# 2.1 SafeSync for Enterprise

## Service Pack 1

## Installation Guide

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

Protected Cloud

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

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

Document Part No.: APEM26485/140711

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

# Table of Contents

## Preface

## Chapter 1: Introducing SafeSync

## Chapter 2: Preparing for Installation

## Chapter 3: Installing SafeSync

## Chapter 4: Installing on Virtual Machines

## Chapter 5: Verifying Installation

## Chapter 6: Post-Installation Tasks

## Chapter 7: Frequently Asked Questions (FAQs)

## Chapter 8: Contacting Technical Support

## Index

# Preface

## Preface

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

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:<br>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<br>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<br>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 in this chapter 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.<br>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.<br>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.<br>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.<br>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<br>• 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<br>• Secure file sharing<br>• 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<br>• Log maintenance<br>• Syslog server settings |
| Administration | • System updates<br>• 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.<br>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

## Preparing for Installation

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

Topics in this chapter include:

# System Requirements

The following table provides the system requirements for using SafeSync.

**TABLE 2-1. System Requirements**

| HARDWARE/SOFTWARE | DESCRIPTION |
|---|---|
| Network switch | 1 GB |
| CPU | 64-bit x86 (dual-core recommended) |
| Memory | 8 GB (32 GB recommended) |
| Network card | Two NICs (1 GB recommended) |
| System disk space | 60 GB (for SafeSync installation) |
| Storage disk space | The disk storage size is dependent on user requirements.<br>**Tip**<br>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. |
| Virtual machine | • VMware ESXi™ 4.x, 5.x<br>• VMware® WorkStation™ 6.x, 7.x or above<br>• Oracle VM VirtualBox™ 4.2.x<br>• Microsoft Hyper-V™ 6.2.9200.16384 |

# Registration Key and Activation Codes

During installation, specify the Activation Codes for the following:

- 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 8-2*.

**Note**

For questions about registration, refer to:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

# Fresh Installation Considerations

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

- *Required Network Settings on page 2-4*
- *High Availability on page 2-7*
- *Network Interface Cards on page 2-10*
- *Ports Used by SafeSync on page 2-11*

## Servers

SafeSync uses the following servers.

**TABLE 2-2. SafeSync Servers**

| SERVER | DESCRIPTION |
|---|---|
| SafeSync | Storage space for installing SafeSync<br>You can choose to install SafeSync on a bare metal server or a virtual machine.<br>For more information, see *Installing SafeSync on page 3-1* and *Installing on Virtual Machines on page 4-1*. |
| Domain Name System (DNS) | Server for storing the DNS records or network settings used by SafeSync<br>For more information, see *Required Network Settings on page 2-4*. |
| SMTP | Email server for sending system notifications<br>Configure the SMTP server and system notification settings from the SafeSync administrator console.<br>For more information, see the *SafeSync Administrator's Guide*. |
| Proxy | Server that acts as an intermediary between the SafeSync server or clients and the Internet<br>If the network requires that SafeSync uses a proxy server, configure the proxy server from the administrator console.<br>For more information, see the *SafeSync Administrator's Guide*. |

## Required Network Settings

SafeSync requires the following network settings.

**TABLE 2-3. Required Network Settings**

| DNS RECORD | DESCRIPTION |
|---|---|
| <subdomain>.<your_domain>.com | Used for domain mapping |
| www.<subdomain>.<your_domain>.com | Used for accessing services |

| DNS Record | Description |
|---|---|
| soap.<subdomain>.<your_domain>.com | Used for connections between SafeSync server and clients |
| dav.<subdomain>.<your_domain>.com | Used for connections between SafeSync server and clients |

**Important**

SafeSync requires a fully qualifiied domain name (FQDN).

For example, if your domain is company and your subdomain is safesync, you will need the following network settings.

- safesync.company.com
- www.safesync.company.com
- soap.safesync.company.com
- dav.safesync.company.com

**Note**

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

## Single-Server Deployment

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

**Table 2-4. Required DNS Settings for Single-Server Deployment**

| FQDN | Type | Data |
|---|---|---|
| <subdomain>.<your_domain>.com | Sub-domain | Primary Server IP<br>For example, 10.20.30.234 |

| FQDN | Type | Data |
|---|---|---|
| www.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |
| soap.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |
| dav.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |

## High Availability Deployment

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

**Table 2-5. Required DNS Settings for High Availability Deployment**

| FQDN | Type | Data |
|---|---|---|
| <subdomain>.<your_domain>.com | Sub-domain | Primary Server IP<br>For example, 10.20.30.234 |
| www.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |
| soap.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |
| dav.<subdomain>.<your_domain>.com | Host (A) | Primary Server IP<br>For example, 10.20.30.234 |
| www.<subdomain>.<your_domain>.com | Host (A) | Secondary Server IP<br>For example, 10.20.30.235 |
| soap.<subdomain>.<your_domain>.com | Host (A) | Secondary Server IP<br>For example, 10.20.30.235 |

| FQDN | TYPE | DATA |
|---|---|---|
| dav.<subdomain>.<your_domain>.com | Host (A) | Secondary Server IP<br>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, the second network interface card (NIC) of the primary server must be connected to the second NIC of the secondary server using a network switch. Use a standalone switch for bare metal server installations and a virtual switch for virtual machine installations.

**TABLE 2-6. Primary and Secondary Servers**

| SERVER | DESCRIPTION |
|---|---|
| Primary server | • Always installed first<br>• Configuration and testing of the primary server must be completed before setting up the secondary server |
| Secondary server | • Installed after configuring and verifying the primary server<br>• Does not need to be configured<br>• Primary server settings are replicated during the installation of the secondary server |

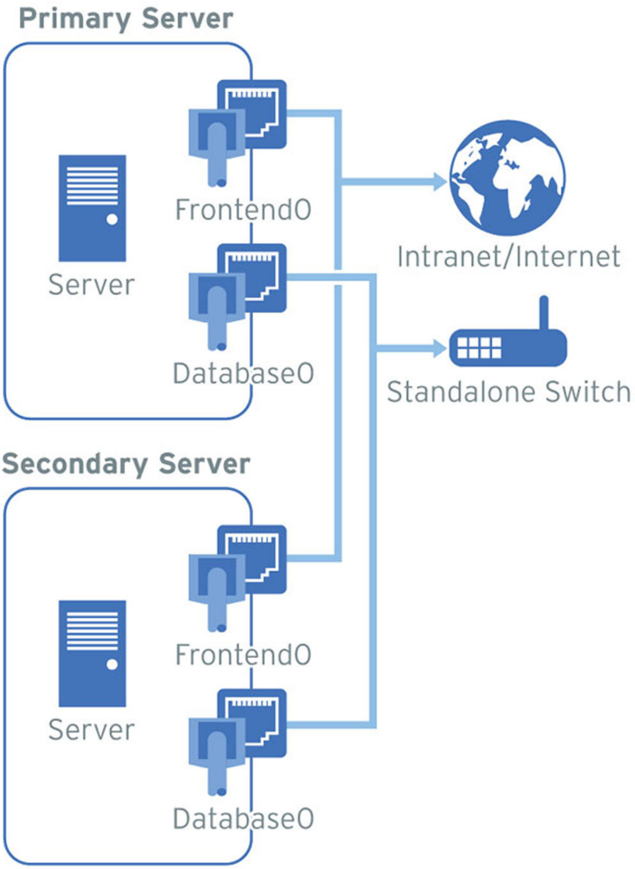


**FIGURE 2-1. High Availability Deployment on Bare Metal Servers**

You may use either file replication or load balancing to achieve high availability in SafeSync.

For more informaion, see *File Replication on page 2-9* and *Load Balancing on page 2-9*.

## 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 two network interface cards (NICs) during installation. The first NIC must be connected to the Internet and/or Intranet. The second NIC must be connected to a network switch. Both NICs must be connected to the right switch during installation.

**Note**

In a high availability deployment, the second NIC of the primary server must be connected to the second NIC of the secondary server.

For more information, see *High Availability on page 2-7*.

## Roles of the Network Interface Cards

SafeSync requires two network interface cards (NICs) for each server. The first NIC is labeled as `frontend0` and the second NIC is labeled as `database0`.

The following table describes the roles of the two NICs.

**TABLE 2-7. NIC Roles**

| LABEL | DESCRIPTION |
|---|---|
| `frontend0` | • Assigned to the first available NIC on the server<br>• Should be connected to the Internet and/or Intranet<br>• The IP addess, subnet, gateway, and DNS server settings are configured during installation<br>• Settings can be changed from the administrator console after installation<br>• Serves as the data port<br>**Note**<br>It is used for communication with other hosts or devices, clients, and users in the network. |

| Label | Description |
|---|---|
| `database0` | • Assigned to the second NIC on the server<br>• Should be connected to a network switch<br>**Note**<br>In a high availability deployment, the second NIC of the primary server must be connected to the second NIC of the secondary server using a network switch. Use a standalone switch for bare metal server installations and a virtual switch for virtual machine installations.<br>• The IP address and subnet are automatically assigned during installation<br>  • For appliance1: 192.168.200.1<br>  • For appliance2: 192.168.200.2<br>**Tip**<br>Trend Micro recommends reserving the network segment with an IP range of 192.168.200.x for SafeSync to avoid conflicts with `database0`.<br>• The IP address settings for this NIC should not be changed<br>• Serves as the database communication port<br>**Note**<br>It is used for database communication and replication traffic between the two servers. |

## Ports Used by SafeSync

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

| Port | Protocol | Function | Purpose |
|---|---|---|---|
| 22 | TCP | Inbound | SafeSync uses this port to:<br>• Allow the administrator to gain remote access to the servers<br>• Establish communication between the primary and secondary servers |
| 80 | TCP | Inbound and Outbound | SafeSync uses this port to:<br>• Connect to the Smart Protection Network or the local Smart Protection Server<br>• Update components by connecting to the ActiveUpdate server<br>• Connect to SafeSync services |
| 443 | TCP | Inbound and Outbound | SafeSync uses this port to:<br>• Connect to all services<br>• Access the administrator console through HTTPS<br>• Access the end-user portal through HTTPS<br>• Connect to SafeSync clients |
| 3443 | TCP | Inbound | SafeSync uses this port to request HTTP access to the administrator console.<br>**Note**<br>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:

  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

# 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.

| KEYBOARD KEY | OPERATION |
|---|---|
| Left and Right arrows | Move between buttons<br>Buttons are enclosed in angle brackets <>. |
|  | Move between characters in a text box |
| Enter | Click the highlighted button |
| Space bar | Select the highlighted item from a choice list |

# Chapter 3

## Installing SafeSync

This chapter explains how to install SafeSync on bare metal servers.

Topics in this chapter include:

# Installing a SafeSync Appliance

Install SafeSync on a bare metal server. The following procedure explains the required steps when installing a single server or when installing the first server in a high availability deployment.

**WARNING!**

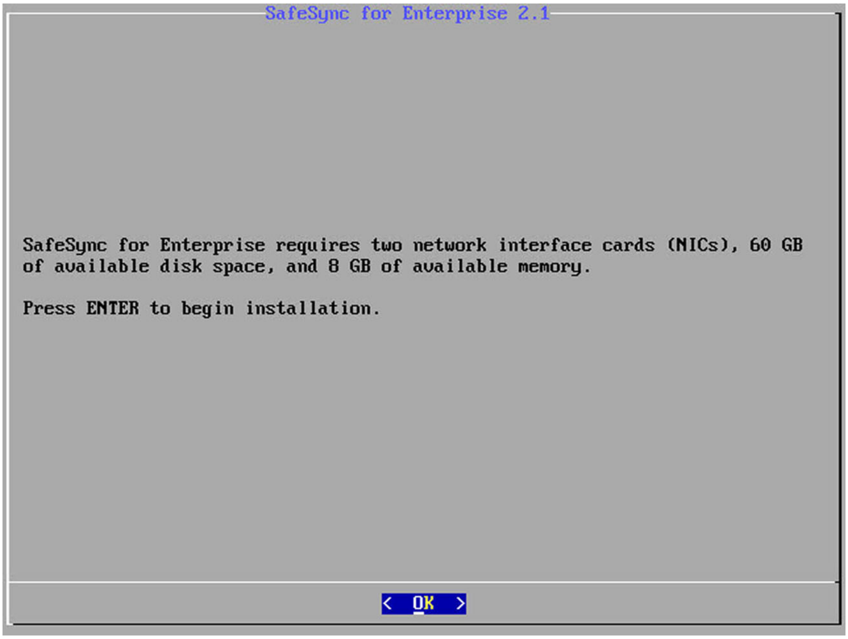
Any existing data or partitions are removed during the installation process. Back up any existing data on the server before installing SafeSync.

### Procedure

1. On a bare metal server, insert the installation DVD into the DVD drive.

2. Power on the bare metal server.

A prompt appears with information about installing SafeSync.

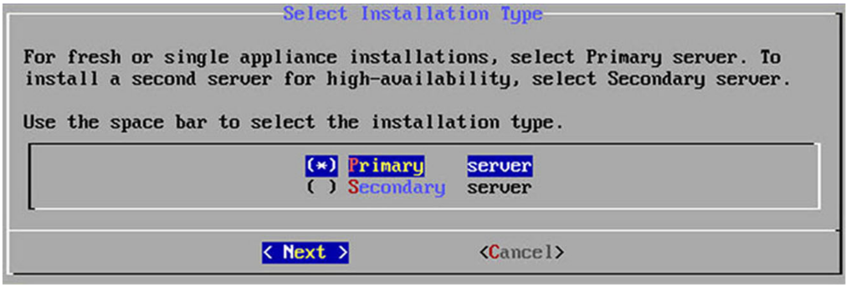


```
SafeSync for Enterprise 2.1

SafeSync for Enterprise requires two network interface cards (NICs), 60 GB
of available disk space, and 8 GB of available memory.

Press ENTER to begin installation.
```

**FIGURE 3-1. SafeSync for Enterprise Installation screen**

3. Select **OK**.

The **Select Installation Type** screen appears.



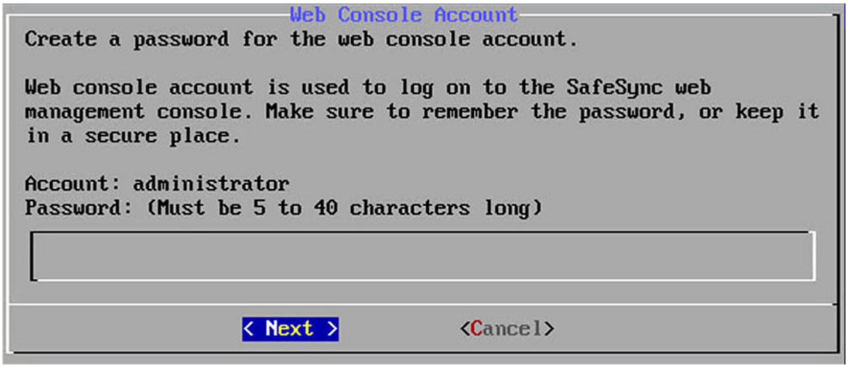
```
Select Installation Type

For fresh or single appliance installations, select Primary server. To
install a second server for high-availability, select Secondary server.

Use the space bar to select the installation type.

(*) Primary     server
( ) Secondary   server
```

**FIGURE 3-2. Select Installation Type screen**

4. Select **Primary server** to install a single server or to install the first server in a high availability deployment.

5. Select **Next**.

   The **Web Console Account** screen displays.



```
Create a password for the web console account.

Web console account is used to log on to the SafeSync web
management console. Make sure to remember the password, or keep it
in a secure place.

Account: administrator
Password: (Must be 5 to 40 characters long)
```

**FIGURE 3-3. Web Console Account screen**

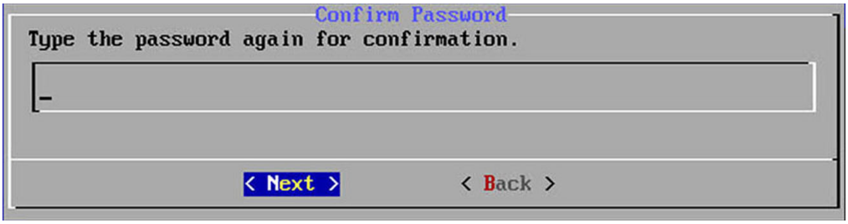
6. Type a password for the web console account.

**Note**

The web console account password is used to log on to the administrator web console.

7. Select **Next**.

   The **Confirm Password** screen displays.

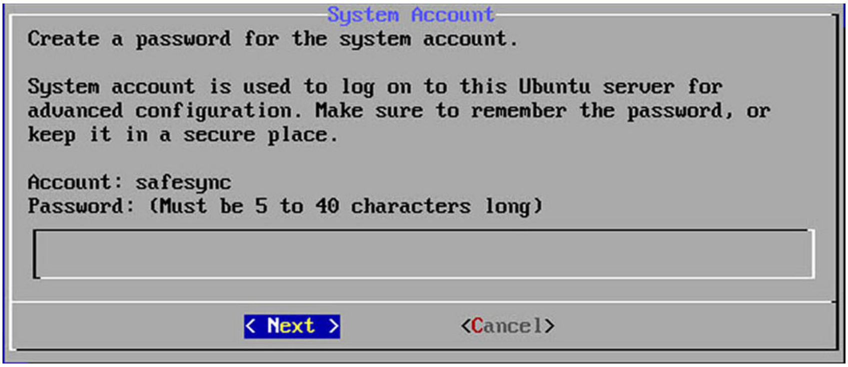


```
Type the password again for confirmation.
```

**FIGURE 3-4. Confirm Password screen**

8. Retype the password and select **Next**.

   The **System Account** screen displays.



```
System Account
Create a password for the system account.

System account is used to log on to this Ubuntu server for
advanced configuration. Make sure to remember the password, or
keep it in a secure place.

Account: safesync
Password: (Must be 5 to 40 characters long)
```

**FIGURE 3-5. System Account screen**

9. Type a password for the server system account.

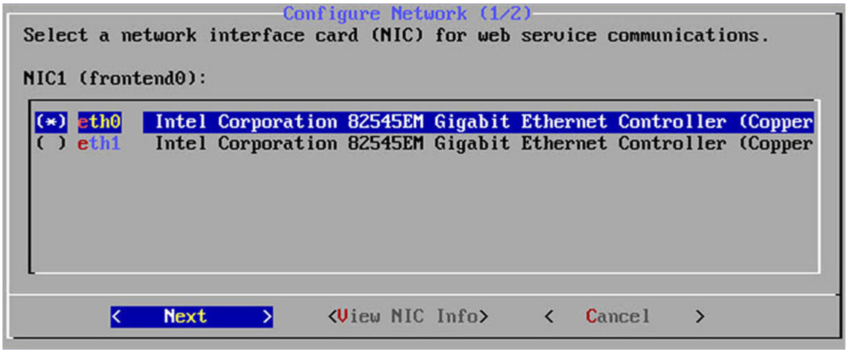
> **Note**
>
> The system account password is used to log on to the command line console of the SafeSync server.

10. Select **Next**.

    The **Confirm Password** screen displays.

11. Retype the password and select **Next**.

The **Configure Network (1/2)** screen displays.

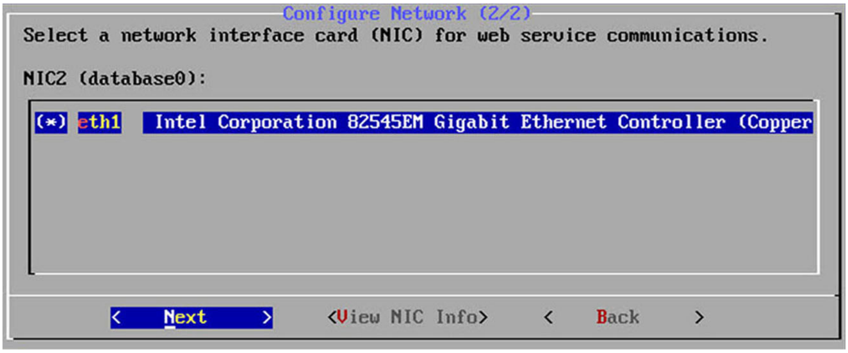


```
Configure Network (1/2)
Select a network interface card (NIC) for web service communications.

NIC1 (frontend0):

(*) eth0   Intel Corporation 82545EM Gigabit Ethernet Controller (Copper
( ) eth1   Intel Corporation 82545EM Gigabit Ethernet Controller (Copper
```

**FIGURE 3-6. Configure Network (1/2) screen**

12. Select a network interface card for `NIC1 (frontend0)`.

The **Configure Network (2/2)** screen displays.



