TREND MICRO™

2.1 SafeSync for Enterprise

Service Pack 1

Administrator's Guide

Securely Share, Distribute, and Control Enterprise Information Within Your Private Cloud

Protected Cloud

Document Part No.: APEM26486/140711

Release Date: October 2014

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://docs.trendmicro.com/en-us/survey.aspx

Table of Contents

Preface

Preface v

SafeSync Documentation vi

Audience vii

Document Conventions vii

Terminology viii

Chapter 1: Introducing SafeSync

About SafeSync 1-2

What's New 1-2

- What's New in This Version 1-2
- What's New in Version 2.1 1-4

Features and Benefits 1-5

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 2-17

Inviting Users to Share Files 2-17

Configuring Policies 2-18

- The Default Policy 2-19
- Adding Policies 2-20
- Editing Policies 2-21

Deleting Policies 2-21
Reviewing Policy Assignments 2-22

Configuring Plans 2-22
The Default Plan 2-22
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 3-17
Forwarding Logs to a Syslog Server 3-18

Chapter 4: Administering SafeSync

Account Settings 4-2
Changing the Administrator Account Settings 4-2

Active Directory Integration 4-3
Configuring Active Directory Integration 4-3

Antivirus Settings 4-5
Configuring Antivirus Settings 4-6
Configuring Smart Protection Server Settings 4-12
Performing a Manual Scan 4-13
Updating Components 4-14

System Settings 4-21
Configuring SafeSync Web Console Settings 4-22

Configuring Proxy Server Settings 4-24
Configuring SMTP Server Settings 4-25
Updating SSL Certificate Information 4-27
Understanding SafeSync Add-Ins 4-28
Configuring the Web Console Language 4-33
System Notifications 4-34
Configuring System Notification Settings 4-34
System Maintenance 4-36
System Updates 4-38
Downloading Update Files 4-38
Performing System Updates 4-38
Rolling Back System Updates 4-39
License Information 4-40
Viewing Product License Information 4-40
Activating or Renewing SafeSync 4-42
Activating SafeSync Add-Ins 4-44

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 5-3
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
How can I add network devices? 5-5
SSL Certificates 5-12
Does SafeSync support PKCS7 certificates? 5-12
Does SafeSync support wildcard certificates? 5-13

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
About Trend Micro Smart Protection A-4

Appendix B: Understanding Components

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

Appendix C: Deploying SafeSync to End Users

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

Appendix D: Glossary

Index

Index IN-1

Preface

Preface

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

Topics include:

- *SafeSync Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*
- *Terminology on page viii*

SafeSync Documentation

SafeSync documentation includes the following.

TABLE 1. SafeSync Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing SafeSync.
Administrator's Guide	A PDF document that provides "how to's", advice, usage and field-specific information.
Quick Start Guide	The Quick Start Guide provides user-friendly instructions on connecting SafeSync to your network and on performing the initial configuration.
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the SafeSync web console.
Readme file	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.
Knowledge Base	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: http://esupport.trendmicro.com

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

http://docs.trendmicro.com/en-us/enterprise/safesync-for-enterprise.aspx

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

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations

Convention	Description
 **WARNING!**	Critical actions and configuration options

Terminology

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

Table 3. SafeSync Terminology

Terminology	Description
Administrator (or SafeSync administrator)	The person managing the SafeSync server
Console	The user interface for configuring and managing SafeSync The console for the SafeSync server program is called "web console".
End user	Users that share content using SafeSync
Portal	The end-user web console for managing SafeSync files

Chapter 1

Introducing SafeSync

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

Topics include:

- *About SafeSync on page 1-2*
- *What's New on page 1-2*
- *Features and Benefits on page 1-5*

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 2.1 SP1.

TABLE 1-1. New Features and Enhancements for SafeSync for Enterprise 2.1 SP1

FEATURE	DESCRIPTION
Antivirus scan	Perform Antivirus scan when users upload or share files. 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.
	Prevent malicious files from spreading. Files detected as malicious are quarantined to prevent users from accidentally opening the files. The detected files are not synchronized, downloaded, or shared.
	Analyze threat detection trends at a glance. 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.
	Specify Active Update and Smart Protection Server sources. Administrators can specify the Active Update and Smart Protection Server sources based on the network environment.
Multiple downloads	End users can download multiple files and folders as an archived file from the end-user portal.

Feature	Description
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 1-2. New Features and Enhancements for SafeSync for Enterprise 2.1

Feature	Description
Active Directory integration	• Enhanced Active Directory integration • Select and assign Active Directory users and groups permission to use the SafeSync service from the SafeSync web console
Shared Protection Extension add-in	• File encryption • Secure file sharing • Encrypt files under a folder automatically
Outlook Extension add-in	Enhanced with the Shared Protection Extension features
Dashboard widget	System Status Alert widget
Policy management	Control how end users share and upload files
Plan management	Assign plans to domain users based on plan priority or specify plans

Feature	Description
Logs	• Log query • Log maintenance • Syslog server settings
Administration	• System updates • License management for SafeSync add-ins
End user mobile apps	User interface enhancements

Features and Benefits

SafeSync provides the following:

Benefit	Description
Access files from anywhere	Anytime, anywhere file accessing, editing, and organizing from any device: PCs, Macs, and Android and iOS mobile devices.
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.

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.
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.
Convenient remote administration	You have the ability to control user accounts and share or revoke access to your shared files at any time.

Benefit	Description
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.

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 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 2-17*
- *Inviting Users to Share Files on page 2-17*
- *Configuring Policies on page 2-18*
- *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.

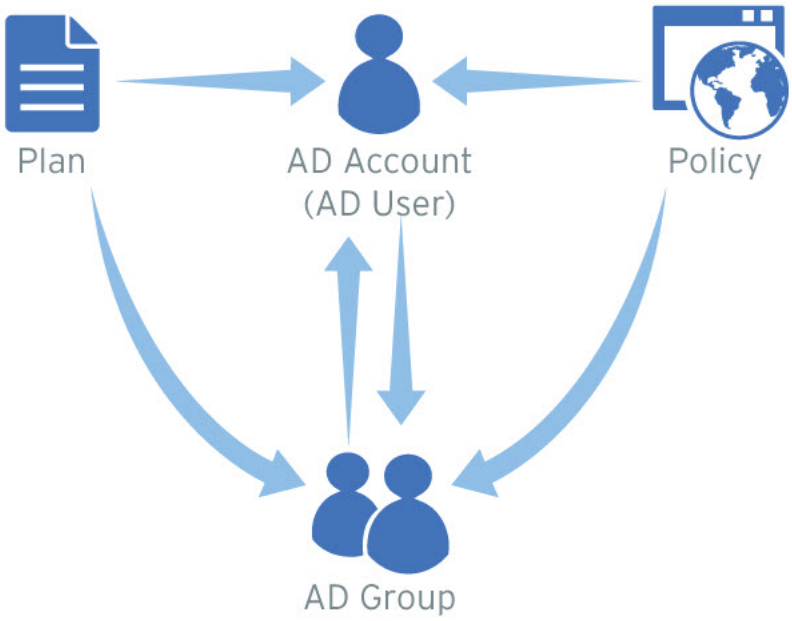


FIGURE 2-1. Active Directory (AD) user policy and plan assignments

When assigning policies and plans by priority, consider the example below.

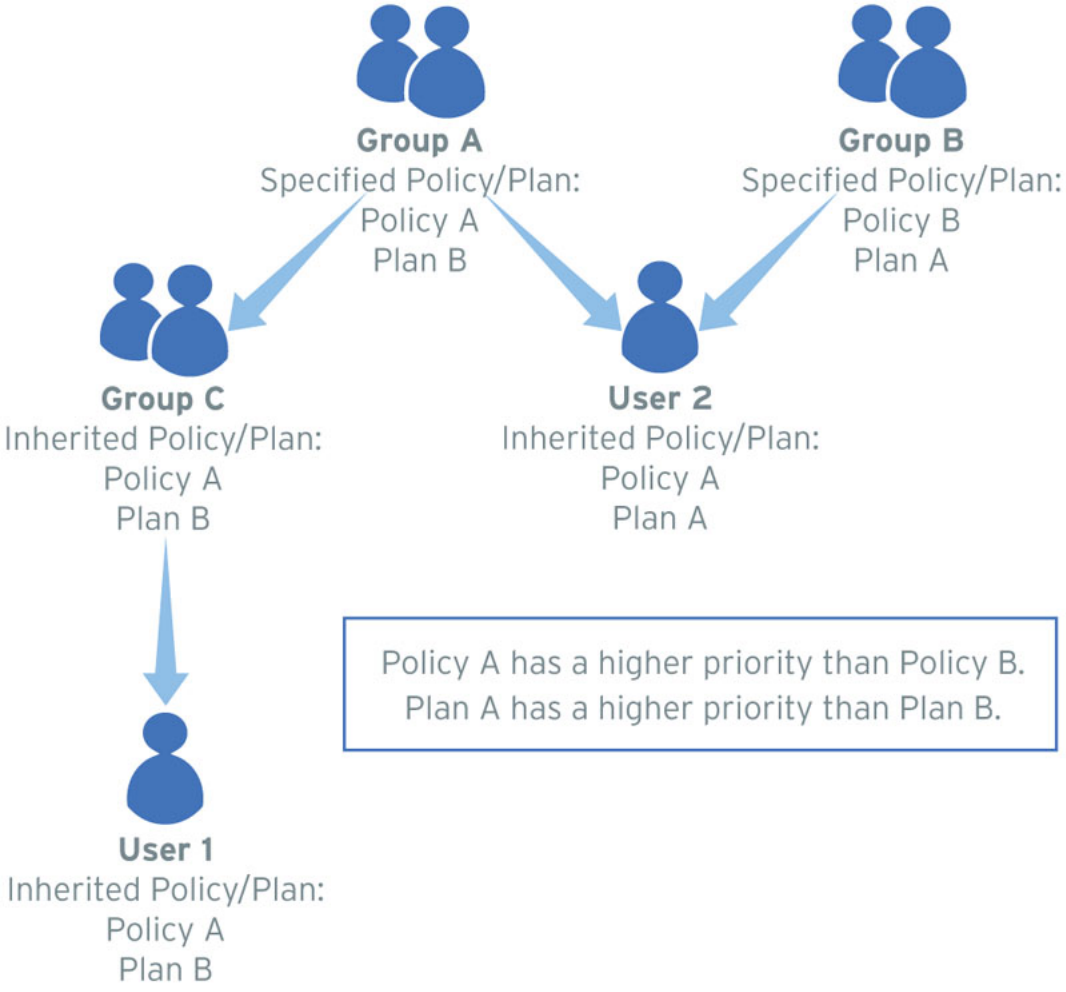


FIGURE 2-2. Active Directory (AD) user policy and plan priority

TABLE 2-1. User Policy and Plan Priority

GROUP/USER	POLICY	PLAN	POLICY/PLAN ASSIGNMENT
Group A	A	B	Assigned by administrator
Group B	B	A	Assigned by administrator
Group C	A	B	Inherited from Group A
User 1	A	B	Inherited from Group C
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.

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

FEATURE	DESCRIPTION
Policy	"Permission Control" that allows you to: • Define the maximum file size that a user can upload to the server • Define the types of files that SafeSync blocks • Grant users permissions to share files, create team folders, and download potentially malicious files • Allow users to download files detected as being malicious from the end-user portal
Plan	"Storage Control" that allows you to: • Assign the maximum amount of storage users receive • Limit the upload and download speeds for file transfers • Define the level of version control assigned to users

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 4-3* and *Configuring SafeSync Web Console Settings on page 4-22*.

SafeSync User Accounts

Define the following types of SafeSync user accounts:

- *Domain Accounts on page 2-7*
- *Manual Accounts on page 2-11*

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 2-11*.

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 4-3* and *Configuring SafeSync Web Console Settings on page 4-22*.

Procedure

1. Go to **Users**.
2. From the left-hand users directory, click  .

The **Add Accounts** screen appears.

