2.1 SafeSync for Enterprise
Administrator’s Guide
Share, Distribute, and Access Enterprise files within your private cloud
Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/

Trend Micro, the Trend Micro t-ball logo, SafeSync 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 © 2013 Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM26022/130802

Release Date: Aug. 2013

The user documentation for Trend Micro SafeSync for Enterprise introduces the installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro’s website.

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.

Please evaluate this documentation on the following site:

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

## Preface

Preface .................................................................................................................. v  
What's New in This Version ........................................................................... vi  
SafeSync Documentation ................................................................................ vii  
Audience ............................................................................................................ vii  
Document Conventions .................................................................................. viii  
Terminology ....................................................................................................... ix

## Chapter 1: Introducing SafeSync

About SafeSync ............................................................................................... 1-2  
Why Use SafeSync .......................................................................................... 1-2

## Chapter 2: Getting Started

Logging On to SafeSync ................................................................................ 2-2  
Changing the Logon Password ..................................................................... 2-2  
Configuring Proxy Server Settings ............................................................... 2-3  
Activating or Renewing SafeSync ................................................................. 2-5  
Performing System Updates ......................................................................... 2-7  
Configuring Active Directory Settings ........................................................ 2-8  
Setting Up SafeSync Users .......................................................................... 2-10  
Configuring SafeSync Web Console Settings ............................................. 2-11  
Configuring SMTP Server Settings .............................................................. 2-13  
Configuring Notification Settings ............................................................... 2-15
Chapter 3: Plans, Policies, and Users

Configuring Plans ................................................................. 3-2
  Adding a Plan ................................................................. 3-2
  Editing a Plan ................................................................. 3-2
  Deleting a Plan ............................................................... 3-3
  Reviewing Groups and Users Assigned to a Plan ............ 3-3

Configuring Policies .......................................................... 3-3
  Adding Policies ............................................................. 3-4
  Editing Policies ............................................................. 3-5
  Deleting Policies ........................................................... 3-5

Managing Users ............................................................... 3-5
  Domain Accounts .......................................................... 3-5
  Manual Accounts .......................................................... 3-7
  Searching for a User Account ......................................... 3-11
  Viewing Individual User Details ..................................... 3-11
  Inviting Users to Share Files .......................................... 3-12
  Managing Disabled Accounts .......................................... 3-12

Chapter 4: Monitoring SafeSync

About the SafeSync Dashboard .............................................. 4-2
  Usage Trends Widget ...................................................... 4-2
  System Status Widget .................................................... 4-3
  System Status Alert Widget ............................................ 4-4

Configuring Reports .......................................................... 4-4

Querying Logs ..................................................................... 4-5
  Deleting Logs .................................................................. 4-7
  Configuring Syslog Server Settings ................................. 4-8

Chapter 5: Deploying SafeSync to End-Users

Deploying SafeSync to Desktops and Laptops ....................... 5-2
  Deploying SafeSync to Mobile Devices ............................ 5-3

Chapter 6: Managing SafeSync Add-Ins

SafeSync Add-Ins ................................................................ 6-2
Table of Contents

Activating SafeSync Add-Ins ................................................................. 6-3
Configuring SafeSync Add-Ins ............................................................. 6-5
Decrypting all Encrypted Files ......................................................... 6-6

Chapter 7: Administering SafeSync

Updating SSL Certificate Information ............................................. 7-2
Restarting SafeSync ......................................................................... 7-4
Configuring the Web Console Language ........................................ 7-5

Chapter 8: Contacting Technical Support

Index

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

This Administrator’s Guide introduces SafeSync and walks you through configuring SafeSync to function according to your needs.