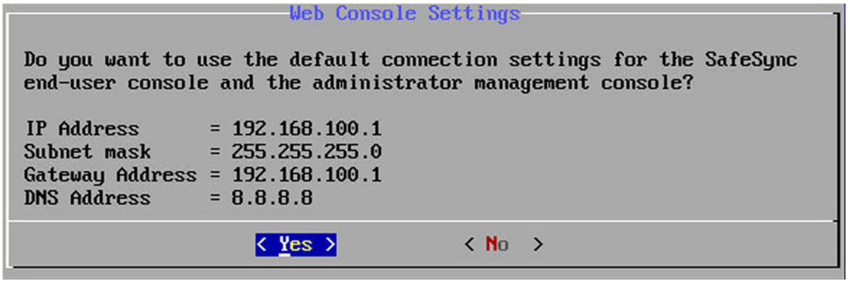
```
Configure Network (2/2)
Select a network interface card (NIC) for web service communications.

NIC2 (database0):

(*) eth1   Intel Corporation 82545EM Gigabit Ethernet Controller (Copper
```

**FIGURE 3-7. Configure Network (2/2) screen**

13. Select a network interface card for `NIC2 (database0)`.

14. Select **Next**.

The **Web Console Settings** screen displays.



```
                         Web Console Settings

 Do you want to use the default connection settings for the SafeSync
 end-user console and the administrator management console?

 IP Address      = 192.168.100.1
 Subnet mask     = 255.255.255.0
 Gateway Address = 192.168.100.1
 DNS Address     = 8.8.8.8

                    < Yes >           < No  >
```

**FIGURE 3-8. Web Console Settings screen**

15. Select one of the following to determine the connection settings for the end-user portal and the administrator web console:

    - Select **Yes** to use the default connection settings.
    - Select **No** to modify the connection settings.

    **Note**

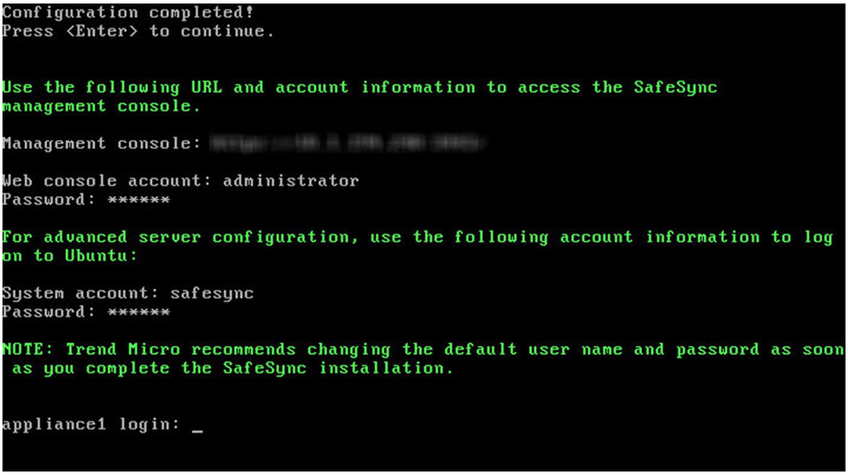
    If you choose to modify the default values, you must type the new connection settings before you can proceed with the installation process.

The installation process begins. An Ubuntu® Linux operating system is first installed on the server, and then SafeSync is installed.

**Note**

Depending on your environment, installation can take as long as 30 minutes up to one hour.

Once installation completes, the **Log On** screen for the command line console appears.



```
Configuration completed!
Press <Enter> to continue.

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

Management console: [redacted]

Web console account: administrator
Password: ******

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

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

NOTE: Trend Micro recommends changing the default user name and password as soon
 as you complete the SafeSync installation.


appliance1 login: _
```

**FIGURE 3-9. Configuration Completed screen**

**16.** Using a web browser, log on to the administrator web console (https://<SafeSync domain name>:3443) using the previously specified password.

# Installing SafeSync Appliances for a High Availability Deployment

Install a secondary server to enable the high availability feature of SafeSync.

**WARNING!**

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

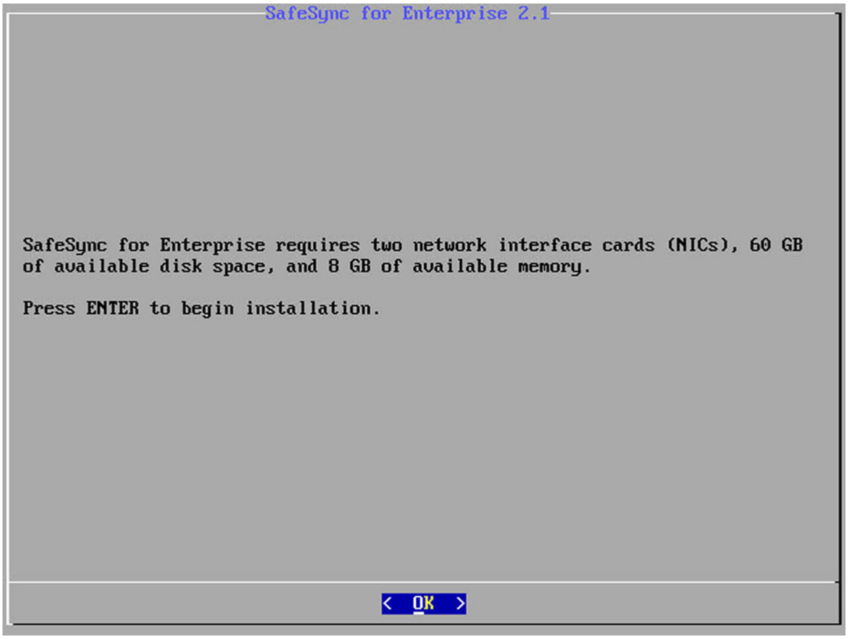
### Procedure

1. On a bare metal server, insert the installation DVD into the DVD drive of the secondary server.

> **Note**
>
> Make sure that the primary server is working before installing the secondary server. You cannot install a secondary server if the primary server is not yet installed.

2. Power on the bare metal server.

   A prompt appears with information about installing SafeSync.

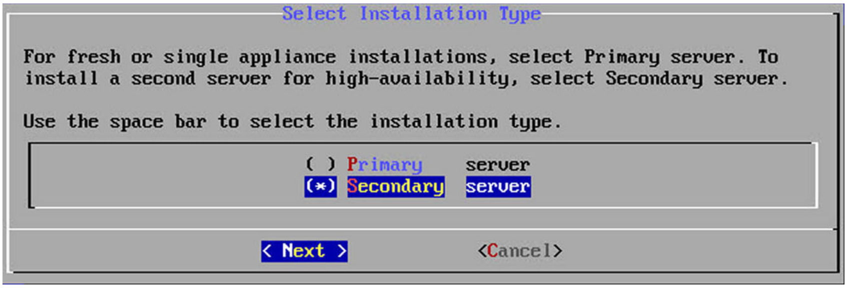


```
SafeSync for Enterprise 2.1

SafeSync for Enterprise requires two network interface cards (NICs), 60 GB
of available disk space, and 8 GB of available memory.

Press ENTER to begin installation.
```

**FIGURE 3-10. SafeSync for Enterprise Installation screen**

3. Select **OK**.

The **Select Installation Type** screen appears.



```
Select Installation Type

For fresh or single appliance installations, select Primary server. To
install a second server for high-availability, select Secondary server.

Use the space bar to select the installation type.

                    ( ) Primary    server
                    (*) Secondary  server

            < Next >              <Cancel>
```

**FIGURE 3-11. Select Installation Type screen**

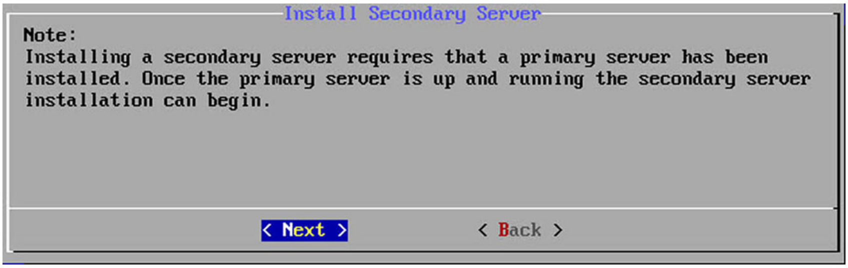
4. Select **Secondary server** to install the second server in a high availability deployment.

**Note**

Press the space bar to select the secondary server.

For more information, see *Basic Installer Operations on page 2-13*.

The **Install Secondary Server** screen displays.

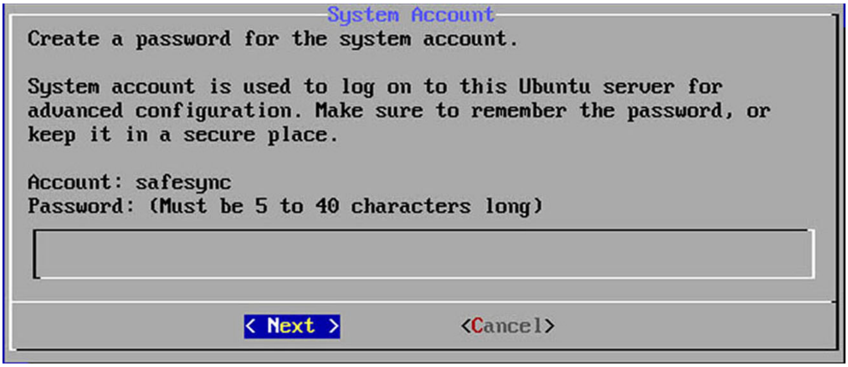


```
Install Secondary Server
Note:
Installing a secondary server requires that a primary server has been
installed. Once the primary server is up and running the secondary server
installation can begin.

            < Next >              < Back >
```

**FIGURE 3-12. Install Secondary Server screen**

5. Select **Next**.

The **System Account** screen displays.



```
System Account
Create a password for the system account.

System account is used to log on to this Ubuntu server for
advanced configuration. Make sure to remember the password, or
keep it in a secure place.

Account: safesync
Password: (Must be 5 to 40 characters long)
```

**FIGURE 3-13. System Account screen**

6. Type a password for the secondary server system account.

**Note**

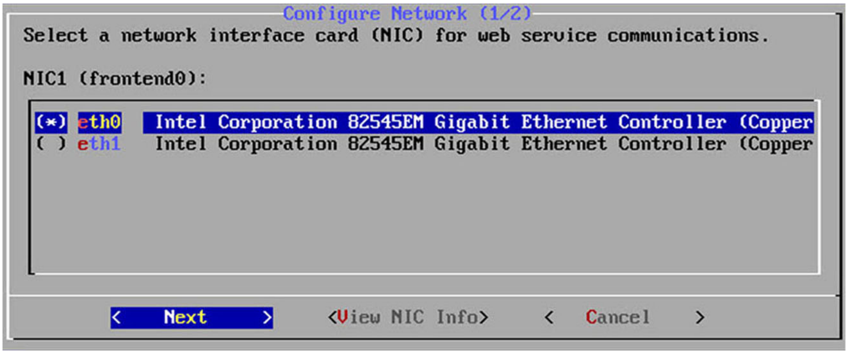
The system account password is used to log on to the command line console of the secondary SafeSync server.

7. Select **Next**.

   The **Confirm Password** screen displays.

8. Retype the password and select **Next**.

The **Configure Network (1/2)** screen displays.



```
Configure Network (1/2)
Select a network interface card (NIC) for web service communications.

NIC1 (frontend0):

(*) eth0   Intel Corporation 82545EM Gigabit Ethernet Controller (Copper
( ) eth1   Intel Corporation 82545EM Gigabit Ethernet Controller (Copper
```

**FIGURE 3-14. Configure Network (1/2) screen**

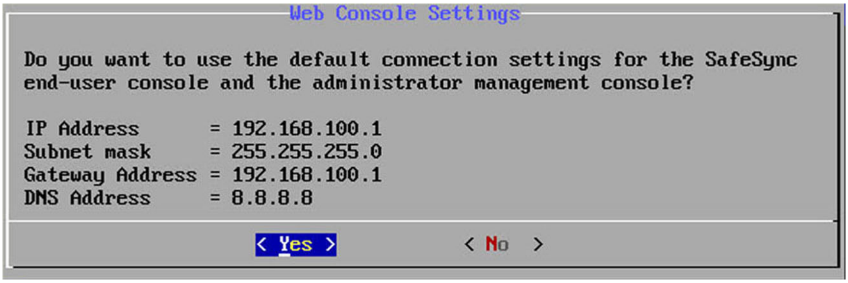
**9.** Select a network interface card for `NIC1 (frontend0)`.

The **Configure Network (2/2)** screen displays.

**10.** Select a network interface card for `NIC2 (database0)`.

**11.** Select **Next**.

The **Web Console Settings** screen displays.



```
Web Console Settings

Do you want to use the default connection settings for the SafeSync
end-user console and the administrator management console?

IP Address       = 192.168.100.1
Subnet mask      = 255.255.255.0
Gateway Address  = 192.168.100.1
DNS Address      = 8.8.8.8
```

**FIGURE 3-15. Web Console Settings screen**

**12.** Select one of the following to determine the connection settings for the end-user and management web consoles:

- Select **Yes** to use the default connection settings.
- Select **No** to modify the connection settings.

Once installation completes, the **Log On** screen for the command line interface appears.

# Chapter 4

## Installing on Virtual Machines

This chapter explains how to install SafeSync on virtual machines.

Topics in this chapter include:

- *Installing on VMware ESXi on page 4-2*
- *Installing on Microsoft Hyper-V on page 4-12*
- *Installing on a VMware Workstation on page 4-29*
- *Installing on an Oracle VM VirtualBox on page 4-50*

# Installing on VMware ESXi

When installing SafeSync on a VMware ESXi, the virtual machine requires the following:

| System | Minimum Requirement |
|---|---|
| Virtual machine | VMware ESXi™ 4.x, 5.x |
| CPU | 64-bit single core |
| RAM | 8 GB |
| Hard disk | 60 GB |
| Network cards | Two NICs (1 GB recommended) |

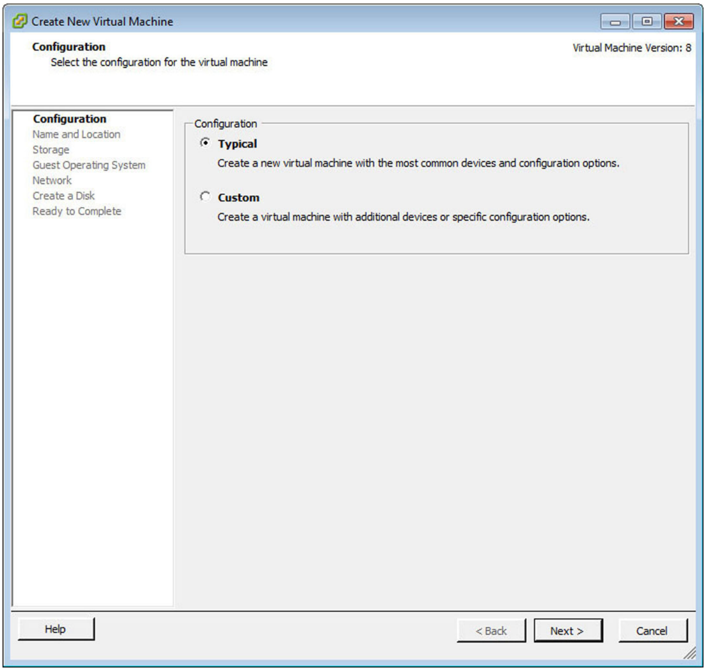
**Note**

The following procedure uses VMware ESXi 5.5.0 as an example.

**Procedure**

1. Launch VMware ESXi.
2. Select **File** > **New** > **Virtual Machine** from the menu.

The **Create New Virtual Machine** screen appears.



Create New Virtual Machine

**Configuration**
Select the configuration for the virtual machine

Virtual Machine Version: 8

Configuration

● **Typical**
Create a new virtual machine with the most common devices and configuration options.

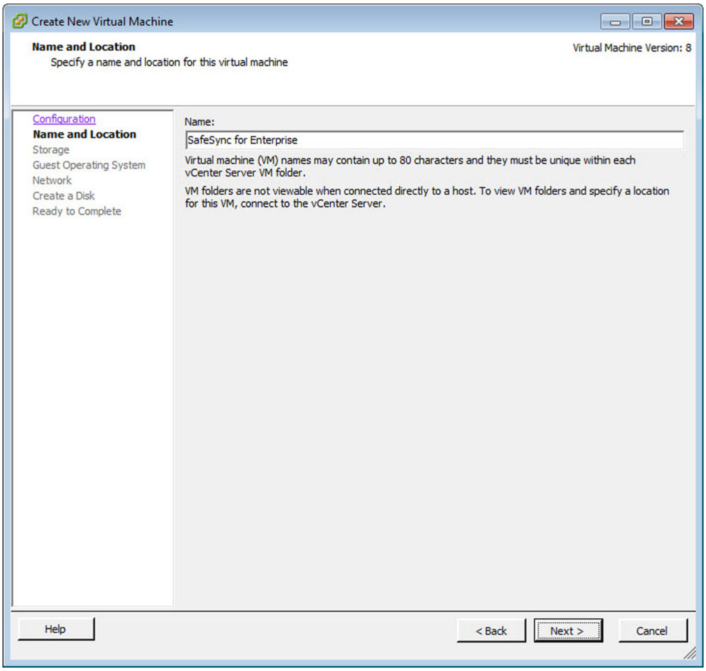
○ **Custom**
Create a virtual machine with additional devices or specific configuration options.

**FIGURE 4-1. Configuration screen**

3. Select **Typical**.

4. Click **Next**.

The **Name and Location** screen appears.



Create New Virtual Machine

**Name and Location**

Specify a name and location for this virtual machine

Virtual Machine Version: 8

Name: SafeSync for Enterprise

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

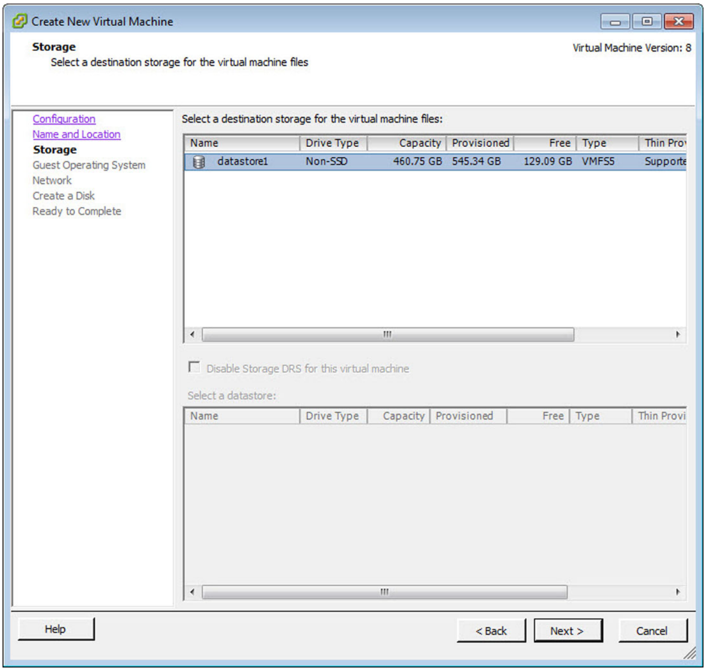
VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

**FIGURE 4-2. Name and Location screen**

5. Type a name for the virtual machine.

6. Click **Next**.

The **Storage** screen appears.



Create New Virtual Machine

**Storage**
Select a destination storage for the virtual machine files

Virtual Machine Version: 8

- Configuration
- Name and Location
- **Storage**
- Guest Operating System
- Network
- Create a Disk
- Ready to Complete

Select a destination storage for the virtual machine files:

| Name | Drive Type | Capacity | Provisioned | Free | Type | Thin Pro |
|---|---|---|---|---|---|---|
| datastore1 | Non-SSD | 460.75 GB | 545.34 GB | 129.09 GB | VMFS5 | Supporte |

☐ Disable Storage DRS for this virtual machine

Select a datastore:

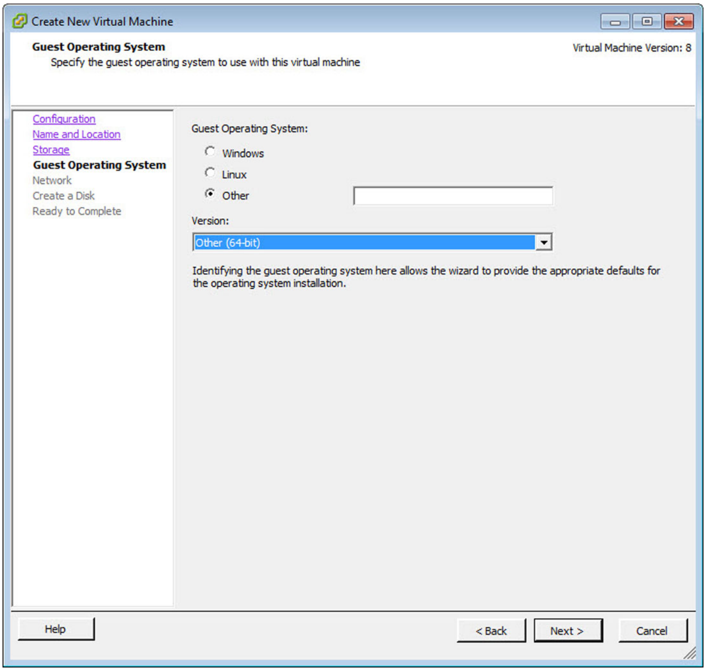
| Name | Drive Type | Capacity | Provisioned | Free | Type | Thin Provi |
|---|---|---|---|---|---|---|

**FIGURE 4-3. Storage screen**

7. Select a storage location for the virtual machine files.

8. Click **Next**.

The **Guest Operating System** screen appears.