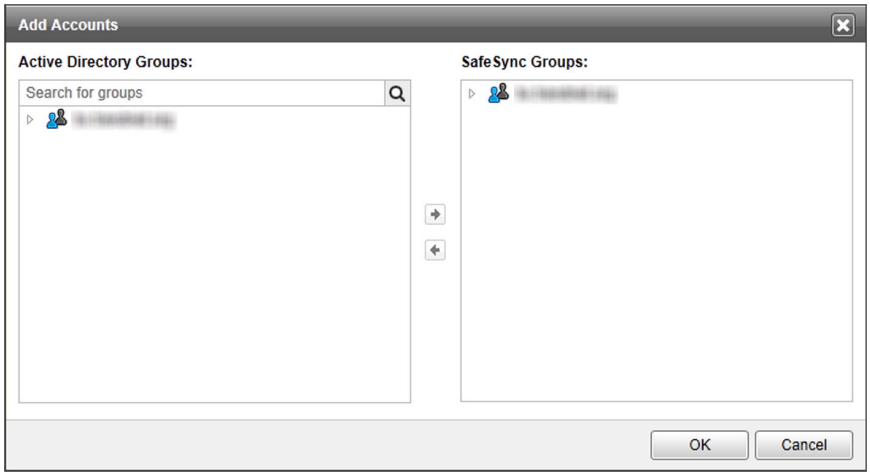


FIGURE 2-4. The Add Accounts screen

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.

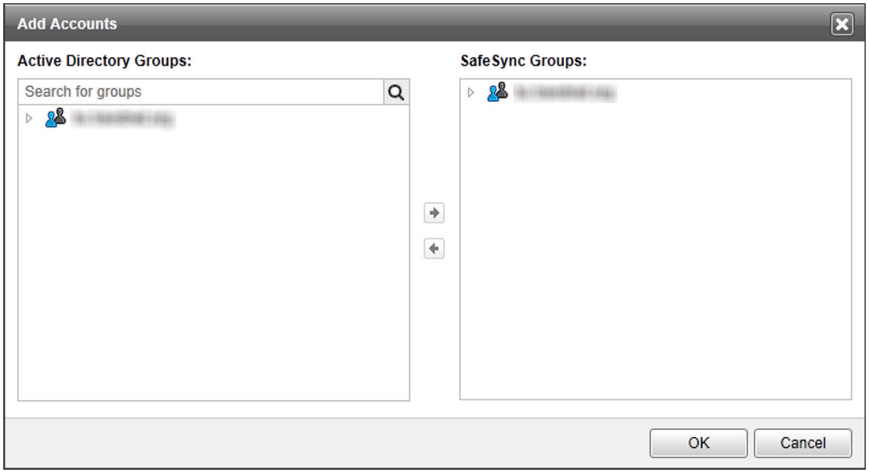


FIGURE 2-5. The Add Accounts screen

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 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 2-3. Manual Account Tasks

OPTION	DESCRIPTION
Add	Click to add a new manual account.

OPTION	DESCRIPTION
Delete	Select the check box next to a manual account and click **Delete** to remove the user account. **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.
Change Policy	Select the check box next to a manual account and click **Change Policy** to select the new policy that SafeSync applies.
Change Plan	Select the check box next to a manual account and click **Change Plan** to select the new plan that SafeSync applies.
Enable	Select the check box next to a manual account and click to enable the account. The user can log on to SafeSync and access data normally.
Disable	Select the check box next to a manual account and click to disable the account. The user is blocked from logging onto SafeSync. All data is retained.

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 2-17*.
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 prioirty 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

RESTRICTION	DESCRIPTION
Upload control	• Maximum upload size in MB • Blocked file types **Note** 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.

RESTRICTION	DESCRIPTION
Sharing control	• Usage of shareable links • Creation of team folders **Note** Disabling this option only prevents end users from creating new team folders. Users can still access all existing team folders.
Download control	• Download of malicious files

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:

- **Name**: Default Policy
- **Use shareable links**: Enabled
  - **Require users to sign in when accessing sharable links**: Disabled
- **Allow users to create team folders**: Enabled
- **Allow users to download files detected as being malicious**: Disabled

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 **Use 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.
7. Select **Require users to sign in when accessing shareable links** to enforce additional security on the people allowed to access SafeSync files.
8. 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.
9. Select **Allow users to download files detected as being malicious** to allow users to download files that 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.

10. 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. Click any policy name.
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 **Yes**.

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

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.

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 prioirty 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 TeamFolder User 1GB" 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.

The "Default TeamFolder User 1GB" plan also manages the size of team folders that users can create. To allow users to create larger team folders, modify the "Default TeamFolder User 1GB" plan using the web console. After modifying the size of the "Default TeamFolder User 1GB" plan, all previously created team folders adjust to the new settings. If the storage space used by a team folder exceeds the new settings, SafeSync does not allow users to upload new files. SafeSync does not delete any previously uploaded files to accommodate new files.

Note

You cannot delete the "Default TeamFolder User 1GB" 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 TeamFolder User 1GB
- **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 TeamFolder User 1GB" 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 **Yes**.

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 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

TAB	DESCRIPTION
Threat Detections	Displays real-time malware detection statistics and component status updates For more information, see *Threat Detections on page 3-3*.
Usage Overview	Displays usage statistics and trends over a specified period For more information, see *Usage Overview on page 3-9*.
System Status	Displays system usage statistics and receive system status alerts For more information, see *System Status on page 3-11*.

Working with Widgets

The following table lists widget-related tasks:

TABLE 3-2. Widget Tasks

TASK	STEPS
Refresh widget data	Click the refresh icon ().
Export widget data to CSV file	Click the export to CSV icon ().
Change time range	If available, click the drop-down list on the left-hand corner of the widget to change the time range.
Change displayed data	If available, click the drop-down list on the left-hand corner of the widget to change the displayed information.

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.

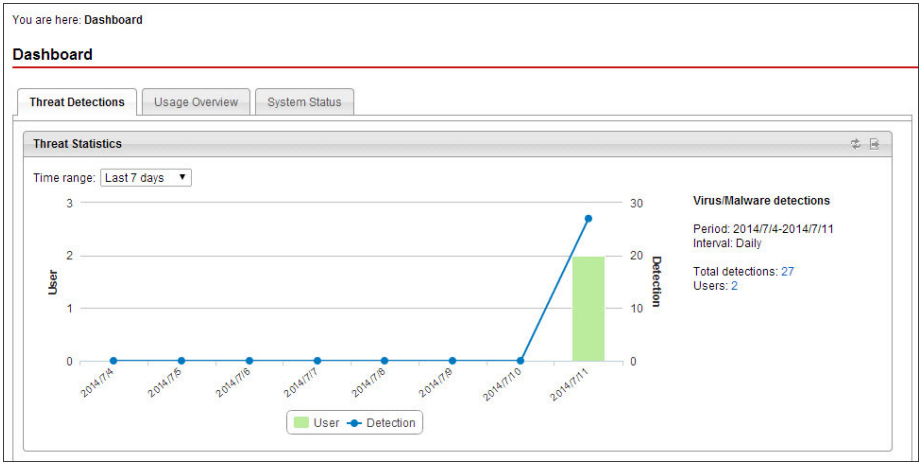


FIGURE 3-1. Threat Statistics Widget

The following table describes the information available on the widget.

TABLE 3-3. Threat Statistics Widget

ITEM	DESCRIPTION
Time range	Displays the specified time range Displays data from the **Last 7 days**, **Last 14 days**, **Last 30 days**, **Last 60 days**, or **Last 90 days**.
Period	Displays the dates of the specified time range
Interval	Displays the time interval used in the graph Displays either **Daily** or **Weekly**.
Total detections	Displays the total number of virus/malware detections during the specified time range Click the link to view the virus/malware detection log for all detections.

ITEM	DESCRIPTION
Users	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.
Daily/Weekly statistics	Displays the daily or weekly summary for each interval Hover over the graph line to view the daily or weekly totals.

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.

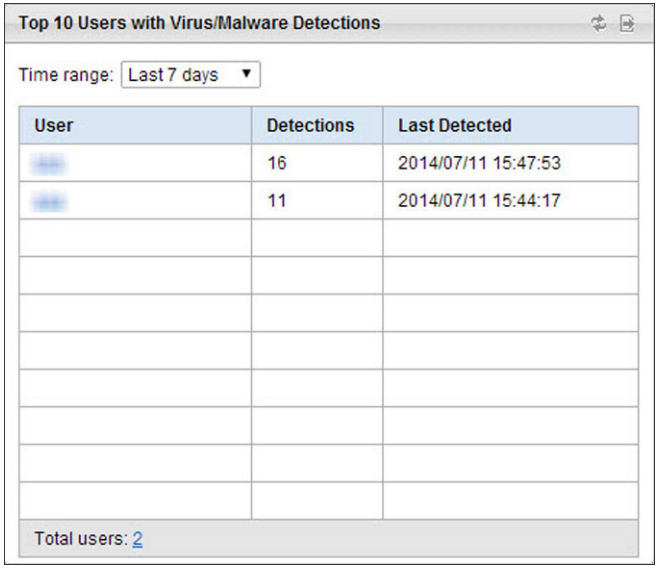


FIGURE 3-2. Top 10 Users with Virus/Malware Detections Widget

The following table describes the information available on the widget.

TABLE 3-4. Top 10 Users with Virus/Malware Detections Widget

ITEM	DESCRIPTION
Time range	Displays the specified time range Displays data from the **Last 7 days**, **Last 14 days**, **Last 30 days**, **Last 60 days**, or **Last 90 days**.
User	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.
Detections	Displays the total number of virus/malware detections for each user on the list during the specified time range.
Last Detected	Displays the timestamp of the last virus/malware detection
Total users	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.

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.

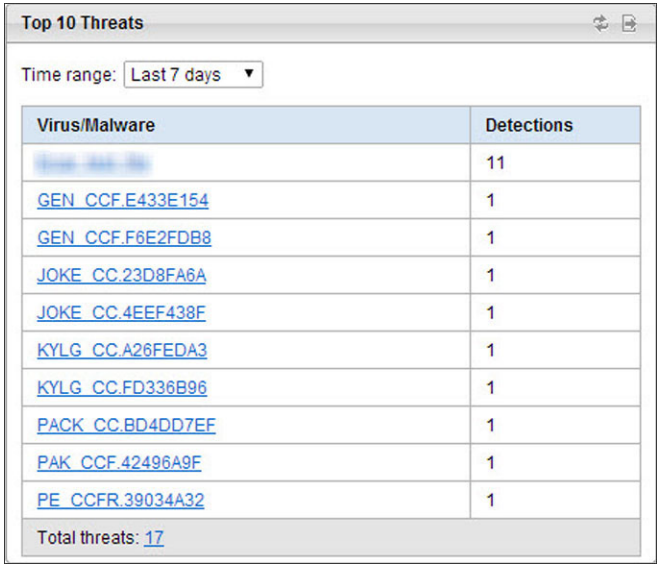


FIGURE 3-3. Top 10 Threats Widget

The following table describes the information available on the widget.

TABLE 3-5. Top 10 Threats Widget

ITEM	DESCRIPTION
Time range	Displays the specified time range Displays data from the **Last 7 days**, **Last 14 days**, **Last 30 days**, **Last 60 days**, or **Last 90 days**.

ITEM	DESCRIPTION
Virus/Malware	Displays the name of the malware detected Click the link to view the virus/malware detection log for each user detection.
Detections	Displays the total number of virus/malware detections for each user on the list during the specified time range.
Total threats	Displays the total number of unique unique malware threat types detected Click the link to view the virus/malware detection log for all detections.

Component Status Widget

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

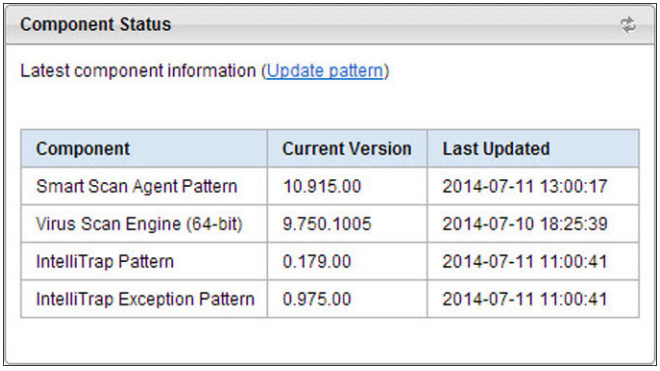


FIGURE 3-4. Component Status Widget

The following table describes the information available on the widget:

TABLE 3-6. Threat Statistics Widget

ITEM	DESCRIPTION
Component	Displays the component names
Current Version	Displays the version number of the current pattern or engine
Last Updated	Displays the timestamp of the last update

Note

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

For more information on updating components, see *Updating Components on page 4-14*.

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.