Topics in this chapter include:

- What's New in This Version on page vi
- SafeSync Documentation on page vii
- Audience on page vii
- Document Conventions on page viii
- Terminology on page ix
What's New in This Version

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

**TABLE 1. New Features and Enhancements**

<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</td>
</tr>
<tr>
<td></td>
<td>the 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 users by plan order or select a specific plan for them</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>
SafeSync Documentation

SafeSync documentation includes the following:

**TABLE 2. SafeSync Documentation**

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</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 discusses getting started information and SafeSync usage and management.</td>
</tr>
<tr>
<td>Help</td>
<td>Hosted HTML files that provide &quot;how to's&quot;, usage advice, and field-specific information. The Help is accessible from the SafeSync web console.</td>
</tr>
<tr>
<td>Readme file</td>
<td>Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation.</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:

[http://docs.trendmicro.com](http://docs.trendmicro.com)

**Audience**

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

The documentation uses the following conventions.

**TABLE 3. Document Conventions**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPERCASE</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><em>Italics</em></td>
<td>References to other documents</td>
</tr>
<tr>
<td><strong>Monospace</strong></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>
</tbody>
</table>

- **Note** | Configuration notes            |
- **Tip**   | Recommendations or suggestions  |
- **Important** | Information regarding required or default configuration settings and product limitations |
- **WARNING!** | Critical actions and configuration options |
Terminology

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

**Table 4. 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. 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>
</tbody>
</table>
Chapter 1

Introducing SafeSync

This section introduces SafeSync and the benefits SafeSync brings to enterprises.

Topics in this chapter include:

• *About SafeSync on page 1-2*
• *Why Use SafeSync on page 1-2*
About SafeSync

Trend Micro SafeSync is a turnkey solution for the Enterprise to the private cloud. SafeSync provides a seamless data accessing experience to users in a more secure, flexible and convenient way.

- Integrated with most external storage types (SAN or NAS).
- Support Active Directory integration.
- Secure your data in the private cloud at any time. SafeSync supports file version control and redundant backups of your data.
- Access your data using various devices (PC, Mac, Android, iOS devices)
- Enhance teamwork using a shared collaborative data space.

Why Use SafeSync

SafeSync provides the following:

<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>
<tr>
<td>Sync files continuously and automatically</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Folder pairing enables automatic syncing of an entire folder without the need to drag and drop into the SafeSync folder.</td>
</tr>
</tbody>
</table>
Introducing SafeSync

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share files easily and securely</td>
<td>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.</td>
</tr>
<tr>
<td>Easily create and control user accounts</td>
<td>SafeSync supports centralized administration for creating and controlling users.</td>
</tr>
<tr>
<td>Recover previous versions of files</td>
<td>Recovery of deleted files or previous file versions allows you to turn back time.</td>
</tr>
<tr>
<td>Control your own data</td>
<td>You operate the data center, so no third party has access to your data.</td>
</tr>
<tr>
<td>Protect files with encryption</td>
<td>Protect files with the same Advanced Encryption Standard (AES) 256-bit encryption used by government and the military.</td>
</tr>
<tr>
<td>Securely share email attachments sent from Microsoft Outlook</td>
<td>When the <strong>SafeSync Outlook Extension</strong> 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 <strong>SafeSync Outlook Extension</strong> helps to prevent unintentional data leakage through misdirected or forwarded emails, or device loss.</td>
</tr>
<tr>
<td>Automatically encrypt files using an auto-encryption folder</td>
<td>When the <strong>Shared Protection Extension</strong> 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.</td>
</tr>
<tr>
<td><strong>Benefit</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Convenient remote administration</td>
<td>You have the ability to control user accounts and share or revoke access to your shared files at any time.</td>
</tr>
<tr>
<td>Built-in security</td>
<td>SafeSync has a built-in firewall that stops network traffic that is not required for sharing files.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Installing two SafeSync appliances ensures constant availability of online backup and file restoration, even in the event of equipment failure.</td>
</tr>
<tr>
<td>Redundant server and Internet connections</td>
<td>Two copies of data are stored on two separate servers plus two separate service providers connecting the data center ensuring availability of data.</td>
</tr>
</tbody>
</table>
Chapter 2

Getting Started

Trend Micro recommends performing all tasks in this section before using SafeSync.

