TREND MICRO™
SafeSync for Enterprise
Installation Guide
Securely Share, Distribute, and Control Enterprise Information Within Your Private Cloud
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

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

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

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

## Preface

Preface ........................................................................................................... iii
SafeSync Documentation ........................................................................ iv
Audience ..................................................................................................... iv
Document Conventions ........................................................................... v
Terminology ............................................................................................ vi

## Chapter 1: Introducing SafeSync

About SafeSync ....................................................................................... 1-2
What's New ............................................................................................ 1-2
  What's New in This Version ................................................................. 1-2
Features and Benefits ........................................................................... 1-8

## Chapter 2: Preparing for Installation

System Requirements .................................................................................. 2-2
Registration Key and Activation Codes ................................................... 2-2
Fresh Installation Considerations ............................................................ 2-3
  Servers .................................................................................................. 2-4
  Required Network Settings ................................................................. 2-5
  High Availability ............................................................................... 2-6
  Network Interface Cards ................................................................. 2-8
  Ports Used by SafeSync ................................................................. 2-9
  SSL Certificate ................................................................................... 2-10
Basic Installer Operations ....................................................................... 2-11

## Chapter 3: Installing SafeSync

Installation Methods .................................................................................. 3-2
Installing a SafeSync Appliance Using an ISO Image File ....................... 3-2
Installing a SafeSync Appliance Using an OVF Installation Package ... 3-11

Chapter 4: Verifying Installation

Checking Services ................................................................. 4-2
Checking System Status ......................................................... 4-3
Verifying File Upload and Download ..................................... 4-4

Chapter 5: Post-Installation Tasks

About Adding MogileFS Storage ............................................. 5-2
Mounting Additional Disks ..................................................... 5-3
Adding a Network Device ..................................................... 5-4
  NFS (Client-side) ............................................................... 5-4
  Samba (Mount CIFS) .......................................................... 5-6
  iSCSI ............................................................................... 5-9

Chapter 6: Frequently Asked Questions (FAQs)

Apache Server ................................................................. 6-2
  What should I do if the Apache server does not start after installing SafeSync? ......................................................... 6-2
DNS Settings ........................................................................ 6-2
  Why am I unable to connect to the Administrator Console? .......... 6-2

Chapter 7: Contacting Technical Support

Contacting Trend Micro ..................................................... 7-2
  Speeding Up the Support Call ............................................. 7-2

Index

Index ........................................................................... IN-1
Welcome to the Trend Micro™ SafeSync for Enterprise™ Installation Guide. This document discusses requirements and procedures for installing SafeSync, verifying the installation, and performing post-installation tasks.

Topics in this chapter include:

• SafeSync Documentation on page iv
• Audience on page iv
• Document Conventions on page v
• Terminology on page vi
SafeSync Documentation

SafeSync documentation includes the following.

**TABLE 1. SafeSync Documentation**

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Guide</td>
<td>A PDF document that discusses requirements and procedures for installing SafeSync.</td>
</tr>
<tr>
<td>Administrator's Guide</td>
<td>A PDF document that provides &quot;how to's&quot;, advice, usage and field-specific information.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides the basic requirements and procedures for installing SafeSync.</td>
</tr>
<tr>
<td>Readme file</td>
<td>Text-based documentation that contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

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


**Audience**

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

The documentation uses the following conventions.

**TABLE 2. Document Conventions**

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

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

**TABLE 3. SafeSync Terminology**

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

Introducing SafeSync

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

Topics in this chapter include:

• *About SafeSync on page 1-2*
• *What's New on page 1-2*
• *Features and Benefits on page 1-8*
About SafeSync

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

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

What's New

What's New in This Version

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

| TABLE 1-1. New Features and Enhancements for SafeSync for Enterprise 3.2 |
|-----------------|-------------------------------------------------------------------|
| FEATURE           | DESCRIPTION                                                                |
| Cache servers     | Set up and manage cache servers to reduce the amount of network traffic on the SafeSync server. |
| Storage management | Add and manage local disks, iSCSI storage, or NFS storage from the administrator web console. |
| SSL certificate import | Enhanced certificate import interface. |
Introducing SafeSync

### Platform support

This version supports the following:
- Windows Server 2008 R2 and 2012 R2 - Active Directory server
- Mac 10.11
- Android 6.x
- iOS 9.1, 9.2
- Outlook 2016

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Side</td>
<td></td>
</tr>
<tr>
<td>Server installation</td>
<td>There are two ways to install SafeSync, either from an ISO image file or an Open Virtualization Format (OVF) installation package. Both methods allow you to set up a high availability deployment and add additional hard disks for storage expansion.</td>
</tr>
<tr>
<td></td>
<td>• ISO image file: can be installed on a bare metal server or a virtual machine.</td>
</tr>
<tr>
<td></td>
<td>• OVF installation package: can only be installed on a virtual machine. The installation process is fast (about 10 minutes). This method is suitable for proof of concept evaluation.</td>
</tr>
<tr>
<td>Administrator accounts</td>
<td>Set up multiple administrator accounts to manage SafeSync.</td>
</tr>
<tr>
<td>Active Directory integration</td>
<td>Integrate SafeSync with multiple Active Directory structures. Administrators can selectively choose the users or groups to synchronize with SafeSync.</td>
</tr>
</tbody>
</table>

