TREND MICRO™

2.0 TREND MICRO™ Safe Mobile Workforce

Installation and Deployment Guide

Centrally-managed workspace for mobile users

Endpoint Security

Document Part No.: MWEM26892/150318

Release Date: April 2015

Protected by U.S. Patent No.: 5,951,698

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 in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introducing Safe Mobile Workforce

Chapter 2: Installing on Bare Metal Servers

Chapter 3: Installing on VMware vSphere ESXi Hypervisor

Chapter 4: Installing on VMware Workstation

Chapter 5: Installing on Microsoft Hyper-V

Chapter 6: Installing on Citrix XenServer

Chapter 7: Post-Installation Configuration

Appendix A: Network Port Configurations

Preface

Preface

Welcome to the Trend Micro™Safe Mobile Workforce™ version 2.0 Administrator's Guide. This guide provides detailed information about all Safe Mobile Workforce configuration options. Topics include how to update your software to keep protection current against the latest security risks, how to configure and use policies to support your security objectives, configuring scanning, synchronizing policies on mobile devices, and using logs and reports.

This preface discusses the following topics:

Audience

The Safe Mobile Workforce documentation is intended for both administrators—who are responsible for administering and managing Mobile Device Agents in enterprise environments—and mobile device users.

Administrators should have an intermediate to advanced knowledge of Windows system administration and mobile device policies, including:

- Installing and configuring Windows servers
- Installing software on Windows servers
- Configuring and managing mobile devices (such as smartphones and Pocket PC/ Pocket PC Phone)
- Network concepts (such as IP address, netmask, topology, and LAN settings)
- Various network topologies
- Network devices and their administration
- Network configurations (such as the use of VLAN, HTTP, and HTTPS)

Safe Mobile Workforce Documentation

The Safe Mobile Workforce documentation consists of the following:

- *Installation and Deployment Guide*—this guide helps you get "up and running" by introducing Safe Mobile Workforce, and assisting with network planning and installation.
- *Administrator's Guide*—this guide provides detailed Safe Mobile Workforce technologies and configuration.
- *Online help*—the purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values.

- *Readme*—the Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

Tip

Trend Micro recommends checking the corresponding link from the Documentation Center (http://www.docs.trendmicro.com/) for updates to the product documentation.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

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

Convention	Description
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Chapter 1

Introducing Safe Mobile Workforce

This chapter assists administrators in planning the server components for Trend Micro™Safe Mobile Workforce™.

This chapter contains the following sections:

About Safe Mobile Workforce

Trend Micro Safe Mobile Workforce is a service that hosts independent workspaces for every user. A user workspace is based on Android operating system, which is accessible via Safe Mobile Workforce mobile client application installed on an Android, iOS or a Windows mobile device. Using the mobile client application, users can access the same mobile environment that includes all their applications and data from any location, without being tied to a single mobile device. The mobile client application preserves the original Android user experience by providing all the Android features and their controls to the user.

Since all the workspaces are hosted onto the server and maintained by the administrator, Safe Mobile Workforce enables a clear separation between the personal and corporate data available to the users. This clear separation ensures data safety and provides more centralized and efficient workspaces that are easier to manage and maintain.

Why Use Safe Mobile Workforce

Safe Mobile Workforce provides the following benefits:

BENEFIT	DESCRIPTION
Data Protection	All enterprise applications and data are saved in secure corporate servers under administrator's control.
Good User Experience	Users can use their personal mobile device to access corporate data, and therefore the mobile OS user experience is preserved.
	Easy-to-use system to access corporate virtual workspace.
	Natural screen touch experience for smartphones and tablets.
Simplified Management	Administrator can centrally manage all users from single Web console.

Benefit	Description
Single Sign-On	Reducing time spent in re-entering passwords in virtual workspace.
	Reducing administration cost due to lower number of IT help desk calls about passwords.
Workspace Customization	Administrator can create a personal virtual mobile workspace for each employee.
	Administrator can centrally customize applications for employees in their virtual workspaces from the server.
User-based Profile	Provides user based profile management.
	Users can use their own virtual workspace from any of their mobile devices.
Manageable Life Cycle	Administrator can remotely manage a workspace's entire life cycle-from provisioning to the end of life.
Easy Deployment	Provides on-premise deployment.
	Provides self-contained Linux-based operating system for easy deployment.
Integration with Trend Micro SafeSync	Provides integration with Trend Micro SafeSync to provide cloud based file storage to all users.
Integration with Enterprise Infrastructure	Provides integration with LDAP and external storage.

System Requirements

Review the following requirements before installing Safe Mobile Workforce.

Table 1-1. System Requirements for Server

Component	Requirements
Processor	64-bit x86 four-core Intel processor with SSSE3 support

Component	Requirements
Memory	4-GB
Hard disk	30-GB available for installation
Network Cards (NIC)	Two 1-GB NICs

Table 1-2. System Requirements for Secure Access

Component	Requirements
Processor	64-bit x86 four-core
Memory	4-GB
Hard disk	30-GB available for installation
Network Cards (NIC)	One 1-GB NIC

Table 1-3. System Requirements for Safe Mobile Workforce mobile client

Component	Requirements
Operating system	• iOS 4.3 or later • Android 2.3 or later • Windows 8.1/RT 8.1/Windows Phone 8.1

Architecture of Safe Mobile Workforce

Depending on your company scale and requirements, Trend Micro Safe Mobile Workforce enables you to deploy single or multiple Servers and Secure Access. In the case of multiple servers, Safe Mobile Workforce balances the load between servers to achieve maximum efficiency.

Single Server Installation Model

The Single Server Installation Model is the deployment of only one Safe Mobile Workforce Server and Secure Access.

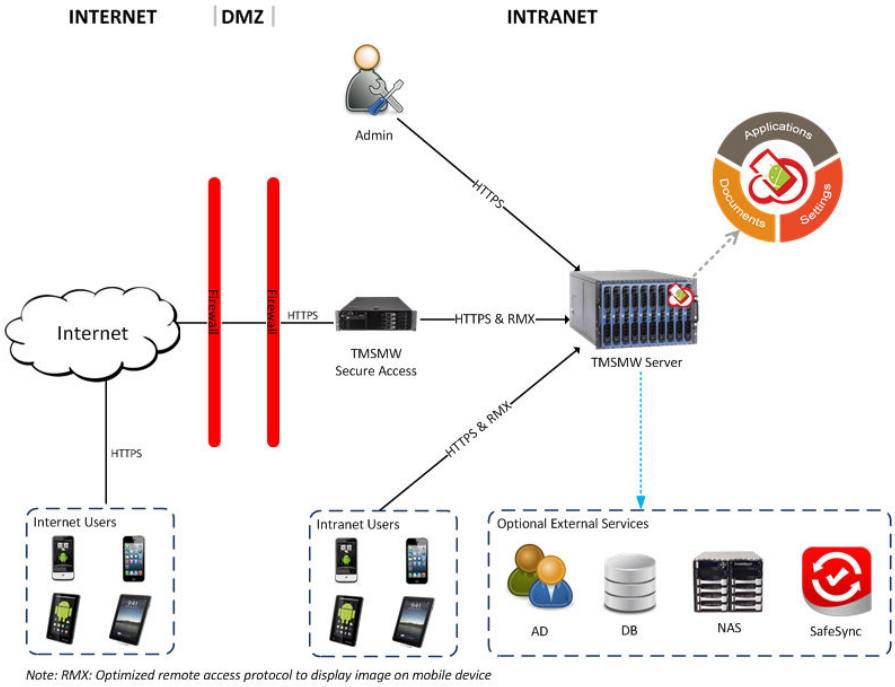


FIGURE 1-1. Trend Micro Safe Mobile Workforce Single Server Installation Model

Multiple Server Installation Model

The Multiple Server Installation Model is the deployment of more than one Safe Mobile Workforce Server and Secure Access.

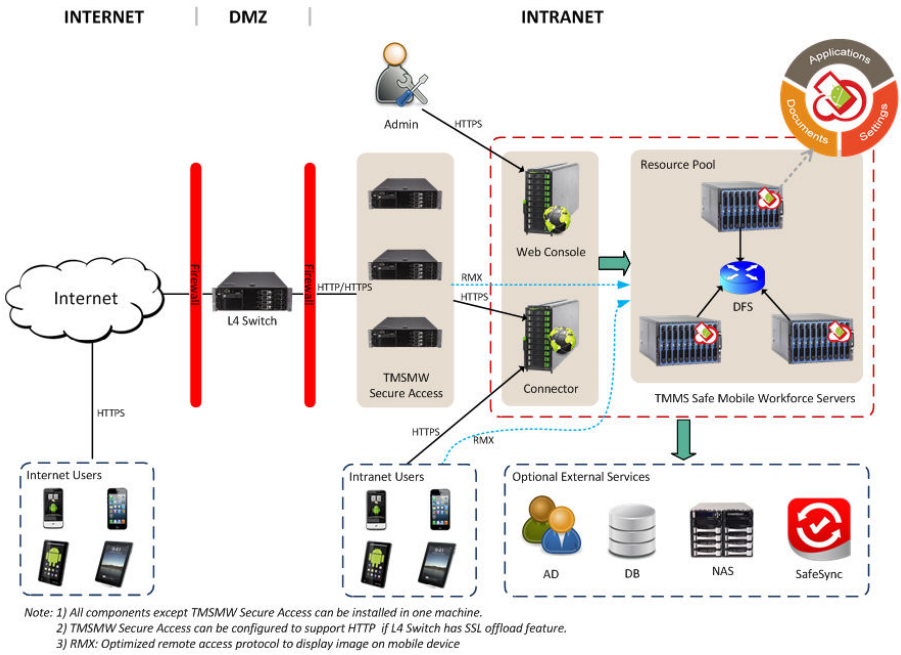


FIGURE 1-2. Trend Micro Safe Mobile Workforce Multiple Server Installation Model

Components of Safe Mobile Workforce

The Safe Mobile Workforce system includes the following components:

TABLE 1-4. Safe Mobile Workforce Components

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Safe Mobile Workforce Server	The Safe Mobile Workforce Server contains Web Console, Web Service, Controller and Resource Pool. • Web console provides central management console for administrator. • Web service manages user logon, logoff and the connection to user's workspace. • Controller allows Web console to manage a resource pool. • Resource pool hosts workspaces. Each workspace runs as a Safe Mobile Workforce instance.	Required
Safe Mobile Workforce Mobile Client Application	The mobile client application is installed on the mobile devices. The client application connects with the Safe Mobile Workforce server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Safe Mobile Workforce Secure Access enables mobile clients to access Safe Mobile Workforce server via Internet. See *Why Use Secure Access on page 1-8* for more information.	Optional
Active Directory	The Safe Mobile Workforce server imports groups and users from Active Directory.	Optional
External Database	External Database provides scalable data storage for user data. By default, Safe Mobile Workforce server maintains a database on its local hard drive. However, if you want to store the data on an external location, then you will need to configure External Database.	Optional

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
External Storage	Using this option will enable you to store the user data in an external storage.	Optional
SafeSync Server	SafeSync Server provides file storage for all users.	Optional

Why Use Secure Access

Safe Mobile Workforce Secure Access enables mobile device clients to securely access the Safe Mobile Workforce server via the Internet. If you do not want to expose the Safe Mobile Workforce Server on the Internet, not even in the DMZ, you will need to install Secure Access. If required, you can install multiple Secure Access through an L4 switch for load balancing.