Topics in this chapter include:

- Logging On to SafeSync on page 2-2
- Changing the Logon Password on page 2-2
- Configuring Proxy Server Settings on page 2-3
- Activating or Renewing SafeSync on page 2-5
- Configuring Active Directory Settings on page 2-8
- Setting Up SafeSync Users on page 2-10
- Configuring SafeSync Web Console Settings on page 2-11
- Configuring SMTP Server Settings on page 2-13
- Configuring Notification Settings on page 2-15
Logging On to SafeSync

After installation, log on to the SafeSync web console. Use the following log on credentials:

- User name: administrator
- Password: safesync

Changing the Logon Password

After installing SafeSync, change the logon password immediately.

Tip

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

Procedure

1. Go to Administration > My Account.

   The My Account screen appears.

   ![My Account Screen](image.png)
2. Type a password in the **New password** field.

3. Type the same password in the **Confirm password** field.

4. Click **Save**.

---

**Configuring Proxy Server Settings**

If the network where SafeSync installs uses a proxy server, administrators must configure proxy settings to register and activate SafeSync.

**Procedure**

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

![Proxy Server Screen](image)

**Figure 2-1. The Proxy Server tab**

2. Select **Use a proxy server for the connection**.

3. Type the IP address or host name 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. Type the user name and password in the fields.

8. Click **Save**.

   SafeSync tests the connection and saves the proxy server settings.

---

**Activating or Renewing SafeSync**

SafeSync needs to be activated after installation.

---

**Procedure**

1. Go to **Administration > License Information**.
The **License Information** screen appears.

![License Information Screen](image)

**Figure 2-2. The License Information screen**

2. Click **Specify New Activation Code**.
The **New Activation Code** screen appears.

![New Activation Code](image)

**FIGURE 2-3. The New Activation Code screen**

3. Type the Activation Code for SafeSync.
4. Click **OK**.

---

**Performing System Updates**

Keep SafeSync up-to-date for optimal system performance and functionality.

---

**Important**

Performing updates will shut down SafeSync and disconnect all end users. Choose a time that has the minimal impact on end users to perform the task.

---

**Procedure**

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

![System Updates Screen](image)

**Figure 2-4. The System Updates screen**

2. Click **Browse...** and select the update file.

3. Click **Update** and then click **Yes**.

SafeSync starts the update process and redirects to the Logon screen when the process completes.

---

### Configuring Active Directory Settings

Integrate SafeSync with the Active Directory structure to efficiently manage user and group permissions. Use the **Active Directory Integration** screen to configure the required settings.

**Procedure**

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

**FIGURE 2-5. The Active Directory Integration screen**

2. In the Settings tab, select Enable Active Directory integration.

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. To use an LDAP search filter, type the information in the field.

An LDAP-syntax search filter can restrict the data sent across the network. Administrators can use the search filter to synchronize a subset of users in the Active Directory.

For example, to synchronize all groups and the users under the `safesync-users` permission group, use the following syntax:

```latex
(| (objectClass=group)(&(objectClass=user)(memberOf=CN=safesync-users,OU=new_ou,DC=ldc,DC=domain,DC=com)))
```

8. To determine how often to synchronize content with the Active Directory server, select a time from the Update frequency list.

9. Click Save.

SafeSync performs a test connection and saves the Active Directory settings.

---

### Setting Up SafeSync Users

Grant selected domain accounts permission to use the SafeSync service.

To manually create SafeSync accounts, see *Adding a Manual Account on page 3-7* for details.

---

**Note**

Set up Active Directory integration before performing this task. See *Configuring Active Directory Settings on page 2-8* for details.