Create New Virtual Machine

**Guest Operating System**

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 8

- Configuration
- Name and Location
- Storage
- **Guest Operating System**
- Network
- Create a Disk
- Ready to Complete

Guest Operating System:

○ Windows

○ Linux

● Other

Version: Other (64-bit)

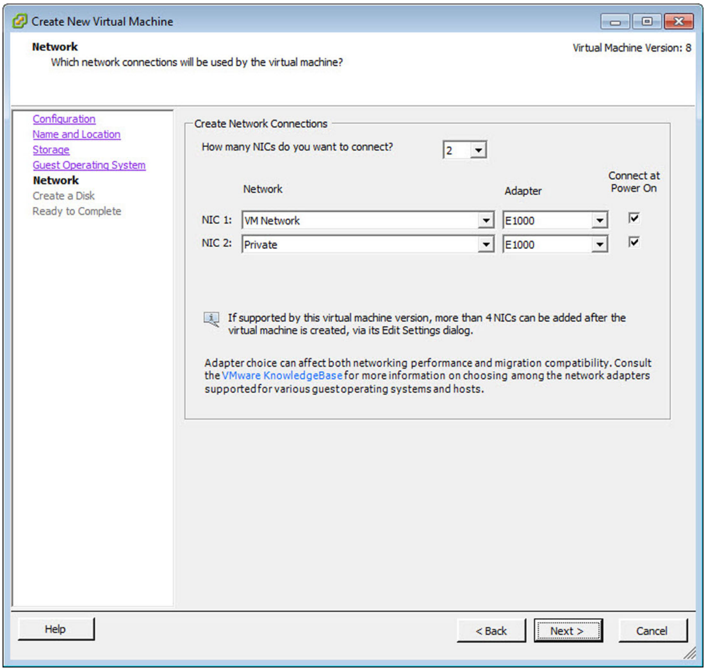
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

**FIGURE 4-4. Guest Operating System screen**

9. Select **Other** and choose **Other (64-bit)** from the drop-down list.

10. Click **Next**.

The **Network** screen appears.



Create New Virtual Machine

**Network**

Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

How many NICs do you want to connect? 2

|  | Network | Adapter | Connect at Power On |
|---|---|---|---|
| NIC 1: | VM Network | E1000 | ☑ |
| NIC 2: | Private | E1000 | ☑ |

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

**FIGURE 4-5. Network screen**

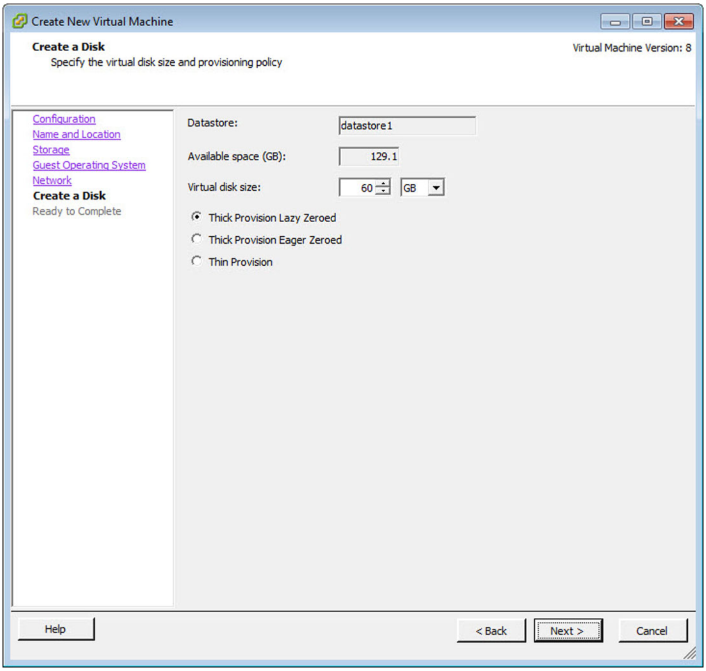
11. Select 2 NICs and specify the following settings.

**TABLE 4-1. Network Settings for SafeSync**

| NAME | NETWORK | ADAPTOR | CONNECT AT POWER ON |
|---|---|---|---|
| NIC 1 | VM Network<br>**Note**<br>The VM network is the virtual switch connected to the Internet and/or Intranet. This switch may have a different name in actual environments. | E1000 | Enabled |
| NIC 2 | Private<br>**Note**<br>The private network is the private virtual switch that is not connected to the Internet and Intranet. This switch may have a different name in actual environments. | E1000 | Enabled |

12. Click **Next**.

The **Create a Disk** screen appears.



Create New Virtual Machine

**Create a Disk**
Specify the virtual disk size and provisioning policy

Virtual Machine Version: 8

Datastore: datastore1

Available space (GB): 129.1

Virtual disk size: 60 GB

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

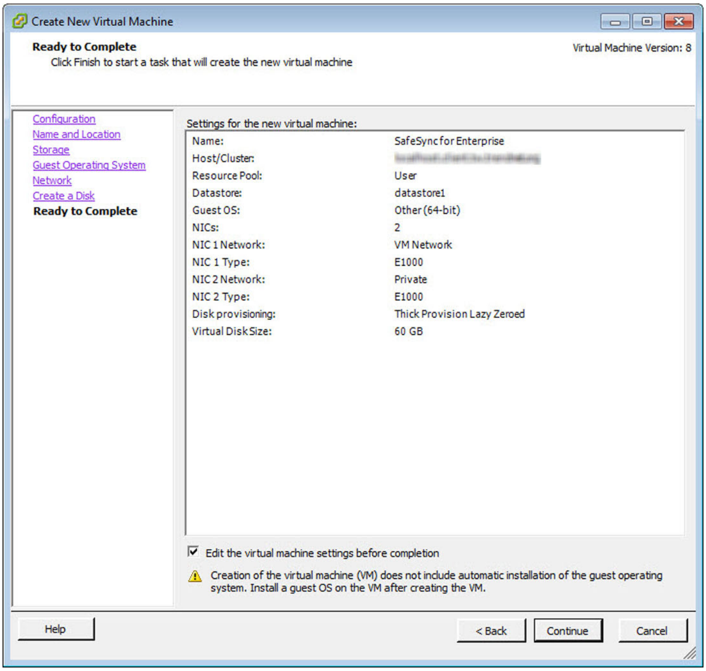
**FIGURE 4-6. Create a Disk screen**

13. Specify at least **60GB** of disk space for SafeSync.

14. Select **Thick Provision Lazy Zeroed**.

15. Click **Next**.

The **Ready to Complete** screen appears.



**Ready to Complete**

Click Finish to start a task that will create the new virtual machine

Virtual Machine Version: 8

Settings for the new virtual machine:

| | |
|---|---|
| Name: | SafeSync for Enterprise |
| Host/Cluster: | [redacted] |
| Resource Pool: | User |
| Datastore: | datastore1 |
| Guest OS: | Other (64-bit) |
| NICs: | 2 |
| NIC 1 Network: | VM Network |
| NIC 1 Type: | E1000 |
| NIC 2 Network: | Private |
| NIC 2 Type: | E1000 |
| Disk provisioning: | Thick Provision Lazy Zeroed |
| Virtual Disk Size: | 60 GB |

☑ Edit the virtual machine settings before completion

⚠ Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

**FIGURE 4-7. Ready to Complete screen**

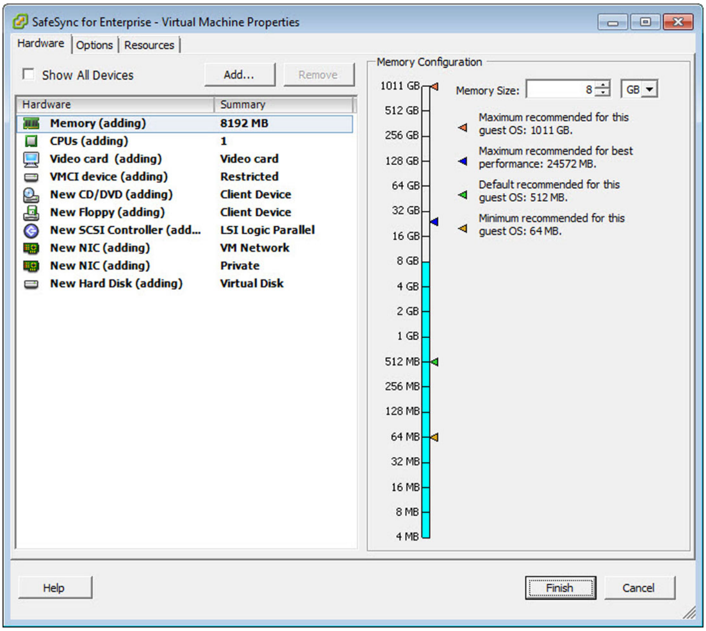
16. Select **Edit the virtual machine settings before completion**.

17. Verify the settings for the new virtual machine and then click **Continue**.

    The **Virtual Machine Properties** screen appears.

18. Open the **Hardware** tab and select **Memory (adding)**.

**Memory Configuration** appears in the right pane.



| Hardware | Summary |
|---|---|
| Memory (adding) | 8192 MB |
| CPUs (adding) | 1 |
| Video card (adding) | Video card |
| VMCI device (adding) | Restricted |
| New CD/DVD (adding) | Client Device |
| New Floppy (adding) | Client Device |
| New SCSI Controller (add... | LSI Logic Parallel |
| New NIC (adding) | VM Network |
| New NIC (adding) | Private |
| New Hard Disk (adding) | Virtual Disk |

Memory Size: 8 GB

Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 24572 MB.

Default recommended for this guest OS: 512 MB.

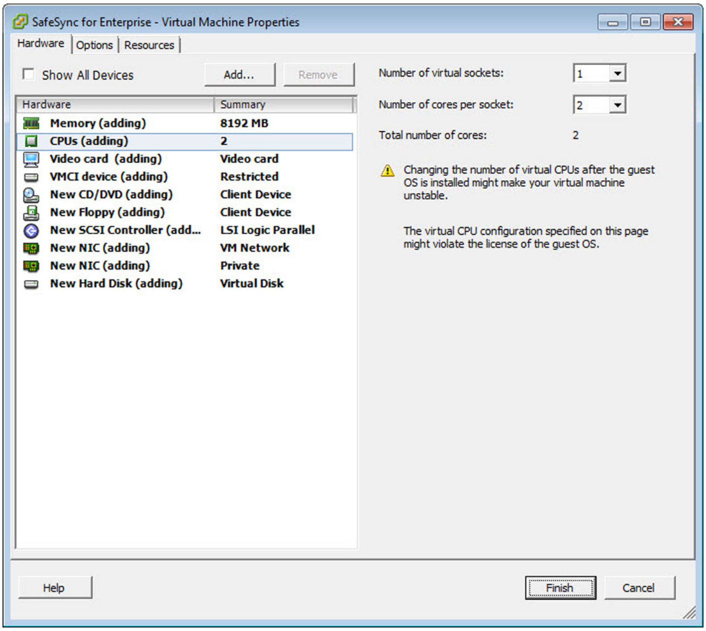
Minimum recommended for this guest OS: 64 MB.

**FIGURE 4-8. Memory Configuration screen**

19. In the **Memory Size** field, select at least 8 GB.

20. From the **Hardware** tab, select **CPU (adding)**.

CPU settings appear in the right pane.



□ Show All Devices

| Hardware | Summary |
|---|---|
| Memory (adding) | 8192 MB |
| CPUs (adding) | 2 |
| Video card (adding) | Video card |
| VMCI device (adding) | Restricted |
| New CD/DVD (adding) | Client Device |
| New Floppy (adding) | Client Device |
| New SCSI Controller (add... | LSI Logic Parallel |
| New NIC (adding) | VM Network |
| New NIC (adding) | Private |
| New Hard Disk (adding) | Virtual Disk |

Number of virtual sockets: 1

Number of cores per socket: 2

Total number of cores: 2

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

**FIGURE 4-9. CPUs (adding) screen**

21. In the **Number of virtual sockets** field, select **1**.

22. In the **Number of cores per socket** field, select **2**.

23. Click **Finish**.

    The virtual machine is created.

# Installing on Microsoft Hyper-V

Installing SafeSync on Microsoft Hyper-V requires the following:

| System | Minimum Requirement |
|---|---|
| Virtual machine | Microsoft Hyper-V™ 6.2.9200.16384 |
| CPU | 64-bit single core |
| RAM | 8GB |
| Hard disk | 60GB |
| Network cards | Two NICs (1GB recommended) |

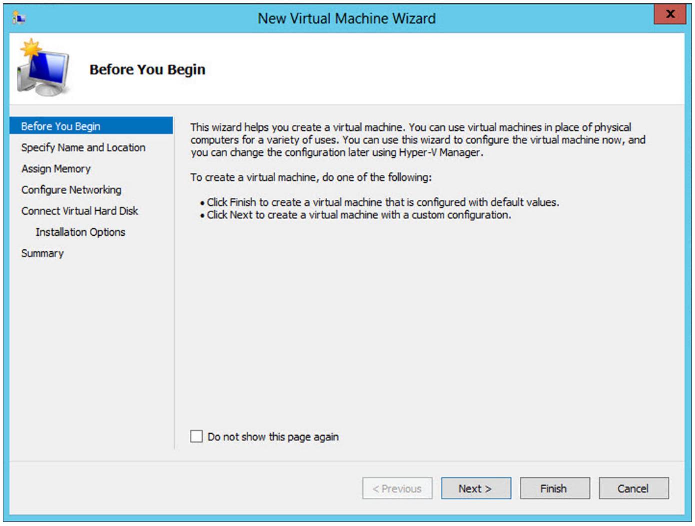
**Note**

The following procedure uses Microsoft Hyper-V 6.2.9200 as an example.

**Procedure**

1. Launch Hyper-V Manager.
2. Select the host server.
3. Click **Action** > **New** > **Virtual Machine** from the main menu.

   The **New Virtual Machine Wizard** screen appears.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

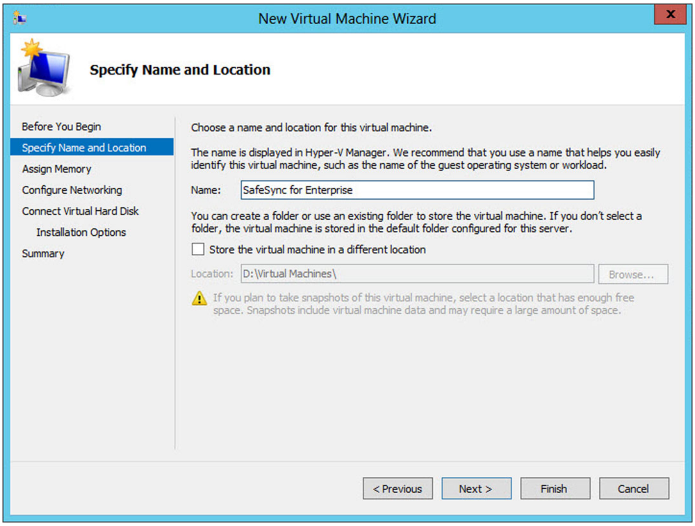
- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

□ Do not show this page again

**FIGURE 4-10. New Virtual Machine Wizard screen**

4. Click **Next**.

   The **Specify Name and Location** screen appears.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: SafeSync for Enterprise

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

□ Store the virtual machine in a different location

Location: D:\Virtual Machines\

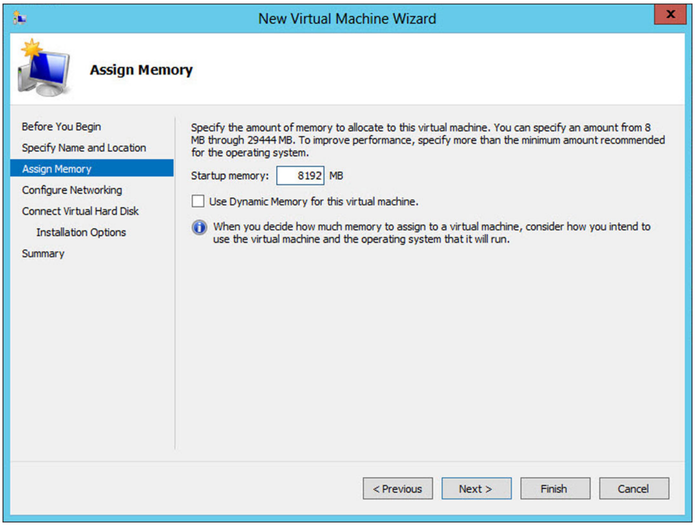
If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.

**FIGURE 4-11. Specify Name and Location screen**

5. Type a name for the virtual machine.

6. Click **Next**.

   The **Assign Memory** screen appears.



Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 29444 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 8192 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

**FIGURE 4-12. Assign Memory screen**

7. Specify at least 8GB of startup memory.

---

**Tip**

Trend Micro recommends allocating 32GB of startup memory for optimal performance.

---

8. Specify whether memory is allocated dynamically or not.

---

**Note**

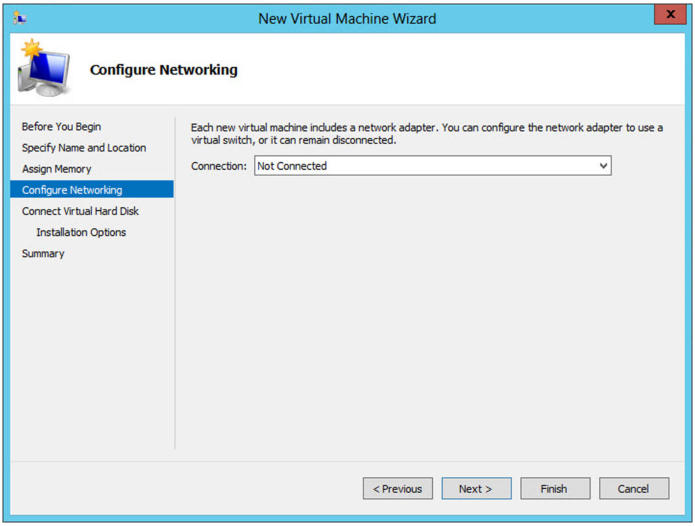
Dynamically allocated space is allocated as the space fills up.

Fixed memory only takes as much space as you allocate, but is often faster to use.

---

9. Click **Next**.

   The **Configure Networking** screen appears.



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

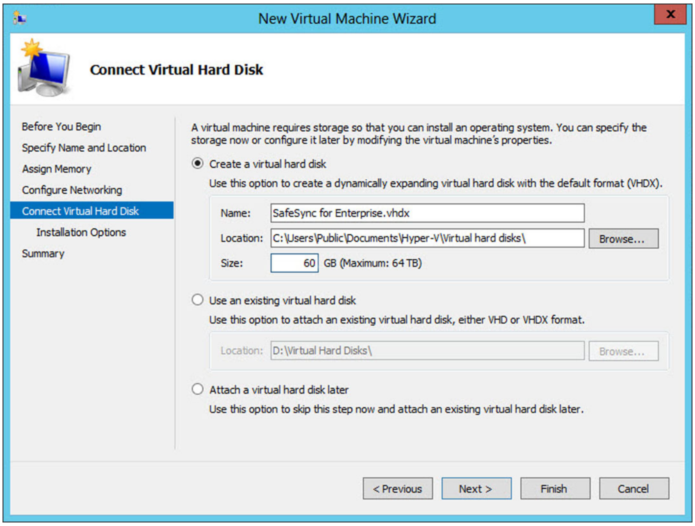
Connection: Not Connected

**FIGURE 4-13. Configure Networking screen**

10. Under **Connection**, select **Not Connected**.

11. Click **Next**.

    The **Connect Virtual Hard Disk** screen appears.



A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a dynamically expanding virtual hard disk with the default format (VHDX).

