extension, 4-23
    Shared Protection Extension, 4-24
administration
    Active Directory integration, 4-7
    administrator accounts, 4-4, 4-5
    antivirus settings, 4-9
    cache server program, D-1, D-2
    cache servers, 4-41–4-43
    high availability, 4-31, 4-32
    license information, 4-54
    my account, 4-3
    security control, 4-39, 4-40
    storage management, 4-44–4-48, 4-50, 5-3
    system maintenance, 4-51
    system notifications, 4-6
    system settings, 4-19
    system updates, 4-52
administrator accounts, 4-4, 4-5
    adding, 4-4
    deleting, 4-5
    disabling, 4-5
    editing, 4-3, 4-4
    enabling, 4-5
B
boot sector virus, A-3
C
cache server program, D-1
    installation, D-2
    installation methods, D-2
    system requirements, D-2
cache servers, 4-41
    adding, 4-42
    assigning end users, 4-42, 4-43
    deleting, 4-43
    editing, 4-42
    pairing code, 4-42, D-2
    Test URL, 4-41
changing
    password, 4-3
    storage owner, 4-49
COM file infector, A-3
Component Status widget, 3-8
configuring
   Active Directory settings, 4-7
   add-ins, 4-25
   high availability, 4-31, 4-32
   notification settings, 4-6
   policies, 2-17
   primary server, 4-31
   proxy server settings, 4-20
   secondary server, 4-32
   SMTP server settings, 4-21
   SSL certificate settings, 4-22
   syslog server, 3-17
   virtual IP address, 4-31
   web console settings, 4-19

Dashboard
   about, 3-2
   Component Status widget, 3-8
   System Status Alert widget, 3-13
   System Status widget, 3-12
   Threat Statistics widget, 3-3
   Top 10 Threats widget, 3-7
   Top 10 Users with Virus/Malware Detections widget, 3-5
   Usage Trends widget, 3-10
   widgets, 3-3, 3-5, 3-7–3-10, 3-12, 3-13

decrypting files, 4-26
deleted users
   transferring file ownership, 4-49
deleting
   administrator accounts, 4-5
   cache servers, 4-43
   logs, 3-16
   policies, 2-21
   disabled users, 2-9, 2-13

disabling
   administrator accounts, 4-5
   shareable links, 4-39

DNS records, 4-20
documentation, viii
domain accounts, 2-7
   changing plans, 2-9
   disabled, 2-9

Editing
   administrator accounts, 4-3, 4-4
   cache servers, 4-42
   policies, 2-21
   storage, 4-47
   EICAR test script, A-2
   email address, 4-3
      notification recipients, 4-6
      SMTP server, 4-21

Enabling
   Active Directory integration, 4-8
   administrator accounts, 4-5
   shareable links, 4-39
   End User License Agreement (EULA), E-2
   EXE file infector, A-3

Forwarding
   logs, 3-16

High availability, 4-28
   configuring, 4-31, 4-32
   primary server, 4-31
   secondary server, 4-32
   virtual IP address, 4-31
   HTML virus, A-3
### I
- installation methods, 1-3
- integrating Active Directory structure, 4-7
- IntelliTrap Exception Pattern, B-3
- IntelliTrap Pattern, B-3
- iSCSI storage, 4-45
- ISO installation, 1-3

### J
- Java malicious code, A-3
- JavaScript virus, A-3
- joke program, A-2

### L
- license, 4-54, 4-55
- local disks, 4-45
- logs
  - deletion, 3-16
  - email address, 4-3
  - querying, 3-16
  - syslog server, 3-17

### M
- macro virus, A-3
- maintenance
  - logs, 3-16
  - manual accounts
    - adding, 2-10
    - changing plans, 2-14
    - deleting, 2-12
    - disabled, 2-13
    - editing, 2-11
    - enabling/disabling, 2-12
- my account, 4-3
  - changing password, 4-3
  - email address, 4-3