---

**Procedure**

1. Go to Users.

2. From the left-hand users directory, click 📚.
The **Add Accounts** screen appears.

![Add Accounts Screen](image)

**FIGURE 2-6. The Add Accounts screen**

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

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

4. Click **OK**.

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

### Configuring SafeSync Web Console Settings

Use the **Web Consoles** tab to configure the network connection information to access the end-user web console and the SafeSync administrator’s management console.

**Procedure**

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

![System Settings Screen](image)

**Figure 2-7. The System Settings screen**

2. In 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.

   - The DNS server requires three DNS records to function. To activate the service for SafeSync users, add three DNS records to the DNS server and map them to the IP address of the user console.

3. Click **Save**.
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.

![SMTP Server Screen](image)

**Figure 2-8. The SMTP Server tab**

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

3. Type the IP address or host name 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 in the fields.

8. Click **Save**.

   SafeSync performs a test connection and saves the SMTP server settings.

---

**Configuring Notification Settings**

SafeSync can periodically notify administrators when issues occur in the system.

**Procedure**

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

![System Notifications Screen](image)

**FIGURE 2-9. The System Notifications screen**

2. Select one of the following:
   - **Administrator**
   - **Other recipients**
     
     Type email addresses in the field.

3. Under **Delivery Frequency**, specify how often to receive notifications.
Note
SafeSync sends notifications only when issues have occurred in the system. If the system is in good condition, administrators will not receive notifications.

4. Click Save.
Chapter 3

Plans, Policies, and Users

Before configuring plans and policies or adding new accounts, administrators have to configure the Active Directory and end user web console connection settings.

Topics in this chapter include:

• Configuring Plans on page 3-2
• Configuring Policies on page 3-3
• Managing Users on page 3-5
Configuring Plans

Most organizations have many departments, business units, or projects that each have users with different storage requirements. Plans allow for granularity to set different storage privileges for different SafeSync users. Plans control the maximum allowed storage, upload or download speeds, and number of version backups.

Adding a Plan

Procedure

1. Go to Plans.
2. Click Add.
3. Specify the name and description for the new plan.
4. Specify the storage in GB.
5. Specify the maximum upload and download speeds.
6. Select the number of version backups to keep.

Tip

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

7. Click Save.

SafeSync adds the new plan to the top of the list. Reorder the plans if necessary.

Editing a Plan

Procedure

1. Go to Plans.
2. Click any plan name in the Name column.
3. Specify any changes to the plan and then click Save.

Deleting a Plan

After deleting a plan, all users or groups currently assigned to this plan will be reassigned based on the order of the list.

Procedure
1. Go to Plans.
2. Select the check box next to all plans to delete.
3. Click Delete.
4. Review all users and groups affected by the change and then click Yes.

Reviewing Groups and Users Assigned to a Plan

For details about changing plan assignments, see Managing Users on page 3-5.

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

Configuring Policies

Use policies to control how end users upload and share files. Administrators can restrict the following:
• File size
• File type
• Shareable link usage
• Team folder usage

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.
6. Select Use shareable links to allow end users to share files using shareable links.
   To enforce additional security, select **Force users to sign in to access shareable links**.
7. Select Use team folders to allow end users to create and access team folders.
8. Click Save.
   SafeSync adds the new policy to the top of the list. Reorder the policies if necessary.
Editing Policies

**Procedure**

1. Go to Policies.
2. Click any policy name in the Name column.
3. Specify any changes to the policy.
4. Click Save.

Deleting Policies

After deleting a policy, all users or groups currently assigned to this policy will be reassigned based on the order of the list.

**Procedure**

1. Go to Policies.
2. Select the policies to delete.
3. Click Delete.
4. Review all users and groups affected by the change and then click Yes.

Managing Users

Administrators can integrate the Active Directory structure with SafeSync to define and manage SafeSync users. Accounts that are only used for SafeSync can also be added manually.

Domain Accounts

SafeSync inherits all user account information from the Active Directory Domain Controller. Any domain user account or AD group cannot be modified from within
SafeSync. For details about setting up Active Directory integration, see Configuring Active Directory Settings on page 2-8.