Name: SafeSync for Enterprise.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual hard disks\

Size: 60 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: D:\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

**FIGURE 4-14. Connect Virtual Hard Disk screen**

12. Specify at least **60GB** of disk space for SafeSync.

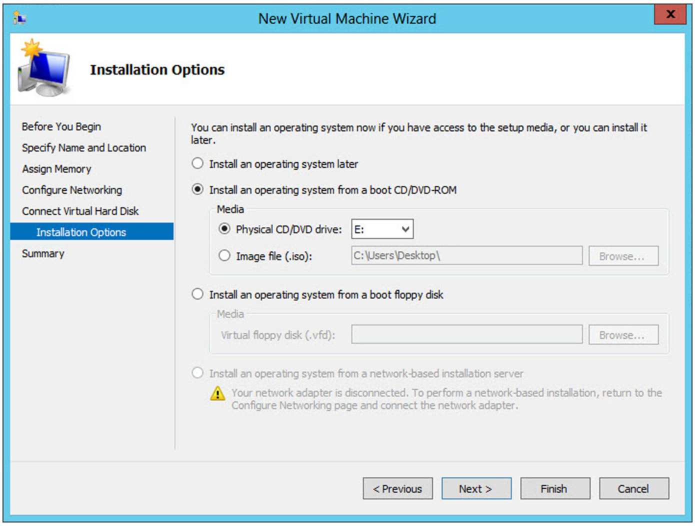
13. Click **Next**.

    The **Installation Options** screen appears.

14. Select **Install an operating system from a boot CD/DVD-ROM**.

15. Select one of the following options.

- **Physical CD/DVD drive**: Use the drop-down list to select a drive.



Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a boot CD/DVD-ROM

Media

● Physical CD/DVD drive: E:

○ Image file (.iso): C:\Users\Desktop\

○ Install an operating system from a boot floppy disk

Media

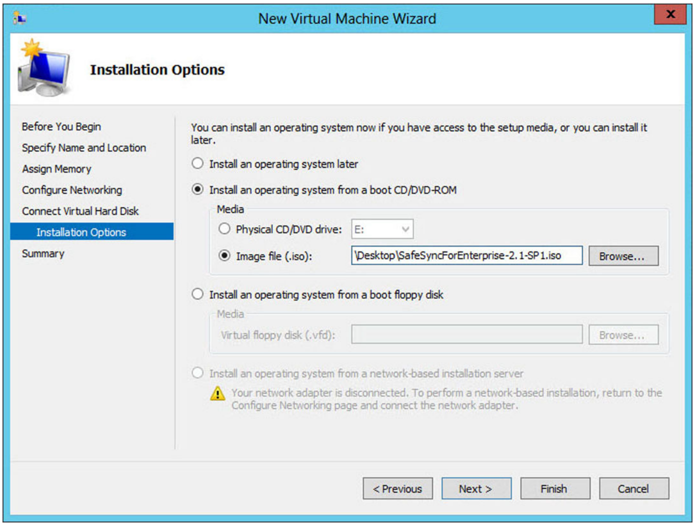
Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

Your network adapter is disconnected. To perform a network-based installation, return to the Configure Networking page and connect the network adapter.

**FIGURE 4-15. Installation Options screen - Install an operating system later**

- **Image file (.iso)**: Click **Browse** and locate the SafeSync .iso file.



You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a boot CD/DVD-ROM

Media

○ Physical CD/DVD drive: E:

● Image file (.iso): \Desktop\SafeSyncForEnterprise-2.1-SP1.iso Browse...

○ Install an operating system from a boot floppy disk

Media

Virtual floppy disk (.vfd): Browse...

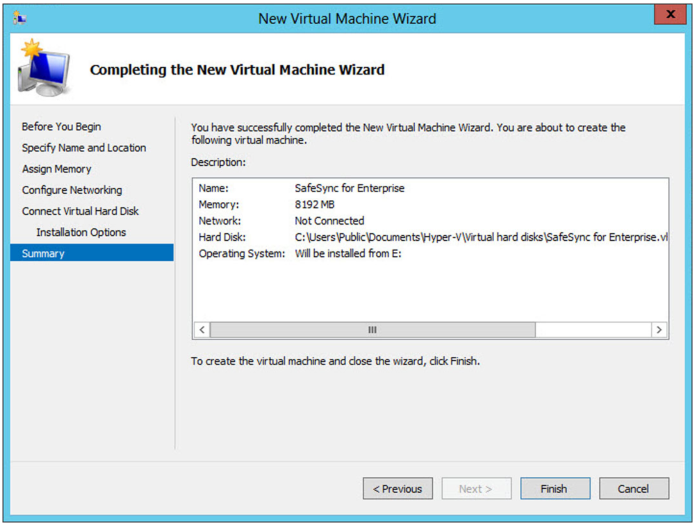
○ Install an operating system from a network-based installation server

⚠ Your network adapter is disconnected. To perform a network-based installation, return to the Configure Networking page and connect the network adapter.

**FIGURE 4-16. Installation Options screen - Install an operating system from a boot CD/DVD-ROM**

16. Click **Next**.

    The **Completing the New Virtual Machine Wizard** screen appears.



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

```
Name:              SafeSync for Enterprise
Memory:            8192 MB
Network:           Not Connected
Hard Disk:         C:\Users\Public\Documents\Hyper-V\Virtual hard disks\SafeSync for Enterprise.vl
Operating System:  Will be installed from E:
```

To create the virtual machine and close the wizard, click Finish.

**FIGURE 4-17. Completing the New Virtual Machine Wizard screen**

17. Verify that the settings are correct.

18. Click **Finish**.

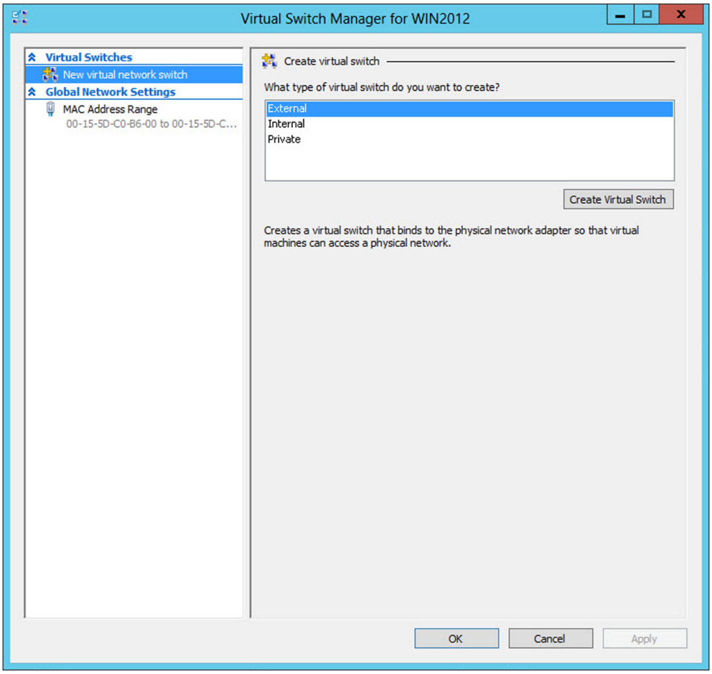
    The SafeSync virtual machine appears in the VM List.

19. Select the SafeSync virtual machine.

20. Create an external virtual switch.

    a. Select **Action** > **Virtual Switch Manager**.

The **Virtual Switch Manager** screen appears.



What type of virtual switch do you want to create?

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

**FIGURE 4-18. Virtual Switch Manager screen**

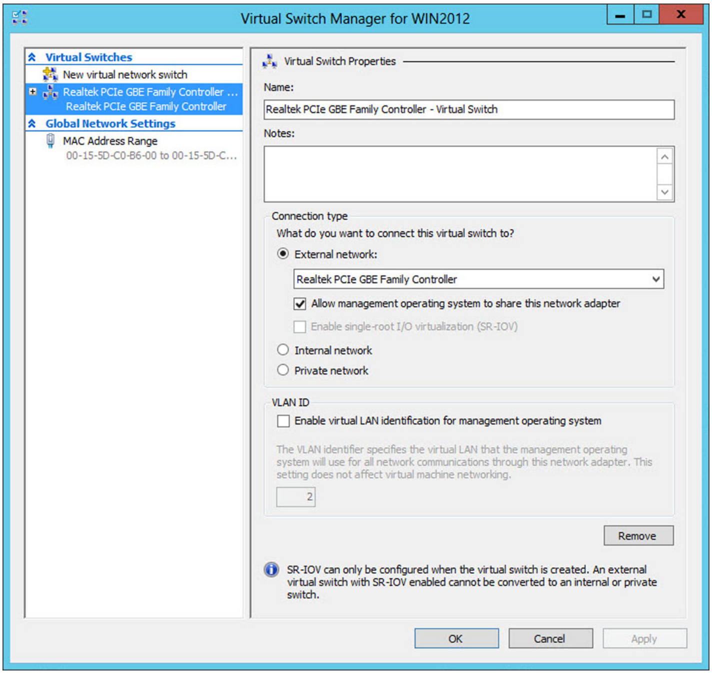
b. Select **External**.

c. Click **Create Virtual Switch**.

**21.** Specify the settings of the external virtual switch.

a. Under **Virtual Switches**, select the new virtual switch.

The **Virtual Switch Properties** panel is updated.



Virtual Switch Manager for WIN2012

Virtual Switches
- New virtual network switch
- Realtek PCIe GBE Family Controller ...
  Realtek PCIe GBE Family Controller

Global Network Settings
- MAC Address Range
  00-15-5D-C0-B6-00 to 00-15-5D-C...

Virtual Switch Properties

Name: Realtek PCIe GBE Family Controller - Virtual Switch

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network:

Realtek PCIe GBE Family Controller

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

**FIGURE 4-19. Virtual Switch Manager screen**

b. Type a name for the virtual switch.

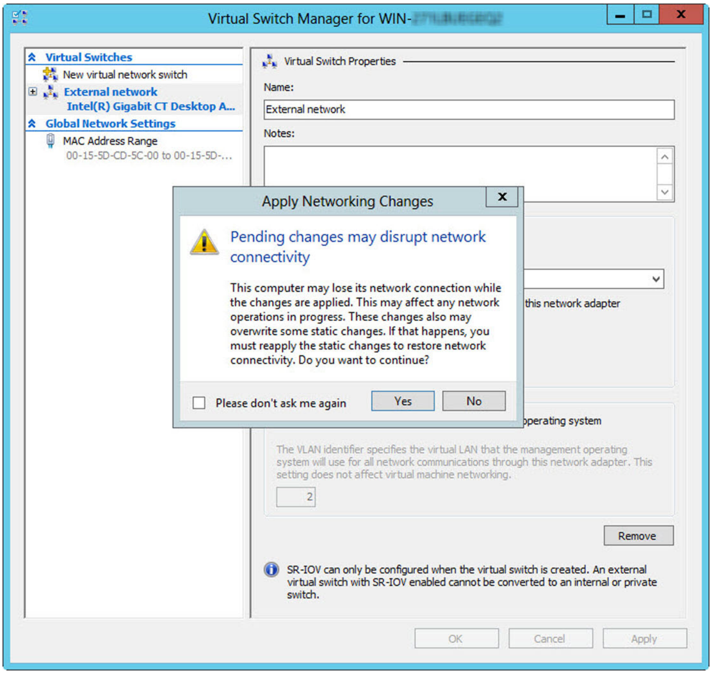
c. Select **External network**.

d. Select a network switch from the drop-down list.

e. Select **Allow management operating system to share this network adapter**.

f. Click **Apply**.

A confirmation screen appears. Click **Yes**.



Virtual Switch Manager for WIN-[redacted]

Virtual Switches
New virtual network switch
External network
Intel(R) Gigabit CT Desktop A...
Global Network Settings
MAC Address Range
00-15-5D-CD-5C-00 to 00-15-5D-...

Virtual Switch Properties

Name: External network

Notes:

this network adapter

operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

Apply Networking Changes

Pending changes may disrupt network connectivity

This computer may lose its network connection while the changes are applied. This may affect any network operations in progress. These changes also may overwrite some static changes. If that happens, you must reapply the static changes to restore network connectivity. Do you want to continue?

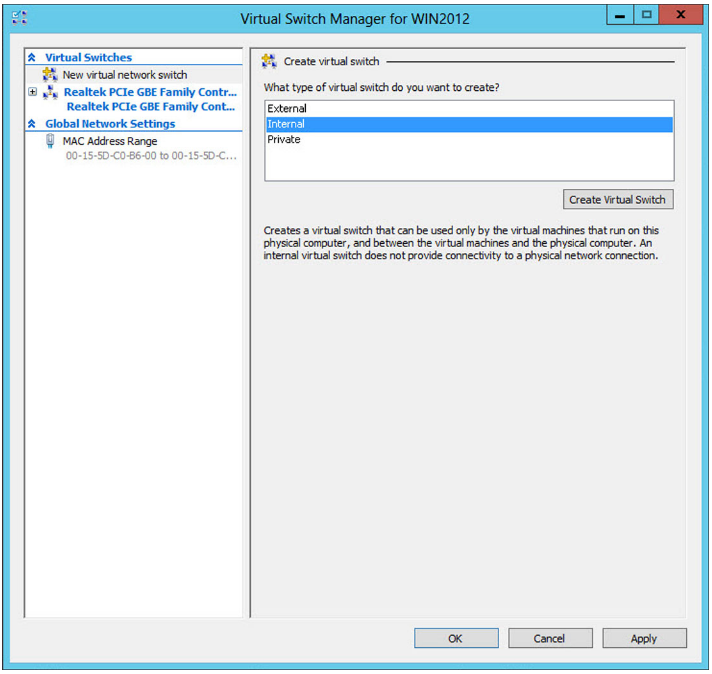
□ Please don't ask me again

**FIGURE 4-20. Apply Networking Changes screen**

**22.** Create an internal virtual switch.

a. Under **Virtual Switches**, click **New virtual network switch**.

The **Virtual Switch Manager** screen appears.


Virtual Switch Manager for WIN2012
Virtual Switches
New virtual network switch
Realtek PCIe GBE Family Contr...
Realtek PCIe GBE Family Cont...
Global Network Settings
MAC Address Range
00-15-5D-C0-B6-00 to 00-15-5D-C...
Create virtual switch
External
Internal
Private
Create Virtual Switch
OK
Cancel
Apply

What type of virtual switch do you want to create?

Creates a virtual switch that can be used only by the virtual machines that run on this physical computer, and between the virtual machines and the physical computer. An internal virtual switch does not provide connectivity to a physical network connection.

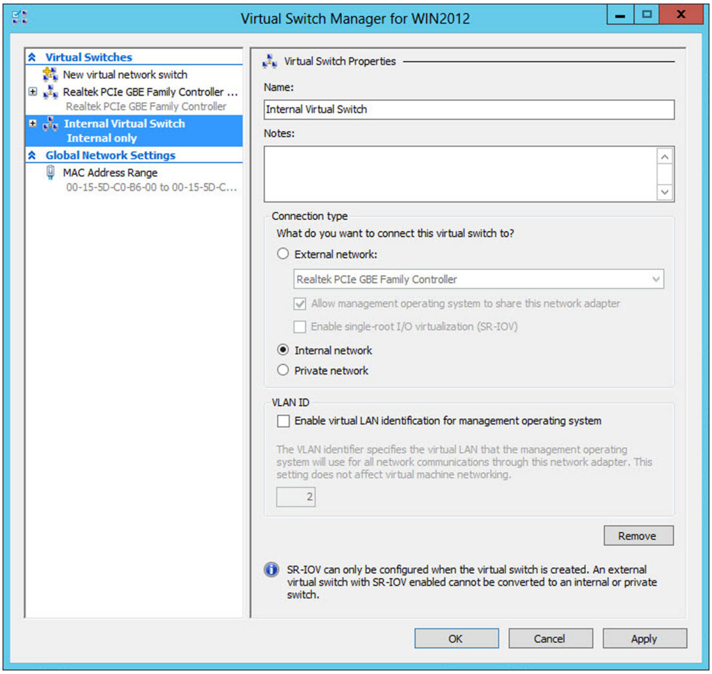
**FIGURE 4-21. Virtual Switch Manager screen**

b. Select **Internal**.

c. Click **Create Virtual Switch**.

**23.** Specify the settings of the internal virtual switch.

a. Under **Virtual Switches**, select the new virtual switch.


Virtual Switch Manager for WIN2012
Virtual Switches
New virtual network switch
Realtek PCIe GBE Family Controller ...
Realtek PCIe GBE Family Controller
Internal Virtual Switch
Internal only
Global Network Settings
MAC Address Range
00-15-5D-C0-B6-00 to 00-15-5D-C...
Virtual Switch Properties
Remove
OK
Cancel
Apply

Name: Internal Virtual Switch

Notes:

Connection type

What do you want to connect this virtual switch to?

○ External network:

Realtek PCIe GBE Family Controller

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

● Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

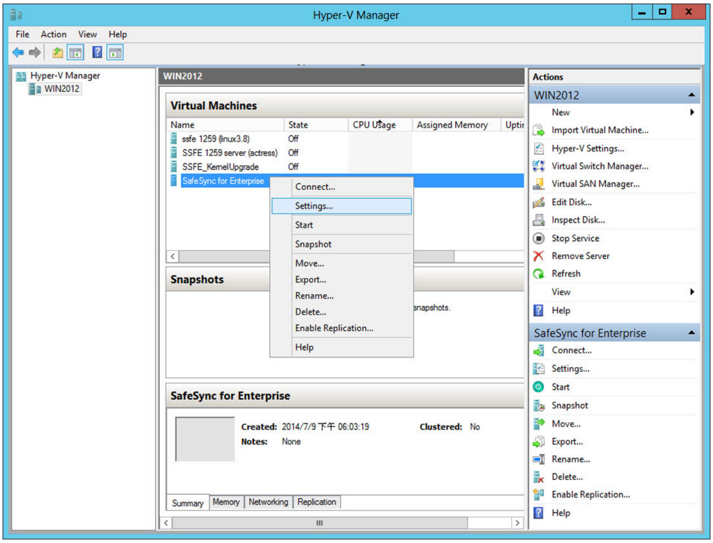
**FIGURE 4-22. Virtual Switch Manager screen**

b. Type a name for the virtual switch.

c. Select **Internal network**.

24. Click **Apply**.

The **Virtual Machines** list appears.



| Name | State | CPU Usage | Assigned Memory | Upti |
|---|---|---|---|---|
| ssfe 1259 (linux3.8) | Off | | | |
| SSFE 1259 server (actress) | Off | | | |
| SSFE_KernelUpgrade | Off | | | |
| SafeSync for Enterprise | | | | |

**Created:** 2014/7/9 下午 06:03:19 **Clustered:** No
**Notes:** None

**FIGURE 4-23. Virtual Machines list**

25. Right-click the SafeSync virtual machine.

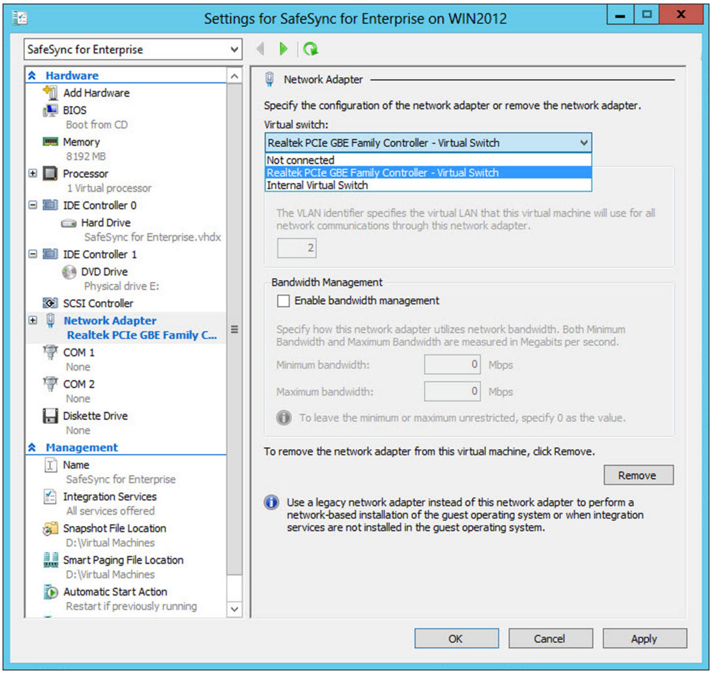
26. Select **Settings**.

    The **Settings** screen appears.

27. Configure the network settings of the external switch.

    a. Under **Hardware**, select **Network Adapter**.

The **Network Adapter** screen appears.



Settings for SafeSync for Enterprise on WIN2012

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Realtek PCIe GBE Family Controller - Virtual Switch

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

**FIGURE 4-24. Network Adapter screen**

b. Under **Network Adapter**, select the previously created external switch from the drop-down list.