**What's New in Version 3.1**

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

**TABLE 1-2. New Features and Enhancements for SafeSync for Enterprise 3.1**
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web consoles settings</td>
<td>Set up web console settings using single-level domain and access SafeSync using the configured domain name.</td>
</tr>
<tr>
<td>High availability deployment</td>
<td>Set up a high availability deployment from the administrator web console.</td>
</tr>
<tr>
<td>Shareable links</td>
<td>Administrators can enforce security control on shareable links in policy settings. End users may be required to sign in or provide a password to access a link.</td>
</tr>
<tr>
<td></td>
<td>End users can now exchange files through shareable links and set access permissions to the files they share.</td>
</tr>
<tr>
<td>User session control</td>
<td>Administrators can enforce strong security control on user sessions by requiring end users to sign in every time they access SafeSync. Administrators can also configure the security control setting to automatically sign out inactive users.</td>
</tr>
<tr>
<td>Storage management</td>
<td>Administrators can manage team folder storage and owners.</td>
</tr>
<tr>
<td>End-User Side</td>
<td></td>
</tr>
<tr>
<td>Online file preview</td>
<td>View files like PDFs, Microsoft Office files, images, and videos directly in the end-user portal.</td>
</tr>
<tr>
<td></td>
<td>Users with permissions to open encrypted files can also view them in the end-user portal.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Notify users of important events in the end-user portal and Windows client, such as new team folders or malicious file detections.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Make files or folders as Favorites for easy access in the end-user portal.</td>
</tr>
<tr>
<td>Sub-folder level permission control</td>
<td>Control team folder permissions on the sub-folder level. Set permissions on each sub-level folder by different users or groups.</td>
</tr>
<tr>
<td>End-user portal interface</td>
<td>Brand new design and better user experience.</td>
</tr>
</tbody>
</table>
### What's New in Version 2.1 Service Pack 1

The following new features and enhancements are available in version 2.1 SP1.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic tool in Android and iOS apps</td>
<td>Collect SafeSync event logs that Support uses for troubleshooting purposes.</td>
</tr>
</tbody>
</table>
| Platform support | • Administrator web console and end-user portal support Microsoft Edge  
• Mac client supports Mac 10.10  
• Windows client supports Windows 10  
• Android app supports Android 5.x  
• iOS app supports iOS 9.0 |
<table>
<thead>
<tr>
<th><strong>FEATURE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus scan</td>
<td>Perform Antivirus scan when users upload or share files.</td>
</tr>
<tr>
<td></td>
<td>After installing this service pack, SafeSync for Enterprise can perform antivirus scan on files and quarantine files detected as malicious. SafeSync for Enterprise provides a configurable secure environment for data uploading, sharing, downloading, and synchronization.</td>
</tr>
<tr>
<td></td>
<td>Prevent malicious files from spreading.</td>
</tr>
<tr>
<td></td>
<td>Files detected as malicious are quarantined to prevent users from accidentally opening the files. The detected files are not synchronized, downloaded, or shared.</td>
</tr>
<tr>
<td></td>
<td>Analyze threat detection trends at a glance.</td>
</tr>
<tr>
<td></td>
<td>Administrators can easily manage the threat status using widgets. Threat detection widgets include threat statistics, top 10 detection and top 10 threats, and component status. Administrators have the option of exporting the data into CSV files.</td>
</tr>
<tr>
<td></td>
<td>Specify Active Update and Smart Protection Server sources.</td>
</tr>
<tr>
<td></td>
<td>Administrators can specify the Active Update and Smart Protection Server sources based on the network environment.</td>
</tr>
<tr>
<td>Multiple downloads</td>
<td>End users can download multiple files and folders as an archived file from the end-user portal.</td>
</tr>
</tbody>
</table>
Introducing SafeSync

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

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

SafeSync provides the following features and benefits.