Changing Domain Account Plans and Policies

Procedure

1. Go to Users.
2. From the left-hand users directory, select a domain account or group.
   The selected account or group information appears in the center pane.
3. Select the accounts or groups to apply the changes and click Change Plan or Change Policy.
   The Change Plan or Change Policy screen appears.
4. Do one of the following for the plan or policy:
   • Select Assign by plan order or Assign by policy order.
     SafeSync goes through the list from the top until the account information matches a plan or policy.
   • Select a specific plan or policy from the list.
5. Click OK.

Removing Domain Accounts from SafeSync

Use one of the following methods to remove domain accounts from the Users screen:

Procedure

• From the left-hand users directory, click .
The **Add Accounts** screen appears.

![Add Accounts Screen](image)

**FIGURE 3-1. The Add Accounts screen**

- From the center pane, select the domain accounts to remove and click **Remove**.

  The confirmation screen appears. Confirm the action and click **Yes**.

---

**Manual Accounts**

For many reasons, an end-user may not be part of or have access to an organization’s Active Directory domain. Administrators can add these end-users to SafeSync manually.

**Adding a Manual Account**

**Procedure**

1. Go to **Users**.

2. Use one of the following ways to add a manual account:
From the left-hand users directory, click the plus sign next to Manual Accounts.

From the left-hand users directory, click Manual Accounts and click Add.

The Add User screen appears.

3. Specify the new account details and select a plan.

4. Click Add.

A new account is added to the list of users.

---

**Editing a Manual Account**

**Procedure**

1. Go to Users.

2. From the left-hand users directory, click any user name.

   The individual user view loads in the center pane.

3. From the top of the center pane, click edit.

   The Edit User screen appears.

4. Make any changes and then click Save.

---

**Deleting a Manual Account**

Deleting an account removes all personal data stored in SafeSync. Any content that was created in team folders will not be deleted.

**Procedure**

1. Go to Users.

2. From the left-hand users directory, click the arrow next to any user name and select Manual Accounts.
3. From the table in the center pane, select the check box next to all accounts to delete.

4. Click Delete.

Enabling/Disabling a Manual Account

Procedure

1. Go to Users.

2. Use one of the following ways to enable or disable a manual account:
   - From the left-hand users directory, click the arrow next to any user name and select **Enable** or **Disable**.
   - From the left-hand users directory, click any user name and then click **edit** at the top of the center pane. From the **Edit User** screen that appears, change the **Status** and click **Save**.
   - From the left-hand users directory, click **Manual Accounts**. From the table in the center pane, select the check box next to all accounts to enable or disable and click **Enable** or **Disable**.

Changing Manual Account Plans and Policies

Procedure

1. Go to **Users**.

2. From the left-hand users directory, select a manual account.

   The selected account information appears in the center pane.

3. Click **edit**.

   The **Edit User** screen appears.
4. Do one of the following for the plan or policy:
   • Select Assign by plan order or Assign by policy order.
     SafeSync goes through the list from the top until the account information
     matches a plan or policy.
   • Select a specific plan or policy from the list.
5. Click Save.

---

**Editing Multiple Accounts Simultaneously**

**Procedure**

1. Go to Users.
2. From the left-hand users directory, click Manual Accounts.
3. Select the check box next to the account and select one of the following options:

   **Table 3-1. Account Editing Options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a new manual account.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete all selected accounts. Their personal data folders will be purged, but any team folder data will remain.</td>
</tr>
<tr>
<td>Change Policy</td>
<td>Change the policy for all users.</td>
</tr>
<tr>
<td>Change Plan</td>
<td>Change the plan for all users.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enable the account. The user can log on to SafeSync and access data normally.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disable the account. The user is blocked from logging onto SafeSync. Their data will remain saved.</td>
</tr>
</tbody>
</table>
4. Depending on the selected option, follow the instructions on the screen that appears.