**28.** Configure the network settings of the internal switch.

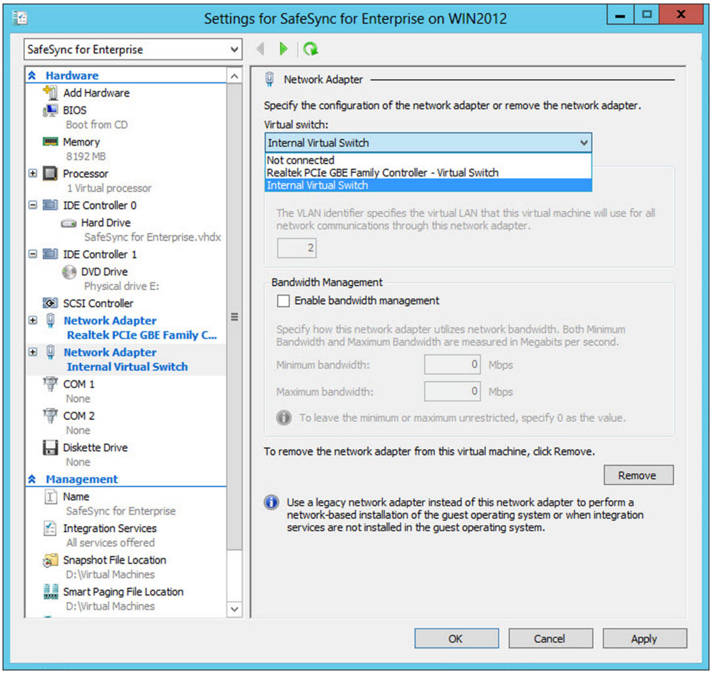
a. Under **Hardware**, click **Add Hardware**.

The **Add Hardware** screen appears.

b. Select **Network Adapter**.

c. Click **Add**.

The new network adapter appears under the **Hardware** pane.



Settings for SafeSync for Enterprise on WIN2012

SafeSync for Enterprise

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  8192 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    SafeSync for Enterprise.vhdx
- IDE Controller 1
  - DVD Drive
    Physical drive E:
- SCSI Controller
- Network Adapter
  Realtek PCIe GBE Family C...
- Network Adapter
  Internal Virtual Switch
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  SafeSync for Enterprise
- Integration Services
  All services offered
- Snapshot File Location
  D:\Virtual Machines
- Smart Paging File Location
  D:\Virtual Machines

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:
Internal Virtual Switch
- Not connected
- Realtek PCIe GBE Family Controller - Virtual Switch
- Internal Virtual Switch

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

**FIGURE 4-25. Network Adapter screen**

d. Under **Network Adapter**, select **Internal Virtual Switch**.

29. Click **OK**.

The virtual machine is created.

# Installing on a VMware Workstation

**Tip**

Trend Micro does not recommend installing SafeSync on a VMware Workstation virtual machine.

When installing SafeSync on a VMware Workstation, the virtual machine requires the following:

| SYSTEM | MINIMUM REQUIREMENT |
|---|---|
| Virtual machine | VMware® WorkStation™ 6.x, 7.x or above |
| CPU | 64-bit single core |
| RAM | 8GB |
| Hard disk | 60GB |
| Network cards | Two NICs (1GB recommended) |

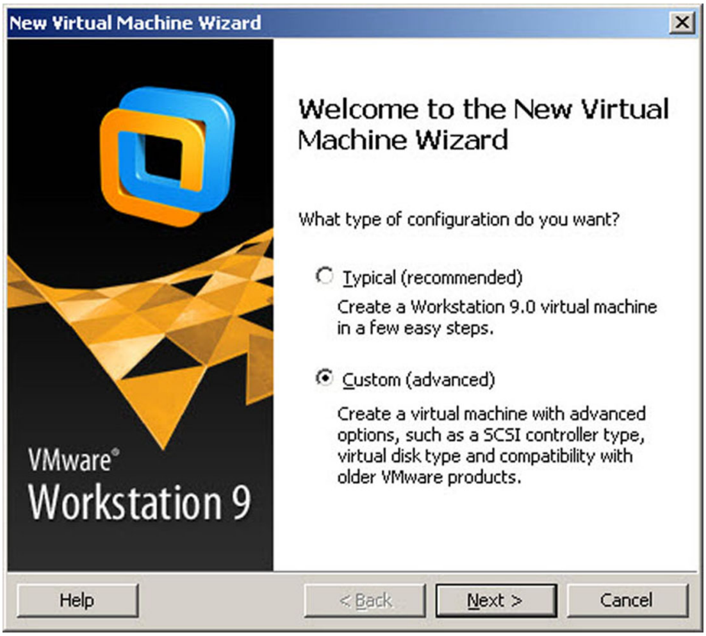
**Note**

The following procedure uses VMware Workstation 9.0.3 as an example.

### Procedure

1. Launch a VMware WorkStation.
2. Select **File** > **New** > **Virtual Machine** from the menu.

A setup wizard appears.



Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

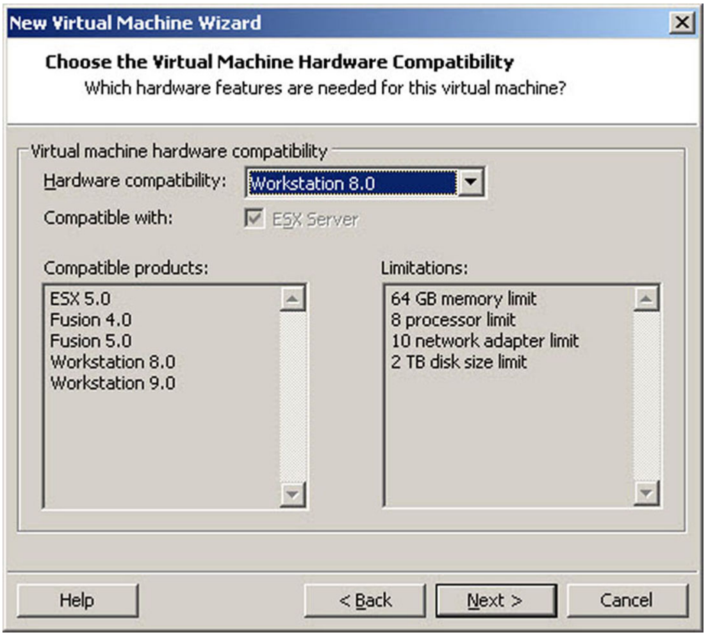
○ Typical (recommended)
Create a Workstation 9.0 virtual machine in a few easy steps.

● Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

**FIGURE 4-26. Virtual Machine Configuration**

3. Select **Custom (advanced)**.
4. Click **Next**.

The **Virtual Machine Hardware Compatibility** screen appears.



New Virtual Machine Wizard

**Choose the Virtual Machine Hardware Compatibility**

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 8.0

Compatible with: ☑ ESX Server

Compatible products:

ESX 5.0
Fusion 4.0
Fusion 5.0
Workstation 8.0
Workstation 9.0

Limitations:

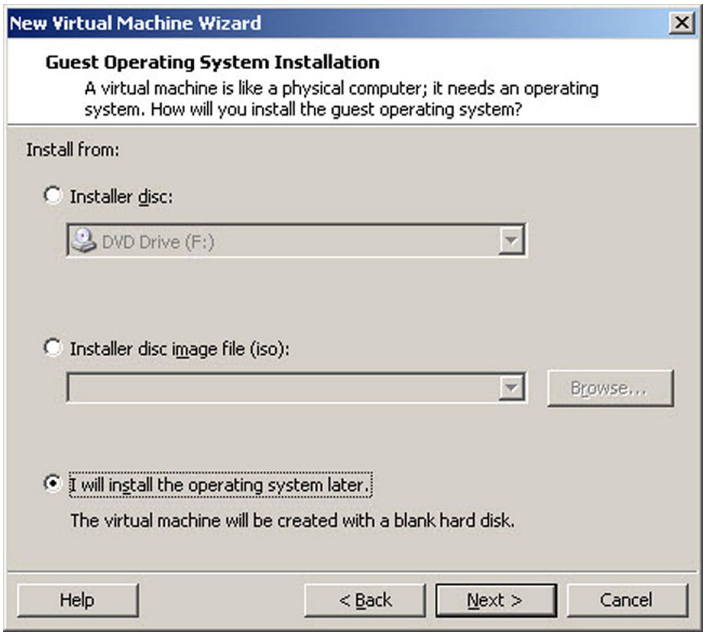
64 GB memory limit
8 processor limit
10 network adapter limit
2 TB disk size limit

**FIGURE 4-27. Virtual Machine Hardware Compatibility screen**

**5.** Select **Workstation 8.0** from the drop-down list.

**6.** Click **Next**.

The **Guest Operating System Installation** screen appears.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD Drive (F:)

○ Installer disc image file (iso):

● I will install the operating system later.

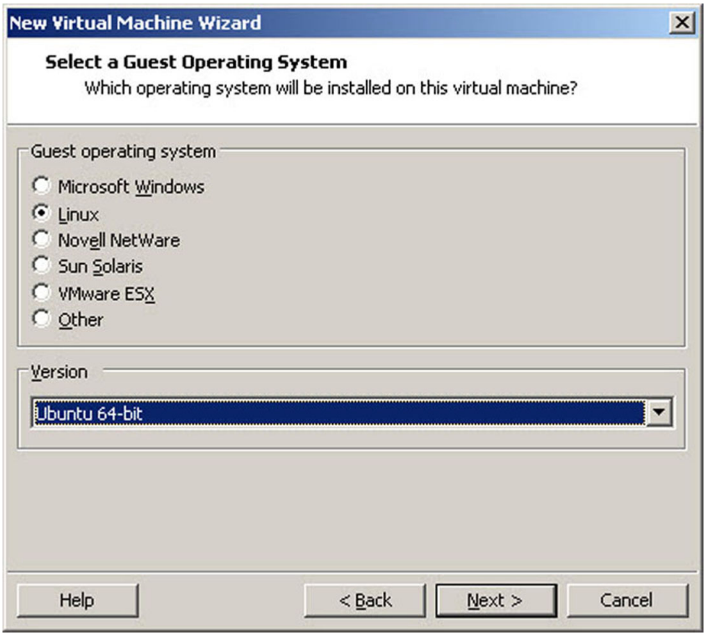
The virtual machine will be created with a blank hard disk.

**FIGURE 4-28. Guest Operating System Installation screen**

7. Select **I will install the operating system later.**.

8. Click **Next**.

The **Select a Guest Operating System** screen appears.



New Virtual Machine Wizard

**Select a Guest Operating System**

Which operating system will be installed on this virtual machine?

Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Sun Solaris
○ VMware ESX
○ Other

Version

Ubuntu 64-bit

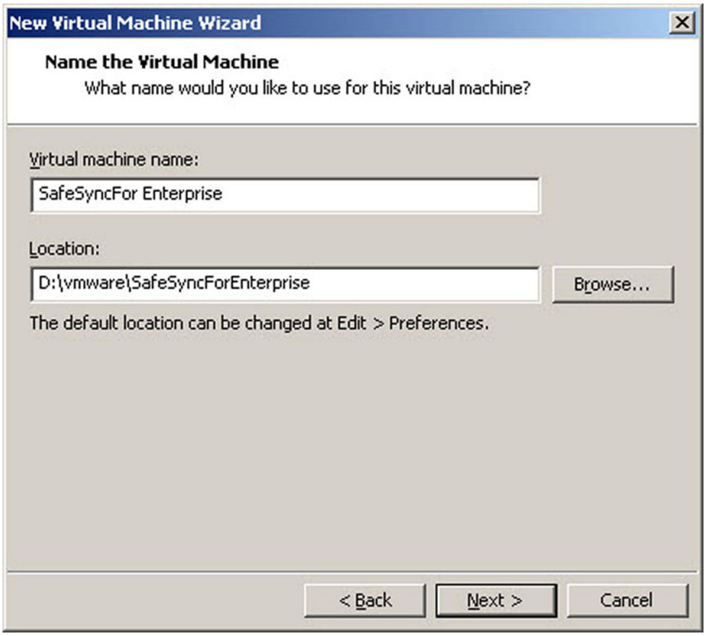
**FIGURE 4-29. Select a Guest Operating System screen**

**9.** Specify the following:

- **Guest operating system**: **Other**
- **Version**: **Other 64-bit**

**10.** Click **Next**.

The **Name the Virtual Machine** screen appears.


New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name: SafeSyncFor Enterprise

Location: D:\vmware\SafeSyncForEnterprise

The default location can be changed at Edit > Preferences.

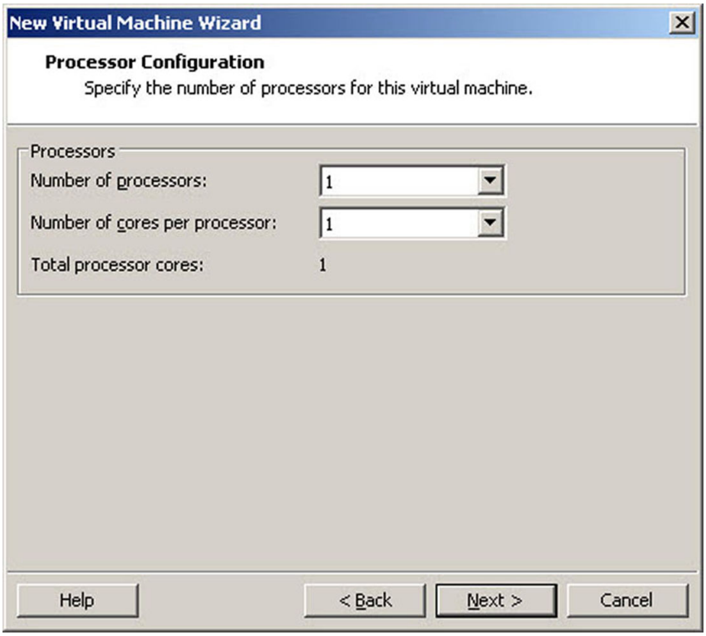
**FIGURE 4-30. Name the Virtual Machine screen**

**11.** Type a name for the virtual machine.

**12.** Type a path for file storage.

**13.** Click **Next**.

The **Processor Configuration** screen appears.


New Virtual Machine Wizard
Processor Configuration
Specify the number of processors for this virtual machine.
Processors
Help
< Back
Next >
Cancel

Number of processors: 1

Number of cores per processor: 1

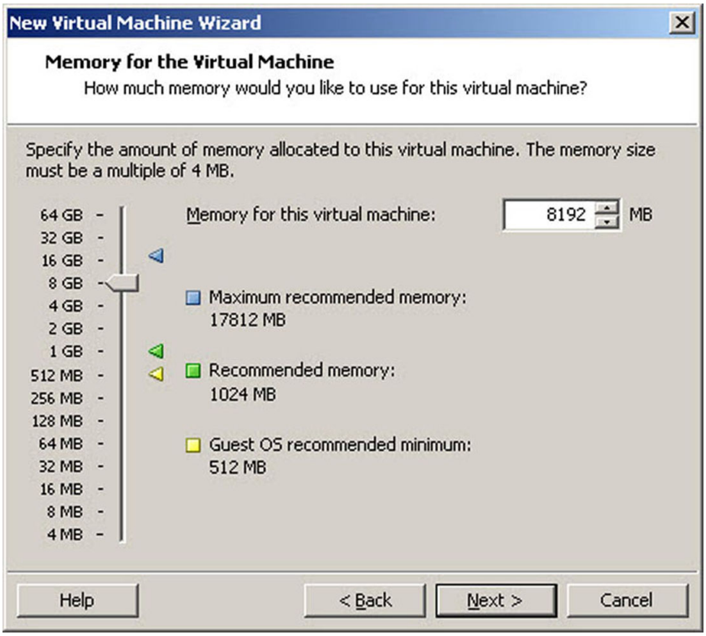
Total processor cores: 1

**FIGURE 4-31. Processor Configuration screen**

14. Provide the number of processors and the number of cores per processor that the virtual machine uses.

15. Click **Next**.

The **Memory for the Virtual Machine** screen appears.



New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 8192 MB

🟦 Maximum recommended memory: 17812 MB

🟩 Recommended memory: 1024 MB

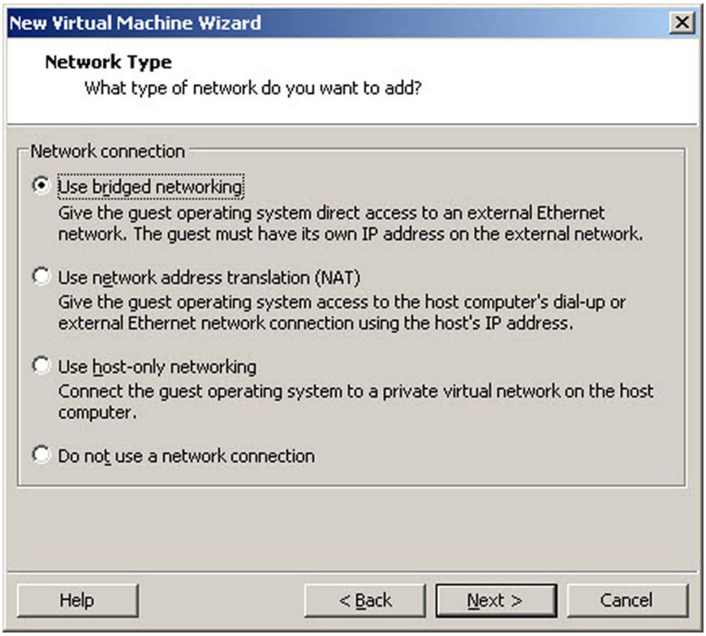
🟨 Guest OS recommended minimum: 512 MB

**FIGURE 4-32. Memory for the Virtual Machine screen**

16. Specify at least **8GB** RAM for SafeSync.

17. Click **Next**.

The **Network Type** screen appears.



New Virtual Machine Wizard

**Network Type**

What type of network do you want to add?

Network connection

● Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

○ Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

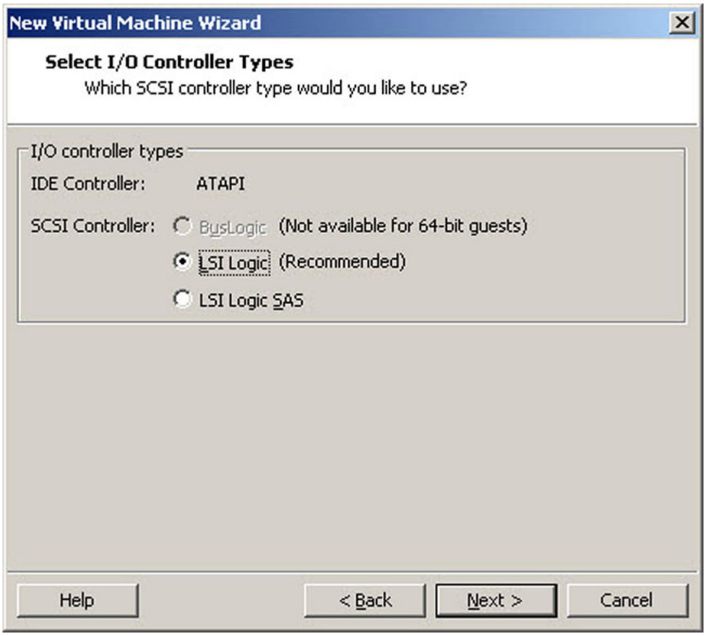
○ Do not use a network connection

**FIGURE 4-33. Network Type screen**

18. Select **Use bridged networking**.

19. Click **Next**.

The **Select I/O Controller Types** screen appears.



Select I/O Controller Types

Which SCSI controller type would you like to use?

I/O controller types

IDE Controller: ATAPI

SCSI Controller: ○ BusLogic (Not available for 64-bit guests)

● LSI Logic (Recommended)

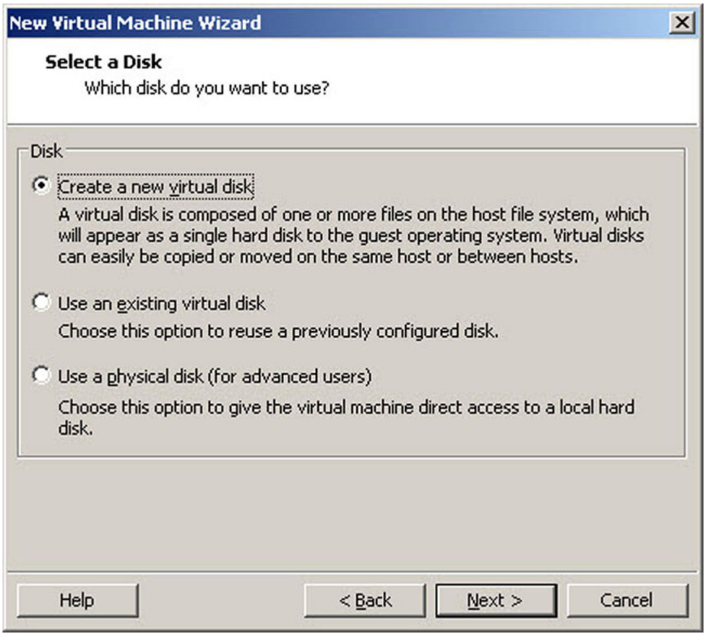
○ LSI Logic SAS

**FIGURE 4-34. Select I/O Controller Types screen**

20. Select **LSI Logic (Recommended)**.

21. Click **Next**.

The **Select a Disk** screen appears.