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

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share files easily and securely</td>
<td>Fast and secure file and folder sharing with the shareable link. Set links with passwords that expire for additional security.</td>
</tr>
<tr>
<td></td>
<td>“Team Folders” for effective group collaboration that can be created on the fly by staff and administrators.</td>
</tr>
<tr>
<td></td>
<td>View files like PDFs, Microsoft Office files, images, and videos directly in the end-user portal.</td>
</tr>
<tr>
<td>Easily create and control user accounts</td>
<td>SafeSync supports centralized administration for creating and controlling users.</td>
</tr>
<tr>
<td>Recover previous versions of files</td>
<td>Recover deleted files or previous file versions from the end user portal.</td>
</tr>
<tr>
<td>Protect files with encryption</td>
<td>Protect files with the same Advanced Encryption Standard (AES) 256-bit encryption used by the government and military.</td>
</tr>
<tr>
<td>Securely share email attachments sent from Microsoft Outlook</td>
<td>When the <strong>SafeSync Outlook Extension</strong> is enabled, users can either upload their attachments to SafeSync and send a shareable link in the email, or use the auto-encryption option to automatically encrypt file attachments.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The <strong>SafeSync Outlook Extension</strong> helps to prevent unintentional data leakage through misdirected or forwarded emails, or device loss.</td>
</tr>
<tr>
<td>Automatically encrypt files using an auto-encryption folder</td>
<td>When the <strong>Shared Protection Extension</strong> is enabled, users can create an auto-encryption folder. All files added to this folder are encrypted automatically.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Use the auto-encryption folder to securely share sensitive files, such as those used by Human Resources or Finance.</td>
</tr>
<tr>
<td><strong>Benefit</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Convenient remote administration</td>
<td>You have the ability to control user accounts and share or revoke access to your shared files at any time.</td>
</tr>
<tr>
<td>Prevent data loss</td>
<td>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.</td>
</tr>
<tr>
<td>Scan files for virus/malware threats</td>
<td>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.</td>
</tr>
</tbody>
</table>
Preparing for Installation

This chapter explains how to plan and prepare for a SafeSync installation.

Topics in this chapter include:

• System Requirements on page 2-2
• Registration Key and Activation Codes on page 2-2
• Fresh Installation Considerations on page 2-3
• Basic Installer Operations on page 2-11
System Requirements

The following table provides the system requirements for installing SafeSync.

**TABLE 2-1. System Requirements**

<table>
<thead>
<tr>
<th>HARDWARE/SOFTWARE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network switch</td>
<td>1 Gb</td>
</tr>
<tr>
<td>CPU</td>
<td>64-bit x86 (dual-core recommended)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB (32 GB recommended)</td>
</tr>
<tr>
<td>Network card</td>
<td>1 NIC (1 Gb recommended)</td>
</tr>
<tr>
<td>System disk space</td>
<td>200 GB (for SafeSync installation, 500 GB recommended)</td>
</tr>
<tr>
<td>Storage disk space</td>
<td>The disk storage size is dependent on user requirements.</td>
</tr>
</tbody>
</table>

**Tip**

Trend Micro recommends allocating 8 to 10 GB for each user. If you want to replicate all of the users’ files, the allocated space is doubled (16 to 20 GB). For example, if you intend to have 100 users, the recommended storage space is 2TB.

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>VMware ESXi™ 4.x, 5.x, 6.x</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware® WorkStation™ 6.x, 7.x, 8.x, 9.x, 10.x, 11.x, or above</td>
</tr>
<tr>
<td></td>
<td>Oracle VM VirtualBox™ 4.2.x</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V™ 6.2.9200.16384</td>
</tr>
</tbody>
</table>

Registration Key and Activation Codes

During installation, specify the Activation Codes for the following:
Preparing for Installation

- SafeSync
- Outlook Extension (optional)
- Shared Protection Extension (optional)

Use the Registration Key that came with the product to obtain Activation Codes (if not already obtained). Setup automatically redirects to the Trend Micro website for product registration.

http://olr.trendmicro.com

After registering the product, Trend Micro sends the Activation Codes.

Contact a Trend Micro sales representative to obtain the Registration Key or Activation Codes, if neither is available at the time of installation. For more information, see Contacting Trend Micro on page 7-2.

---

**Note**

For questions about registration, refer to:


---

Fresh Installation Considerations

Consider the following when performing a fresh installation of the SafeSync server:

- Servers on page 2-4
- Required Network Settings on page 2-5
- High Availability on page 2-6
- Network Interface Cards on page 2-8
- Ports Used by SafeSync on page 2-9
- SSL Certificate on page 2-10
Servers

SafeSync requires the following servers to function. Configure the server settings during SafeSync installation.

**Table 2-2. SafeSync Servers**

<table>
<thead>
<tr>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeSync</td>
<td>Storage space for installing SafeSync</td>
</tr>
<tr>
<td></td>
<td>You can choose to install SafeSync on a bare metal server or a virtual machine.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Installing SafeSync on page 3-1</em>.</td>
</tr>
<tr>
<td>Domain Name System (DNS)</td>
<td>Server for storing the DNS records or network settings used by SafeSync</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Required Network Settings on page 2-5</em>.</td>
</tr>
</tbody>
</table>

SafeSync also uses the following servers to utilize some important features. For more information on server configurations, see the *SafeSync for Enterprise Administrator's Guide*.