### N
- network virus, A-4
- NFS storage, 4-47
- notifications
  - recipients, 4-6
  - settings, 4-6

### O
- Outlook Extension, 4-23
  - activating, 4-56
  - configuring, 4-25
- OVF installation, 1-3

### P
- packer, A-2
- pairing code, 4-42, D-2
- password, 4-3
- pattern files
  - Smart Scan Agent Pattern, B-2
- performing system updates, 4-52
- plans, 2-22
  - adding, 2-23
  - changing assignment, 2-9, 2-14, 2-15
  - deleting, 2-25
  - editing, 2-24
  - reviewing user and group assignment, 2-22, 2-25
- policies, 2-17
  - adding, 2-20
  - deleting, 2-21
  - editing, 2-21
- primary server, 4-28, 4-31
- probable virus/malware, A-4
- proxy server settings, 4-20

### Q
- querying logs, 3-16
R
recipients, 4-6
renewing, 4-55
reports, 3-14
root DN, 4-8
rootkit, A-2

S
SafeSync
about, 1-2
add-ins, 4-22
documentation, viii
system requirements, 1-10
terminology, x
users, 2-7
secondary server, 4-28, 4-32
security control, 4-39, 4-40
shareable links, 4-39
user sessions, 4-40
setting up SafeSync users, 2-7
shareable links, 4-39
disabling, 4-39
enabling, 4-39
Shared Protection Extension, 4-24
activating, 4-56
configuring, 4-25
decrypting files, 4-26
smart protection, A-4, B-2
pattern files, B-2
Smart Scan Agent Pattern, B-2
Smart Protection Network, A-4
Smart Protection Network, A-4
Smart Scan Agent Pattern, B-2
SMTP server settings, 4-21
SSL certificate, 4-22
stay signed in, 4-40
storage
editing, 4-47
iSCSI, 4-45
local disks, 4-45
management, 4-44–4-48, 4-50, 5-3
NFS, 4-47
owner, 4-49
support
resolve issues faster, 6-2
syslog server, 3-17
system requirements
cache server program, D-2
SafeSync, 1-10
system settings
proxy server, 4-20
SMTP server, 4-21
SSL certificate, 4-22
syslog server, 3-17
web console, 4-19
System Status Alert widget, 3-13
System Status widget, 3-12

T
team folders
storage management, 4-44, 4-48
storage owner, 4-49
terminology, x
Test URL, 4-41
test virus, A-2
Threat Statistics widget, 3-3
Top 10 Threats widget, 3-7
Top 10 Users with Virus/Malware
Detections widget, 3-5
transferring file ownership, 4-49
Trojan horse program, A-3

U
updating
SSL certificate, 4-22
system, 4-52
Usage Trends widget, 3-10
users, 2-6
  adding, 2-10
  changing multiple accounts simultaneously, 2-15
  changing plans, 2-14
deleted, 4-44, 4-49
deleting, 2-12
disabled, 2-9, 2-13
domain accounts, 2-7
typing, 2-11
enabling/disabling, 2-12
individual user details, 2-16
manual accounts, 2-10
sessions, 4-39, 4-40
types, 2-7

V
VBScript virus, A-3
virtual IP address, 4-28, 4-31
virus/malware, A-2–A-4
  ActiveX malicious code, A-3
  boot sector virus, A-3
  COM and EXE file infector, A-3
  Java malicious code, A-3
  joke program, A-2
  macro virus, A-3
  packer, A-2
  probable virus/malware, A-4
  rootkit, A-2
  test virus, A-2
  Trojan horse program, A-3
types, A-2–A-4
  VBS/Script, JavaScript or HTML virus, A-3
  worm, A-3
  Virus Encyclopedia, A-4
  Virus Scan Engine, B-2

W
web console settings, 4-19
  DNS records, 4-20
widgets
  Component Status, 3-8
  overview, 3-9
  System Status, 3-12
  System Status Alert, 3-13
  Threat Statistics, 3-3
  Top 10 Threats, 3-7
  Top 10 Users with Virus/Malware Detections, 3-5
  Usage Trends, 3-10
worm, A-3