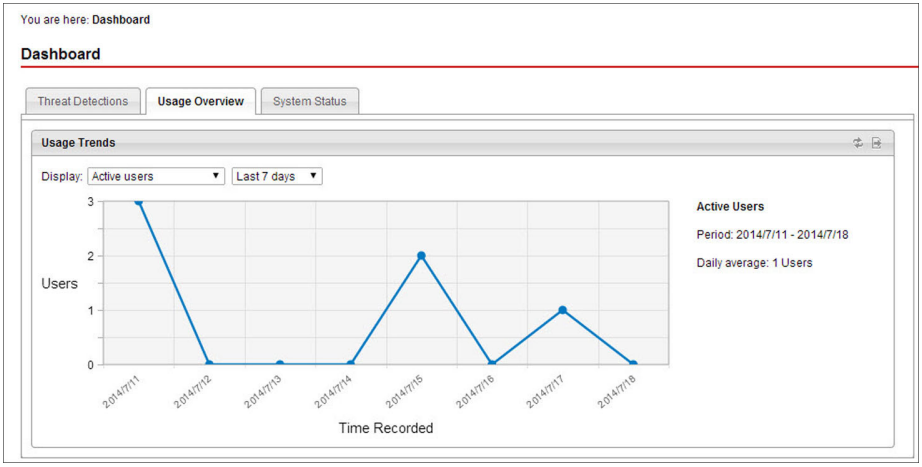


FIGURE 3-5. Usage Trends widget displaying active user statistics

The following table describes the information available on the widget.

TABLE 3-7. Usage Trends Widget

ITEM	DESCRIPTION
Display	Displays the usage trend information for the specified time range Displays the total number of “Active users”, “Connected devices”, “Total files”, “Shared files”, “System storage used”, and “Average storage used”. Displays data from the **Last 7 days**, **Last 14 days**, or **Last 30 days** . **Note** You can also generate reports about SafeSync usage statistics. For more information, see *Reports on page 3-14*.
Period	Displays the dates of the specified time range
Daily average	Displays the daily average for the requested information
Daily statistics	Displays the daily summary for each interval Hover over the graph line to view the daily totals.

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.

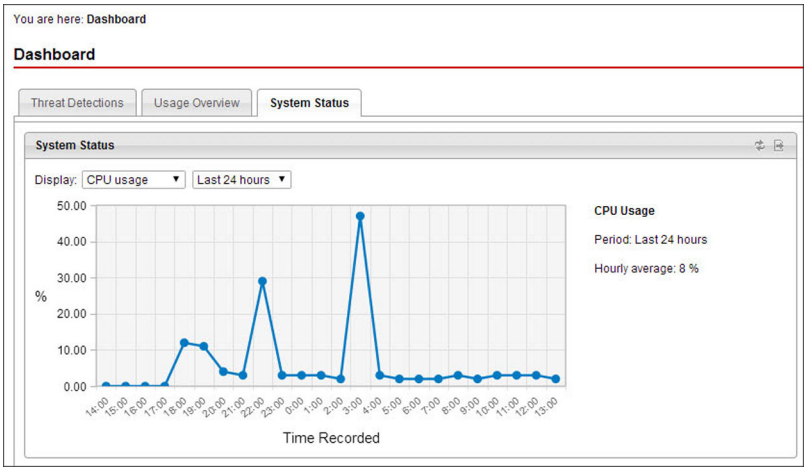


FIGURE 3-6. System Status widget displaying disk usage statistics

The following table describes the information available on the widget.

TABLE 3-8. System Status Widget

ITEM	DESCRIPTION
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
Hourly/Daily average	Displays the hourly or daily average for the requested information The displayed average depends on the selected time range.
Hourly/Daily statistics	Displays the hourly or daily summary for each interval Hover over the graph line to view the hourly or daily totals.

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.

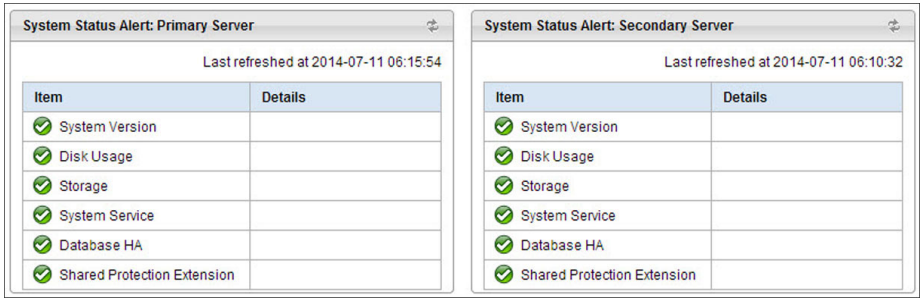


FIGURE 3-7. System Status Alert widget displaying primary and secondary server status

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

- : Normal
- : Warning

The following table describes the information available on the widget:

TABLE 3-9. System Status Alert Widget

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

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

TYPE	DESCRIPTION
Active users	The number of users that logged on to the SafeSync end-user portal
Connected devices	The number of devices that connected to the SafeSync end-user portal
Total files	The total number of files stored on SafeSync
Shared files	The total number of files being shared by users
System storage used	The amount of storage used by files
Average storage used	The average amount of storage used per user

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.

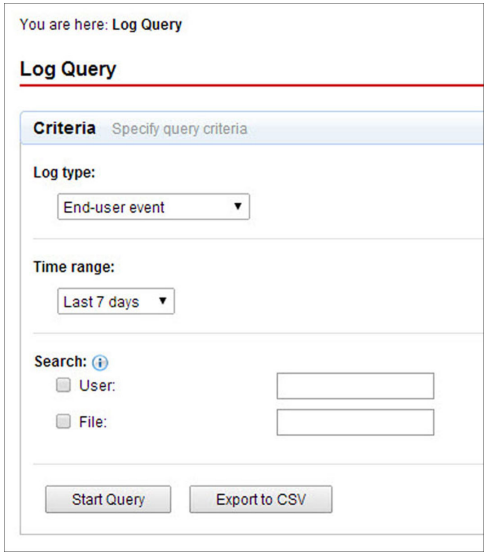


FIGURE 3-8. The Log Query screen

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 **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.

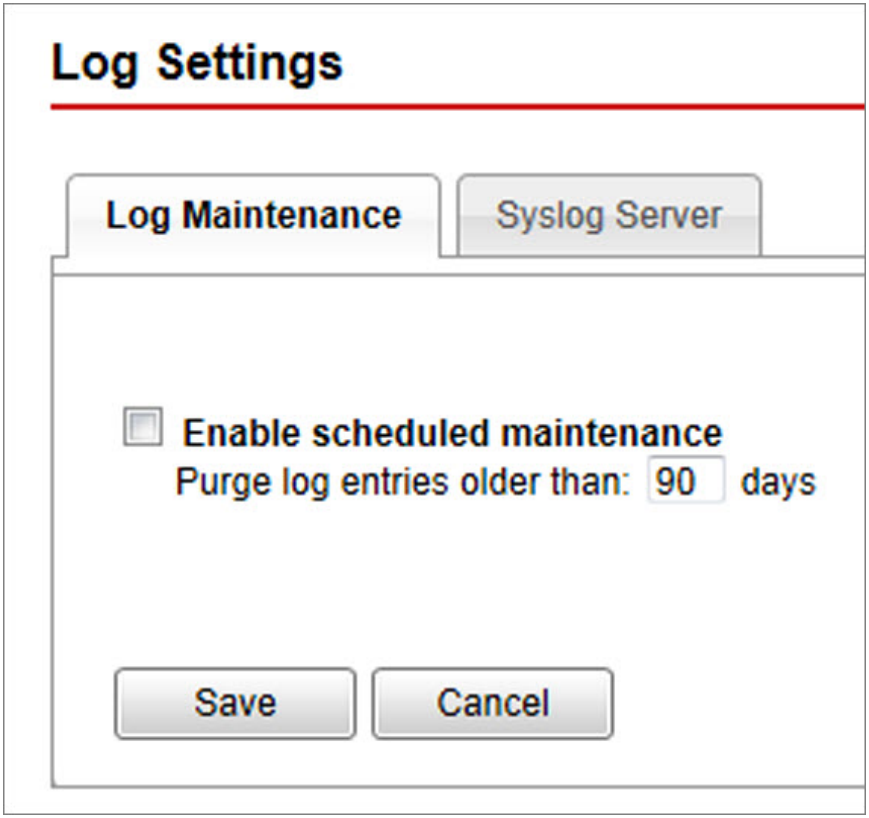


FIGURE 3-9. The Log Maintenance tab

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.

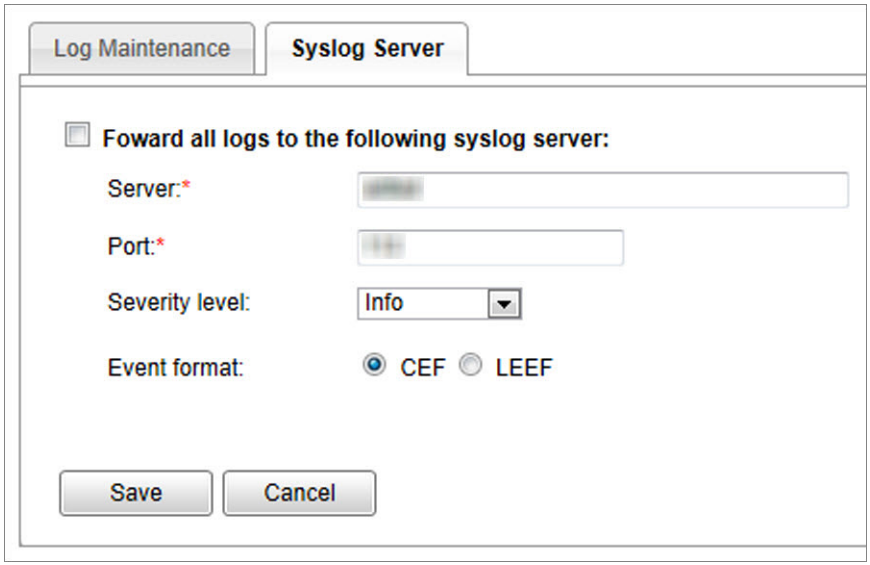


FIGURE 3-10. The Syslog Server tab

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**.

Chapter 4

Administering SafeSync

This chapter explains how to perform SafeSync administrative tasks.

Topics include:

- *Account Settings on page 4-2*
- *Active Directory Integration on page 4-3*
- *Antivirus Settings on page 4-5*
- *System Settings on page 4-21*
- *System Notifications on page 4-34*
- *System Maintenance on page 4-36*
- *System Updates on page 4-38*
- *License Information on page 4-40*

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.

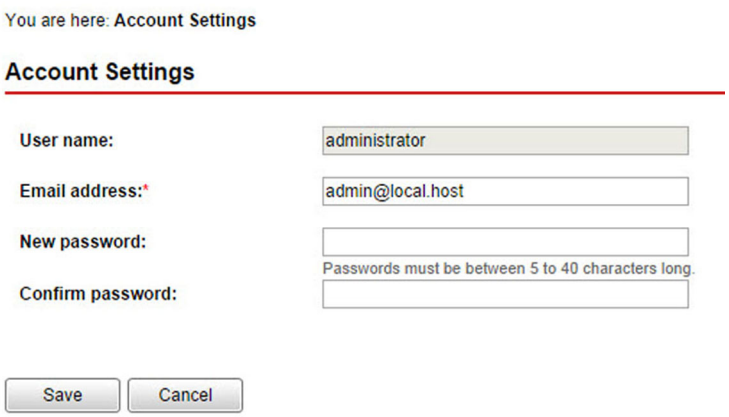


FIGURE 4-1. The Account Settings screen

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**.

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.

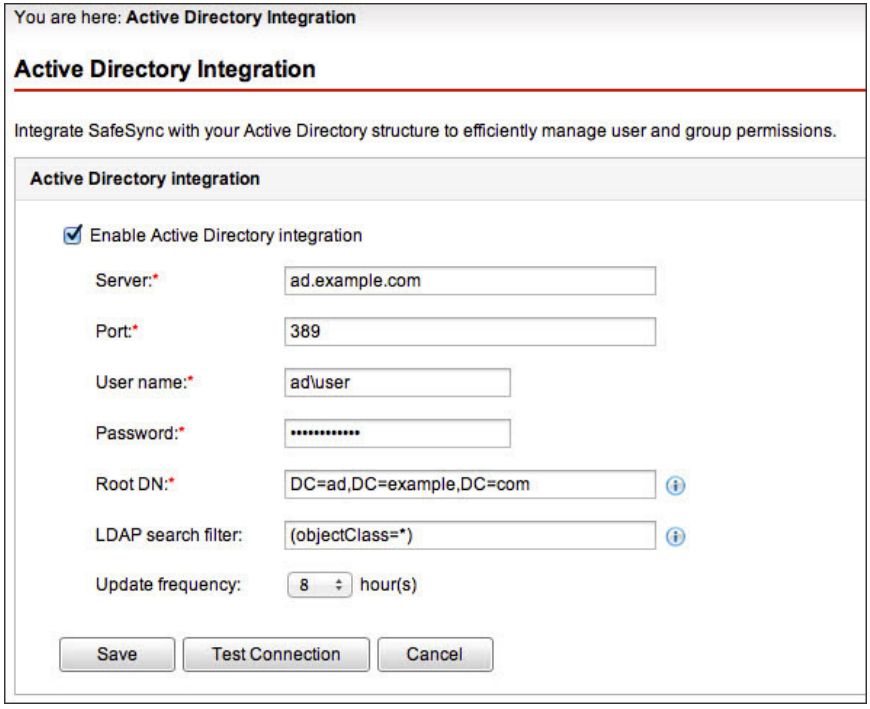


FIGURE 4-2. The Active Directory Integration screen

2. 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 appropriate syntax in the field.