New Virtual Machine Wizard

**Select a Disk**

Which disk do you want to use?

Disk

● Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

○ Use an existing virtual disk

Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

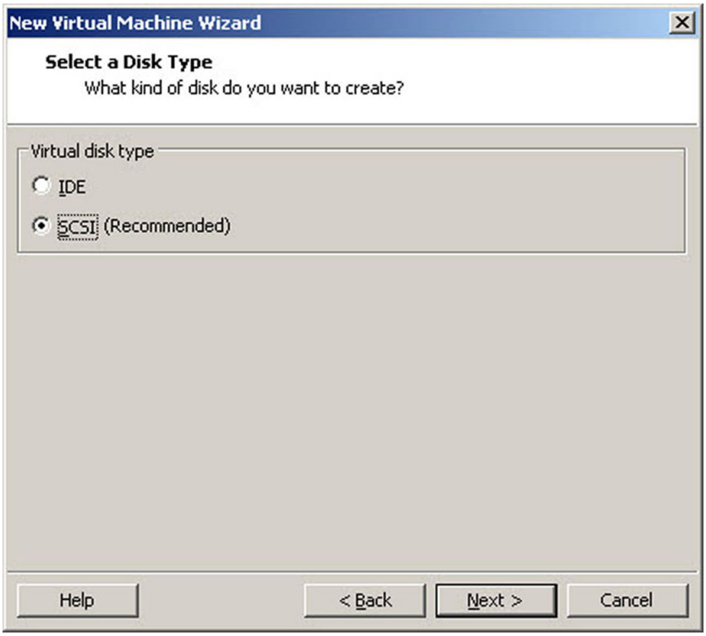
Choose this option to give the virtual machine direct access to a local hard disk.

**FIGURE 4-35. Select a Disk screen**

22. Select **Create a new virtual disk**.

23. Click **Next**.

The **Select a Disk Type** screen appears.



New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

○ IDE

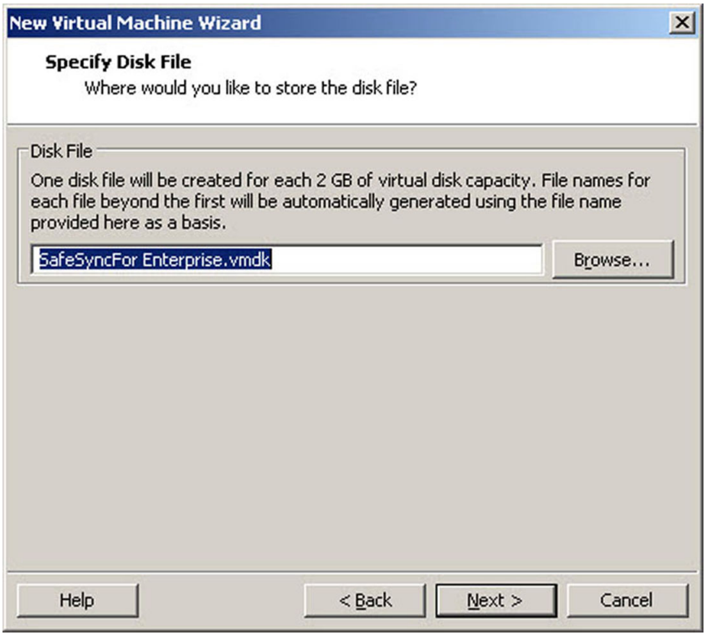
● SCSI (Recommended)

**FIGURE 4-36. Select a Disk Type screen**

24. Select the **SCSI (Recommended)** disk type.

25. Click **Next**.

The **Specify Disk File** screen appears.



New Virtual Machine Wizard

**Specify Disk File**

Where would you like to store the disk file?

Disk File

One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.

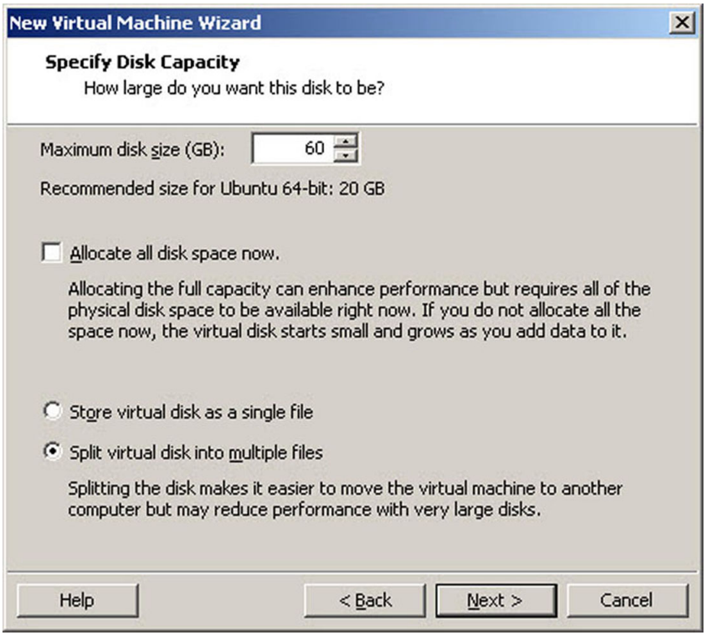
SafeSyncFor Enterprise.vmdk

**FIGURE 4-37. Specify Disk File screen**

26. Specify where to store the disk file.

27. Click **Next**.

The **Specify Disk Capacity** screen appears.



New Virtual Machine Wizard

**Specify Disk Capacity**

How large do you want this disk to be?

Maximum disk size (GB): 60

Recommended size for Ubuntu 64-bit: 20 GB

□ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

○ Store virtual disk as a single file

● Split virtual disk into multiple files

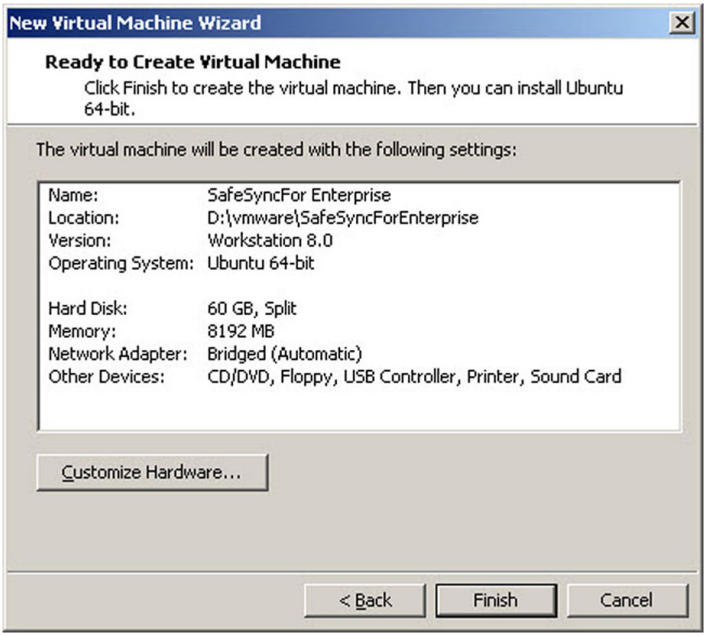
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

**FIGURE 4-38. Specify Disk Capacity screen**

28. Specify at least **60GB** of disk space for SafeSync.

29. Click **Next**.

The **Ready to Create Virtual Machine** screen appears.



New Virtual Machine Wizard

**Ready to Create Virtual Machine**

Click Finish to create the virtual machine. Then you can install Ubuntu 64-bit.

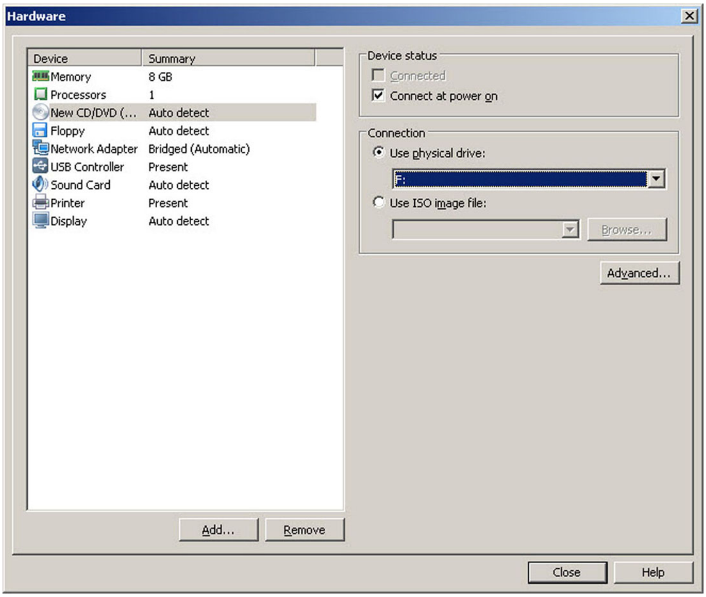
The virtual machine will be created with the following settings:

| | |
|---|---|
| Name: | SafeSyncFor Enterprise |
| Location: | D:\vmware\SafeSyncForEnterprise |
| Version: | Workstation 8.0 |
| Operating System: | Ubuntu 64-bit |
| Hard Disk: | 60 GB, Split |
| Memory: | 8192 MB |
| Network Adapter: | Bridged (Automatic) |
| Other Devices: | CD/DVD, Floppy, USB Controller, Printer, Sound Card |

**FIGURE 4-39. Ready to Create Virtual Machine screen**

30. Click **Customize Hardware**.

The **Hardware** screen appears.



| Device | Summary |
|---|---|
| Memory | 8 GB |
| Processors | 1 |
| New CD/DVD (... | Auto detect |
| Floppy | Auto detect |
| Network Adapter | Bridged (Automatic) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Device status

□ Connected

☑ Connect at power on

Connection

● Use physical drive: F:

○ Use ISO image file:

**FIGURE 4-40. Hardware screen**

31. Select **New CD/DVD**.

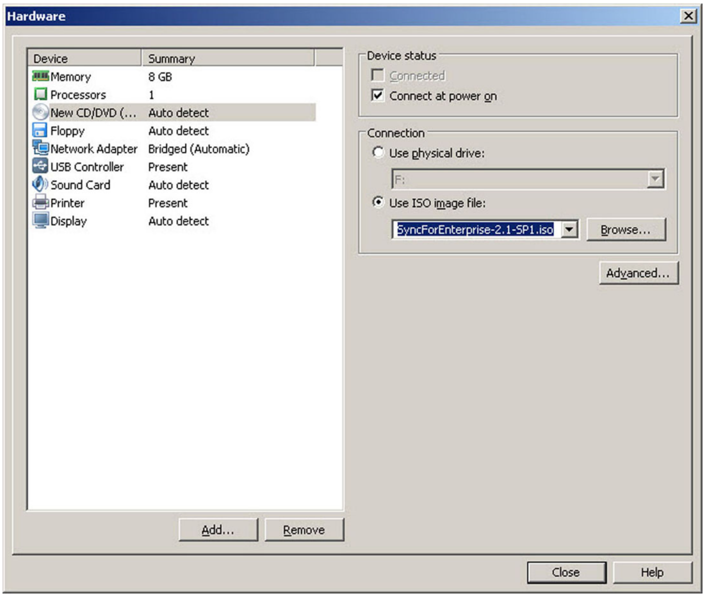
    The **Select New CD/DVD** screen appears.

32. Under **Device status**, select **Connect at power on**.

33. Under **Connection**, select one of the following.

    - **Use phyiscal drive**: Use the drop-down list to select a drive.

- **Use ISO image file**: Click **Browse** and locate the SafeSync .iso file.



| Device | Summary |
|---|---|
| Memory | 8 GB |
| Processors | 1 |
| New CD/DVD (... | Auto detect |
| Floppy | Auto detect |
| Network Adapter | Bridged (Automatic) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

F:

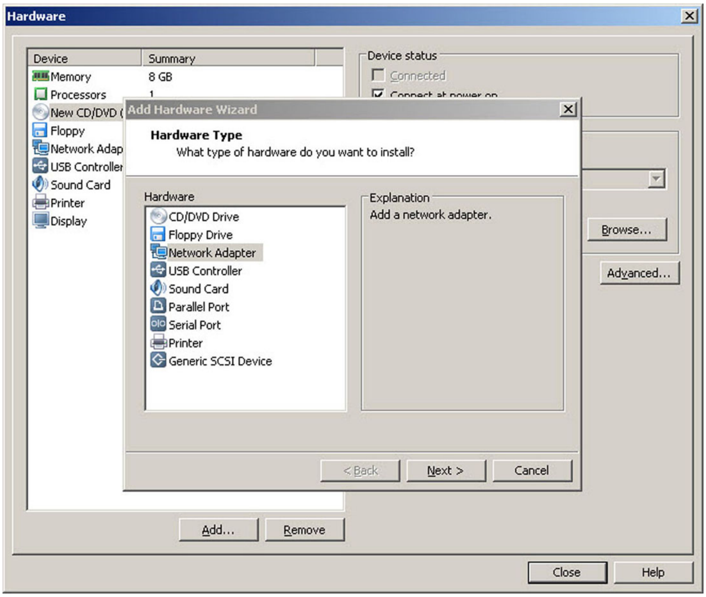
● Use ISO image file:

SyncForEnterprise-2.1-SP1.iso

**FIGURE 4-41. Hardware screen**

34. Click **Add**.

The **Hardware Type** screen appears.



Add Hardware Wizard

**Hardware Type**

What type of hardware do you want to install?

| Device | Summary |
|---|---|
| Memory | 8 GB |
| Processors | 1 |
| New CD/DVD ( | |
| Floppy | |
| Network Adap | |
| USB Controller | |
| Sound Card | |
| Printer | |
| Display | |

Device status

☐ Connected

☑ Connect at power on

Explanation

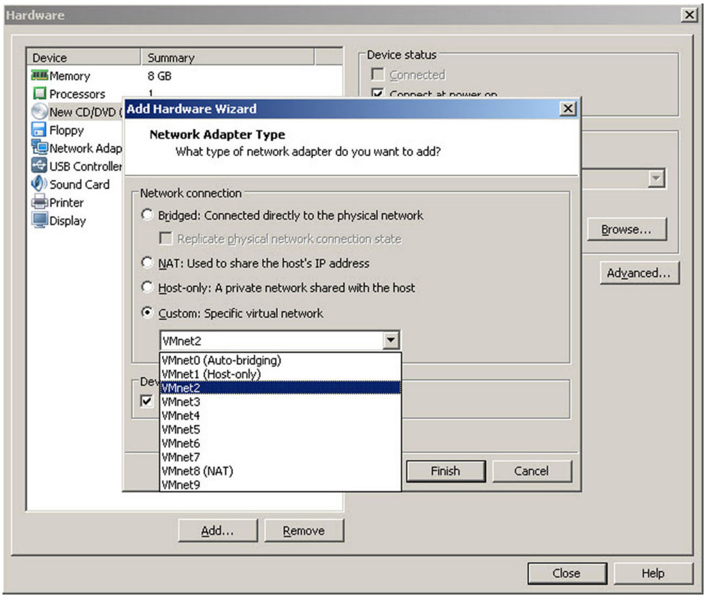
Add a network adapter.

**FIGURE 4-42. Hardware Type screen**

35. Select **Network Adapter**.

36. Click **Next**.

The **Network Adapter Type** screen appears.



Add Hardware Wizard

**Network Adapter Type**

What type of network adapter do you want to add?

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet2

**FIGURE 4-43. Network Adapter Type screen**

37. Select **Custom** and specify a virtual network from the drop-down list.

**Tip**

Trend Micro recommends using any of the virtual networks between **VMnet2** to **VMnet7**.

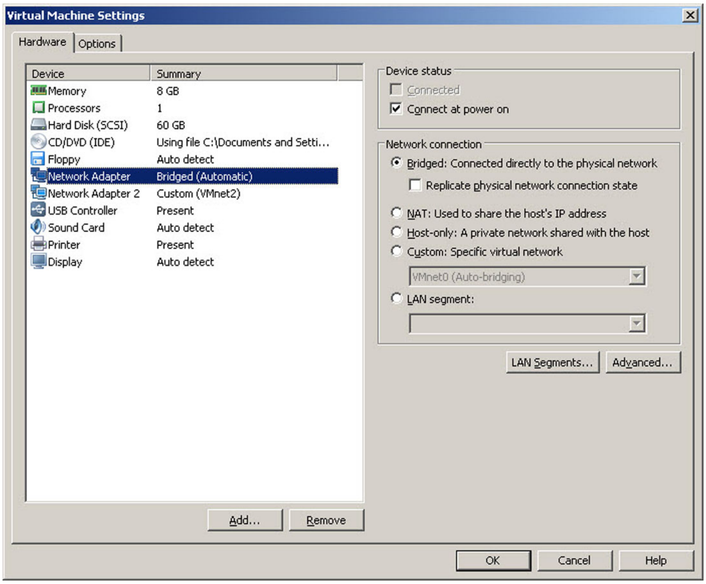
38. Select **Connect at power on**.

**Note**

Take note of the virtual machine settings. The network adapater settings should be identical on both servers in a high availability deployment.

39. Click **Finish**.

The **Hardware** screen appears.



| Device | Summary |
|---|---|
| Memory | 8 GB |
| Processors | 1 |
| Hard Disk (SCSI) | 60 GB |
| CD/DVD (IDE) | Using file C:\Documents and Setti... |
| Floppy | Auto detect |
| Network Adapter | Bridged (Automatic) |
| Network Adapter 2 | Custom (VMnet2) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Device status

□ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

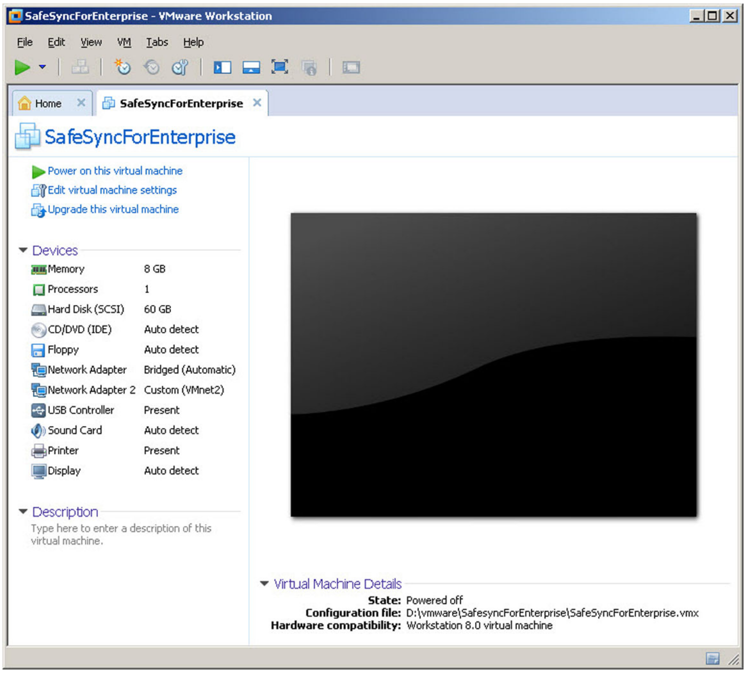
VMnet0 (Auto-bridging)

○ LAN segment:

**FIGURE 4-44. Hardware screen**

40. Click **OK**.

The virtual machine is created.


SafeSyncForEnterprise - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
SafeSyncForEnterprise
SafeSyncForEnterprise
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Description

| | |
|---|---|
| Memory | 8 GB |
| Processors | 1 |
| Hard Disk (SCSI) | 60 GB |
| CD/DVD (IDE) | Auto detect |
| Floppy | Auto detect |
| Network Adapter | Bridged (Automatic) |
| Network Adapter 2 | Custom (VMnet2) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Type here to enter a description of this virtual machine.

Virtual Machine Details

**State:** Powered off
**Configuration file:** D:\vmware\SafesyncForEnterprise\SafeSyncForEnterprise.vmx
**Hardware compatibility:** Workstation 8.0 virtual machine

**FIGURE 4-45. SafeSync Virtual Machine**

# Installing on an Oracle VM VirtualBox

**Tip**

Trend Micro does not recommend installing SafeSync on an Oracle VM VirtualBox virtual machine.