**Searching for a User Account**

**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.

If there is a match, the results display in the center pane.

**Viewing Individual User Details**

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

**Procedure**

1. Use one of the following ways to navigate to the individual user view:
   - From the left-hand users directory, click any account or expand the AD group and click any domain account.
   - From the left-hand users directory, click either Active Directory or Manual Accounts, and then navigate to the desired user account in the center pane.

The individual user details appear.

2. Review the account details in the center pane. To make changes, to a manual account click **edit**, or to a domain account click **change**.
Inviting Users to Share Files

After adding user accounts and assigning plans, the user must be notified about how to access SafeSync.

Procedure

1. Follow the steps in *Viewing Individual User Details on page 3-11*.

2. At the top of the center pane, click send invitation.

   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.

Managing Disabled 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 decide whether to enable or remove the accounts from SafeSync.

Procedure

1. Go to Users.

2. Click the number next to Disabled at the top right corner of the screen.
The **Disabled Accounts** screen appears.

3. Use the **Enable** and **Remove** buttons to manage the disabled accounts.
Chapter 4

Monitoring SafeSync

Monitor SafeSync and SafeSync users to assist in managing the sharing and storage of files.

Topics in this chapter include:

- *About the SafeSync Dashboard on page 4-2*
- *Configuring Reports on page 4-4*
- *Querying Logs on page 4-5*
About the SafeSync Dashboard

SafeSync for Enterprise provides widgets on the Dashboard that display specific information regarding usage trends over time and the system status statistics and alerts. Administrators can use these widgets as a quick visual reference to assist in the management of SafeSync resources and users.

Usage Trends Widget

The Usage Trends widget displays real-time usage statistics and trends over a specified period.

![Usage Trends widget displaying active user statistics](image)

**Figure 4-1. Usage Trends widget displaying active user statistics**

In this widget, administrators can:

- View usage trends by selecting a display type and time period
- View daily statistics by hovering over the graph line
- View monthly changes in trends
• Export the displayed data to a comma-separated values (CSV) file
• Refresh the widget’s data

System Status Widget

The System Status widget displays real-time usage statistics and averages over a specified period.

Figure 4-2. System Status widget displaying disk usage statistics

In this widget, administrators can:
• View CPU, memory, and disk usage statistics by selecting a display type and time period
• View hourly or daily statistics by hovering over the graph line
• View average usage statistics based on the selected time period
• Export the displayed data to a comma-separated values (CSV) file
• Refresh the widget’s data
System Status Alert Widget

The System Status Alert widget displays issues that have occurred on the system.

In this widget, administrators can:

• View issues on system version, storage, and database
• Compare system status on the primary and secondary servers

Configuring Reports

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

<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 console</td>
</tr>
<tr>
<td>Connected devices</td>
<td>The number of devices that connected to the SafeSync console</td>
</tr>
<tr>
<td>Total files</td>
<td>The total number of files stored on the SafeSync server</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>

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**.

---

**Querying Logs**

Administrators can query the following types of events:

- 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

**Procedure**

1. Go to **Logs > Log Query**.
The Log Query screen appears.

![Log Query Screen](image)

**Figure 4-3. The Log Query screen**

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 Search.

Deleting Logs

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

Procedure

1. Go to Logs > Log Settings.

   The Log Maintenance tab appears.

   ![Log Settings](image)

   **Figure 4-4. The Log Maintenance tab**

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

3. Click Save.
Configuring Syslog Server Settings

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

\[\text{FIGURE 4-5. The Syslog Server tab}\]
6. Click **Save**.
Chapter 5

Deploying SafeSync to End-Users

Before deploying SafeSync to end-users, administrators must complete the tasks outlined in the previous sections.

Topics in this chapter include:

- Deploying SafeSync to Desktops and Laptops on page 5-2
- Deploying SafeSync to Mobile Devices on page 5-3
Deploying SafeSync to Desktops and Laptops

Administrators can push SafeSync to the desktops or laptops (Mac or PC) of their end-users using an MSI file.