Note

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:

```
(|(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.

Antivirus Settings

Use the **Antivirus Settings** screen to perform the following tasks.

TABLE 4-1. Antivirus Settings Tabs

TAB	TASKS
Settings	Configure the antivirus scan settings and provide exclusion lists. For more information, see *Configuring Antivirus Settings on page 4-6*.
Smart Protection Server	Integrate with a local Smart Protection Server or connect to the Smart Protection Network. For more information, see *Configuring Smart Protection Server Settings on page 4-12*

TAB	TASKS
Manual Scan	Perform a manual scan. For more information, see *Performing a Manual Scan on page 4-13*
Update	Update antivirus components, schedule automatic updates, select an update source, and roll back components to their previous versions. For more information, see *Updating Components on page 4-14*

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.

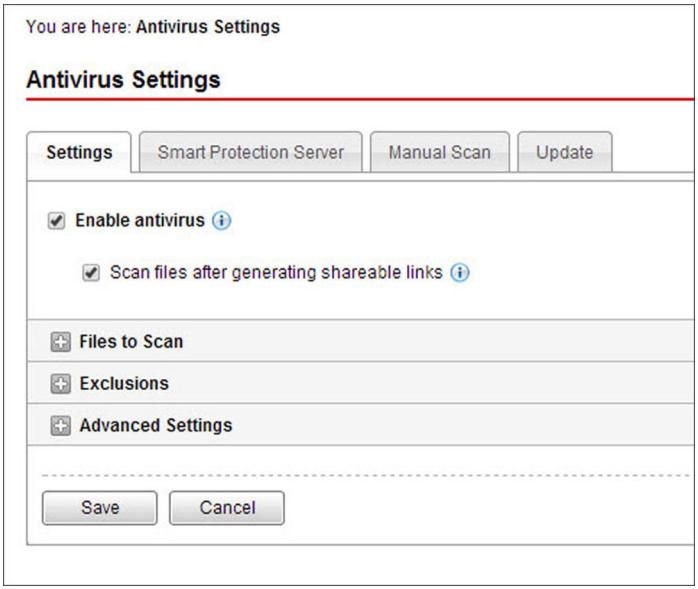


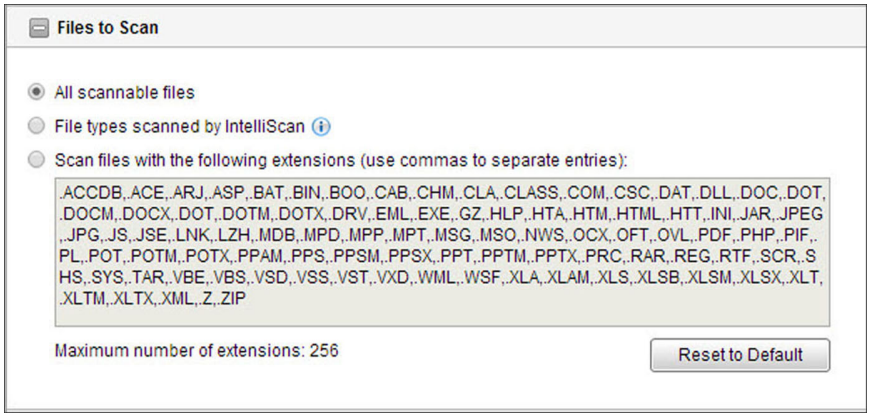
FIGURE 4-3. The Antivirus Settings screen

2. Select **Enable antivirus protection**.

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

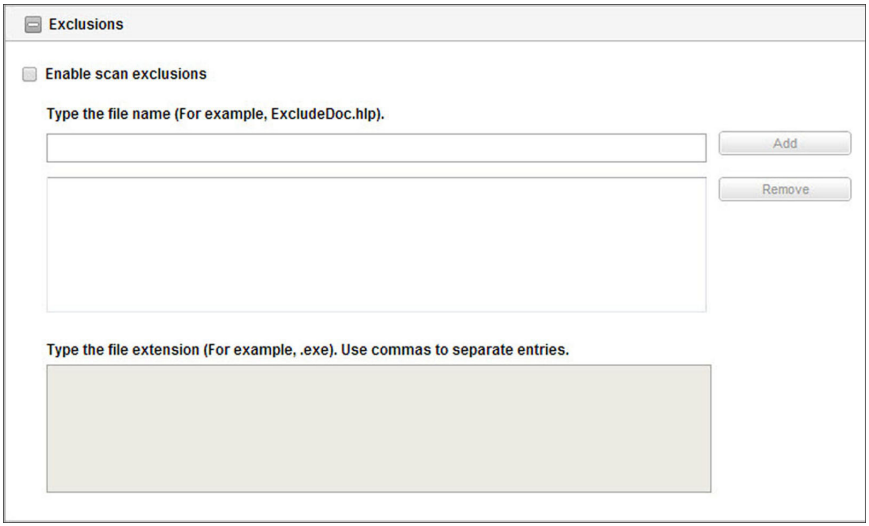
  This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

- **File types identified 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 D-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.



- 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.

6. Specify advanced settings.

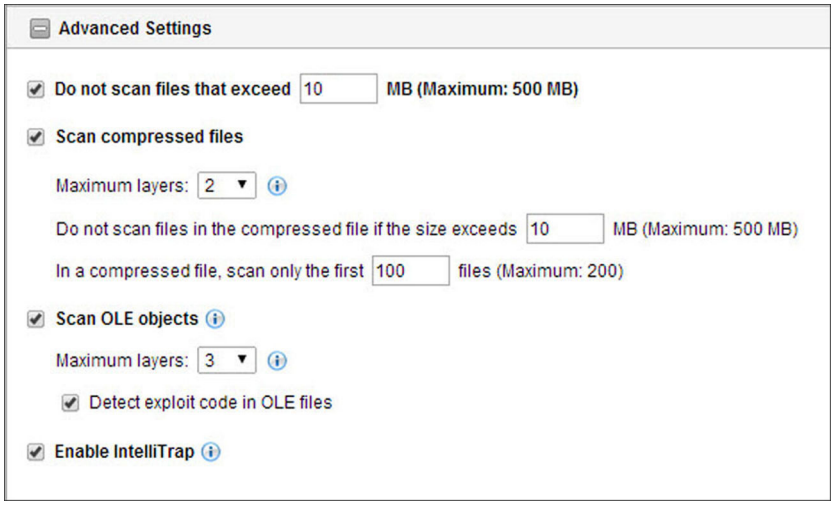


TABLE 4-2. Advanced Scan Settings

OPTION	DESCRIPTION
Do not scan files that exceed ___ MB	SafeSync does not scan files that exceed the value specified.

Option	Description
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.
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.

OPTION	DESCRIPTION
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.

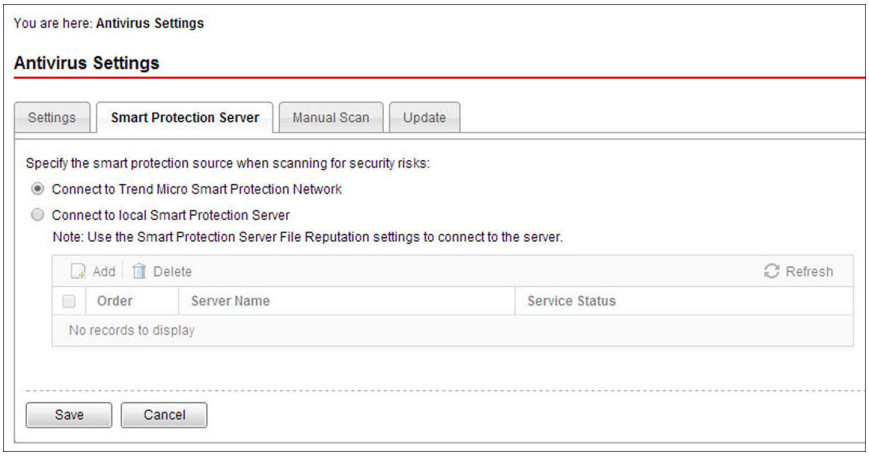


FIGURE 4-4. Smart Protection Server screen

2. Select one of the following:

   - **Connect to the 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 *About Trend Micro Smart Protection 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.

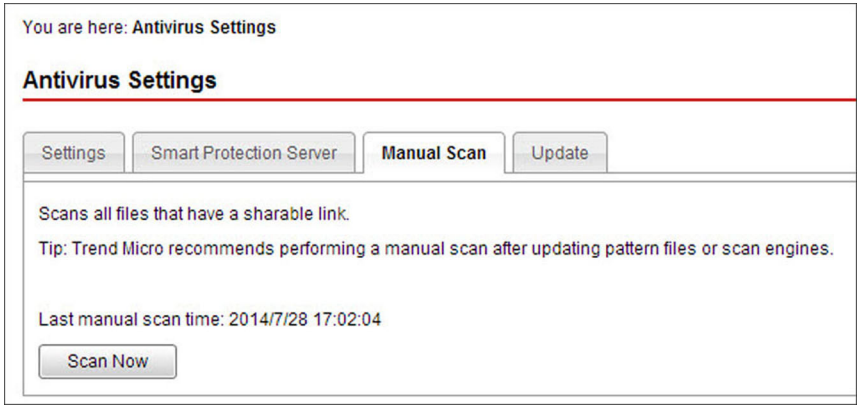


FIGURE 4-5. Manual Scan screen

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.

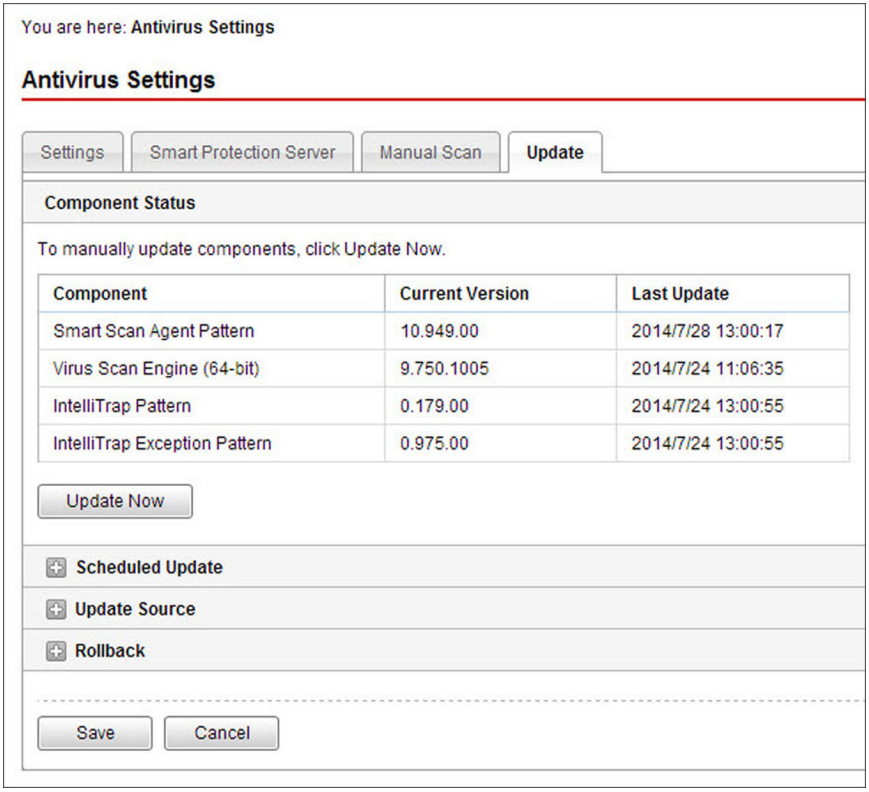


FIGURE 4-6. Update screen

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.

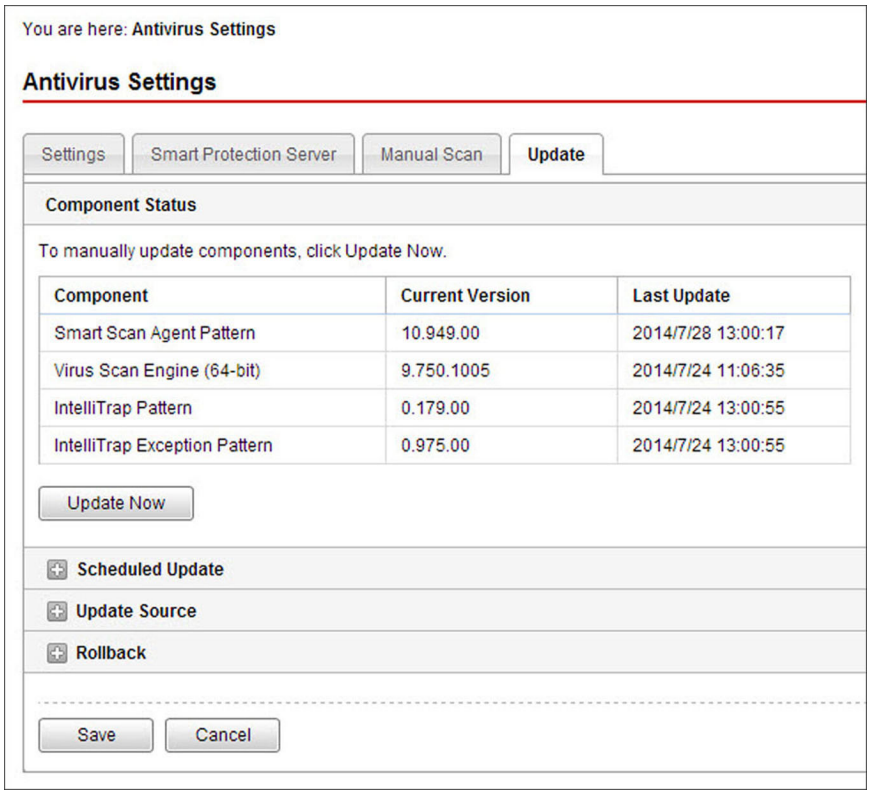


FIGURE 4-7. Update screen

2. Expand the **Scheduled Update** section.

The **Scheduled Update** section appears.

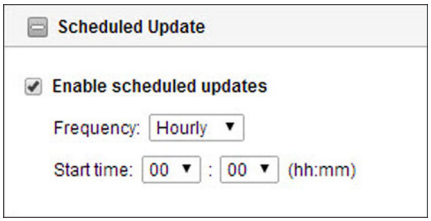


FIGURE 4-8. Scheduled Update section

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.

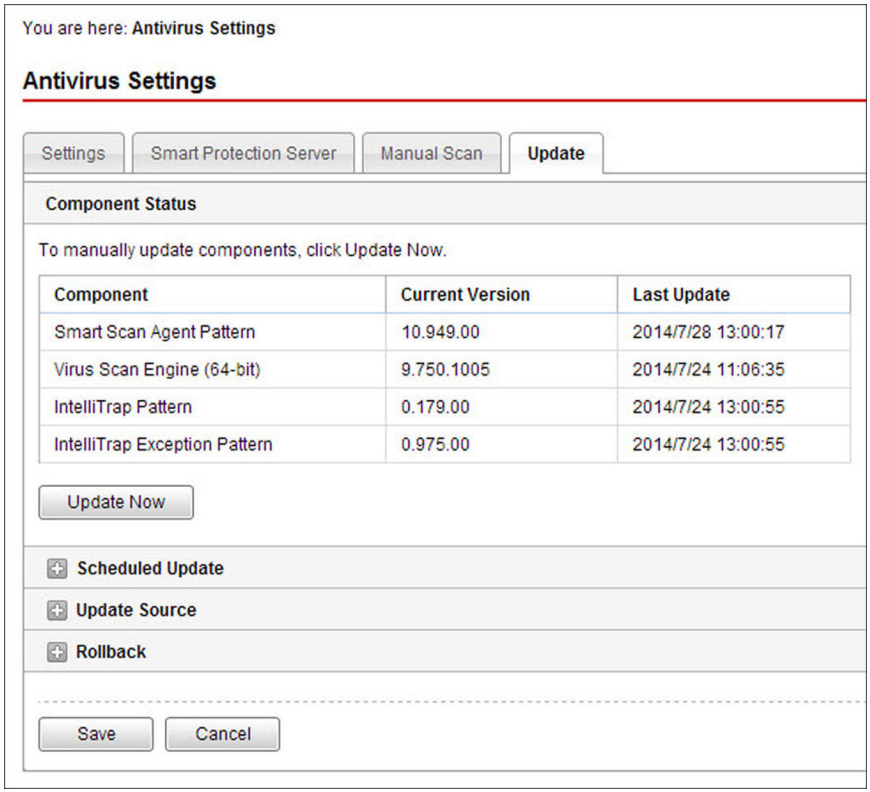


FIGURE 4-9. Update screen

2. Expand the **Update Source** section.

The **Update Source** section appears.

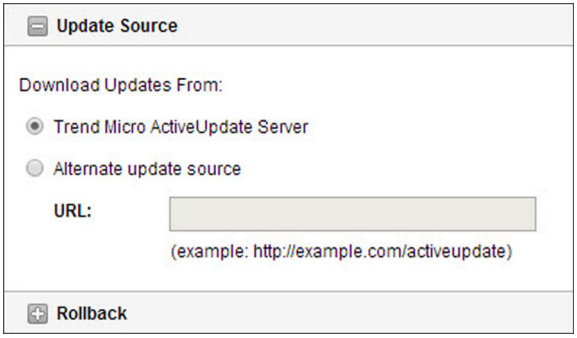


FIGURE 4-10. Update Source section

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.

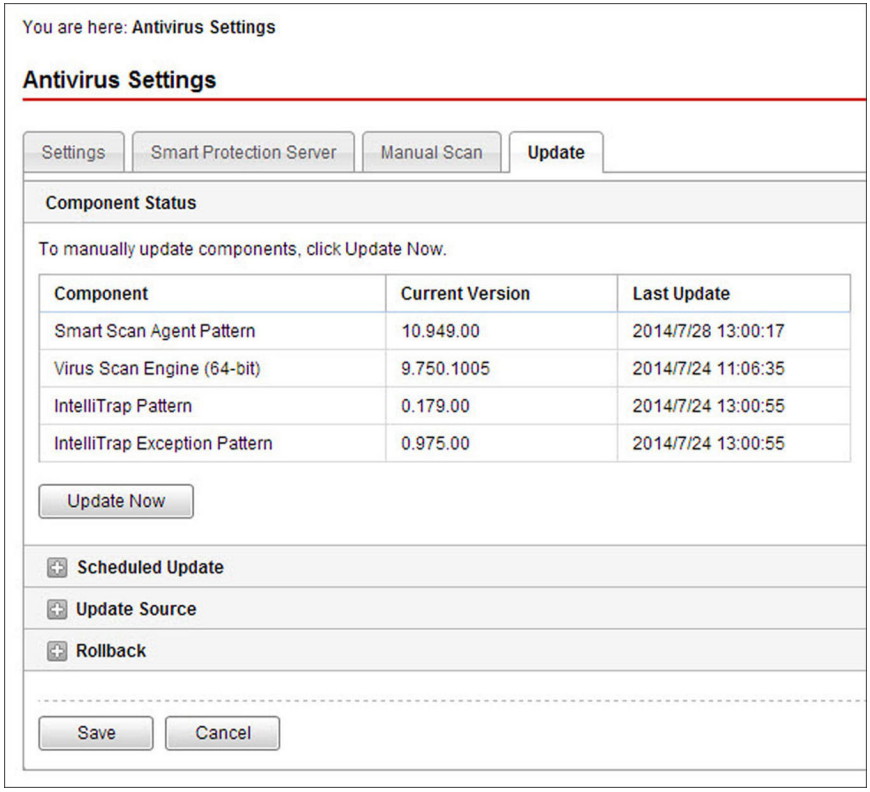


FIGURE 4-11. Update screen

2. Expand the **Rollback** section.

The **Rollback** section appears.

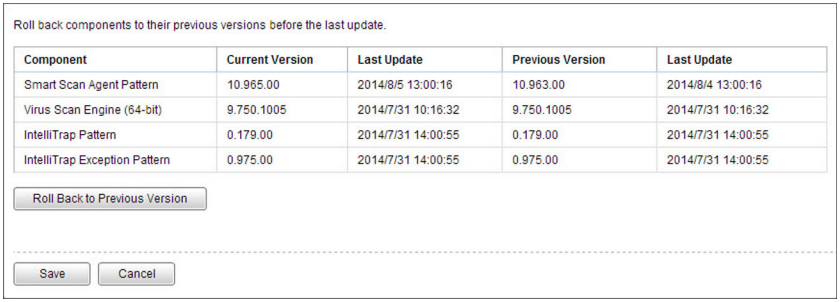


FIGURE 4-12. Rollback section

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 4-3. System Settings Tabs

TAB	TASKS
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 4-22*.

TAB	TASKS
Proxy Server	Configure the proxy server settings. For more information, see *Configuring Proxy Server Settings on page 4-24*
SMTP Server	Specify the SMTP server settings. For more information, see *Configuring SMTP Server Settings on page 4-25*
SSL Certificate	Paste the SSL certificate text and upload the private key file. For more information, see *Updating SSL Certificate Information on page 4-27*
Add-Ins	Enable the add-ins and decrypt encrypted files. For more information, see *Understanding SafeSync Add-Ins on page 4-28*
Language	Specify the administrator web console language. For more information, see *Configuring the Web Console Language on page 4-33*

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.

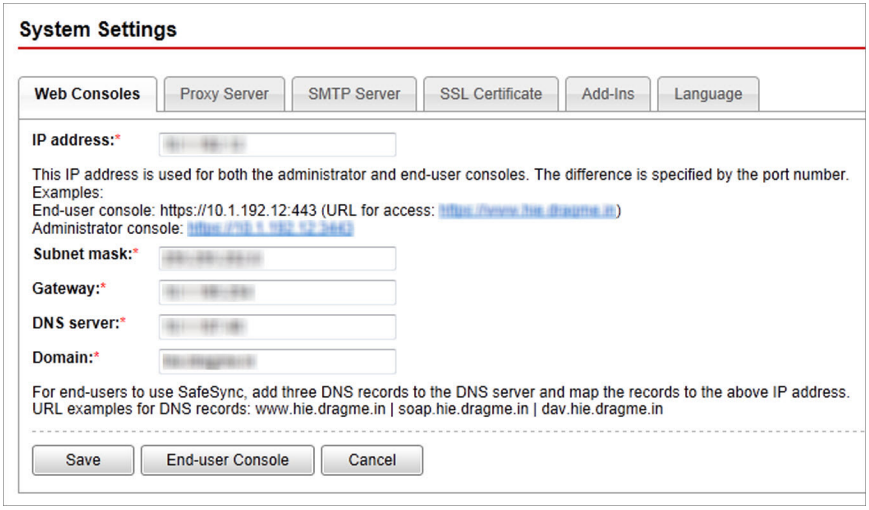


FIGURE 4-13. The System Settings screen

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.
- 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.

  For more information, see 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.

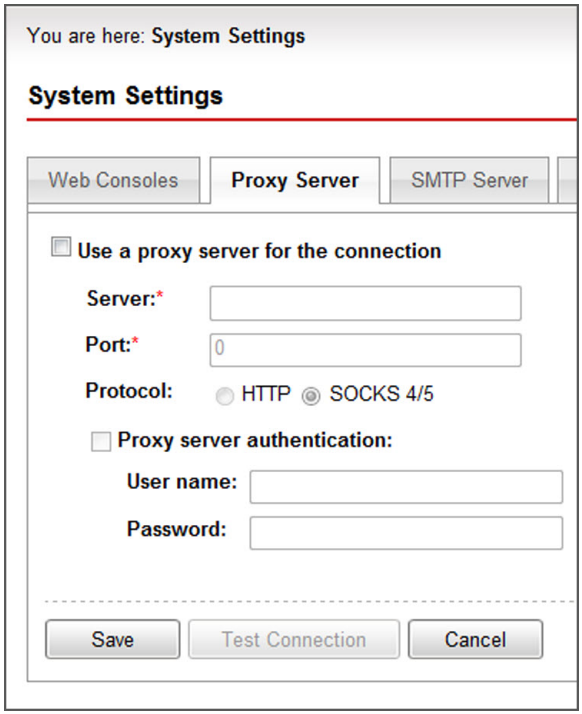


FIGURE 4-14. The Proxy Server tab

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.

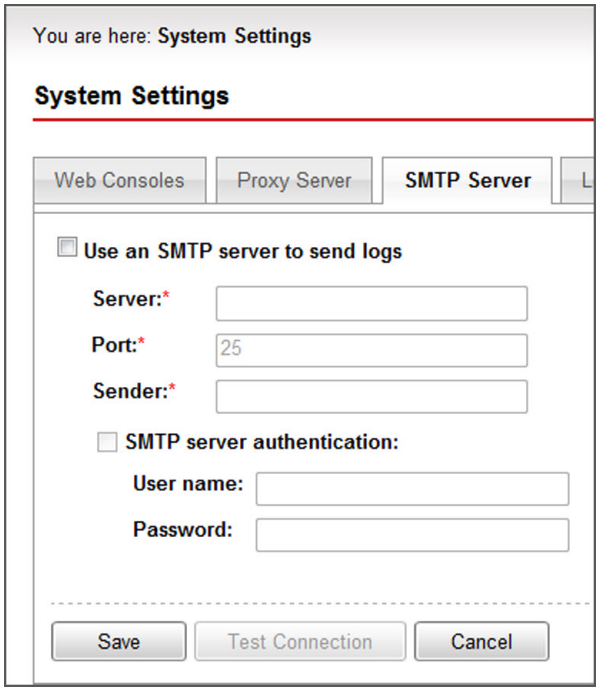


FIGURE 4-15. The SMTP Server tab

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:

  Server Certificate > Intermediate Certificate > Root Certificate
- The certificate chain must be copied into 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:
  `*.<subdomain>.<your_domain>.com`