**Table 2-3. Other Servers Used by SafeSync**

<table>
<thead>
<tr>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog</td>
<td>Server that stores SafeSync event logs</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Integrate SafeSync with one or more Active Directory servers to efficiently manage user and group permissions</td>
</tr>
<tr>
<td>Smart Protection</td>
<td>Server that accepts data about unknown and potentially malicious files from SafeSync</td>
</tr>
<tr>
<td>Proxy</td>
<td>Server that acts as an intermediary between the SafeSync server or clients and the Internet</td>
</tr>
<tr>
<td></td>
<td>If the network requires that SafeSync uses a proxy server, configure the proxy server from the administrator console.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Email server for sending system notifications</td>
</tr>
</tbody>
</table>
Required Network Settings

SafeSync uses a fully qualified domain name (FQDN) for domain mapping. For example, your environment uses the following domain names:

- Domain: safesyncstorage
- Top-level domain: com

You need to use safesyncstorage.com for domain mapping.

Note

If you use a subdomain, ensure that you also include it in domain mapping.

If the network settings are incorrect, the following error message appears when you try to access the end-user portal: The connection has timed out.

Single-Server Deployment

SafeSync requires the following DNS settings for a single-server deployment:

- FQDN: <your_domain>.<top-level_domain>
- Type: Host (A)
- IP address: For example, 10.20.30.234

High Availability Deployment

SafeSync requires the following DNS settings for a high availability deployment:

Primary server

- FQDN: <your_domain>.<top-level_domain>
- Type: Host (A)
- IP address: For example, 10.20.30.234

Secondary server
• FQDN: `<your_domain>`.`<top-level_domain>`
• Type: Host (A)
• IP address: For example, `10.20.30.235`

### High Availability

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

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

**Table 2-4. Primary and Secondary Servers**

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

For more information, see File Replication on page 2-7 and Load Balancing on page 2-8.

### File Replication

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

The default file replication number is 2. This means that all files uploaded by users are stored on both servers. File replication has two main benefits:

- Prevents having a single point of failure by using two servers
- Increases service performance by providing access to two different physical locations
SafeSync automatically generates streaming and thumbnail files when users upload certain file types. The auto-generated files’ replication number is 1.

---

**Note**

Storage space is used by balanced percentages. This means newly added storage is used first.

---

### Load Balancing

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

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

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

### Network Interface Cards

SafeSync requires each server to have one network interface card (NIC) during installation. The NIC must be connected to the right switch during installation.

### Roles of the Network Interface Cards

The following list describes the roles of the NIC:

- Connects to the Internet and/or Intranet

---

**Note**

The IP address, subnet, gateway, and DNS server settings are configured during installation, and these settings can be changed from the administrator console after installation.
• Serves as the data port
• Used for communication with other hosts or devices, clients, and users in the network
• Used for database communication and replication traffic between the two servers in a high availability deployment

Ports Used by SafeSync

The following table shows the ports that are used with SafeSync and why they are used.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Inbound</td>
<td>SafeSync uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Allow the administrator to gain remote access to the servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Establish communication between the primary and secondary servers</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Inbound and Outbound</td>
<td>SafeSync uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to the Smart Protection Network or the local Smart Protection Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Update components by connecting to the ActiveUpdate server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to SafeSync services</td>
</tr>
</tbody>
</table>
### Port and Protocol

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Function</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Inbound and Outbound</td>
<td>SafeSync uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Connect to all services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access the administrator console through HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access the end-user portal through HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Connect to SafeSync clients</td>
</tr>
<tr>
<td>3443</td>
<td>TCP</td>
<td>Inbound</td>
<td>SafeSync uses this port to request HTTP access to the administrator console.</td>
</tr>
</tbody>
</table>

**Note**

The administrator console can be accessed using `https://<SafeSync IP address or FQDN>:3443`.

### SSL Certificate

SafeSync requires SSL certificates to enable secure connections between the server and browsers.

**Note**

The SSL certificate is imported from the SafeSync administrator console.

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:

Preparing for Installation

- 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: 
  
  *.<your_domain>.<top-level_domain>

---

**Note**

If you use a subdomain, ensure that you also include it in domain mapping.

---

**Basic Installer Operations**

Use the following keyboard keys to perform basic operations during the installation process.

---

**Important**

Disable scroll lock (using the Scroll Lock key on the keyboard) to perform the following operations.

---

<table>
<thead>
<tr>
<th><strong>Keyboard Key</strong></th>
<th><strong>Operation</strong></th>
</tr>
</thead>
</table>
| Arrow keys       | Move between buttons  
|                  | Buttons are enclosed in angle brackets <>  
|                  | Move between characters in a text box |
| ENTER            | Click the highlighted button |
Chapter 3

Installing SafeSync

This chapter explains how to install SafeSync.

Topics in this chapter include:

• Installation Methods on page 3-2
• Installing a SafeSync Appliance Using an ISO Image File on page 3-2
• Installing a SafeSync Appliance Using an OVF Installation Package on page 3-11
Installation Methods

There are two ways to install SafeSync, either from an ISO image file or an Open Virtualization Format (OVF) installation package. Both methods allow you to set up a high availability deployment and add additional hard disks for storage expansion.