When installing SafeSync on an Oracle VM VirtualBox, the virtual machine requires the following:

| SYSTEM | MINIMUM REQUIREMENT |
|---|---|
| Virtual machine | Oracle VM VirtualBox™ 4.2.x |
| CPU | 64-bit single core |
| RAM | 8GB |
| Hard disk | 60GB |
| Network cards | Two NICs (1GB recommended) |

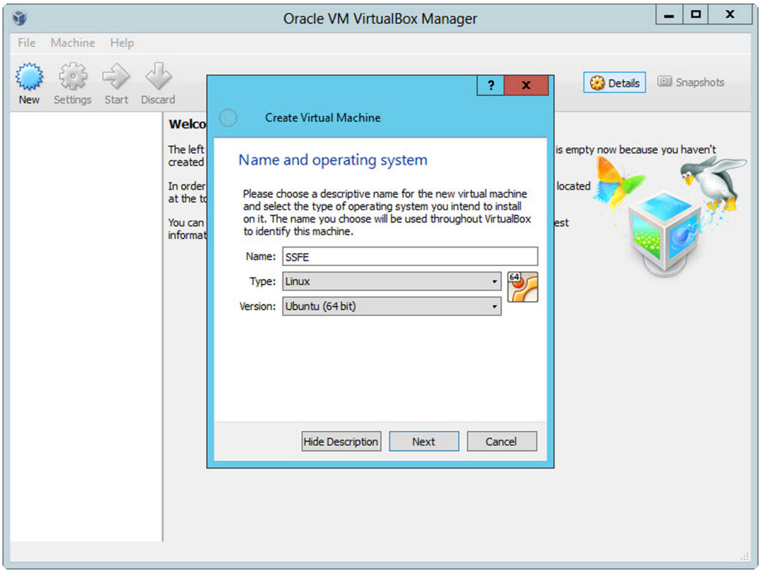
**Note**

The following procedure uses Oracle VM VirtualBox 4.3.14 as an example.

### Procedure

1. Log on to the Oracle VM VirtualBox.
2. Click the **New** button on the toolbar to add a new virtual machine.
3. Click **Next**.

The **Name and operating system** screen appears.



Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: SSFE

Type: Linux

Version: Ubuntu (64 bit)

**Figure 4-46. Name and operating system screen**

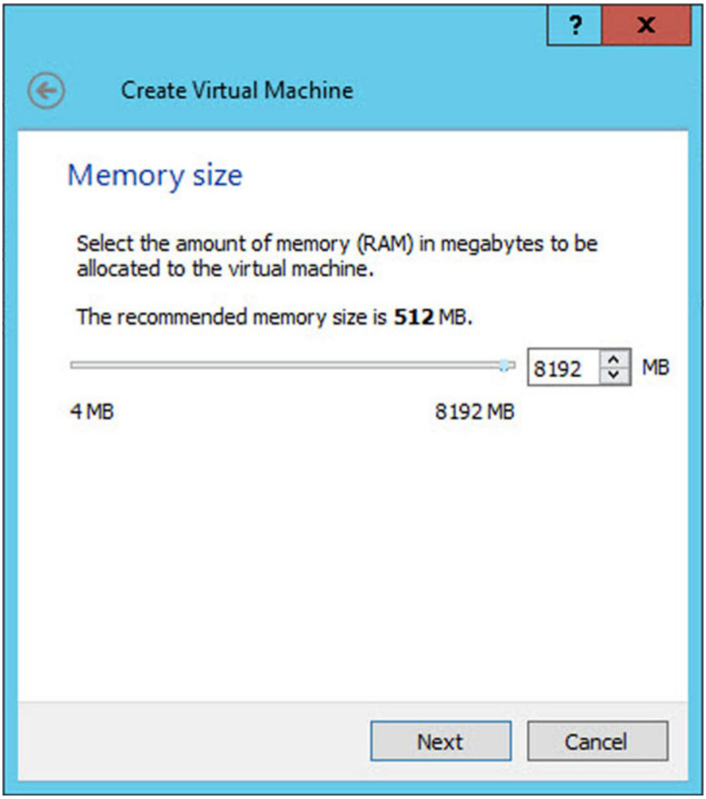
4. Type a name for the virtual machine.

5. Select the following for the operating system type and version:

   - **Linux**
   - **Ubuntu (64-bit)**

6. Click **Next**.

The **Memory size** screen appears.



Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512** MB.

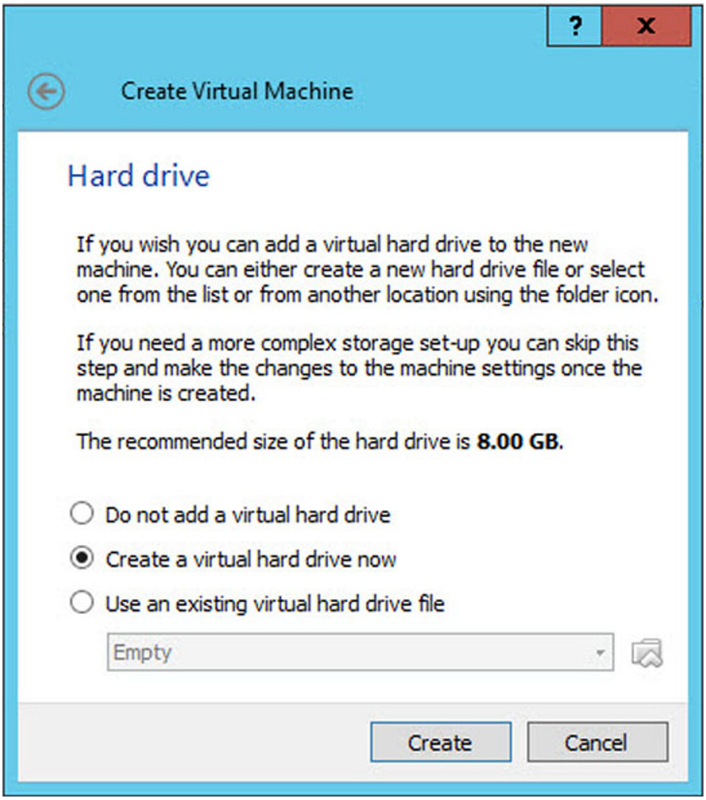
8192 MB

**FIGURE 4-47. Memory size screen**

7. Specify at least **8GB** RAM for SafeSync.

8. Click **Next**.

The **Hard drive** screen appears.



Create Virtual Machine

Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB**.

○ Do not add a virtual hard drive

● Create a virtual hard drive now

○ Use an existing virtual hard drive file

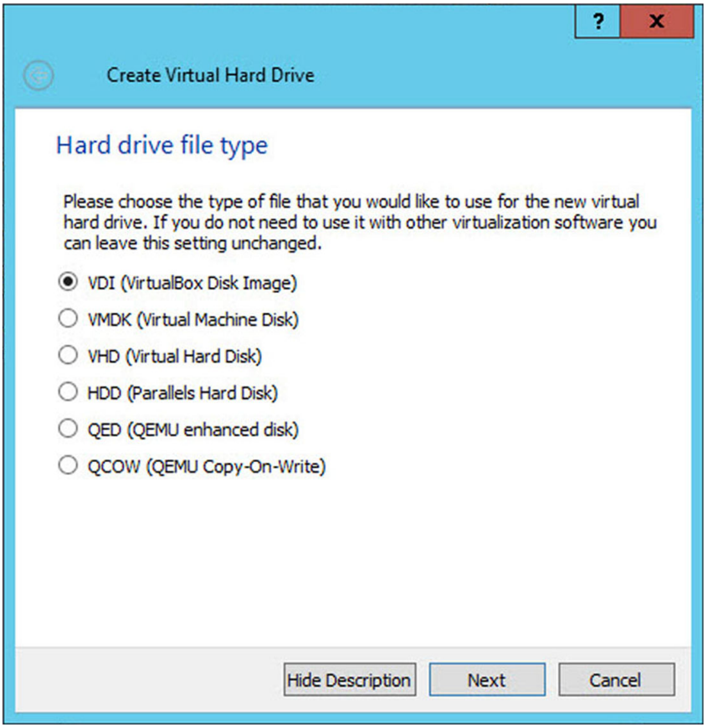
Empty

**FIGURE 4-48. Hard drive screen**

9. Select **Create a virtual hard drive now**.

10. Click **Create**.

The **Hard drive file type** screen appears.



Hard drive file type

Please choose the type of file that you would like to use for the new virtual hard drive. If you do not need to use it with other virtualization software you can leave this setting unchanged.

- ● VDI (VirtualBox Disk Image)
- ○ VMDK (Virtual Machine Disk)
- ○ VHD (Virtual Hard Disk)
- ○ HDD (Parallels Hard Disk)
- ○ QED (QEMU enhanced disk)
- ○ QCOW (QEMU Copy-On-Write)

**FIGURE 4-49. Hard drive file type screen**

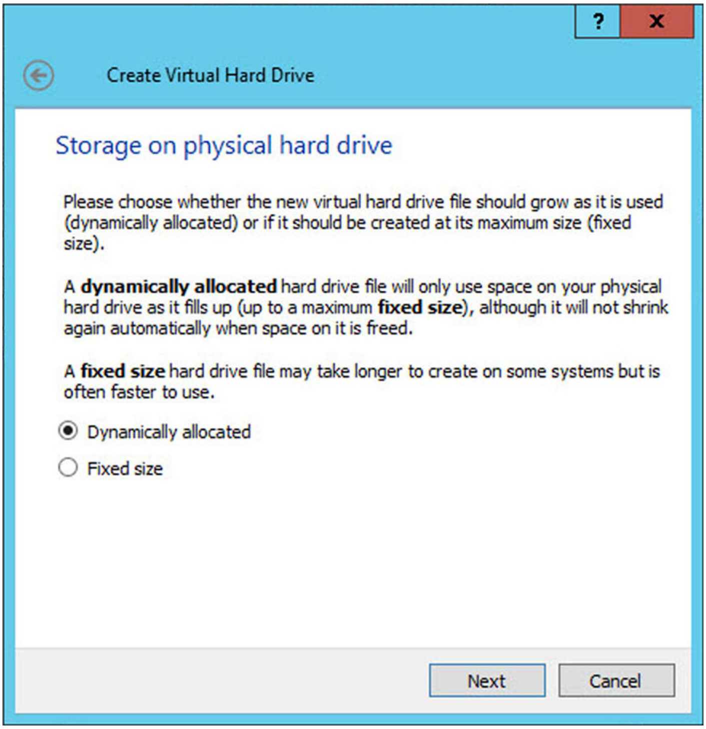
**11.** Specify the type of virtual disk to use.

**Tip**

If you do not intend to use the virtual machine with other virtualization software, leave the setting as **VDI (VirtualBox Disk Image)**.

**12.** Click **Next**.

The **Storage on physcial hard drive** screen appears.



Create Virtual Hard Drive

Storage on physical hard drive

Please choose whether the new virtual hard drive file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard drive file will only use space on your physical hard drive as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard drive file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size

**FIGURE 4-50. Storage on physcial hard drive screen**

**13.** Specify whether disk space is allocated dynamically or if disk space is fixed.

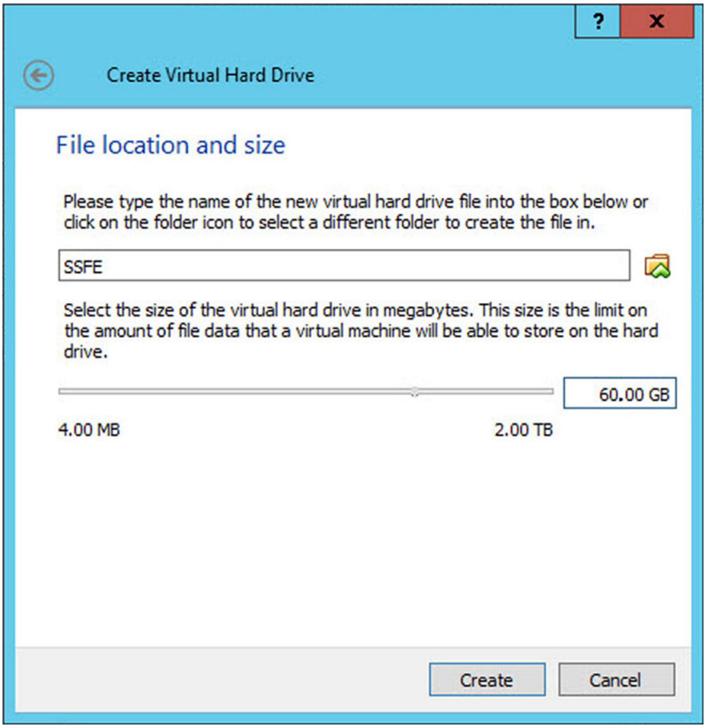
**Note**

Dynamically allocated space is allocated as the space fills up.

Fixed disk space only takes up as much space as you allocate, but the fixed size disk is often faster to use.

**14.** Click **Next**.

The **File location and size** screen appears.



File location and size

Please type the name of the new virtual hard drive file into the box below or click on the folder icon to select a different folder to create the file in.

SSFE

Select the size of the virtual hard drive in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard drive.

60.00 GB

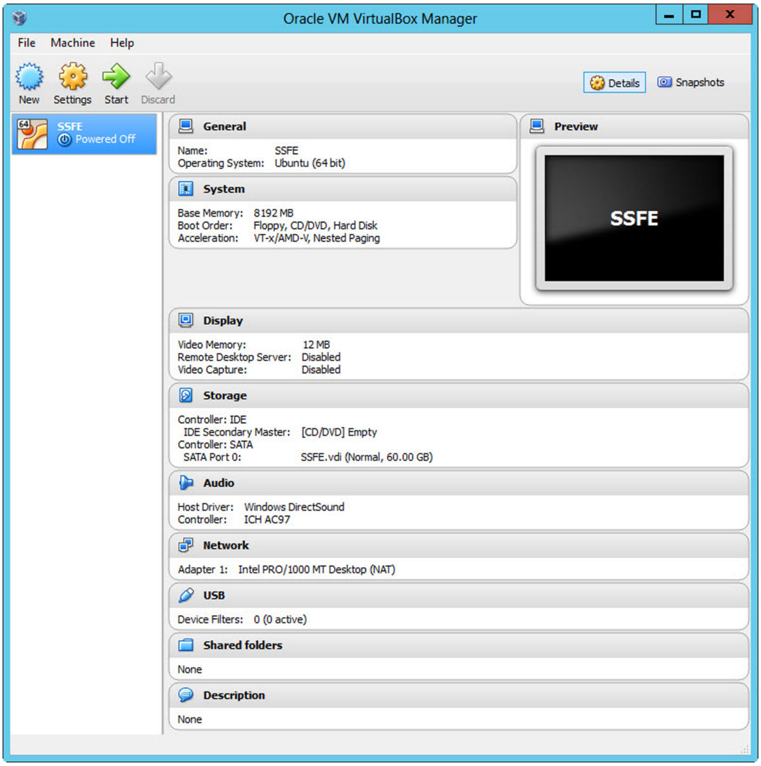
**FIGURE 4-51. File location and size screen**

15. Specify a name and location for the virtual disk.

16. Specify at least **60GB** of disk space for SafeSync.

17. Click **Create**.

The virtual machine appears in the virtual machine list.



General

Name: SSFE
Operating System: Ubuntu (64 bit)

System

Base Memory: 8192 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: SSFE.vdi (Normal, 60.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

Device Filters: 0 (0 active)

Shared folders

None

Description

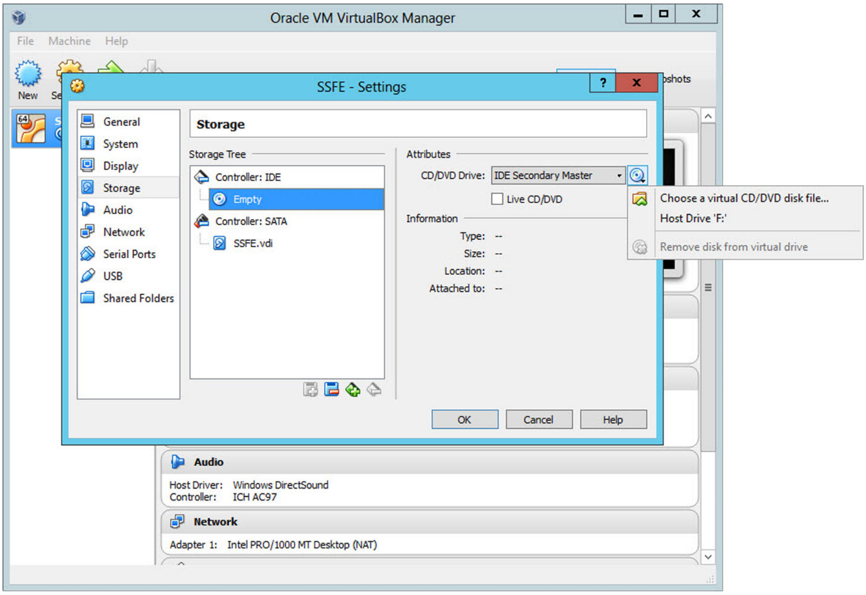
None

**FIGURE 4-52. Virtual Machine Summary screen**

18. Select the SafeSync virtual machine from the list.

19. Click **Settings** from the main menu to set up the environment for SafeSync.

The **Settings** screen for the virtual machine appears.



CD/DVD Drive: IDE Secondary Master

□ Live CD/DVD

Type: --

Size: --

Location: --

Attached to: --

Host Driver: Windows DirectSound

Controller: ICH AC97

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

**FIGURE 4-53. Settings - Storage screen**

**20.** Mount the SafeSync installation CD/DVD or import the SafeSync .iso file.

a. Click **Storage** from the left pane of the **Settings** screen.

The content for **Storage** appears.

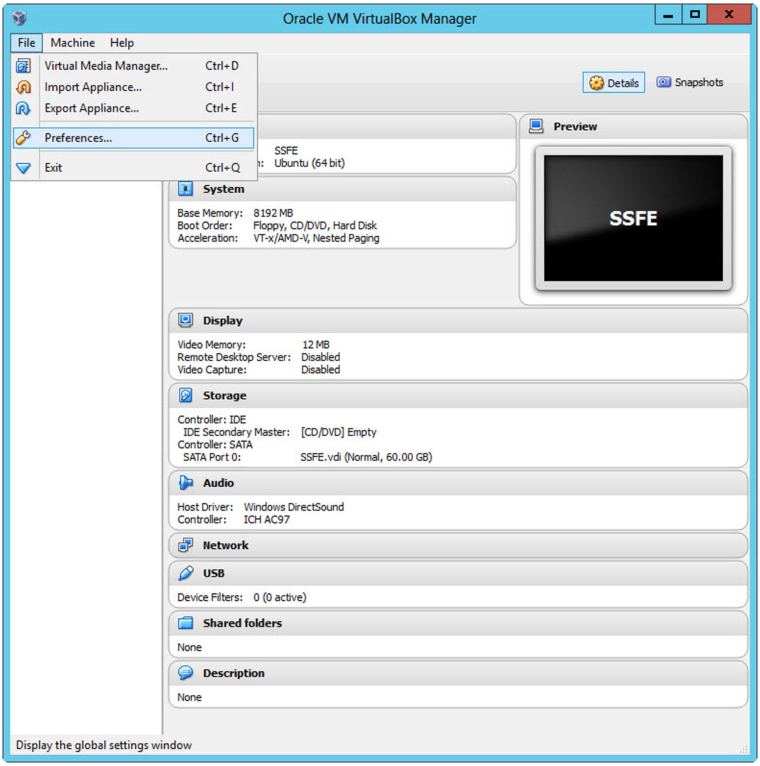
b. Select **Controller: IDE**.

c. Right-click the **CD/DVD** drop-down list and select either a physical drive or a virtual CD/DVD disk file.

The SafeSync installation files are ready to be installed.

**21.** Add a host-only network.

a. Go to **File** > **Preferences**.


Oracle VM VirtualBox Manager
File
Machine
Help
Virtual Media Manager... Ctrl+D
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Preferences... Ctrl+G
Exit Ctrl+Q
Details
Snapshots
Preview
SSFE

SSFE
n: Ubuntu (64 bit)

**System**

Base Memory: 8192 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

**Display**

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

**Storage**

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: SSFE.vdi (Normal, 60.00 GB)

**Audio**

Host Driver: Windows DirectSound
Controller: ICH AC97

**Network**

**USB**

Device Filters: 0 (0 active)

**Shared folders**

None

**Description**

None

Display the global settings window

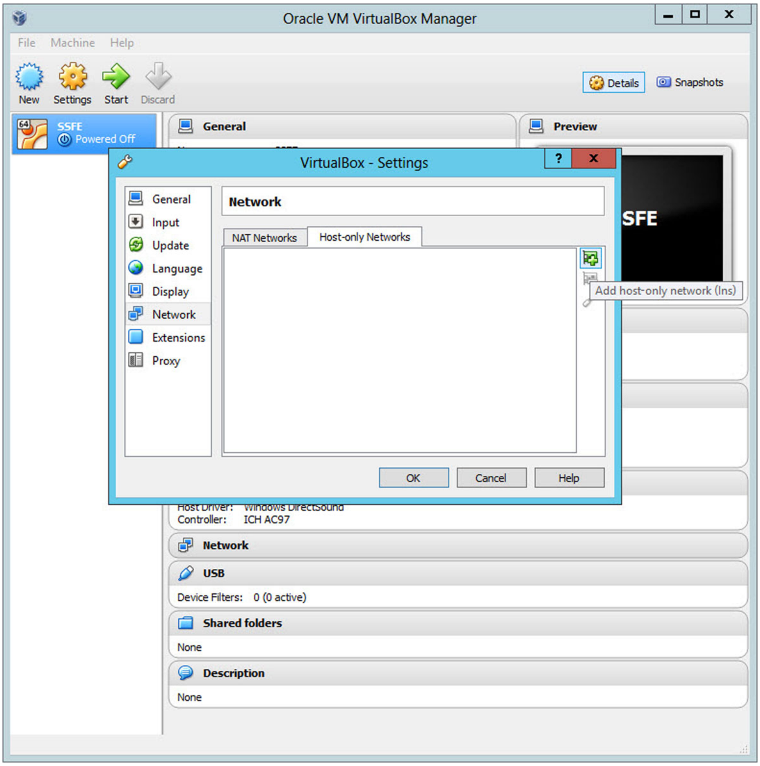
**FIGURE 4-54. Oracle VM VirtualBox File menu**

The **VirtualBox - Settings** screen appears.

b. Click **Network** from the left pane.