The following are the advantages of using Secure Access:

- If using Secure Access, you only need to open one IP Address and one port number for mobile clients. The Secure Access receives mobile device client enrollment request through HTTPS, and relays it to the Safe Mobile Workforce server.
- Secure Access and SMW server use firewall for outbound network connections to ensure security.

Secure Access can be deployed in DMZ or Intranet, using single or two network cards:

- You need only one network card, if you configure the Internet mobile devices and Secure Access in different networks.
- You need two network cards, if you configure the Internet mobile devices and Secure Access in the same network, in bridge mode. That is, one network card provides connection between the mobile device clients and Secure Access, while the other network card connects Secure Access with the Safe Mobile Workforce server.

Chapter 2

Installing on Bare Metal Servers

This chapter provides the information that you will need to install Trend Micro Safe Mobile Workforce.

This chapter contains the following sections:

Installing Safe Mobile Workforce Server on a Bare Metal Server

Any existing data or partitions are removed during the installation process. Back up any existing data on the system (if any) before installing Safe Mobile Workforce.

Procedure

1. Power on the Bare Metal server where you want to install Safe Mobile Workforce.
2. Insert the installation DVD into the DVD drive, and reboot the server.

   The Safe Mobile Workforce installation menu appears.
3. Select **Install Safe Mobile Workforce Server** and press **Enter**.

   The setup starts loading the installation image file. After it completes, **Trend Micro License Agreement** screen appears.
4. Click **Accept** to agree to the license agreement.

   A screen appears where you can select a keyboard for the operating system.
5. Select a keyboard for the operating system, and then click **Next**.

   A screen appears displaying the hardware components.
6. Click **Next**.

   A screen appears where you can configure network and general settings.
7. Configure the following:
   - **Interface Settings for eth0**:
     - **IP address**: the internal IP address for Safe Mobile Workforce server Web console.
     - **Subnet mask**: the subnet mask for the Safe Mobile Workforce server internal IP address.
   - **Interface Settings for eth1**:

- **IP address**: the external IP address for mobile client application to access Safe Mobile Workforce server.
- **Subnet mask**: the subnet mask for the external IP address.

- **General Settings**:
  - **Host name**: type a Host name for Safe Mobile Workforce server.
  - **Gateway**
  - **Primary DNS**
  - **Secondary DNS**

Note

Make sure that the network interfaces **eth0** and **eth1** are connected to the network. If the network interface eth0 is not connected to the network, you will not be able to use the Web Console to access the server. If the network interface **eth1** is not connected to the network, the mobile client application will not be able to connect to the server.

8. Click **Next**.
9. Select your time zone and click **Next**.
10. Set your operating system password for the administrator account, and click **Next**.

    The **Summary** screen appears.
11. Check the summary of your configuration and if you are satisfied with the configuration, click **Next** and then click **Continue** on the confirmation dialog box that appears.

    The setup will start installing Safe Mobile Workforce on the server. After the installation completes, the **Installation Completed** screen appears.
12. Click **Reboot** to reboot the server. After the reboot completes, log on to the server using the password you set up in *step 9 on page 2-3* of this procedure.

Installing Safe Mobile Workforce Secure Access on a Bare Metal Server

Any existing data or partitions are removed during the installation process. Back up any existing data on the system (if any) before installing Secure Access.

Procedure

1. Power on the Bare Metal server where you want to install Safe Mobile Workforce Secure Access.
2. Insert the installation DVD into the DVD drive, and reboot the server.

   The Secure Access installation menu appears.
3. Select **Install Secure Access** and press **Enter**.

   The setup starts loading the installation image file. After it completes, **Trend Micro License Agreement** screen appears.
4. Click **Accept** to agree to the license agreement.

   A screen appears where you can select a keyboard for the operating system.
5. Select a keyboard for the operating system, and then click **Next**.

   A screen appears displaying the hardware components.
6. Click **Next**.

   A screen appears where you can configure network and general settings.
7. Configure the following:
   - **Network Devices**: select the network interface that you want to use to connect to the network. (Usually it is the network interface eth0).
   - **Interface Setting**:
     - **IP address**: the IP address for Safe Mobile Workforce server.
     - **Subnet mask**: the subnet mask for the Safe Mobile Workforce server IP address.

- **General Settings**:
  - **Host name**: type a Host name for Safe Mobile Workforce server.
  - **Gateway**
  - **Primary DNS**
  - **Secondary DNS**

Note

If you are deploying Safe Mobile Workforce server and Secure Access in different networks., you will need to configure another network interface, **eth1**. Use one network interface to connect Secure Access to the Safe Mobile Workforce server, and another network interface to provide connection for Mobile Clients.

8. Click **Next**.

   A screen appears where you can configure Secure Access settings.

9. Configure the following:

   - **Protocol**: select and configure one of the following protocols for mobile devices to connect to Secure Access.
     - **HTTP**
     - **HTTPS**

Note

If your network does not include a layer 4 (L4) switch that can convert HTTPS traffic to HTTP, select HTTPS protocol on this screen.

   - **Safe Mobile Workforce server IP address**: type the IP address you configured for **eth1** of the Safe Mobile Workforce server.

10. Click **Next**.
11. Select your time zone and click **Next**.
12. Set your operating system password for the administrator account, and click **Next**.

The **Summary** screen appears.

13. Check the summary of your configuration and if you are satisfied with the configuration, click **Next** and then click **Continue** on the confirmation dialog box that appears.

    The setup will start installing Secure Access on the server. After the installation completes, the **Installation Completed** screen appears.

14. Click **Reboot** to reboot the server.

    After the reboot completes, log on to the server using the password you set up in *step 11 on page 2-5* of this procedure.

Chapter 3

Installing on VMware vSphere ESXi Hypervisor

This chapter provides the information that you will need to create and configure a virtual machine on VMware VSphere ESXi Hypervisor and install Trend Micro Safe Mobile Workforce.

This chapter contains the following sections:

Installing Safe Mobile Workforce Server

Installing Safe Mobile Workforce on VMware vSphere ESXi Hypervisor involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 3-2*).
2. Configuring VM Network Card (See *Step 2: Configuring VM Network Card (Optional) on page 3-13*).
3. Installing Safe Mobile Workforce (See *Step 3: Installing Safe Mobile Workforce on VMware ESXi on page 3-17*).

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the ESXi server hard drive, or any other location that can be accessed from the computer where ESXi server is installed.
2. Start **VMware vSphere Client**.
3. Click **File** > **New** > **Virtual Machine** from the menu.

   The **Create New Virtual Machine** screen appears.
4. Select **Typical** and click **Next**.

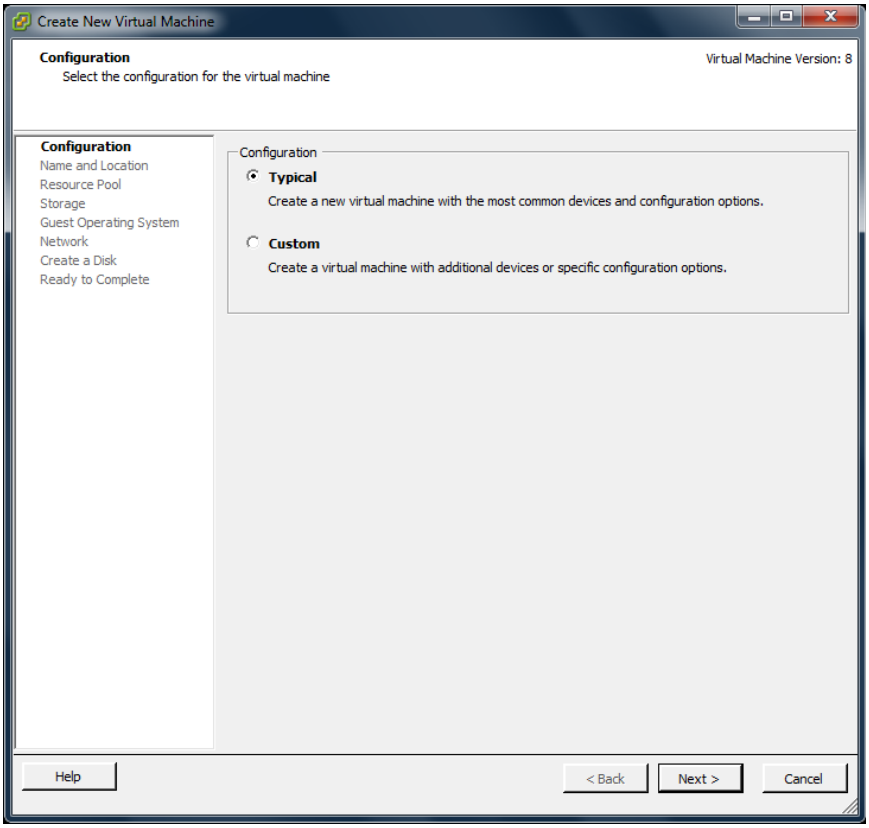


FIGURE 3-1. Select Configuration

The **Name and Location** screen appears.

5. Type a name for the virtual machine, and click **Next**.

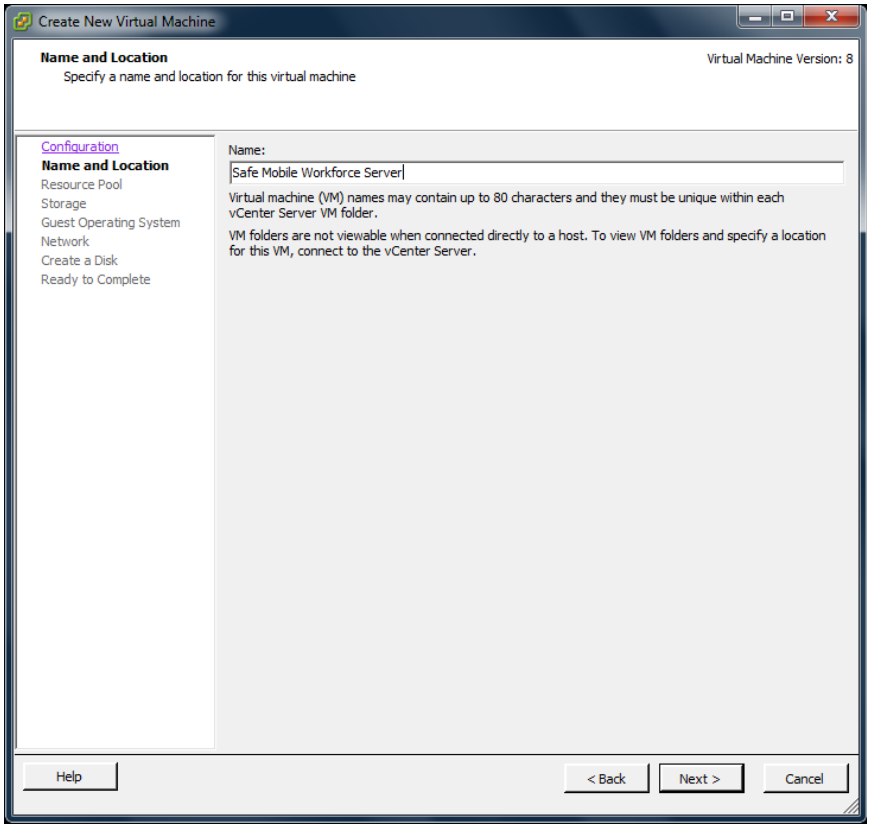


FIGURE 3-2. Type a name for the new virtual machine

The **Resource Pool** screen appears.