- ISO image file: can be installed on a bare metal server or a virtual machine.
- OVF installation package: can only be installed on a virtual machine. The installation process is fast (about 10 minutes). This method is suitable for proof of concept evaluation.

Installing a SafeSync Appliance Using an ISO Image File

The following procedure explains the steps required to install SafeSync using an ISO image file.

**WARNING!**

Any existing data or partitions are removed during the installation process. Back up any existing data on the server before installing SafeSync.

**Note**

When installing SafeSync on a virtual machine, configure and set up the environment first. For details, refer to your virtualization software documentation.

**Procedure**

1. On the server you want to install SafeSync, insert the installation DVD into the DVD drive.
2. Power on the server.
The **Configure the keyboard** screen appears.

3. Select **No** to use the default **English (US)** keyboard layout, or select **Yes** and select the country that matches your keyboard layout.
The **Configure the network** screen appears.

4. Type the IP address used for accessing SafeSync.

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

6. Type the IP address for the subnet mask.

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

8. Type the IP address for the gateway.

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

10. Type the IP address for the DNS server.

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

12. Type a password for the server system account.

   **Note**
   The system account password is used to log on to the command line console of the SafeSync server.

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

14. Retype the password.
15. Select Continue or press the ENTER key.
The installation process completes, and the screen for the command line console appears.

Use the following URL and account information to access the SafeSync management console.

Management console: https://<SafeSync IP address>:3443/
Web console account: administrator
Password: safesync

For advanced server configuration, use the following account information to log on to Ubuntu:
System account: safesync
Password: *****
appliance1 login: _

16. Using a web browser, log on to the administrator web console using the following credentials:

- URL: https://<SafeSync IP address>:3443
- User name: administrator
- Password: safesync

**Note**

To access SafeSync using domain names, configure the URL settings on the System Settings screen in the administrator web console.
The Change Default Password screen appears.

17. Change the default password.

18. (Optional) Repeat the installation process to install the second server and set up a high availability deployment on the administrator web console.

---

**Note**
For details on high availability configurations, see the SafeSync for Enterprise Administrator’s Guide.

---

**Installing a SafeSync Appliance Using an OVF Installation Package**

The following procedure explains the steps required to install SafeSync on a virtual machine using an OVF installation package.

**Procedure**

1. Launch your virtualization software.
2. Import the virtual machine included in the OVF installation package.

   **Note**
   For details on how to import a virtual machine, refer to your virtualization software documentation.

3. Turn on the imported virtual machine.

   The installation process starts and the *Configure IP* screen appears.

   4. Type the IP address used for accessing SafeSync.

   5. Select **OK**.
The **Configure Netmask** screen appears.

6. Type the IP address for the subnet mask.
7. Select **OK**.

The **Configure Gateway** screen appears.
8. Type the IP address for the gateway.

9. Select **OK**.

The **Configure DNS** screen appears.

10. Type the IP address for the DNS server.

11. Select **OK**.
The **Web Console Settings** screen appears.

12. Verify the settings and select **Yes**.

The **System Account** screen appears.
13. Type a password for the server system account.

**Note**
The system account password is used to log on to the command line console of the SafeSync server.

14. Select OK.

The **Confirm Password** screen appears.

15. Retype the password.

16. Select OK.
The installation process completes, and the screen for the command line console appears.

Use the following URL and account information to access the SafeSync management console.

Management console: https://<SafeSync IP address>:3443/

Web console account: administrator
Password: safesync

For advanced server configuration, use the following account information to log on to Ubuntu:

System account: safesync
Password: *******

appliance1 login: _

17. Using a web browser, log on to the administrator web console using the following credentials:

- **URL**: https://<SafeSync IP address>:3443
- **User name**: administrator
- **Password**: safesync

**Note**

To access SafeSync using domain names, configure the URL settings on the **System Settings** screen in the administrator web console.
The **Change Default Password** screen appears

![Change Default Password](image)

**You must change the default SafeSync password to continue.**

**New password:**

```
Passwords must be 5 to 40 characters long.
```

**Confirm password:**

18. Change the default password.

19. (Optional) Repeat the installation process to install the second server and set up a high availability deployment on the administrator web console.

---

**Note**

For details on high availability configurations, see the *SafeSync for Enterprise Administrator’s Guide.*
Chapter 4

Verifying Installation

This chapter explains how to verify a SafeSync installation.

Topics in this chapter include:

• Checking Services on page 4-2
• Checking System Status on page 4-3
• Verifying File Upload and Download on page 4-4
Checking Services

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

- apache2
- avscand
- gearmand
- grunjobs
- healthcheck
- keepalived
- kmsd
- libreoffice
- lighttpd
- memcached
- mgmtui
- mogilefsd
- mogstored
- mysql
- nginx
- perlbal80
- perlbalmgmtui
- safesync-fusedav
- sshd
- thin
- tmsyslog

You can run the following commands to check the status of SafeSync services.