---

**Note**

The MSI file includes the SafeSync 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.

---

**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:

   https://<SSFE Domain Name>/pages/en/smartdrive

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.
Chapter 6

Managing SafeSync Add-Ins

- SafeSync Add-Ins on page 6-2
- Activating SafeSync Add-Ins on page 6-3
- Configuring SafeSync Add-Ins on page 6-5
- Decrypting all Encrypted Files on page 6-6
SafeSync Add-Ins

Licensed SafeSync users can enable the following add-ins:

• **SafeSync 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 their 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.

![SafeSync Outlook Extension](image)

**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, they are prompted to identify who can access the folder. Users can also create auto-encrypted personal folders. Auto-encrypted personal folders can only be accessed by the user that 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`.

---

**Activating SafeSync Add-Ins**

**Procedure**

1. Go to Administration > License Information.
The **License Information** screen appears.

![License Information Screen](image)

**Figure 6-1. The License Information screen**

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

3. Type the Activation Code for the add-in.

4. Click **OK**.

SafeSync activates and enables the feature. To manage the add-in, go to **Administration > System Settings > Add-Ins**.
Note
Activate SafeSync add-ins on the License Information screen. See Activating SafeSync Add-Ins on page 6-3 for details.

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

   The Add-Ins tab appears.

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 encrypted files, configure the following in the File Encryption section:
   
   • Drag the slider from Low to High to indicate how frequently users have to authenticate themselves in order to open and use encrypted files; or
   
   • Use the Force authentication fields to indicate the number of minutes, hours, days, or months that will pass before users have to authenticate themselves in order to open and use encrypted files.
Administrators can also choose to turn off authentication. If authentication is turned off, users are not required to authenticate themselves in order to open or use encrypted files.

4. Click Save.

### 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.

**Procedure**

1. Go to **Administration > System Settings > Add-Ins**.
   
   The **Add-Ins** tab appears.

2. Click the **Decrypt all encrypted SafeSync files** link.
The **Decrypt Files** screen appears.

3. Click **Yes** to begin the decryption process.

   It can take a long time for all files to decrypt. Trend Micro recommends starting the decryption process after work hours. If necessary, cancel the decryption process and restart it at a more convenient time.
Administering SafeSync

This section includes tasks that administrators may have to perform periodically.

Topics in this chapter include:

- Updating SSL Certificate Information on page 7-2
- Restarting SafeSync on page 7-4
- Configuring the Web Console Language on page 7-5
Updating SSL Certificate Information

The **SSL Certificate** tab shows the current SSL certificate information and allows administrators to update the information.

---

**Important**

Have the third party sign the certificate in the following format:

`*.ssfe.YourCompanyDomain.com`

---

**Procedure**

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

**FIGURE 7-1. The SSL Certificate tab**

2. Copy and paste the SSL certificate text in the field under **Step 1: Paste the certificate text**.

3. Under **Step 2: Choose the private key file**, click **Browse** and select the private key file.
4. Click **Update**.

---

**Restarting SafeSync**

Shutting down or restarting SafeSync prevents all end-users from using SafeSync.

**Procedure**

1. Go to **Administration > System Maintenance**.

   The **System Maintenance** screen appears.

   ![System Maintenance Screen]

   **Figure 7-2. The System Maintenance screen**

2. Select one of the following:
   - **Restart service**
   - **Restart server**
   - **Shut down**
- Shut down
3. Click OK.

Configuring the Web Console Language

Procedure
1. Go to Administration > System Settings > Language.

   The Language screen appears.