Note

The **Resource Pool** screen will not appear if you had selected a resource pool on the left resource tree, instead of the root computer. Skip *step 6 on page 3-4* and proceed to *step 7 on page 3-5* to configure the **Storage** screen.

---

6. Select the resource pool in which you want to run this virtual machine and click **Next**.

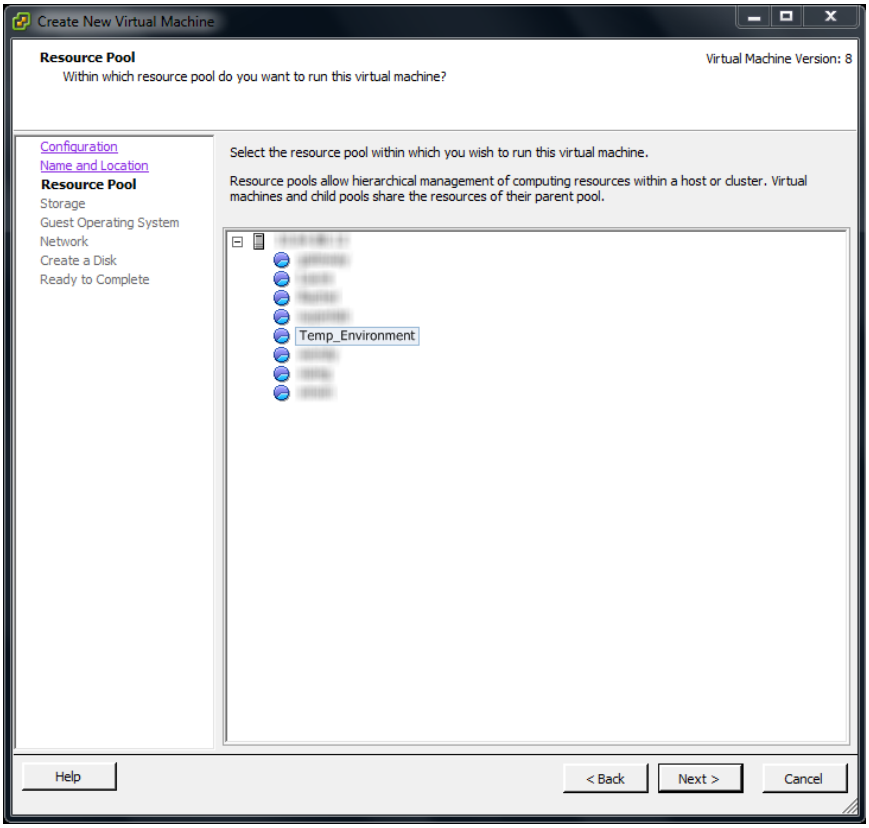


FIGURE 3-3. Select a resource pool

The **Storage** screen appears.

7. Select the disk storage for the virtual machine files and click **Next**.

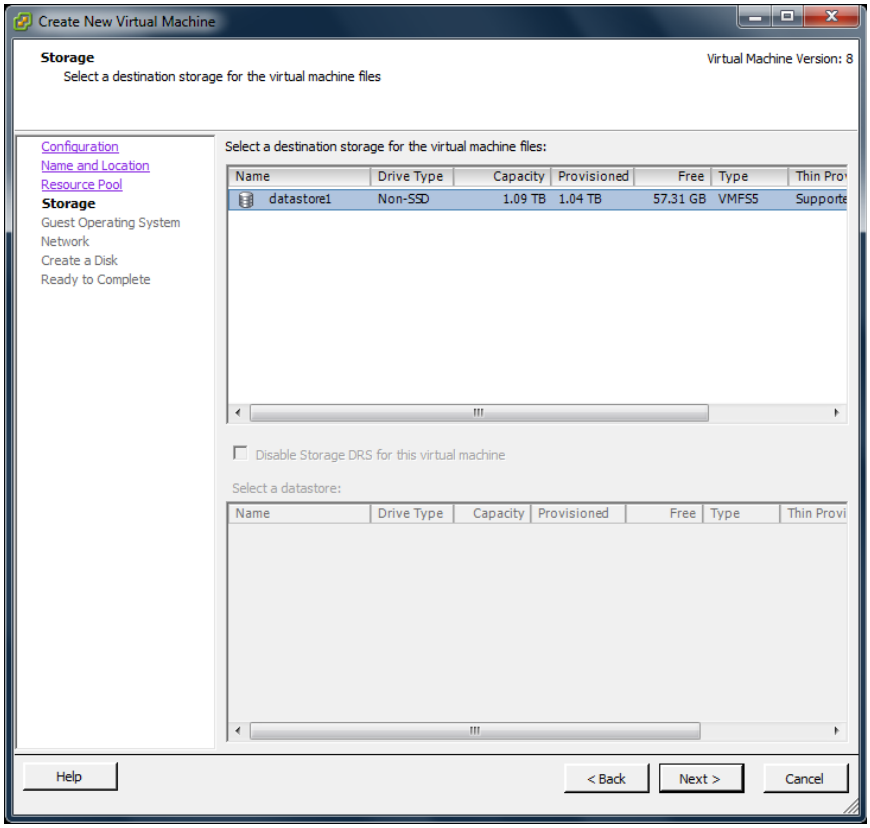


FIGURE 3-4. Select a storage to install Safe Mobile Workforce Server

The **Guest Operating System** screen appears.

8. Select **Linux** and choose **Other Linux (64-bit)** from the drop-down and click **Next**.

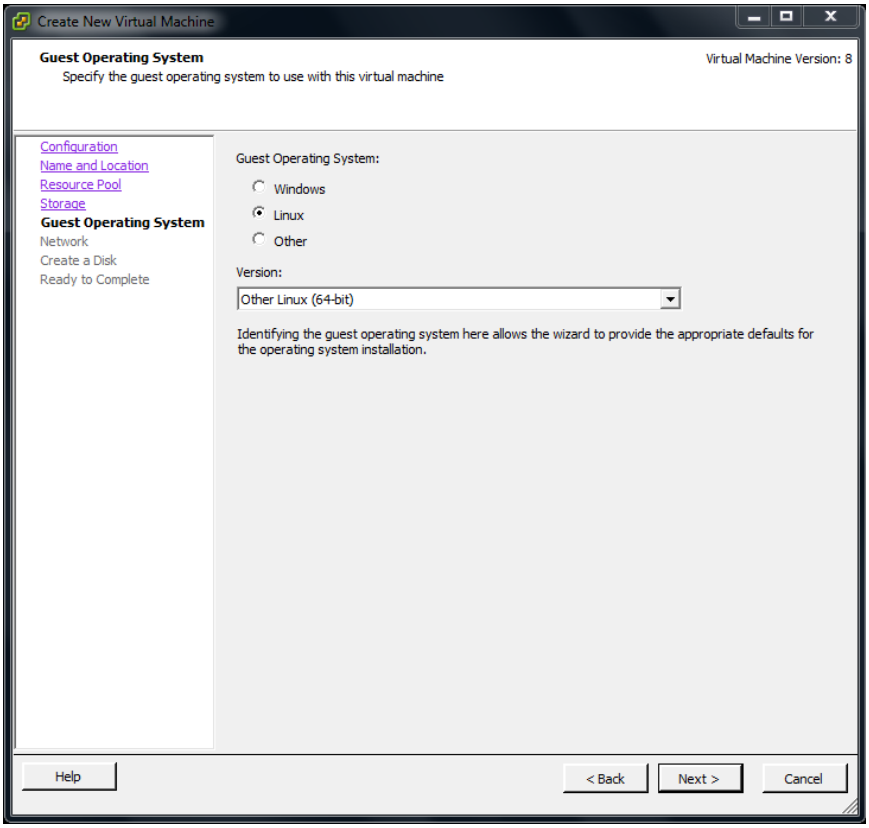


FIGURE 3-5. Select the guest operating system

The **Network** screen appears.

9. Select **2** NICs and specify the following settings:

TABLE 3-1. Network Settings for Safe Mobile Workforce

NAME	NETWORK	ADAPTER	CONNECT AT POWER ON
NIC 1	VM Network	E1000	Enabled

NAME	NETWORK	ADAPTER	CONNECT AT POWER ON
NIC 1	VM Network	E1000	Enabled

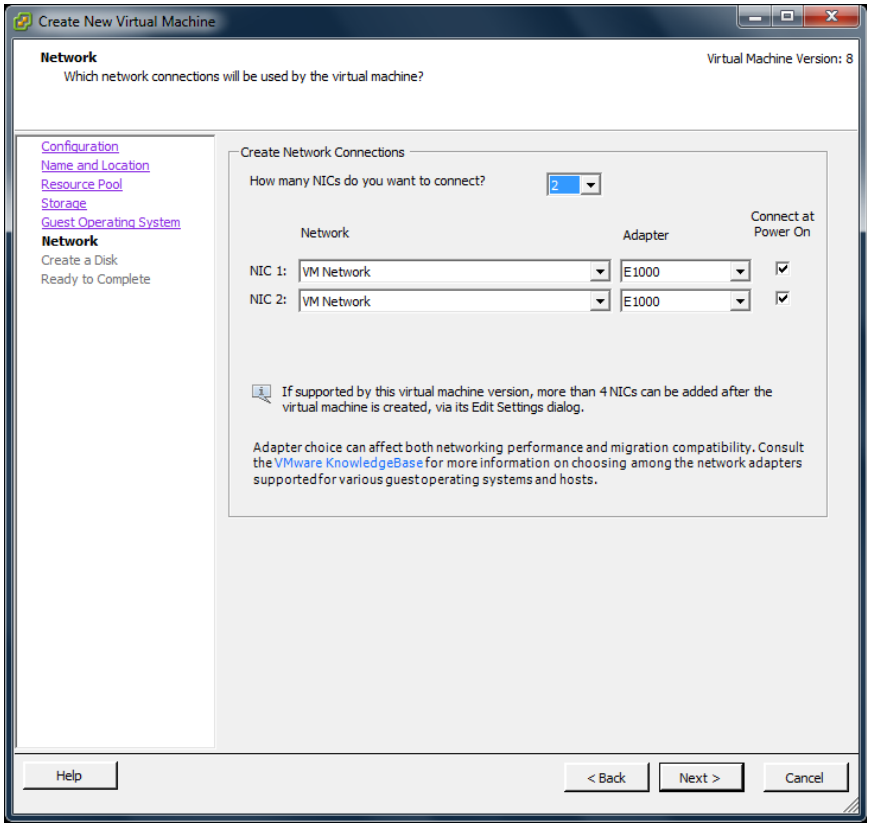


FIGURE 3-6. Create network connections

10. Click **Next**.

    The **Create a Disk** screen appears.

11. On the **Create a Disk** screen, do the following:

a. Select at least 30-GB of virtual disk space for Safe Mobile Workforce.

b. Select **Thick Provision Lazy Zeroed**

c. Click **Next**.