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:
   
   ```
   sudo ./check_all_service_status.sh
   ```
4. Provide the system password.

   If there are no problems, the command line editor displays the following message:
All SafeSync services are working properly

Checking System Status

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.

The following table describes the information available on the widget:

**TABLE 4-1. System Status Alert Widget**

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

**Procedure**

1. Log on to the SafeSync web console.
2. Go to Dashboard > System Status > System Status Alert.
3. Verify the status of the servers using the following icons.
   - ![Normal](image)
   - ![Warning](image)

Verifying File Upload and Download

After installing and activating SafeSync, configure the URL settings for the end-user portal from the administrator web console and then proceed with the following task.

---

**Note**

For more information on activating SafeSync and configuring the URL settings, see the *SafeSync for Enterprise Administrator's Guide*.

---

**Procedure**

1. Using a web browser, sign into the end-user portal (https://<SafeSync domain name>) using the administrator account credentials.
   - User name: administrator
   - Password: <web console account password>

   **Note**

   A warning message may appear when you first visit the portal. Click Proceed.

   To stop seeing this warning, update the SSL certificate from the administrator web console. See the *SafeSync for Enterprise Administrator's Guide* for more information.

2. Click Upload Files.

3. Select the file you want to upload. The example below uses a JPEG image.
Note
SafeSync supports preview for common file and image types.

- Files: Plain text, Microsoft Office, PDF
- Images: JPEG, PNG

The file successfully uploads to SafeSync.

Note
To switch your content to thumbnail view, click the grid icon ( المباشر).  

4. Click the file name to preview it.
5. Click the close button (x) to close the file preview.

6. Select the file you just uploaded.

7. Click **Get Shared Link** to share your file.

SafeSync creates a link to the file. Recipients can use this link to access your file.
8. Click **Close** to return to the main screen.

9. Click **Download**.

   The photo downloads to your computer.
Chapter 5

Post-Installation Tasks

This chapter outlines recommended and optional post-installation tasks for SafeSync.

Topics in this chapter include:

• About Adding MogileFS Storage on page 5-2
• Mounting Additional Disks on page 5-3
• Adding a Network Device on page 5-4
About Adding MogileFS Storage

When existing MogileFS partitions are used up, you can mount additional disks or storage partitions into the server. You may choose to add local disks or external network storage such as NFS, CIFS, or iSCSI.

**Important**
Ensure that the new storage has > 10 GB of storage space available.

SafeSync requires console command-line execution for adding storage devices. The deployment environment of SafeSync contains one or two servers: primary and secondary. The installation process detects all existing hard disks, formats the disks, mounts the disks to the file system, and then adds the disks to the MogileFS system. The mount points for disks in the file system are `/storage/mogdata/dev [primary: 1, secondary: 2] [number]`.

For example, the first disk on the primary server in the MogileFS system is mounted on `/storage/mogdata/dev11`, and the first disk on the secondary server is mounted on `/storage/mogdata/dev21`.

When creating new mount points for new MogileFS storage, mount the disks in the following sequence:

1. Primary server
   a. Second disk: `/storage/mogdata/dev12`
   b. Third disk: `/storage/mogdata/dev13`

2. Secondary server
   a. Second disk: `/storage/mogdata/dev22`
   b. Third disk: `/storage/mogdata/dev23`

**Important**
You cannot reuse a previously deleted mount point.
Mounting Additional Disks

SafeSync automatically mounts only one disk by default. Additional disks need to be manually mounted to SafeSync.

The example below assumes that SafeSync is deployed as a set of paired appliances, and the primary server already has one disk installed. This example describes how to add a new disk to the primary server.

Note
These steps are only required if you want to use more than one disk.

Procedure

1. Log on to SafeSync.
2. Obtain the root permission by typing the following command:
   
   ```
   sudo -i
   ```
3. Specify the root password.
4. Run the following script to mount the new disk:
   
   ```
   bash /opt/SingleInstaller/nodeControl/bin/add-disk-to-mogile.bash sdb
   ```

   Note
   This example uses “sdb” as the new disk name.
5. Check the result by typing the following command:

   ```
   mogadm check
   ```
Adding a Network Device

**WARNING!**
Trend Micro recommends using only network storage to expand SafeSync, because local, externally-mounted storage devices have a high risk of data loss if they are unexpectedly removed.

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

**Important**
- Ensure that you obtain the root permission when running the following commands.
- Use the following format to represent the disk name: dev [primary: 1, secondary: 2] [number]
  For example, use dev12 for the second disk mounted on the primary server and dev23 for the third disk mounted on the secondary server.