Procedure

1. Go to **Administration** > **System Settings** > **SSL Certificate**.

The **SSL Certificate** screen appears.

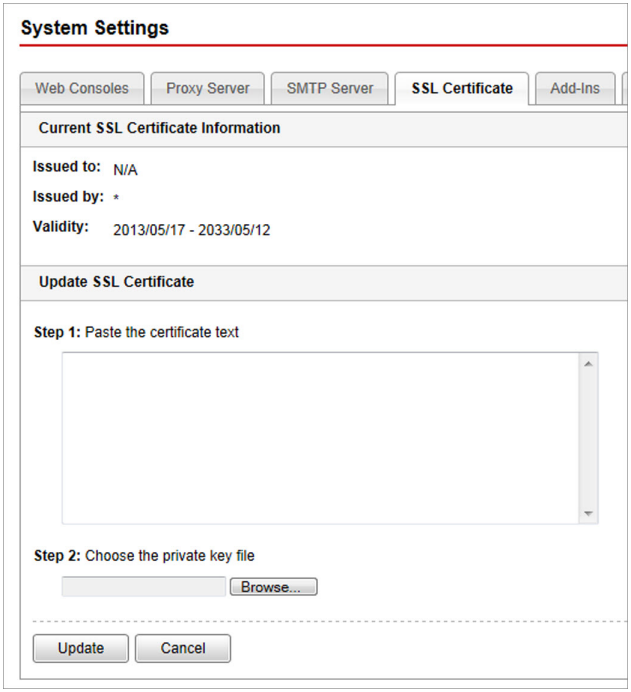


FIGURE 4-16. The SSL Certificate tab

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**.

Understanding SafeSync Add-Ins

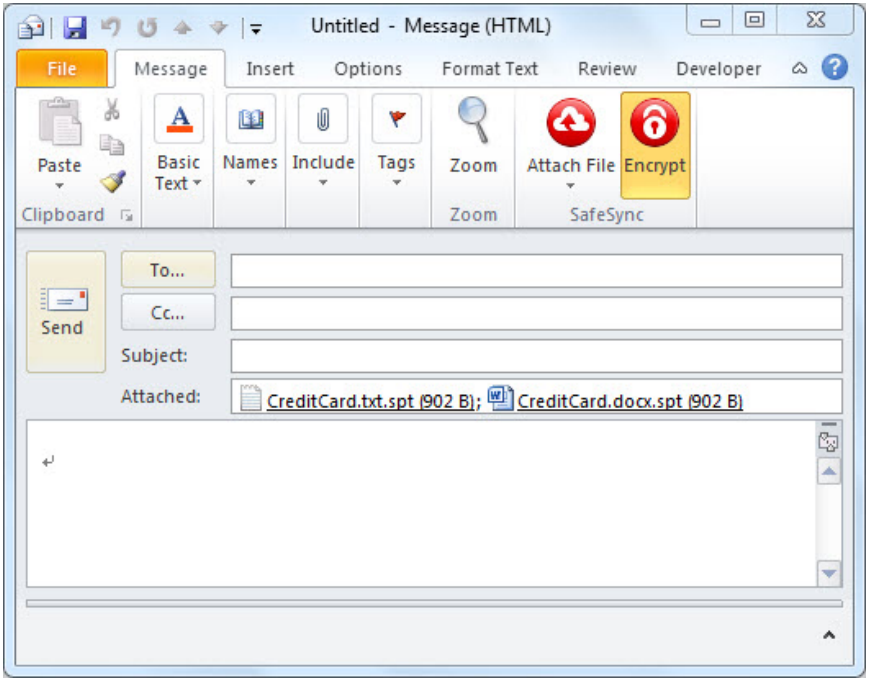
Licensed SafeSync users can enable the following add-ins:

- **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

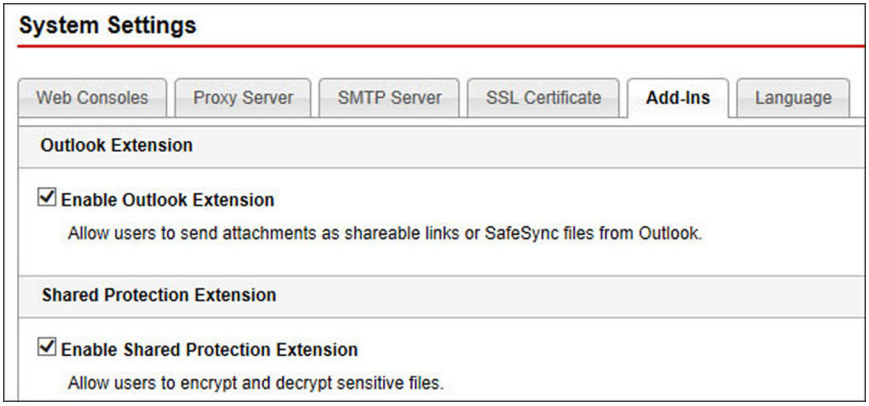
Activate SafeSync add-ins on the **License Information** screen.

For more information, see *Activating SafeSync Add-Ins on page 4-44*.

Procedure

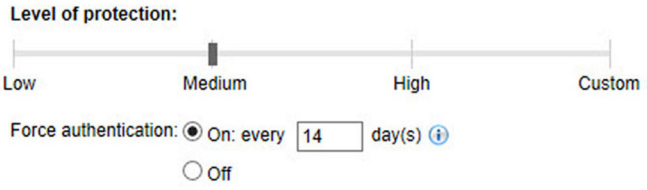
1. Go to **Administration** > **System Settings** > **Add-Ins**.

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.



Note

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.

The **Decrypt Files** screen appears.

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

Configuring 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.

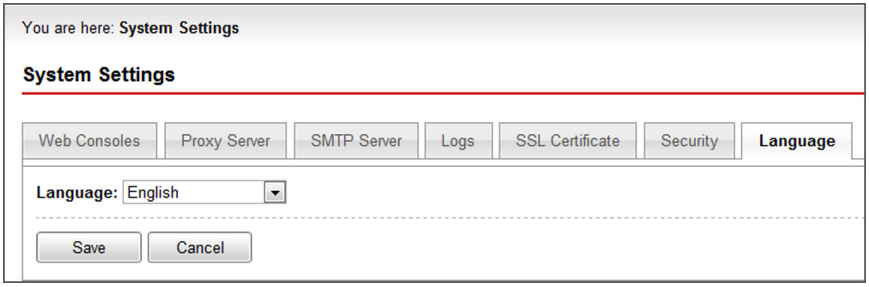


FIGURE 4-17. The Language tab

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.

System Notifications

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

SafeSync sends the following notifications.

TABLE 4-4. System Notifications

ITEM	DESCRIPTION
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 4-42*.
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.

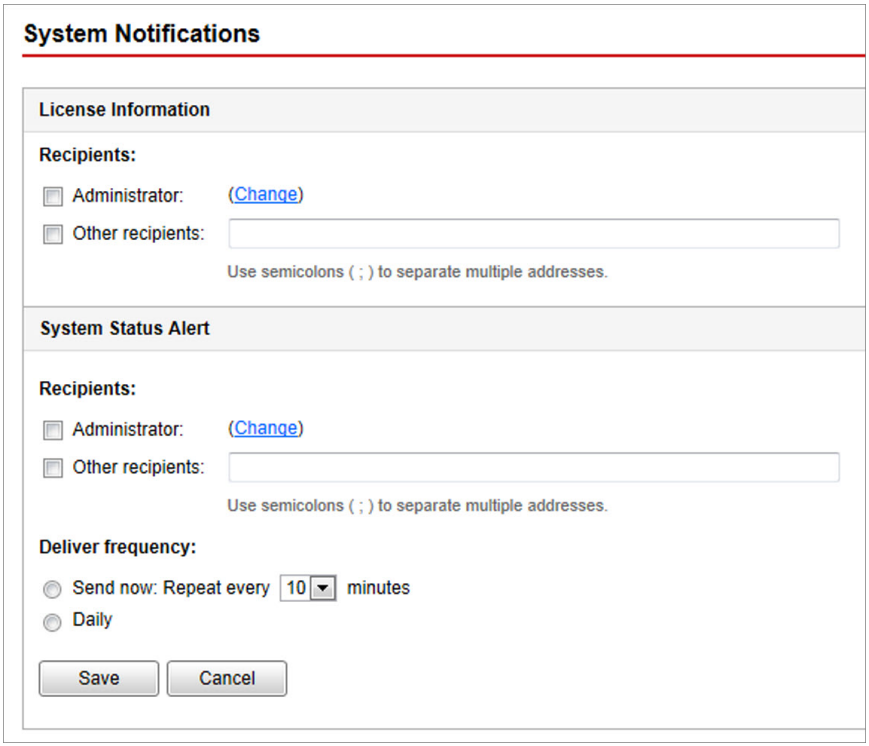


FIGURE 4-18. The System Notifications screen

2. Under **License Information**, select one of the following:

   - **Administrator**: SafeSync uses the **Account Settings** configuration to send email notifications to the configured administrator account. Click **Change** to open the **Account Settings** screen and modify the account settings.
   - **Other recipients**: SafeSync sends email notifications to the email accounts specified.

3. Under **System Status Alert**, select one of the following:

- **Administrator**: SafeSync uses the **Account Settings** configuration to send email notifications to the configured administrator account. Click **Change** to open the **Account Settings** screen and modify the account settings.
- **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**.

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.

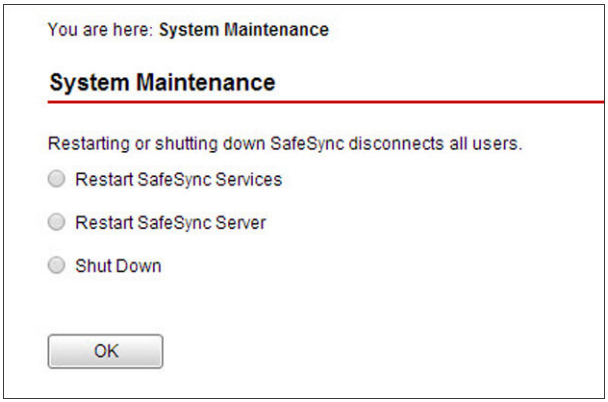


FIGURE 4-19. The System Maintenance screen

2. Select one of the following:

ACTION	DESCRIPTION
Restart SafeSync Services	Restarts the following SafeSync services • mysql • memcached • gearman • lighttpd • mogstored • mogilefsd • apache
Restart SafeSync Server	Restarts the SafeSync server
Shut Down	Shuts down the SafeSync server

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:

   http://downloadcenter.trendmicro.com.

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.

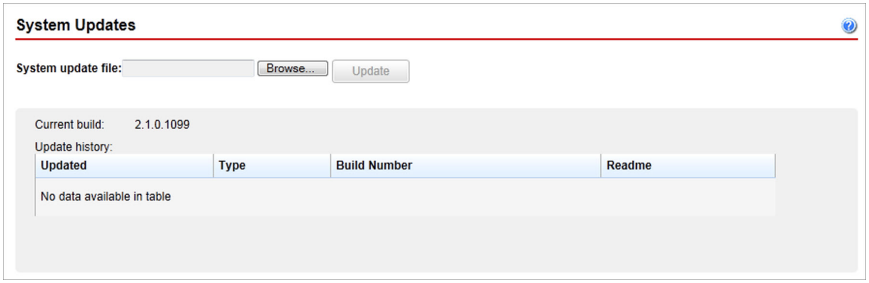


FIGURE 4-20. The System Updates screen

2. Click **Browse...** and select the update file.
3. Click **Update** and then click **Yes**.

   SafeSync starts the update process and 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.

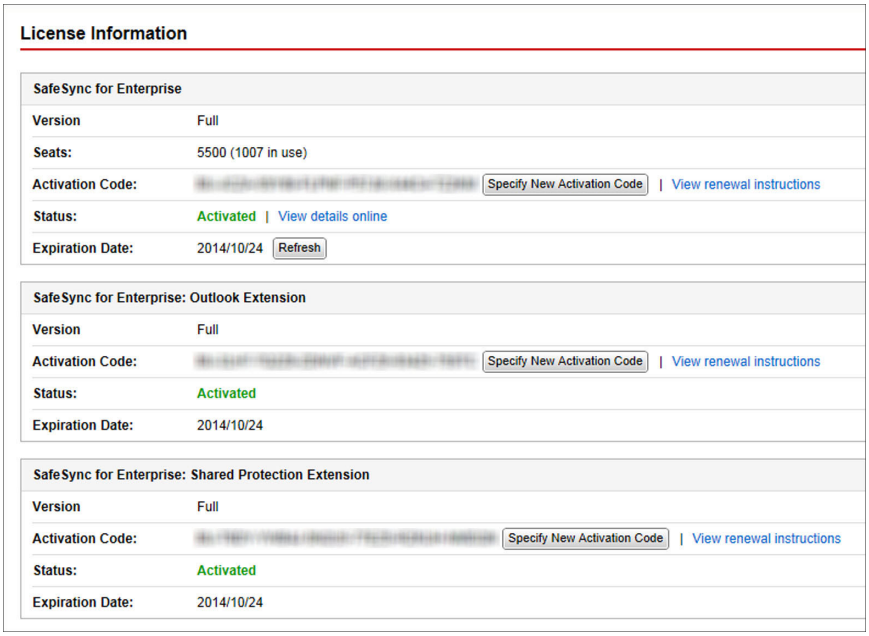


FIGURE 4-21. The License Information screen

2. View the following information:

OPTION	DESCRIPTION
Version	Displays either "Full" or "Trial" version
Seats	Displays the total number of seats and the number of seats in use
Activation Code	Displays the Activation Code
Status	Displays either "Activated", "Not Activated" or "Expired"
Expiration Date	Displays the expiration date

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 4-5. Limitations of Expired Licenses

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

Activating or Renewing SafeSync

SafeSync needs to be activated after installation.

Procedure

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

   The **License Information** screen appears.

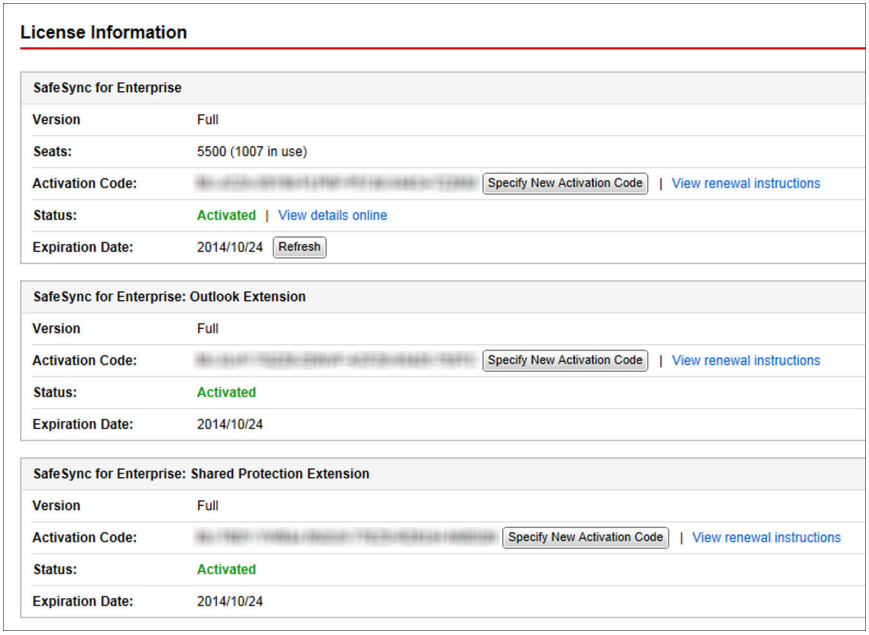


FIGURE 4-22. The License Information screen

2. Under **SafeSync for Enterprise**, click **Specify New Activation Code**.

The **New Activation Code** screen appears.

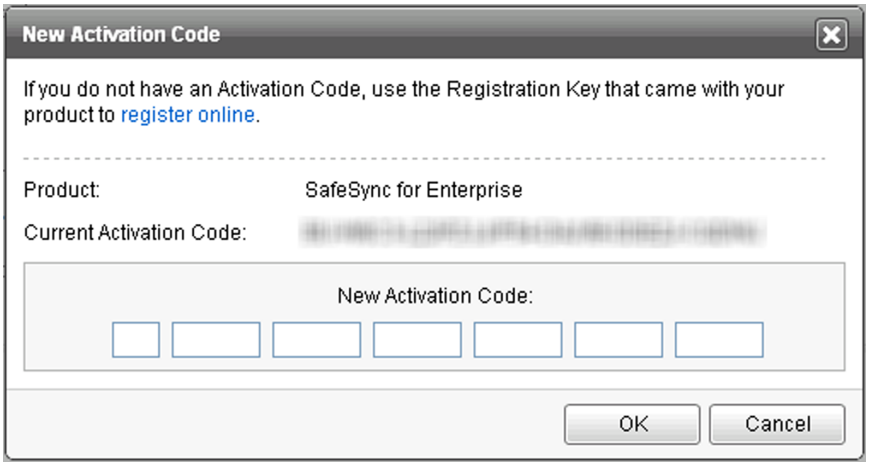


FIGURE 4-23. The New Activation Code screen

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.

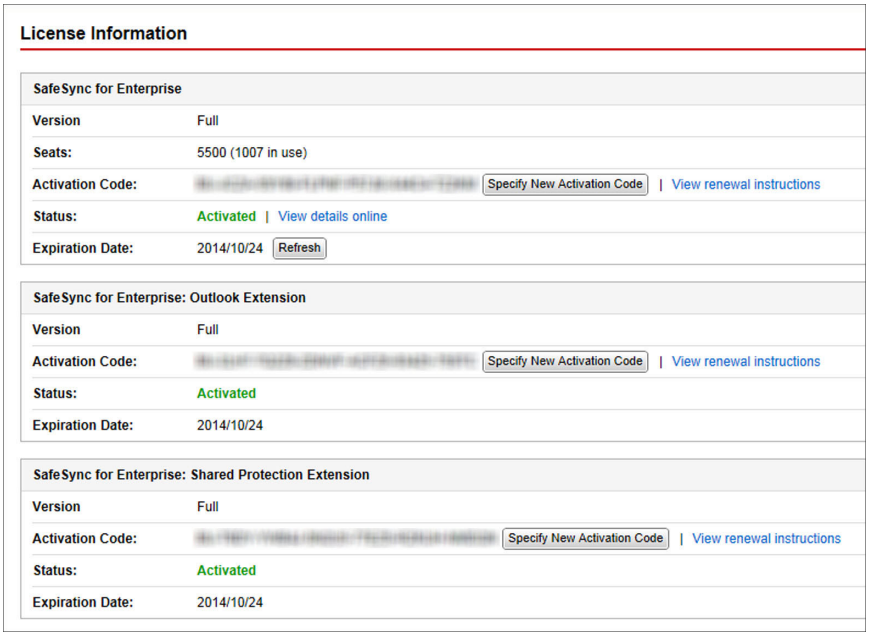


FIGURE 4-24. The License Information screen

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 4-30*.

Chapter 5

Frequently Asked Questions (FAQs)

This chapter answers various Frequently Asked Questions.

Topics include:

- *Files on page 5-2*
- *Services on page 5-3*
- *Storage on page 5-5*
- *SSL Certificates on page 5-12*

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 `/opt/TrendMicro/OSDP/Lib/Storage/Config.pm`.
   a. Locate the following line:

      ```
      MAX_IMAGE_THUMB_BUILD_SIZE => 20 * 1024 * 1024
      ```

   b. Change the line to:

```
MAX_IMAGE_THUMB_BUILD_SIZE => 26 * 1024 * 1024
```

Note

This example changes the thumbnail size limitation to 26 MB.

3. Save and close the file.
4. Restart the `grunjobs` service using the following command.

   ```
   /etc./init.d/grunjobs restart
   ```

5. Double-click the broken thumbnail image.

   The thumbnail images display correctly.

Why am I unable to upload files to a Team folder?

The default Team folder capacity is 1GB. Even if an individual user is allowed 10GB of storage space, Team folder restrictions apply when uploading files to a Team folder.

To resolve the issue, change the default storage capacity of the Team folder.

Procedure

1. Go to **Plans**.
2. Click "Default TeamFolder User 1GB" in the **Name** column.
3. Change the default storage size.
4. 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	mgmtui
avscand	mogilefsd
gearman-job-server	mogstored
grunjobs	mysql
healthcheck	nginx
keepalived	perlbal80
kmsd	perlbalmgmtui
lighttpd	thin
memcached	tmsyslog

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.

How can I add network devices?

You can add any of the following network devices.

- *NFS (Client-side) on page 5-5*
- *Samba (Mount CIFS) on page 5-7*
- *iSCSI on page 5-10*

WARNING!

Local, externally-mounted storages devices introduce a potentially high-risk of data loss if unexpectedly removed from the system. Trend Micro recommends only using network storage when expanding the SafeSync storage capacity.

NFS (Client-side)

SafeSync supports the Network File System (NFS), a client/server application.

Procedure

1. To install the NFS-common portmap, run the following command from a command line editor.