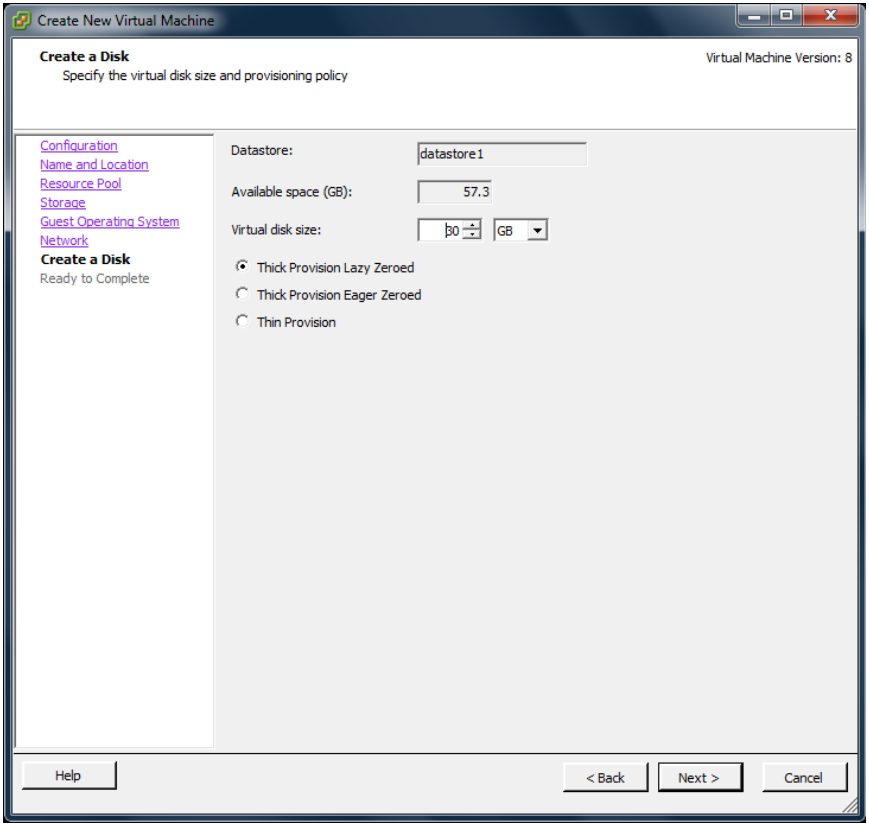


FIGURE 3-7. Specify Hard Disk Space

The **Ready to Complete** screen appears.

12. Select **Edit the virtual machine settings before completion** and click **Continue**.

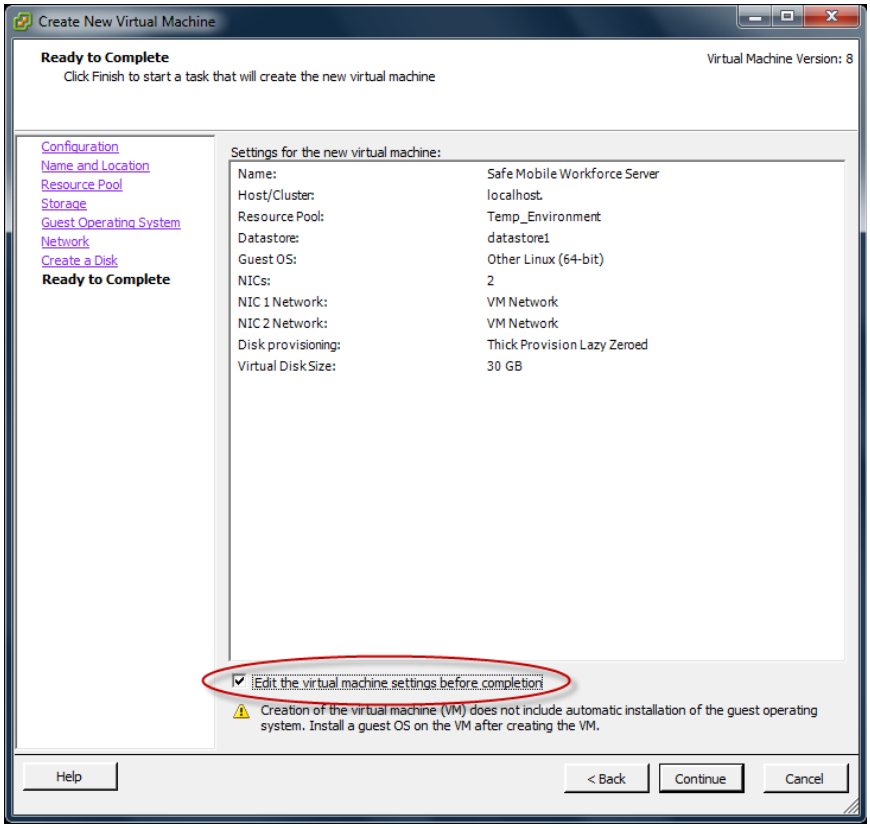


FIGURE 3-8. Ready to Complete

The **Virtual Machine Properties** screen appears.

13. On the **Hardware** tab, do the following:

    a. Select **Memory (adding)**

    Memory Configuration appears in the right pane.

    b. In the **Memory Size** field, select at least 4-GB.

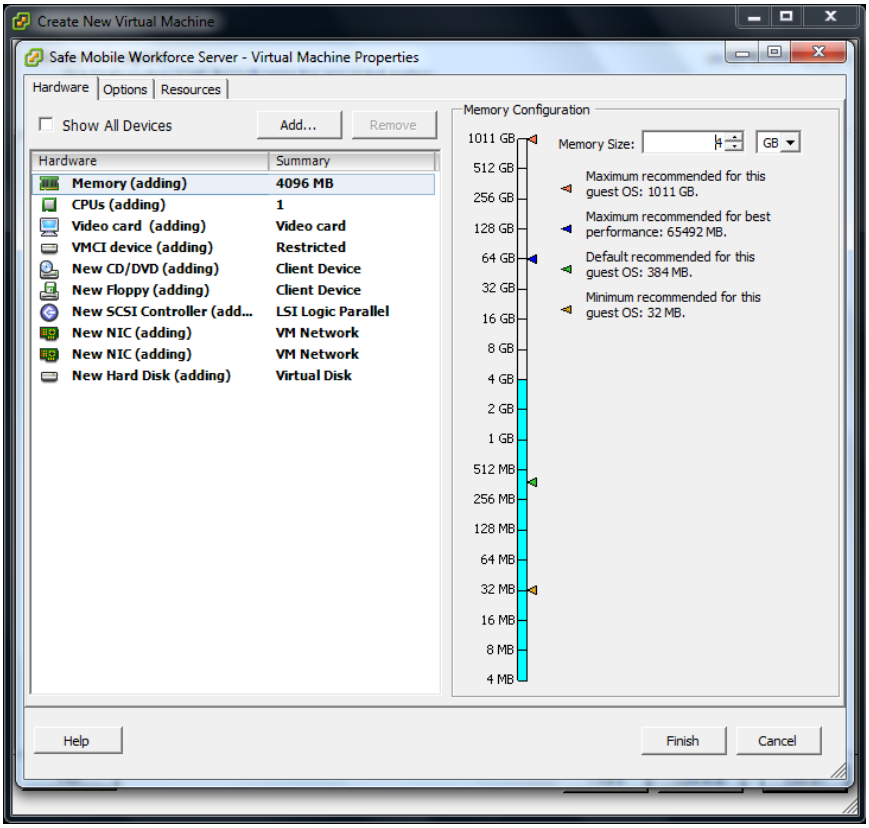


FIGURE 3-9. VM Properties - Memory Configuration

14. On the **Hardware** tab, select **CPU (adding)**.

    CPU settings appear in the right pane.

15. In the CPU settings, do the following:

    - In the **Number of virtual sockets** drop-down list, select **2**.

      In the **Number of cores per socket** drop-down list, select **2**.

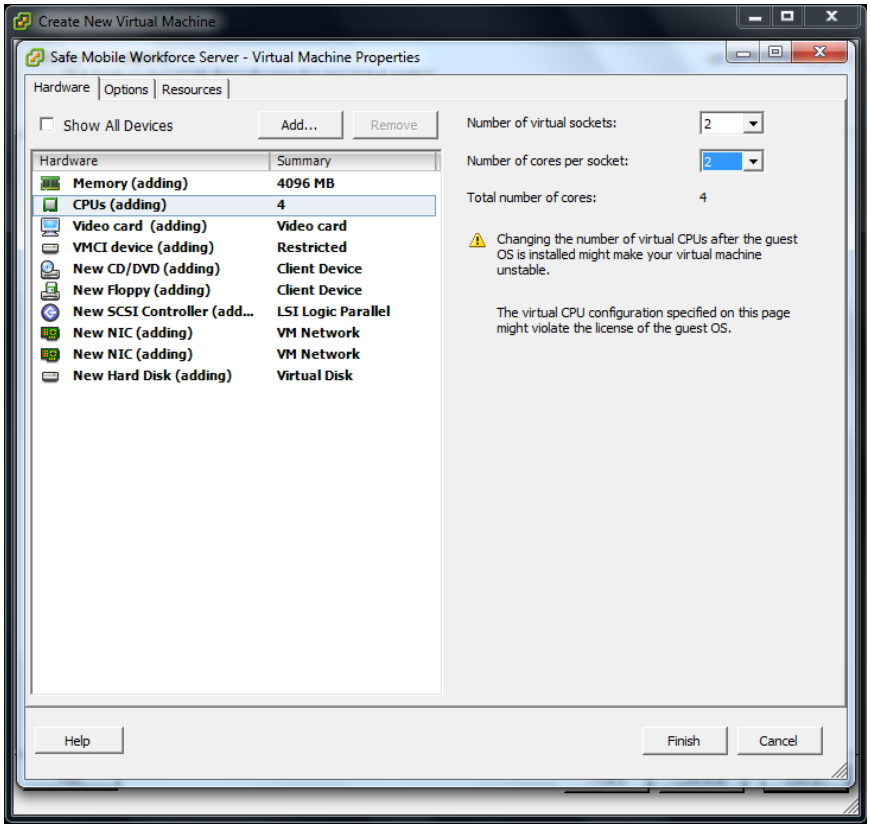


FIGURE 3-10. VM Properties - CPU Settings

16. On the **Hardware** tab, click **New CD/DVD (adding)**.

    The CD/DVD settings appear in the right pane.

17. In the CD/DVD settings, do the following:

    a. Under **Device Type** section, select **Datastore ISO File**, and click **Browse**, and then select the iso setup image file from the ESXi server hard drive.

    b. Under **Device Status** section, select **Connect at power on**.