The **Network** screen appears.

c. Click the **Host-only Networks** tab.



Host Driver: Windows DirectSound
Controller: ICH AC97

Device Filters: 0 (0 active)

Shared folders: None

Description: None

**FIGURE 4-55. Host-only Networks tab**

d. From the right-hand toolbar, click the **Add host-only network (Ins)** icon ().

A new host-only network is added to the list.

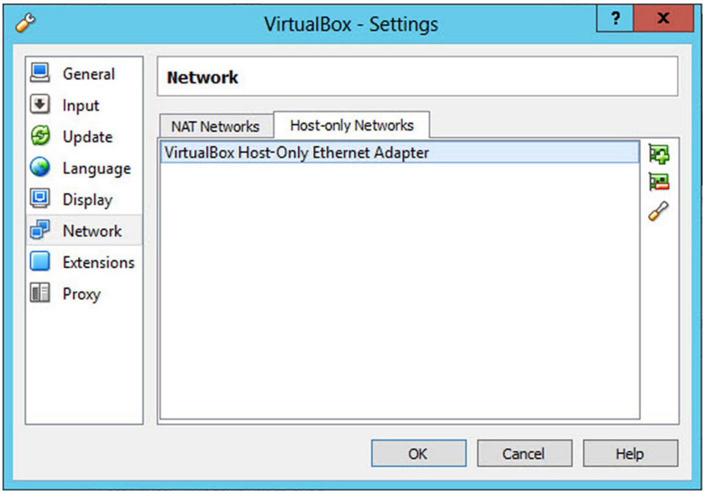


**FIGURE 4-56. New host-only network added**

e. Select the newly created host-only network.

f. Click **OK**.

22. Specify the network settings of **Adapter 1**.

**Note**

In Oracle VM VirtualBox Manager, **Adapter 1** functions as the SafeSync `frontend0` NIC card and **Adapter 2** functions as the SafeSync `database0` NIC card.

For more information, see *Roles of the Network Interface Cards on page 2-10*.

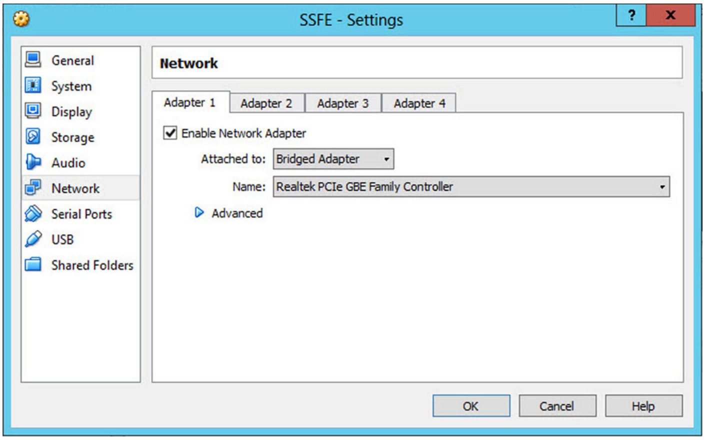
a. Select the SafeSync virtual machine from the list.

b. Click **Settings** from the main menu.

The **Settings** screen for the virtual machine appears.

c. Click **Network** from the left pane of the **Settings** screen.

The content for **Network** appears.



☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

**FIGURE 4-57. Settings - Network (Adapter 1) screen**

d. Select **Enable Network Adapter**.

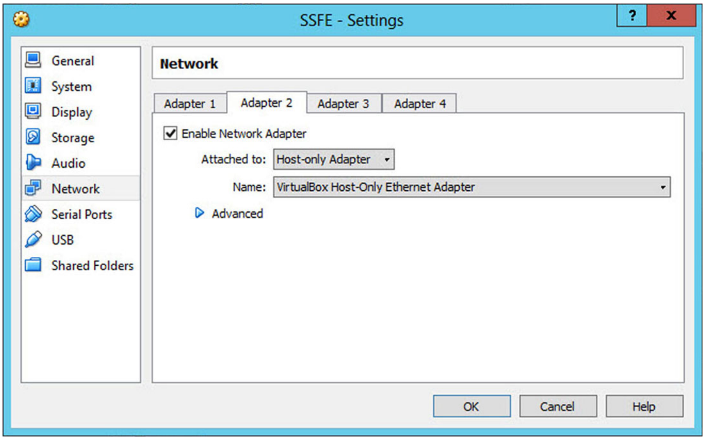
e. Under **Attached to**, select **Bridged Adapter**.

f. Under **Name**, select a network adapter from the list.

**23.** Specify the network settings of **Adapter 2**.

a. Click **Adapter 2**.

The **Adapter 2** tab displays.



☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

**FIGURE 4-58. Settings - Network (Adapter 2) screen**

b. Select **Enable Network Adapter**.

c. Under **Attached to**, select **Host-only Adapter**.

d. Under **Name**, select the host-only adapter from the drop-down list.

**24.** Click **OK**.

The virtual machine is created.

# Chapter 5

# Verifying Installation

This chapter explains how to verify a SafeSync installation.

Topics in this chapter include:

# Verifying File Upload and Download

After installing SafeSync, Trend Micro recommends testing the installation.

### Procedure

1. Using a web browser, log on to the end-user portal ( https://<SafeSync domain name>) using the previously specified password.

   **Note**

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

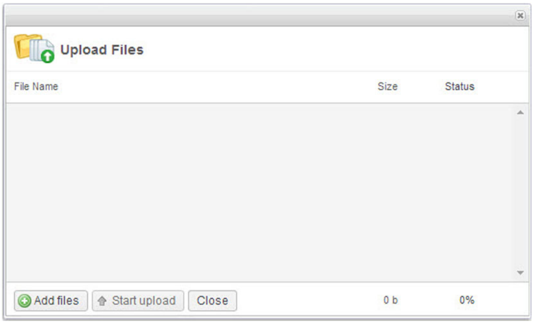
   For more information on updating the SSL certificate, see the SafeSync **Administrator's Guide**.

2. Log on to the SafeSync web console using the administrator account credentials:

   - User name: `administrator`
   - Password: `<web console account password>`

3. Click **Upload Files** to upload files to SafeSync.

   The **Upload Files** screen appears.



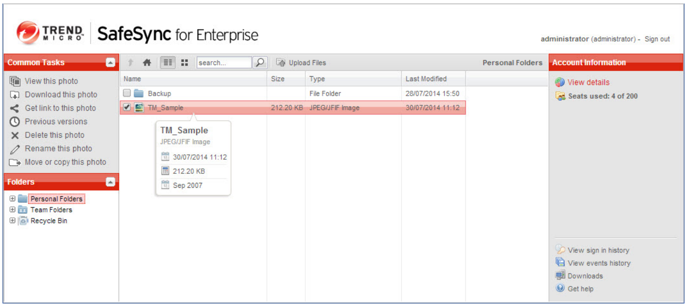
4. Select the files you want to upload and click **Add Files**.

**Note**

Select at least one photo to upload.

5. Click **Start Upload**.

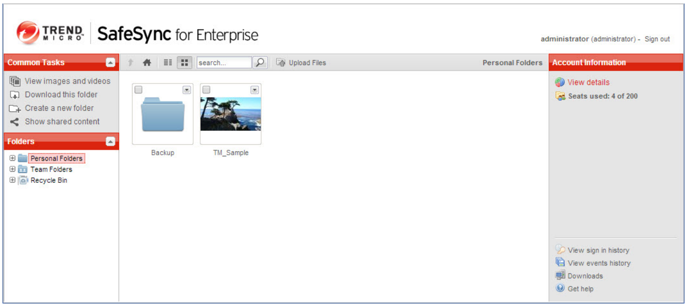
   The files you select will be uploaded to SafeSync.



| | Name | Size | Type | Last Modified |
|---|---|---|---|---|
| □ | Backup | | File Folder | 28/07/2014 15:50 |
| ☑ | TM_Sample | 212.20 KB | JPEG/JFIF Image | 30/07/2014 11:12 |

**Note**

The photos you upload to SafeSync, display as a thumbnail in the content area.



6. Select the files that were just uploaded and click **Download the selected items**.

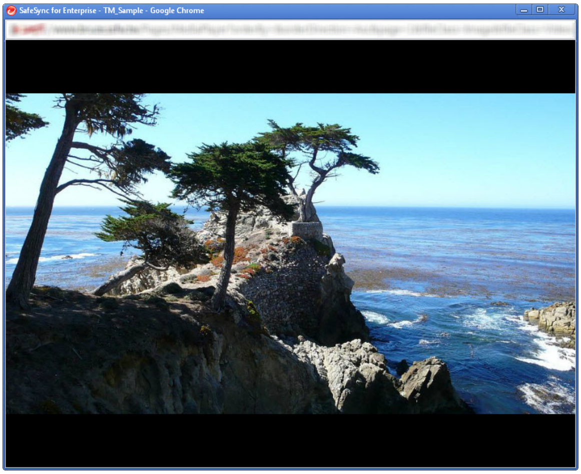
   A dialog box appears.

7. Specify where to download the selected files and click **OK**.

   The selected files download to the location you specify.

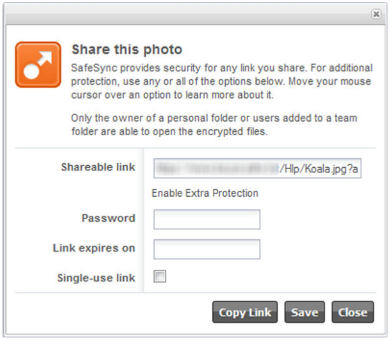
8. Select a photo you uploaded and click **View this photo**.

   The photo appears in its original size.



9. Share your files by selecting a file and clicking **Get link to this file**.

   SafeSync creates a shareable link to that file. Recipients of the link can access the files by clicking the link.



**Share this photo**

SafeSync provides security for any link you share. For additional protection, use any or all of the options below. Move your mouse cursor over an option to learn more about it.

Only the owner of a personal folder or users added to a team folder are able to open the encrypted files.

| | |
|---|---|
| Shareable link | [redacted]/Hlp/Koala.jpg?a |
| | Enable Extra Protection |
| Password | |
| Link expires on | |
| Single-use link | □ |

# 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 5-1. 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. |

### 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

- ⚠: Warning

# Checking Services

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 assume root permission:

   ```
   sudo -i
   ```

3. Provide the system server password when prompted.

4. Run the following commands:

   a. To check if important SafeSync services were installed:

   ```
   root@appliance1:~# supervisorctl status
   ```

   > **Note**
   >
   > For the complete list of required services, see *Services on page 7-3*.

   b. To check if important SafeSync services are working properly:

   ```
   root@appliance1:~# supervisorctl status
   ```

   The following services should be listed as `RUNNING`:

   - healthcheck
   - mgmtui
   - perlbal80
   - perlbalmgmtui
   - thin

5. Run the following commands to check if individual services are running:

| Service | Command |
|---|---|
| apache2 | `root@appliance1:~# /etc/init.d/apache2 status` |
| avscand | `root@appliance1:~# /etc/init.d/avscand status` |
| grunjobs | `root@appliance1:~# /etc/init.d/grunjobs status` |
| kmsd | `root@appliance1:~# /etc/init.d/kmsd status` |
| lighttpd | `root@appliance1:~# /etc/init.d/lighttpd status` |
| memcached | `root@appliance1:~# /etc/init.d/memcached status` |
| mysql | `root@appliance1:~# /etc/init.d/mysql status` |
| nginx | `root@appliance1:~# /etc/init.d/nginx status` |
| tmsyslog | `root@appliance1:~# /etc/init.d/tmsyslog status` |

6. Run the following commands to check service processes:

| Service | Command |
|---|---|
| gearman-job-server | `root@appliance1:~# ps aux \| grep gearman-job-server` |
| keepalived | `root@appliance1:~# ps aux \| grep keepalived` |
| mogilefsd | `root@appliance1:~# ps aux \| grep mogilefsd` |
| mogstored | `root@appliance1:~# ps aux \| grep mogstored` |

# Verifying MySQL HA

Verify the high availability deployment of your MySQL database.

## Procedure

1. On the Primary server, log on to the MySQL console and create database test1.

   a. `root@appliance1:~# mysql -u root -p`

   b. At the resulting prompt, type the MySQL password.

   > **Note**
   >
   > The default password is `safesync`.

   ```
   root@localhost [(none)]> create database test1;
   ```

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

2. On the Secondary server, log on to the MySQL console and verify that database test1 now exists there as well.

   a. `root@appliance2:~# mysql -u root -p`

   b. At the resulting prompt, type the MySQL password.

   c. `root@localhost [(none)]> show databases;`

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| auth               |
| data               |
| gearman            |
| mogilefs           |
| mysql              |
| osdp               |
| shard_1            |
| test1              |
+--------------------+
9 rows in set (0.00 sec)
```

3. After verifying, drop database test1:

   a.
   ```
   root@localhost [(none)]> drop database test1;

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

## Failover

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

1. The Primary and Secondary servers must be installed and running correctly.

2. The administrator must setup name services to provide for failover in DNS.

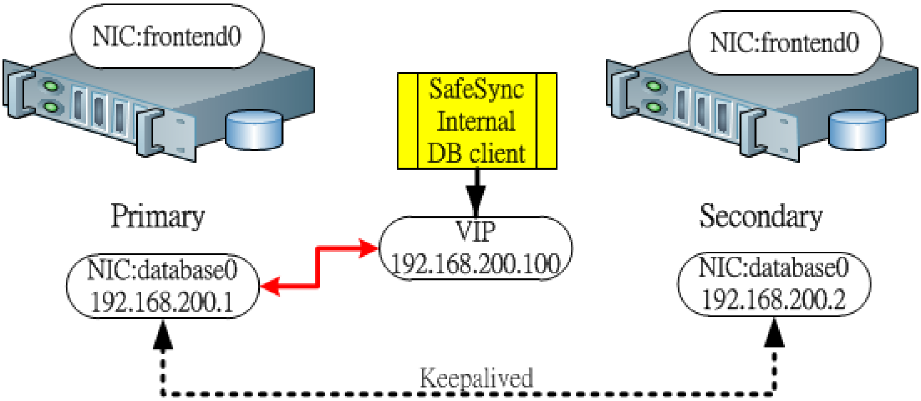
**Note**

Actual partitions and size may vary per server.

## Internal Failover

The SafeSync failover mechanisms rely on **keepalived** and MySQL HA. The third-party service **keepalived** uses the VRRP protocol to provide and manage a virtual IP.

When the primary MySQL cannot provide service, the VIP fails over to the secondary MySQL database.


NIC:frontend0
SafeSync Internal DB client
NIC:frontend0
Primary
VIP 192.168.200.100
Secondary
NIC:database0 192.168.200.1
NIC:database0 192.168.200.2
Keepalived

## Verifying File Replication

Check the file replication status of your high availability deployment.

**Procedure**

1. Upload a test file (test.txt) to SafeSync.
2. Log on to the server shell.
3. Log on to MySQL using the following command.

```
root@appliance1:~# mysql -uroot -p shard_1
```

   a. Type the password when prompted.

**Note**

The default password is “safesync”.

4. Get the file data_id from the database.

```
root@localhost [shard_1]> select data_id from objects where
name=' test.txt ';
```

```
+----------+
| data_id |
+----------+
|     303 |
+----------+
1 row in set (0.00 sec
```

5. Check that two file paths exist in the MogileFS.

```
root@appliance2:~# mogtool --trackers=tracker1:6001 --
domain=osdp locate 303
```

```
http://192.168.200.2:7500/dev21/0/000/001/0000001145.fid
http://192.168.200.1:7500/dev13/0/000/001/0000001145.fid
#2 paths found
```

# Chapter 6

## Post-Installation Tasks

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

Topics in this chapter include:

# 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.

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 file system, and then adds the disk to MogileFS system. The file system mount points for disk are `/storage/mogdata/dev [primary: 1, secondary: 2] [number]`.

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

When creating new mount points for new MogileFS storage, always follow this sequence. In this case, the second disk on the primary server should be mounted to `/storage/mogdata/dev12`, the third disk on `/storage/mogdata/dev13`. Consequently, for the secondary server, the mount points will be `/storage/mogdata/dev22` and `/storage/mogdata/dev23`.

Reusing a mount point that was previously deleted is not allowed.

# 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:

```
# sudo -i
```

3. Specify the root password.

4. Format the disk before mounting it to SafeSync:

   This example uses **sdb** as the name of the new disk.

```
# dmesg | grep sdb

# parted -s /dev/sdb mklabel gpt

# parted -s /dev/sdb mkpart primary ext4 0% 100%

# partprobe /dev/sdb
```

5. Mount the disk:

```
# mkdir /storage/mogdata/dev12

# mkfs -t ext4 /dev/sdb1

# mount /dev/sdb1 -t ext4 /storage/mogdata/dev12
```

6. Add the disk to the mogile system:

```
# chown www-data:mogstored /storage/mogdata/dev12

# chmod g+w /storage/mogdata/dev12

# mogadm --trackers=tracker1:6001 device add osdp-store1 12 --status=alive
```

7. Use the vim editor to change /etc/fstab to check that it contains the new disk data.

```
# vim /etc/fstab
```

   a. Add a line to /etc/fstab with the new disk data.

```
/dev/sdb1 /storage/mogdata/dev12 ext4
defaults,user_xattr,_netdev 1 2
```

8. Check the result.

```
# 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.

**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.

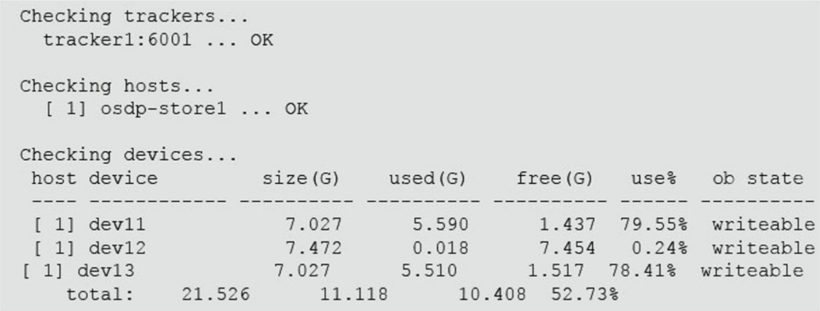
```
# mogadm --trackers=tracker1:6001 device add osdp-store1 13 --
status=alive
```

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
    ```

# Chapter 7

# Frequently Asked Questions (FAQs)

This chapter answers various Frequently Asked Questions.

Topics in this chapter include:

# 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.\nCompilation failed in require at /opt/TrendMicro/
OSDP/Lib/Storage/ForkControl.pm line 4.\nBEGIN failed--compilation aborted
at /opt/TrendMicro/OSDP/Lib/Storage/ForkControl.pm line 4.\nCompilation failed
in require at /opt/TrendMicro/OSDP/Config/startup.pl line 4.\nBEGIN failed--
compilation aborted at /opt/TrendMicro/OSDP/Config/startup.pl line
4.\nCompilation failed in require at (eval 2) line 1.\n[Fri Dec 14 20:56:06 2012] [error]
Can't load Perl file: /opt/TrendMicro/OSDP/Config/startup.pl for server (null):0,
exiting......fail!
```

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 2-4*

# Services

## What services should be installed after a successful SafeSync installation?

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

apache2

avscand

gearman-job-server

grunjobs

healthcheck

keepalived

kmsd

lighttpd

memcached

mgmtui

mogilefsd

mogstored

mysql

nginx

perlbal80

perlbalmgmtui

thin

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
   ```

# Chapter 8

## Contacting Technical Support

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

Topics in this chapter include:

# 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)<br>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

# Index

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: APEM26485/140711