```
# apt-get install nfs-common portmap
```

2. Restart portmap.

```
# service portmap restart
```

3. Create a new mount point on the server.

```
# mkdir /storage/mogdata/dev13
```

4. Mount a new device to the mount point.

```
# mount -t nfs <IP address>:/tmp /storage/mogdata/dev13
```

> **Note**
> `/tmp` is the directory name of the NFS mount path.

5. Check the result.

```
# showmount -e <IP address>
```

6. Change the owner of `/storage/mogdata/dev13`.

```
# chown www-data:mogstored /storage/mogdata/dev13
```

7. Change the file mode of `/storage/mogdata/dev13`, giving it group authority to write.

```
# chmod g+w /storage/mogdata/dev13
```

8. Use the **`vim`** editor to change the disk usage and free space shown by **`df`**. The output should no longer include storage in the local file system.

   a. `# vim /usr/local/share/perl/5.10.1/Mogstored/ChildProcess/DiskUsage.pm`

   b. Go to line 58, which should contain the string `my $rval = `df $gnu_df -l -k $path/$devnum`;`, and change the string to `my $rval = `df $gnu_df -k $path/$devnum`;`.

> **Tip**
> The parameter `-l` has been removed, the string is otherwise unchanged.

c. Save the file and close **vim**.

9. Add a mount point to MogileFS.

```
# mogadm --trackers=tracker1:6001 device add osdp-store1 13 --
status=alive
```

10. Restart **mogstored**.

```
# /etc/init.d/mogstored restart
```

11. Check the result.