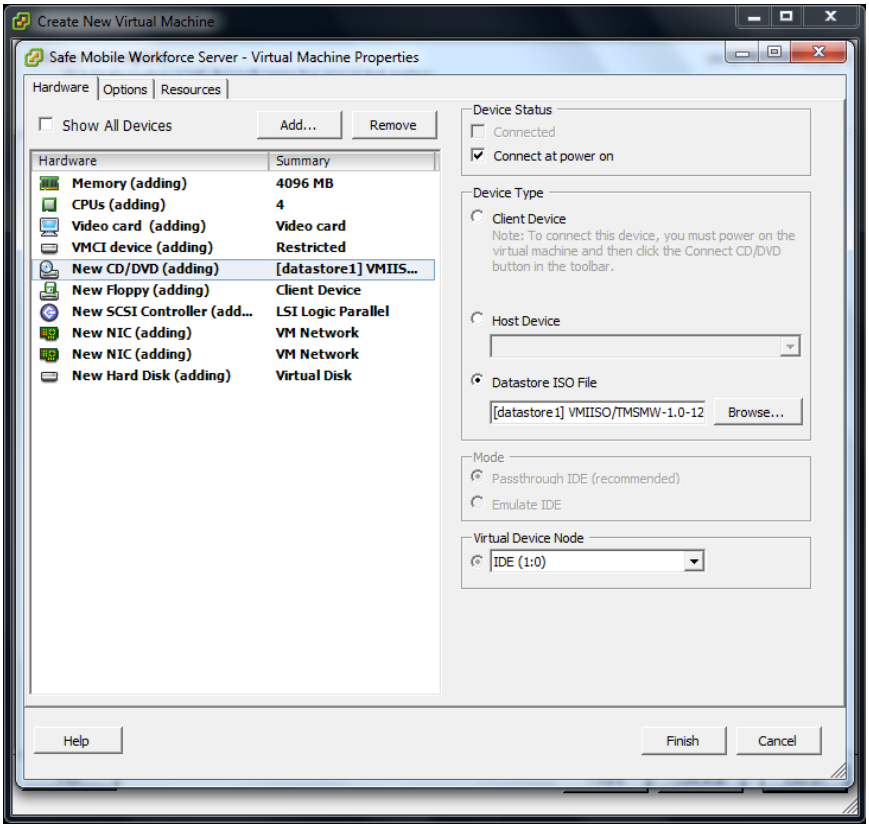


FIGURE 3-11. VM Properties - CD/DVD Settings

18. Click **Finish** to complete the VM configuration and close the window.

Step 2: Configuring VM Network Card (Optional)

Safe Mobile Workforce provides the following two options for configuring network interfaces for mobile devices to connect to the server:

- **NAT: Workspaces share the server's IP address**–this option enables you to share the server's IP address with the workspaces. This option is selected by default.

- **IP Range: Assign IP address to workspaces**–this option enables you to assign individual IP address to each workspace.

Note

If you want to use IP Range then after creating a virtual machine, you must configure the network card that you have used for Safe Mobile Workforce to connect to the network bridge. Otherwise, the mobile devices will not be able to connect to the workspace hosted on the server.

Procedure

1. Start **VMware ESXi**.
2. Select the host (the root computer) from the left resource tree.
3. Click the **Configuration** tab.
4. Under the **Hardware** section, click **Networking**.

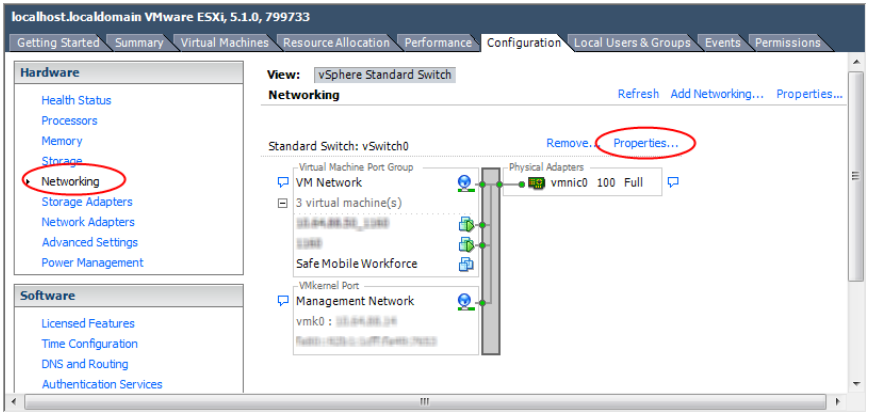


FIGURE 3-12. Networking screen

5. Click **Properties** for the **Standard Switch** under which you have created a virtual machine for Safe Mobile Workforce.

   The switch **Properties** screen appears.

6. On the **Ports** tab, click the **Virtual Machine Port Group** that you configured in *step 9 on page 3-7* of the procedure *Creating a Virtual Machine on page 3-2* and then click **Edit**.

   The **VM Network Properties** screen appears.

7. On the **Security** tab, configure the following under **Policy Exceptions**:

Promiscuous Mode	Selected	**Accept**
MAC Address Changes	Not Selected	-
Forged Transmits	Selected	**Accept**

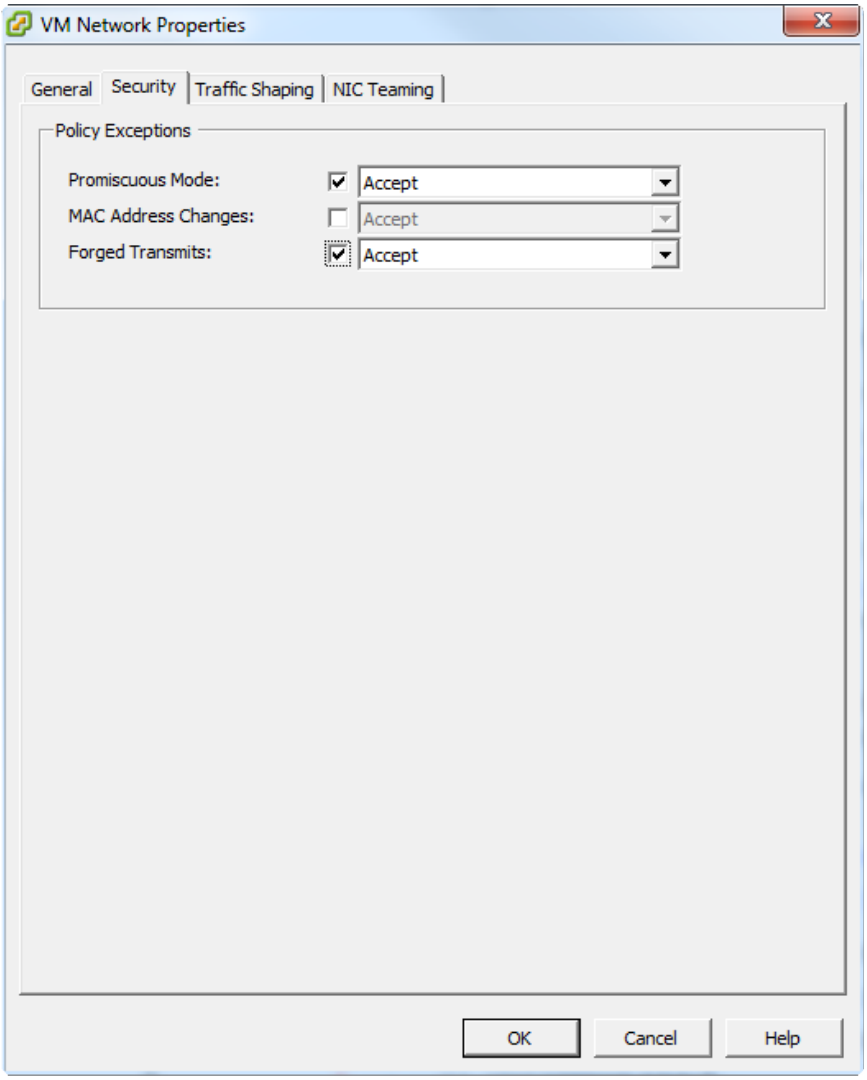


FIGURE 3-13. Configure VM Network Properties on the Security tab

8. Click **OK** and then click **Close** on the switch properties screen.

Step 3: Installing Safe Mobile Workforce on VMware ESXi

Procedure

1. Start VMware ESXi and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 3-2*.
2. Click the **Console** tab on the virtual machine.

   The Safe Mobile Workforce installation menu appears.
3. Follow *step 3 on page 2-2* to *step 11 on page 2-3* of the topic *Installing Safe Mobile Workforce Server on a Bare Metal Server on page 2-2* to complete Safe Mobile Workforce installation.

Installing Safe Mobile Workforce Secure Access

Installing Secure Access on VMware vSphere ESXi Hypervisor involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 3-17*)
2. Installing Secure Access (See *Step 2: Installing Secure Access on VMware ESXi on page 3-29*)

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the ESXi server hard drive, or any other location that can be accessed from the computer where ESXi server is installed.
2. Start **VMware ESXi**.
3. Click **File** > **New** > **Virtual Machine** from the menu.

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

4. Select **Typical** and click **Next**.

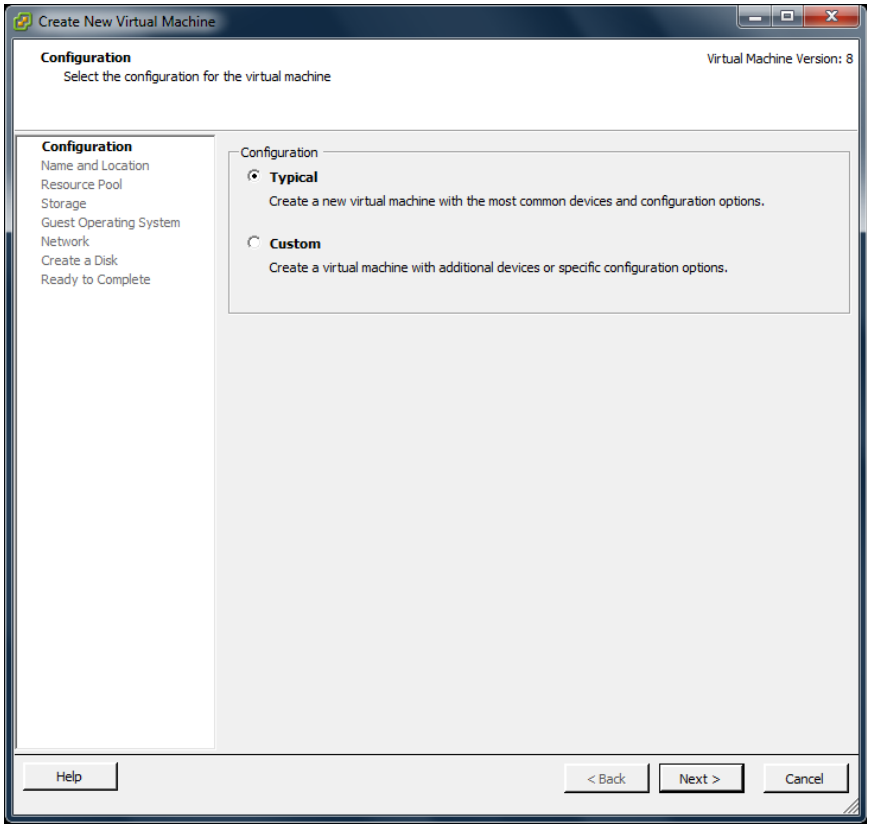


FIGURE 3-14. Select Configuration

The **Name and Location** screen appears.