**Procedure**
1. Log on to SafeSync.
2. Obtain the root permission by typing the following command:
   ```bash
   sudo -i
   ```
3. Specify the root password.
4. Install the NFS-common portmap by typing the following command in a command line editor:
   ```bash
   apt-get install nfs-common portmap
   ```
5. Restart the portmap by typing the following command:
   ```bash
   service portmap restart
   ```
6. Create a new mount point on the server by typing the following command:

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

**Note**
This procedure uses /storage/mogdata/dev13 as an example.

7. Query the NFS mount path information on the remote NFS server by typing the following command:

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

8. Mount a new device to the mount point by typing the following command:

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

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

9. Change the owner of /storage/mogdata/dev13 by typing the following command:

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

10. Give /storage/mogdata/dev13 group authority to write by typing the following command:

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

11. 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. Type the following command:

```
vim /usr/local/share/perl/5.14.2/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`;`.
c. Save the file and close “vim”.

12. Add a mount point to MogileFS by typing the following command:

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

13. Restart mogstored by typing the following command:

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

14. Check the result by typing the following command:

```bash
mogadm check
```

15. Use the NFS mount command at `/etc/rc.local` to auto-mount storage located on NFS after the system reboots by typing the following command:

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

### Samba (Mount CIFS)

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

---

**Important**

- Ensure that you obtain the root permission when running the following commands.
- Use the following format to represent the disk name: dev [primary: 1, secondary: 2] [number]

For example, use dev12 for the second disk mounted on the primary server and dev23 for the third disk mounted on the secondary server.
Procedure
1. Log on to SafeSync.
2. Obtain the root permission by typing the following command:
   
   ```bash
   sudo -i
   ```
3. Specify the root password.
4. Install SMBFS by typing the following command in a command line editor:
   
   ```bash
   apt-get install smbfs
   ```
5. 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. Type the following command:
      
      ```bash
      vim /usr/local/share/perl/5.14.2/Mogstored/ChildProcess/DiskUsage.pm
      ```
   b. Go to line 58, which should contain the string
      
      ```perl
      my $rval = `df $gnu_df -l -k $path/$devnum`;
      ```
      and change the string to
      
      ```perl
      my $rval = `df $gnu_df -k $path/$devnum`;
      ```
   c. Save the file and close “vim”.
6. Change the permissions on the mogstored service.
   a. Edit `/etc/init.d/mogstored` by typing the following command:
      
      ```bash
      vim /etc/init.d/mogstored
      ```
   b. Replace `--chuid mogstored` with `--chuid www-data`.

---

**Tip**

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

---

**Note**

You must modify lines 41 and 61.
c. Save the file and close “vim”.

7. Create a new mount point on the server by typing the following command:

   `mkdir /storage/mogdata/dev14`

   **Note**
   - This procedure uses /storage/mogdata/dev14 as an example.

8. Find out the UID of www-data.
   a. Type the following command:

   `vim /etc/passwd www-data uid gid`

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

   The text to the right of www-data should look something like `:x:33:33:www-data:var/www:/bin/sh`. The number in the middle of `x:33:33` tells us that, in this case, the UID of www-data is 33. You can ignore the GID and other information.

9. Mount CIFS by typing the following command:

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

   **Note**
   - Give the appropriate network user name and password for XXXXX. Use the UID for www-data you found above in place of 33.
   - /tmp is the shared folder name of the CIFS mount path.

10. Use the “vim” editor to change /etc/fstab so it contains the CIFS data.
   a. Type the following command:

   `vim /etc/fstab`

   b. Add a line to /etc/fstab with the CIFS data by typing the following command:
//<IP address>/tmp /storage/mogdata/dev/14 cifs
username=XXXXX,password=XXXXX,uid=33 0 0

---

**Note**

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

---

11. Add a mount point for the new server to MogileFS and set the status to “alive” by typing the following command:

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

12. Check the result by typing the following command:

   ```
   mogadm check
   ```

---

**iSCSI**

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

---

**Important**

- Ensure that you obtain the root permission when running the following commands.
- Use the following format to represent the disk name: dev [primary: 1, secondary: 2] [number]

  For example, use dev12 for the second disk mounted on the primary server and dev23 for the third disk mounted on the secondary server.

---

**Procedure**

1. Log on to SafeSync.

2. Obtain the root permission by typing the following command:

   ```
   sudo -i
   ```
3. Specify the root password.

4. Install Open-iSCSI by typing the following command in a command line editor:

   `apt-get install open-iscsi`

5. Use the “iscsiadm discovery” tool to get the iSCSI target name.