```
# mogadm check
```

```
Checking trackers...
  tracker1:6001 ... OK

Checking hosts...
  [ 1] osdp-store1 ... OK

Checking devices...
 host device         size(G)    used(G)    free(G)   use%   ob state
 ---- ------------ ---------- ---------- ---------- ------ ----------
 [ 1] dev11            7.027      5.590      1.437  79.55%  writeable
 [ 1] dev12            7.472      0.018      7.454   0.24%  writeable
[ 1] dev13            7.027      5.510      1.517  78.41%  writeable
    total:    21.526      11.118      10.408  52.73%
```

12. Use the NFS mount command at `/etc/rc.local` to auto-mount storage located on NFS after the system reboots using the following command.

```
# mount -t nfs <IP address>:/tmp /storage/mogdata/dev13
```

Samba (Mount CIFS)

SafeSync supports the **smbfs filesystem**, a mountable SMB filesystem for Linux.

Procedure

1. To install SMBFS, run the following command from a command line editor.

```
# apt-get install smbfs
```

2. Use the **vim** editor to change the disk usage and free space shown by **df**. The output should no longer include storage in the local file system.

   a. `# vim /usr/local/share/perl/5.10.1/Mogstored/ChildProcess/DiskUsage.pm`

   b. Go to line 58, which should contain the string `my $rval = `df $gnu_df -l -k $path/$devnum`;`, and change the string to `my $rval = `df $gnu_df -k $path/$devnum`;`.

   Tip

   The parameter `-l` has been removed, the string is otherwise unchanged.

   c. Save the file and close **vim**.

3. Change the permissions on the `mogstored` service.

   a. Edit the `/etc/init.d/mogstored`.

   `# vim /etc/init.d/mogstored`

   b. Replace `--chuid mogstored` with `--chuid www-data`.

   Note

   You must modify lines 41 and 61.

   c. Save the file and close **vim**.

4. Create a new mount point on the server.

   `# mkdir /storage/mogdata/dev14`

5. Find out the UID of `www-data`.

   a. `# vim /etc/passwd www-data uid gid`

   b. Look for a line starting with `www-data`.

   Text to the right of `www-data` will be something like `:x:33:33:www-data:var/www:/bin/false`. The number in the middle of `x:33:33` tells

us that, in this case, the UID of `www-data` is 33. The GID and other information can be ignored.

6. Mount CIFS.

> **Note**
>
> Give the appropriate network user name and password for `XXXXX`. Use the UID for `www-data` you found above in place of 33.

```
# mount -t cifs //<IP address>:/tmp /storage/mogdata/dev14 -o
"username=XXXXX,password=XXXXX,uid=33"
```

> **Note**
>
> `/tmp` is the directory name of the NFS mount path.

7. Use the **`vim`** editor to change `/etc/fstab` so it contains the CIFS data.

   a. `# vim /etc/fstab`

   b. Add a line to `/etc/fstab` with the CIFS data.

> **Note**
>
> Give the appropriate network user name and password for `XXXXX`. Use the UID for `www-data` you found above in place of 33.

```
//<IP address>:/tmp /storage/mogdata/dev/14 cifs
username=XXXXX,password=XXXXX,uid=33 0 0
```

8. Add a mount point for the new server to MogileFS, and make its status **alive**.

```
# mogadm --trackers=tracker1:6001 device add osdp-store1 14 --
status=alive
```

9. Check the results.

```
# mogadm check
```

iSCSI

SafeSync supports Internet Small Computer System Interface (iSCSI), an Internet Protocol-based storage networking standard.

Procedure

1. To install Open-iSCSI, run the following command from a command line editor.

   ```
   # apt-get install open-iscsi
   ```

2. Use **iscsiadm discovery** tool to get the iSCSI target name.

   ```
   # iscsiadm -m discovery -t st -p <IP address>
   ```

   ```
   [fd96:7568:9882:c5:211:32ff:fe02:82b7]:3260,0 <target iSCI
   Qualified Name (IQN)> <IP address>:3260,0 <target IQN>
   ```

3. Log on using the iSCSI target name.

   ```
   # iscsiadm -m node --targetname <target IQN> --portal "<IP
   address>:3260" --login
   ```

   ```
   Logging in to [iface: default, target: <target IQN>,
   portal: <IP address>, 3260]
   ```

   ```
   Login to [iface: default, target: <target IQN>, portal: <IP
   address>, 3260]: successful
   ```

4. Check the iSCSI disk name.

   ```
   # ls -l /dev/disk/by-path/ip-*
   ```

5. Add a new partition for the disk `/dev/sdd` (where `sdd` is an iSCSI disk).

   ```
   # parted -s /dev/sdd mklabel gpt #
   parted -s /dev/sdd mkpart primary ext4 0% 100% #
   partprobe /dev/sdd
   ```

6. List the partition table for `/dev/sdd` (`sdd` is an iSCSI disk).

   ```
   # mkfs.ext4 /dev/sdd1
   ```

7. Create a new mount point for the server.

```
# mkdir /storage/mogdata/dev13
```

8. Change the owner of `/storage/mogdata/dev13`.

```
# chown www-data:mogstored /storage/mogdata/dev13
```

9. Change the file mode of `/storage/mogdata/dev13`.

```
# chmod g+w /storage/mogdata/dev13
```

10. Test the mount.

```
# mount /dev/sdd1 /storage/mogdata/dev13
```

11. Add a mount point to MogileFS.

```
# mogadm --trackers=tracker1:6001 device add osdp-store1 13 --
status=alive
```

12. Use the **vim** editor to change `/etc/fstab` so it contains the iSCSI data.

    a. `# vim /etc/fstab`

    b. Add a line to `/etc/fstab` with the iSCSI data.

```
/dev/sdd1 /storage/mogdata/dev13 ext3
defaults,user_xattr,_netdev 1 2
```

13. Set iSCSI auto startup.

```
sudo iscsiadm -m node --targetname "<target IQN>" --portal
"<IP address>:3260" -o update -n node.conn[0].startup -v
automatic
```

Tip

The entire sudo command above should be typed as one line without line feeds.

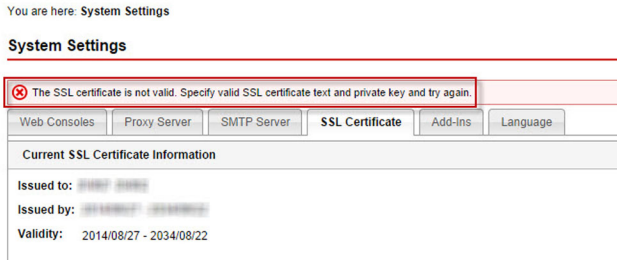
14. Check the results.

```
# mogadm check
```

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 PKSC12 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 private key.

```
-----BEGIN PRIVATE KEY-----

xxxxxxxxxxxxx.....

-----END PRIVATE KEY-----
```

b. Copy the SSL certificate.

```
-----BEGIN CERTIFICATE-----

xxxxxxxxxxxxx.....

-----END CERTIFICATE-----
```

3. Go to **Administration** > **System Settings** > **SSL Certificate**.
4. Under **Step 1**, provide the certificate text from Step 2.
5. Under **Step 2**, click **Choose file** and then provide the private key from Step 2.
6. Click **Update**.

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 `*.<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 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:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  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

VIRUS / MALWARE TYPE	DESCRIPTION
Joke program	Joke programs are virus-like programs that often manipulate the appearance of things on the endpoint's monitor.
Others	"Others" include viruses/malware not categorized under any of the other virus/malware types.
Packer	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.
Rootkit	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.
Test virus	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.

Virus / Malware Type	Description
Trojan horse	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.
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.
Network Virus	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.

VIRUS / MALWARE TYPE	DESCRIPTION
Probable virus/ malware	Probable viruses/malware are suspicious files that have some of the characteristics of viruses/malware. For more information, see the Trend Micro Threat Encyclopedia: http://about-threats.trendmicro.com/us/threatencyclopedia#malware

About Trend Micro Smart Protection

Trend Micro™ smart protectionis a next-generation cloud-agent content security infrastructure designed to protect customers from security risks and web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-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.

By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro smart protection solutions reduce reliance on conventional pattern file downloads and eliminate the delays commonly associated with desktop updates.

Note

SafeSync supports in-the-cloud file reputation and scanning.

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 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://<SSFE Domain Name>/pages/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.

Appendix D

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, 4-2
accounts
    disabled, 2-10, 2-14
activating, 4-42
    add-ins, 4-45
Activation Code, 4-40, 4-42
Active Directory integration, 4-3
    enabling, 4-4
    LDAP search filter, 4-5
    root DN, 4-4
    selecting users, 2-7
    update frequency, 4-5
ActiveX malicious code, A-3
adding
    policies, 2-20
    users, 2-7
add-ins, 4-28
    activating, 4-45
    configuring, 4-31
    Outlook Extension, 4-29
    Shared Protection Extension, 4-30
administration
    Active Directory integration, 4-3
    antivirus settings, 4-5
    license information, 4-40
    my account, 4-2
    system maintenance, 4-36
    system notifications, 4-34
    system settings, 4-21
    system updates, 4-38

B

boot sector virus, A-3

C

changing password, 4-2
COM file infector, A-3
Component Status widget, 3-8
configuring
    Active Directory settings, 4-3
    add-ins, 4-31
    notification settings, 4-34
    policies, 2-18
    proxy server settings, 4-24
    SMTP server settings, 4-25
    SSL certificate settings, 4-27
    syslog server, 3-18
    web console settings, 4-22

D

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, 4-32
deleting
    logs, 3-17
    policies, 2-21
disabled users, 2-10, 2-14

DNS records, 4-23
documentation, vi
domain accounts, 2-7
    changing plans, 2-9
    disabled, 2-10

E

editing
    policies, 2-21
EICAR test script, A-2
email address, 4-2
    notification recipients, 4-34
    SMTP server, 4-25
enabling
    Active Directory integration, 4-4
End User License Agreement (EULA), D-2
EXE file infector, A-3

F

forwarding
    logs, 3-18

H

HTML virus, A-3

I

integrating Active Directory structure, 4-3
IntelliTrap Exception Pattern, B-3
IntelliTrap Pattern, B-3

J

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

L

LDAP search filter, 4-5
license, 4-40, 4-42
logs
    deletion, 3-17, 3-18
    email address, 4-2
    querying, 3-16
    syslog server, 3-18

M

macro virus, A-3
maintenance
    logs, 3-17
manual accounts
    adding, 2-11
    changing plans, 2-14
    deleting, 2-12
    disabled, 2-14
    editing, 2-12
    enabling/disabling, 2-13
my account, 4-2
    changing password, 4-2
    email address, 4-2

N

network virus, A-3
notifications
    recipients, 4-34
    settings, 4-34

O

Outlook Extension, 4-29
    activating, 4-45
    configuring, 4-31

P

packer, A-2
password, 4-2
pattern files
    Smart Scan Agent Pattern, B-2
performing system updates, 4-38
plans, 2-22

adding, 2-23
changing assignment, 2-9, 2-14, 2-15
deleting, 2-24
editing, 2-24, 5-3
reviewing user and group assignment, 2-22, 2-25
policies, 2-18
adding, 2-20
deleting, 2-21
editing, 2-21
probable virus/malware, A-4
proxy server settings, 4-24

Q

querying logs, 3-16

R

recipients, 4-34
renewing, 4-42
reports, 3-14
root DN, 4-4
rootkit, A-2

S

SafeSync
about, 1-2
add-ins, 4-28
documentation, vi
terminology, viii
users, 2-7
setting up SafeSync users, 2-7
Shared Protection Extension, 4-30
activating, 4-45
configuring, 4-31
decrypting files, 4-32
smart protection, B-2
pattern files, B-2
Smart Scan Agent Pattern, B-2
Smart Scan Agent Pattern, B-2
SMTP server settings, 4-25
SSL certificate, 4-27
support
resolve issues faster, 6-2
syslog server, 3-18
system settings
proxy server, 4-24
SMTP server, 4-25
SSL certificate, 4-27
syslog server, 3-18
web console, 4-22
System Status Alert widget, 3-13
System Status widget, 3-12

T

terminology, viii
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
Trojan horse program, A-3

U

update frequency, 4-5
updating
system, 4-38
updating SSL certificate, 4-27
Usage Trends widget, 3-10
users, 2-6
adding, 2-11
changing multiple accounts simultaneously, 2-15
changing plans, 2-14
deleting, 2-12

disabled, 2-10, 2-14
domain accounts, 2-7
editing, 2-12
enabling/disabling, 2-13
individual user details, 2-17
manual accounts, 2-11
types, 2-7

V

VBScript virus, A-3
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
VBScript, JavaScript or HTML virus, A-3
worm, A-3
Virus Encyclopedia, A-4
Virus Scan Engine, B-2

W

web console settings, 4-22
DNS records, 4-23
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

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM26486/140711