5. Type a name for the virtual machine, and click **Next**.

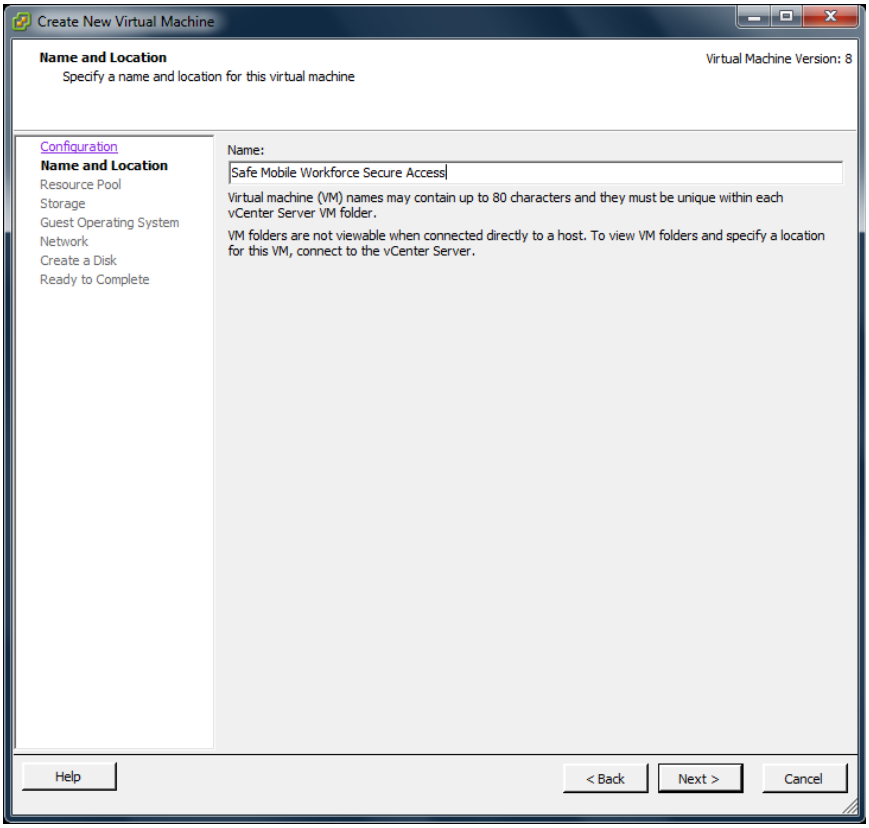


FIGURE 3-15. The Resource Pool screen appears.

The **Resource Pool** screen appears.

Note

The **Resource Pool** screen will not appear if you had selected a resource pool on the left resource tree. Skip *step 6 on page 3-19* and proceed to *step 7 on page 3-20* to configure the **Storage** screen.

---

6. Select the resource pool in which you want to run this virtual machine and click **Next**.

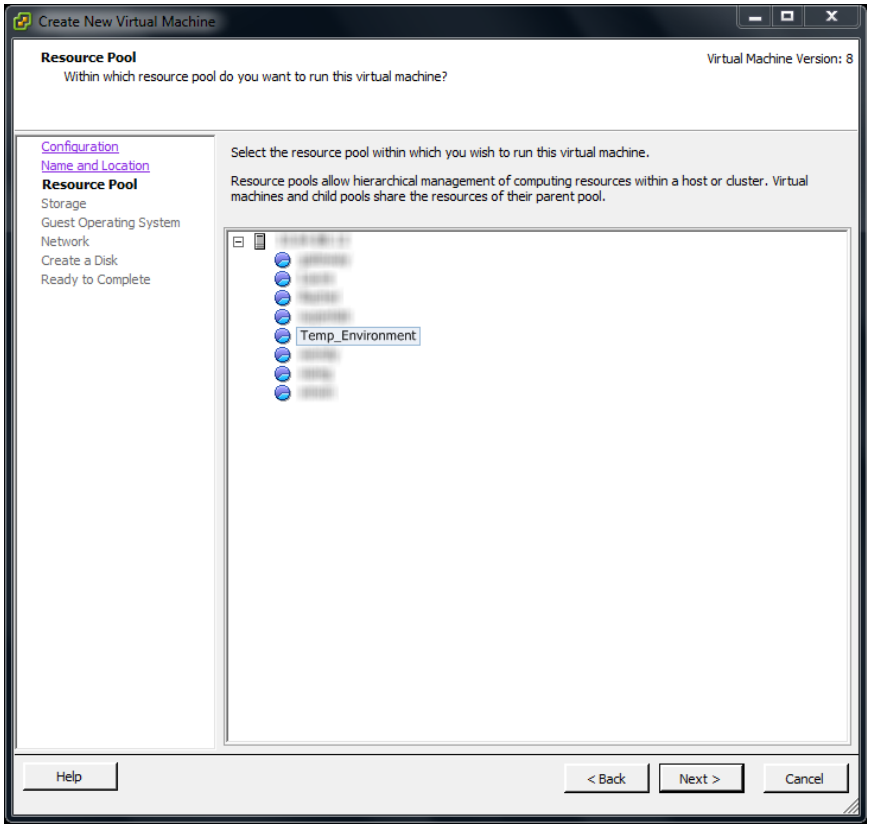


FIGURE 3-16. Select a resource pool

The **Storage** screen appears.

7. Select the disk storage for the virtual machine files and click **Next**.

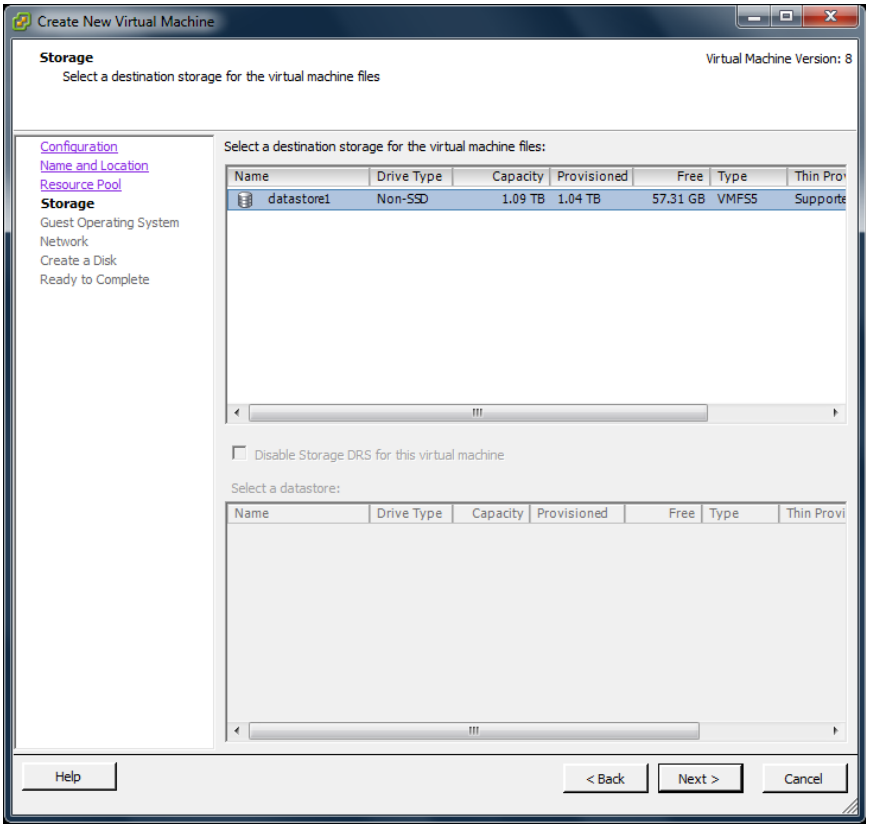


FIGURE 3-17. Select a storage to install Safe Mobile Workforce Server

8. Select **Linux** and choose **Other Linux (64-bit)** from the drop-down and click **Next**.

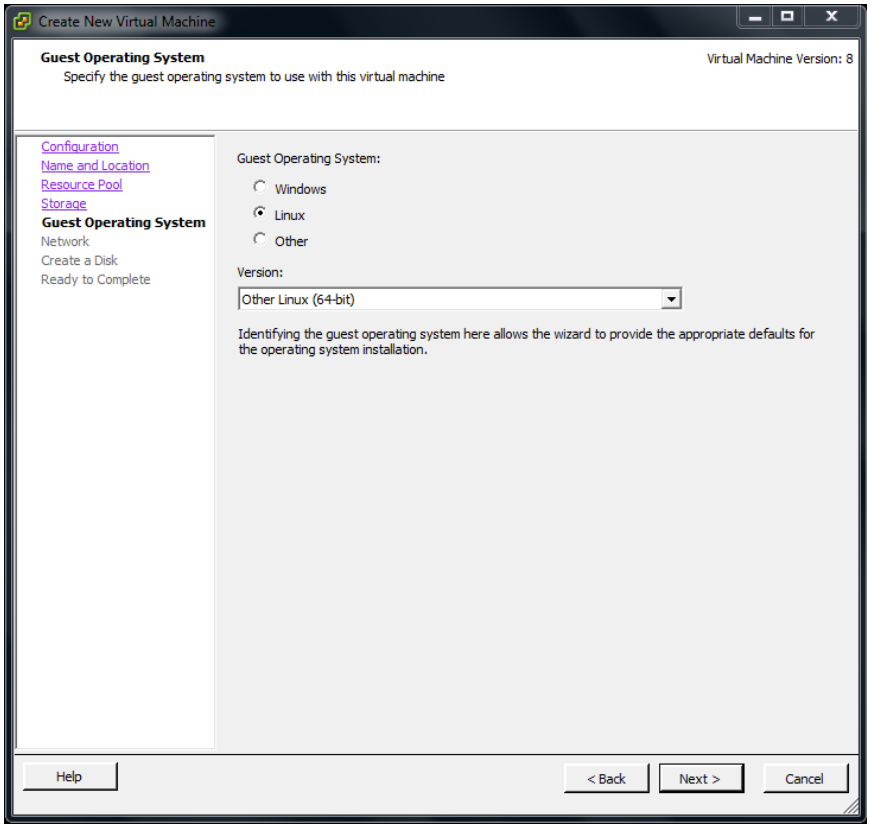


FIGURE 3-18. Guest Operating System

The **Network** screen appears.