   ![Language tab](image)

   **Figure 7-3. The Language tab**

2. Select the preferred language from the list.
3. Click Save.
Chapter 8

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at http://esupport.trendmicro.com
- Get the latest Trend Micro product documentation at http://docs.trendmicro.com

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

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

A
about SafeSync, 1-2
accounts
disabled, 3-12
activating
add-ins, 6-4
activating SafeSync, 2-5
Activation Code, 2-5
Active Directory integration, 2-8
   enabling, 2-9
   LDAP search filter, 2-10
   root DN, 2-9
   selecting users, 2-10
   update frequency, 2-10
adding
   policies, 3-4
   users, 2-10
add-ins, 6-2
   activating, 6-4
   configuring, 6-5
   Outlook Extension, 6-2
   Shared Protection Extension, 6-3
administration
   Active Directory integration, 2-8

C
configuring
   Active Directory settings, 2-8
   add-ins, 6-5
   notification settings, 2-15
   policies, 3-3
   proxy server settings, 2-3
   SMTP server settings, 2-13
   SSL certificate settings, 7-2
   syslog server, 4-8
   web console settings, 2-11

D
dashboard
   about, 4-2
   System Status Alert widget, 4-4
   System Status widget, 4-3
   Usage Trends widget, 4-2
   widgets, 4-2–4-4
decrypting files, 6-6
deleting
   logs, 4-7
   policies, 3-5
disabled users, 3-12
DNS records, 2-12
documentation, vii
domain accounts, 2-10
   Active Directory integration, 3-5
   changing plans, 3-6
   disabled, 3-12

E
editing
   policies, 3-5
email address
   notification recipients, 2-15
   SMTP server, 2-13
enabling
   Active Directory integration, 2-9

I
integrating Active Directory structure, 2-8

L
LDAP search filter, 2-10
license, 2-5
logs
  deletion, 4-7
  querying, 4-5
  syslog server, 4-8
M
  maintenance
    logs, 4-7
manual accounts
  adding, 3-7
  changing plans, 3-9
  deleting, 3-8
  disabled, 3-12
  editing, 3-8
  enabling/disabling, 3-9
N
  notifications
    recipients, 2-15
    settings, 2-15
O
  Outlook Extension, 6-2
    activating, 6-4
    configuring, 6-5
P
  plans, 3-2
    adding, 3-2
    changing assignment, 3-6, 3-9, 3-10
    deleting, 3-3
    editing, 3-2
    reviewing user and group assignment, 3-3
  policies, 3-3
    adding, 3-4
    deleting, 3-5
  editing, 3-5
Q
  querying logs, 4-5
R
  recipients
    notifications, 2-15
  renewing SafeSync, 2-5
  reports, 4-4
  root DN, 2-9
S
  SafeSync
    about, 1-2
    activation, 2-5
    add-ins, 6-2
    documentation, vii
    renewal, 2-5
    terminology, ix
  users, 2-10
  setting up SafeSync users, 2-10
  Shared Protection Extension, 6-3
    activating, 6-4
    configuring, 6-5
    decrypting files, 6-6
  SMTP server settings, 2-13
  SSL certificate, 7-2
  syslog server, 4-8
  system settings
    notifications, 2-15
    proxy server, 2-3
    SMTP server, 2-13
    SSL certificate, 7-2
    syslog server, 4-8
    updates, 2-7
Index

updating
  performing system updates, 2-7
  system, 2-7
  web console, 2-11
System Status Alert widget, 4-4
System Status widget, 4-3

T
terminology, ix

U
update frequency, 2-10
updating SSL certificate, 7-2
Usage Trends widget, 4-2
users, 3-5
  Active Directory integration, 3-5
  adding, 3-7
  changing multiple accounts simultaneously, 3-10
  changing plans, 3-9
  deleting, 3-8
  disabled, 3-12
  domain accounts, 2-10, 3-5
  editing, 3-8
  enabling/disabling, 3-9
  individual user details, 3-11
  manual accounts, 3-7

W
web console settings, 2-11
  DNS records, 2-12
widgets
  System Status, 4-3
  System Status Alert, 4-4
  Usage Trends, 4-2