   Type the following command:

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

   The following result appears:

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

6. (Skip this step if you already configured the Challenge-Handshake Authentication Protocol (CHAP) authentication settings for the iSCSI target.) Configure the CHAP authentication settings by adding the following information to the `/etc/iscsi/iscsid.conf` file:

   `discovery.sendtargets.auth.authmethod = CHAP`
   `discovery.sendtargets.auth.username = [SafeSync user name]`
   `discovery.sendtargets.auth.password = [SafeSync password]`
   `node.session.auth.authmethod = CHAP`
   `node.session.auth.username = [SafeSync user name]`
   `node.session.auth.password = [SafeSync password]`

7. Log on using the iSCSI target name.

   Type the following command:

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

   The following result appears:

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

8. Check the iSCSI disk name by typing the following command:

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

   The disk name appears as `../../sdd`.

   **Note**
   
   This procedure uses `/sdd` as an example.

9. Add a new partition for the disk `/dev/sdd` (sdd is an iSCSI disk) by typing the following commands:

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

10. Format the file system for `/dev/sdd1` (sdd1 is the new partition) by typing the following command:

    `mkfs.ext4 /dev/sdd1`

11. Create a new mount point for the server by typing the following command:

    `mkdir /storage/mogdata/dev15`

    **Note**
    
    This procedure uses `/storage/mogdata/dev15` as an example.

12. Test the mount by typing the following command:

    `mount /dev/sdd1 /storage/mogdata/dev15`

13. Change the owner of `/storage/mogdata/dev15` by typing the following command:

    `chown www-data:mogstored /storage/mogdata/dev15`
14. Change the file mode of `/storage/mogdata/dev15` by typing the following command:

   `chmod g+w /storage/mogdata/dev15`

15. Add a mount point to MogileFS by typing the following command:

   `mogadm --trackers=tracker1:6001 device add osdp-storel 15 --status=alive`

16. Use the “vim” editor to change `/etc/fstab` so it contains the iSCSI data.
   a. Type the following command:

      `vim /etc/fstab`

   b. Add a line to `/etc/fstab` with the iSCSI data by typing the following command:

      `/dev/sdd1 /storage/mogdata/dev15 ext4 defaults,user_xattr,_netdev 1 2`

17. Set iSCSI auto startup by typing the following command:

   `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.

18. Check the result by typing the following command:

   `mogadm check`
Chapter 6

Frequently Asked Questions (FAQs)

This chapter answers various Frequently Asked Questions.

Topics in this chapter include:

- *Apache Server on page 6-2*
- *DNS Settings on page 6-2*
Apache Server

What should I do if the Apache server does not start after installing SafeSync?

When the Apache server does not start after installation, the following error message appears:

* Starting web server apache2[Fri Dec 14 20:56:06 2012] [error] Can't open /var/log/osdp/osdp.log (Permission denied) at /usr/local/share/perl/5.10.1/Log/Log4perl/Appender/File.pm line 103.
Compilation failed in require at /opt/TrendMicro/OSDP/Lib/Storage/ForkControl.pm line 4.
BEGIN failed--compilation aborted at /opt/TrendMicro/OSDP/Lib/Storage/ForkControl.pm line 4.
Compilation failed in require at /opt/TrendMicro/OSDP/Config/startup.pl line 4.
BEGIN failed--compilation aborted at /opt/TrendMicro/OSDP/Config/startup.pl line 4.
Compilation failed in require at (eval 2) line 1.

This error occurs when the minimum system requirements are not met during installation.

To resolve this issue, make sure your environment meets the minimum system requirements. For more information, see *System Requirements on page 2-2*.

DNS Settings

Why am I unable to connect to the Administrator Console?

Creating proper DNS records is a critical part of SafeSync deployment. If these are not created correctly, users will not be able to access SafeSync.
For more information, see *Required Network Settings on page 2-5*
Chapter 7

Contacting Technical Support

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

Topics in this chapter include:

- Contacting Trend Micro on page 7-2
- Speeding Up the Support Call on page 7-2
Contacting Trend Micro

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

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

- Worldwide support offices:
  

- Trend Micro product documentation:
  
  http://docs.trendmicro.com

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
Index

A
about SafeSync, 1-2
Activation Code, 2-2

C
changing password, 3-11, 3-18
considerations
fresh installation, 2-3

D
dashboard
  System Status Alert widget, 4-3
  widgets, 4-3
default password, 3-10, 3-17
  changing, 3-11, 3-18
documentation, iv

F
fresh installation
  considerations, 2-3

H
high availability, 2-6, 3-11, 3-18

I
installation
  ISO, 3-2
  methods, 1-3, 3-2
  OVF, 3-11
  verifying, 4-4
ISO installation, 1-3, 3-2

O
OVF installation, 1-3, 3-2, 3-11

P
password
  changing, 3-11, 3-18
  default, 3-10, 3-17
  server system account, 3-8, 3-16
  primary server, 2-6

R
Registration Key, 2-2

S
SafeSync
  about, 1-2
  documentation, iv
  system requirements, 2-2
  terminology, vi
secondary server, 2-6
server
  system account password, 3-8, 3-16
  support
    resolve issues faster, 7-2
  system account password, 3-8, 3-16
  system requirements, 2-2
System Status Alert widget, 4-3

T
terminology, vi

V
verifying installation, 4-4
virtual IP address, 2-6
VMware installation
  ESXi version, 2-2
  WorkStation version, 2-2

W
widgets
  System Status Alert, 4-3