9. Select **1** NIC, and specify the following settings:

TABLE 3-2. Network Settings for Secure Access

NAME	NETWORK	ADAPTER	CONNECT AT POWER ON
NIC 1	VM Network	E1000	Enabled

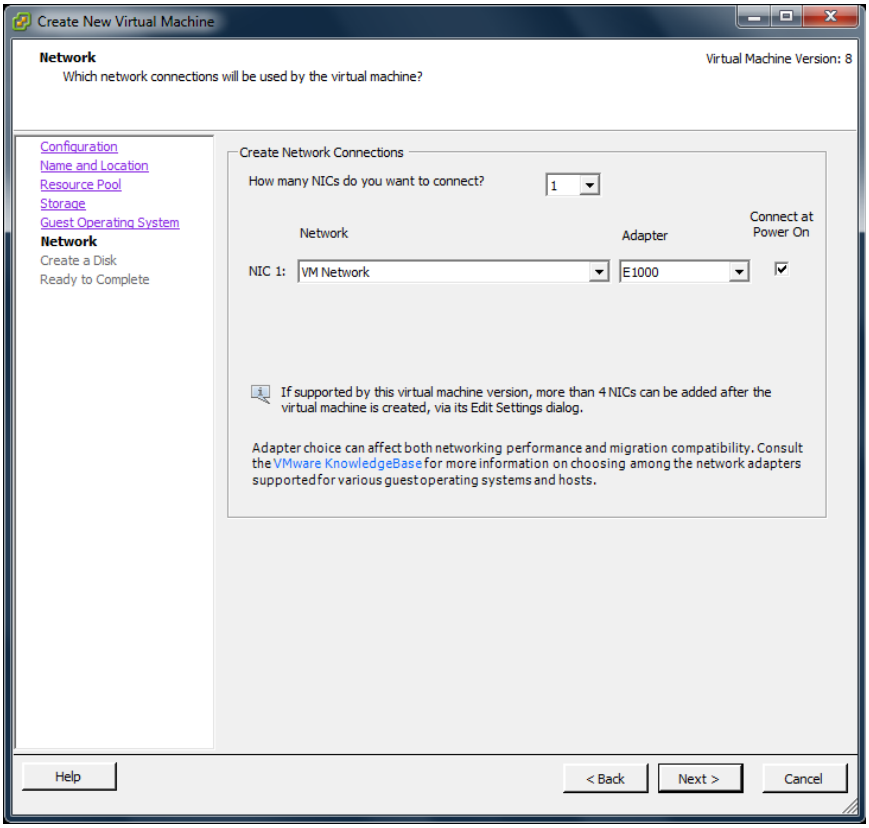


FIGURE 3-19. Create Network Connections

10. Click **Next**.

    The **Create a Disk** screen appears.

11. On the **Create a Disk** screen, do the following:

    a. Select at least 30-GB of virtual disk space for Safe Mobile Workforce.

    b. Select **Thick Provision Lazy Zeroed**.

    c. Click **Next**.

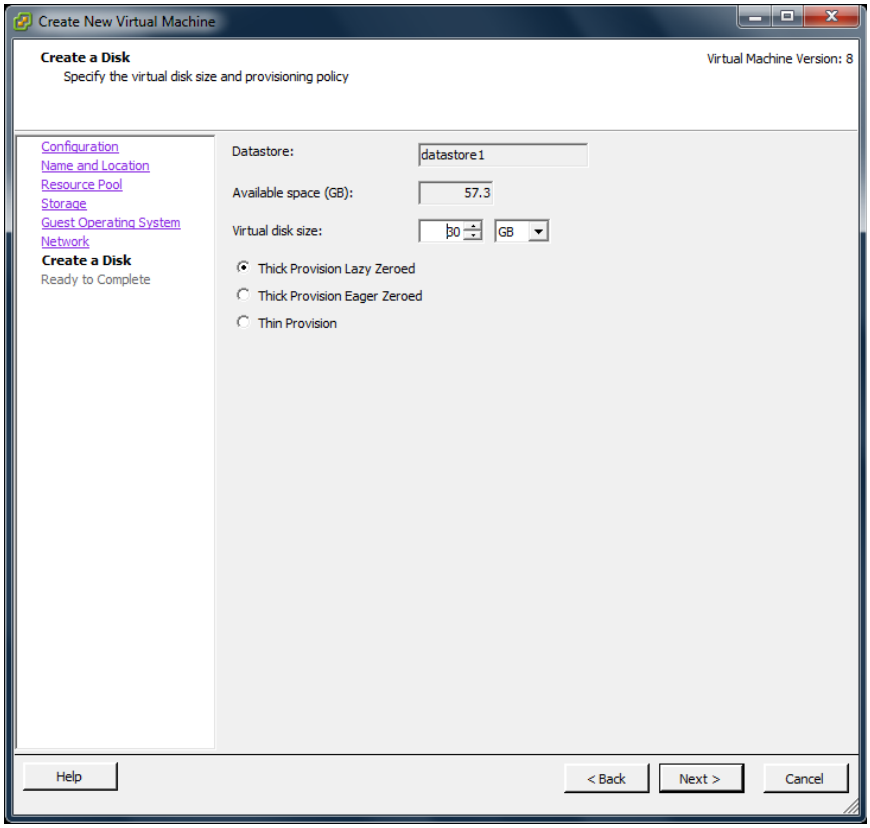


FIGURE 3-20. Specify Hard Disk Space

The **Ready to Complete** screen appears.

12. Select **Edit the virtual machine settings before completion** and click **Continue**.

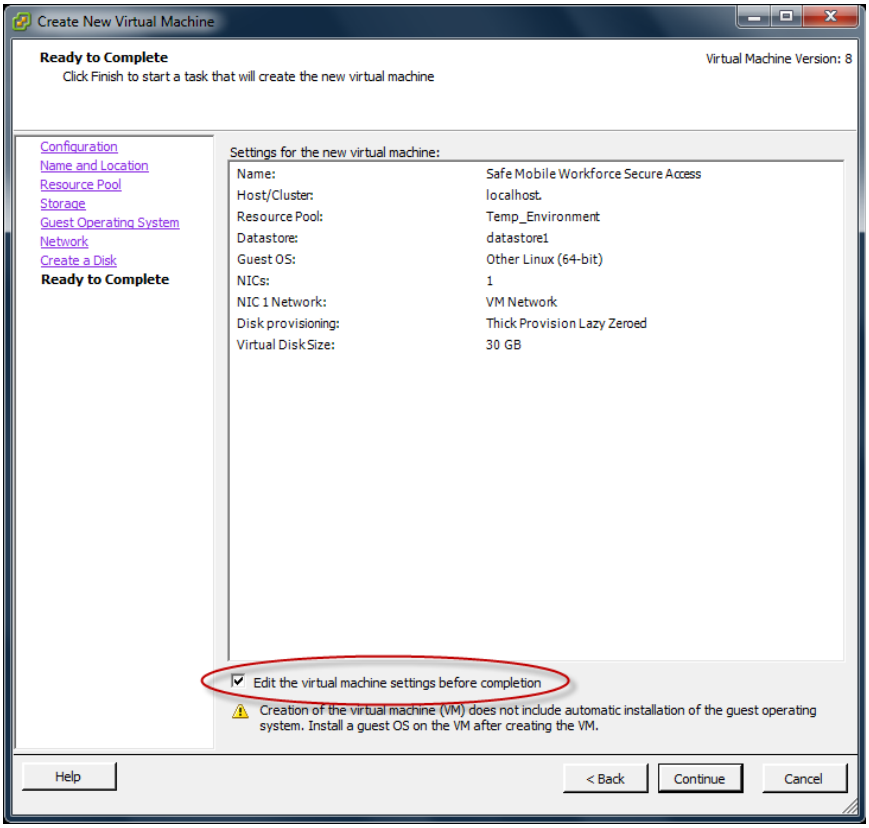


FIGURE 3-21. Ready to Complete

The Virtual Machine Properties screen appears.

13. On the **Hardware** tab, do the following:

    a. Select **Memory (adding)**.

    Memory Configuration appears in the right pane.

    b. In the **Memory Size** field, select at least 4-GB.

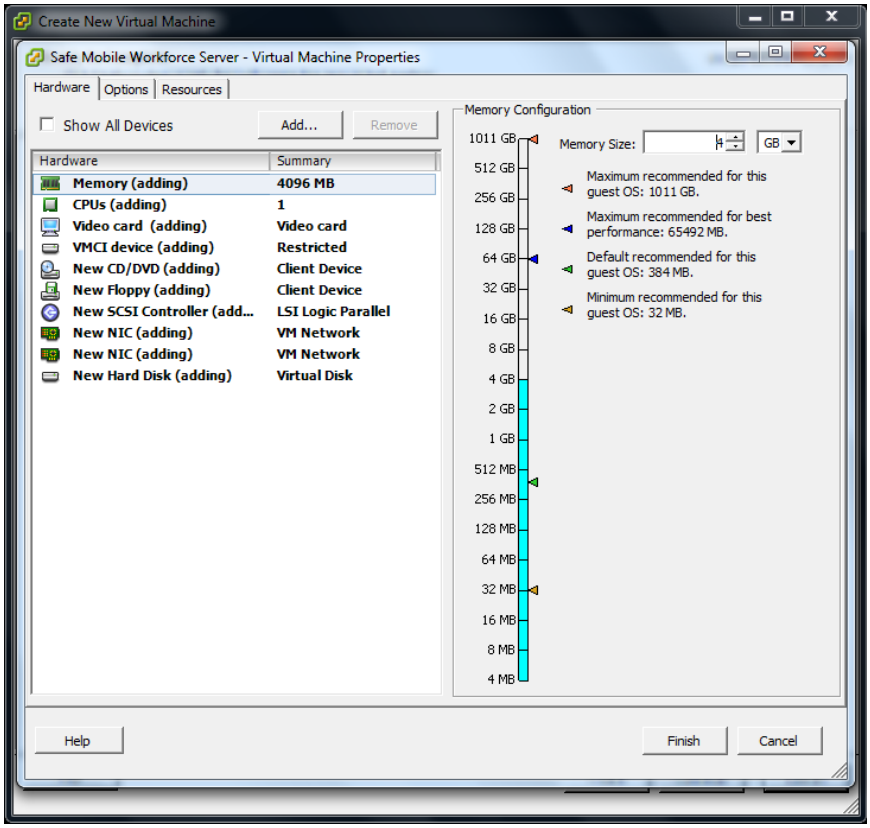


FIGURE 3-22. VM Properties - Memory Configuration

14. On the **Hardware** tab, select **CPU (adding)**.

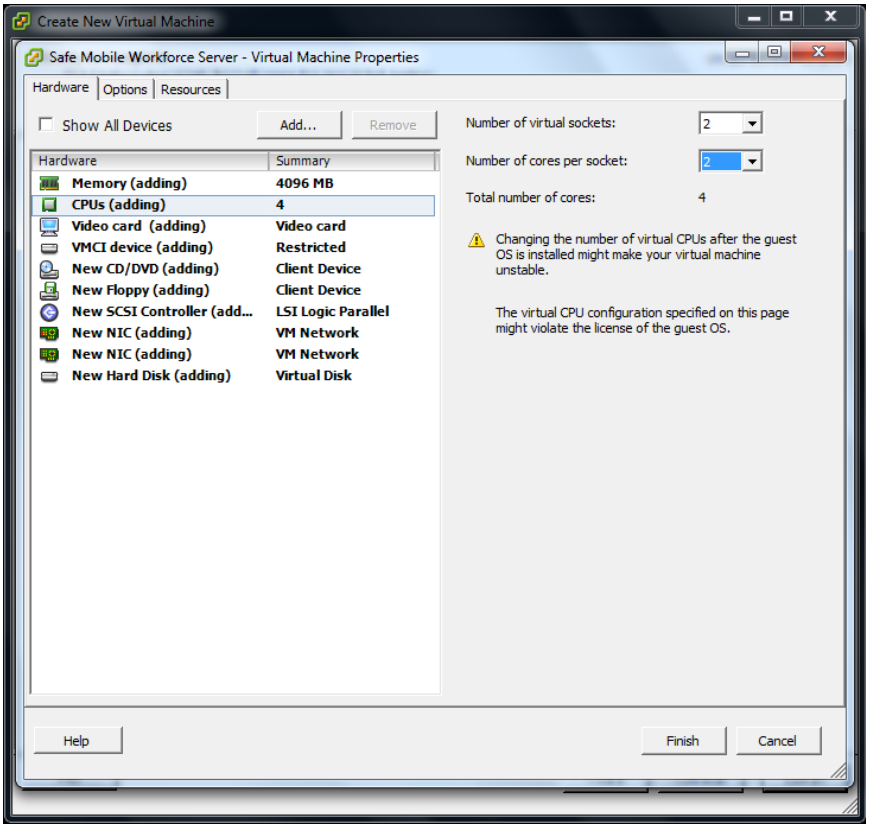


FIGURE 3-23. VM PROPERTIES - CPU SETTINGS

CPU settings appear in the right pane.

15. In the **CPU settings**, do the following:

    a. In the **Number of virtual sockets** field, select **2**.

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

16. On the **Hardware** tab, click **New CD/DVD (adding)**.

    The CD/DVD settings appear in the right pane.

17. In the CD/DVD settings, do the following:

    a. Under **Device Type** section, select **Datastore ISO File**, and click **Browse**, and then select the iso setup image file from the ESXi server hard drive.

    b. Under **Device Status** section, select **Connect at power on**.

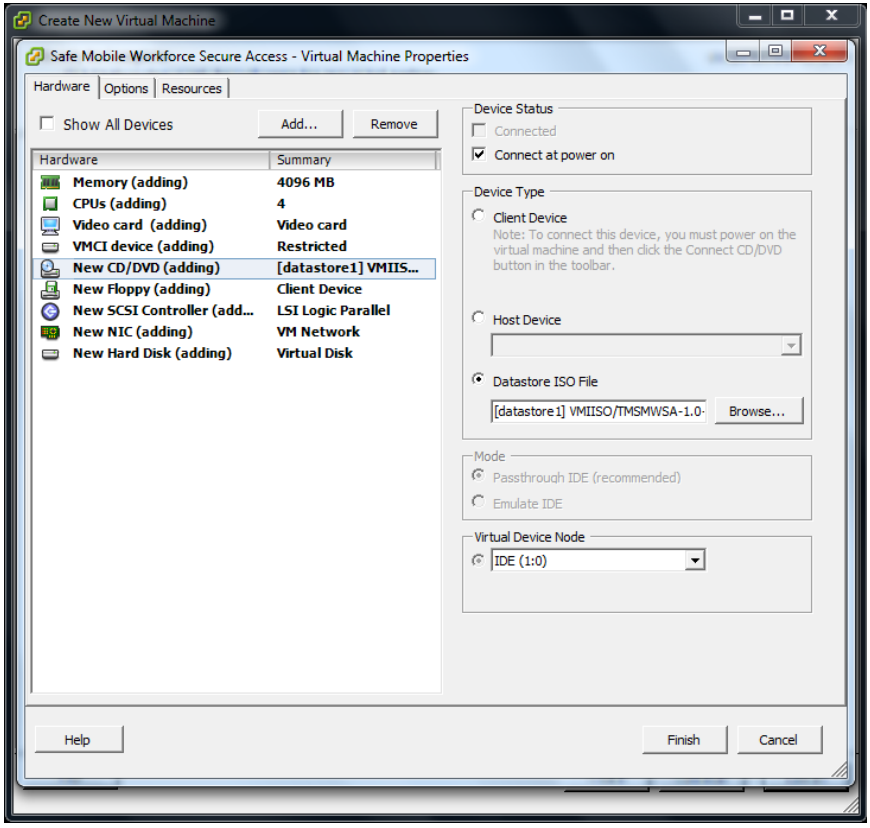


FIGURE 3-24. VM Properties - CD/DVD Settings

18. Click **Finish** to complete the VM configuration and close the window.

Step 2: Installing Secure Access on VMware ESXi

Procedure

1. Start VMware ESXi and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 3-17*.
2. Click the **Console** tab on the virtual machine.

   The Secure Access installation menu appears.
3. Follow *step 3 on page 2-4* to *step 13 on page 2-6* of the topic *Installing Safe Mobile Workforce Secure Access on a Bare Metal Server on page 2-4* to complete Secure Access installation.

Chapter 4

Installing on VMware Workstation

This chapter provides the information that you will need to create and configure a virtual machine on VMware Workstation and install Trend Micro Safe Mobile Workforce.

This chapter contains the following sections:

Installing Safe Mobile Workforce Server

Installing Safe Mobile Workforce on VMware Workstation involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 4-2*)
2. Installing Safe Mobile Workforce (See *Step 2: Installing Safe Mobile Workforce on VMware Workstation on page 4-9*)

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the VM Workstation hard drive, or any other location that can be accessed from the computer where VM Workstation is installed.
2. Start VMware Workstation.
3. Click **File** > **New** > **Virtual Machine** from the menu.

   The **New Virtual Machine Wizard** screen appears.
4. Select **Custom (Advanced)** and click **Next**.

   The **Choose the Virtual Machine Hardware Compatibility** screen appears.
5. Select an appropriate option from the Hardware compatibility drop-down list.

   Note

   This document uses Workstation 10.0 hardware compatibility.

   The **Guest Operating System Installation** screen appears.
6. Select **I will install the operating system later**, and click **Next**.

   The **Select a Guest Operating System** screen appears.
7. On the **Select a Guest Operating System** screen, configure the following settings:

a. **Guest operating system**: Linux

b. **Version**: Other Linux 2.6.x kernel 64-bit

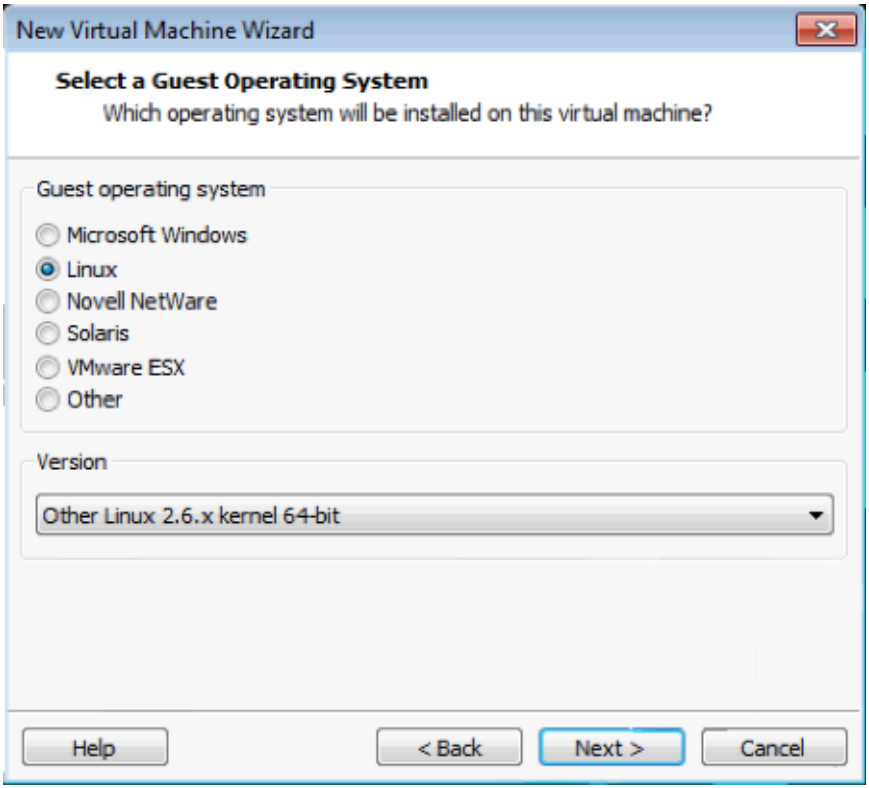


FIGURE 4-1. Select a guest operating system

8. Click **Next**.

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

9. Type a name for the virtual machine, and click **Next**.

   The **Processor Configuration** screen appears.

10. Under the **Processor** section, do the following:

- In the **Number of processors** drop-down list, select **2**.
- In the **Number of cores per processor** drop-down list, select **2**.

11. Click **Next**.

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

12. In the **Memory for the virtual machine** field, select at least **2048-MB**, and click **Next**.

    The **Network Type** screen appears.

13. Select **Use bridged networking**, and click **Next**.

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

14. From the **SCSI Controller** list, select the recommended type: **LSI Logic**, and click **Next**.

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

15. Select the recommended disk type: **SCSI**, and click **Next**.

    The **Select a Disk** screen appears.

16. Select **Create a new virtual disk** and click **Next**.

    The **Specify Disk Capacity** screen appears.

17. Do the following:

    - Select **30-GB** for the **Maximum disk size**.
    - Select **Split virtual disk into multiple files**.

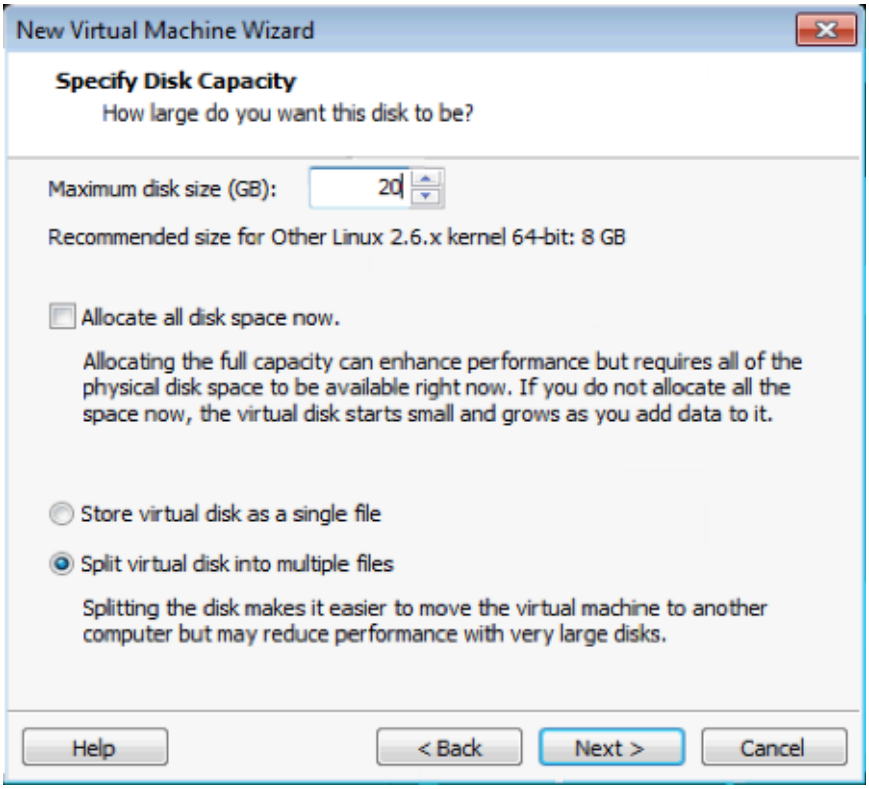


FIGURE 4-2. Specify disk capacity

18. Click **Next**.

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

19. Click **Customize Hardware**.

    The **Hardware** screen appears.

20. Click **Add**.

    The **Add Hardware Wizard** appears displaying **Hardware Type** screen.

21. Select **Network Adapter** and click **Next**.

The **Network Adapter Type** screen appears.

22. Configure the following:

    - Under **Network Connection** section, select **Bridged Connected directly to the physical network**.
    - Under **Device status** section, select **Connect at power on**.

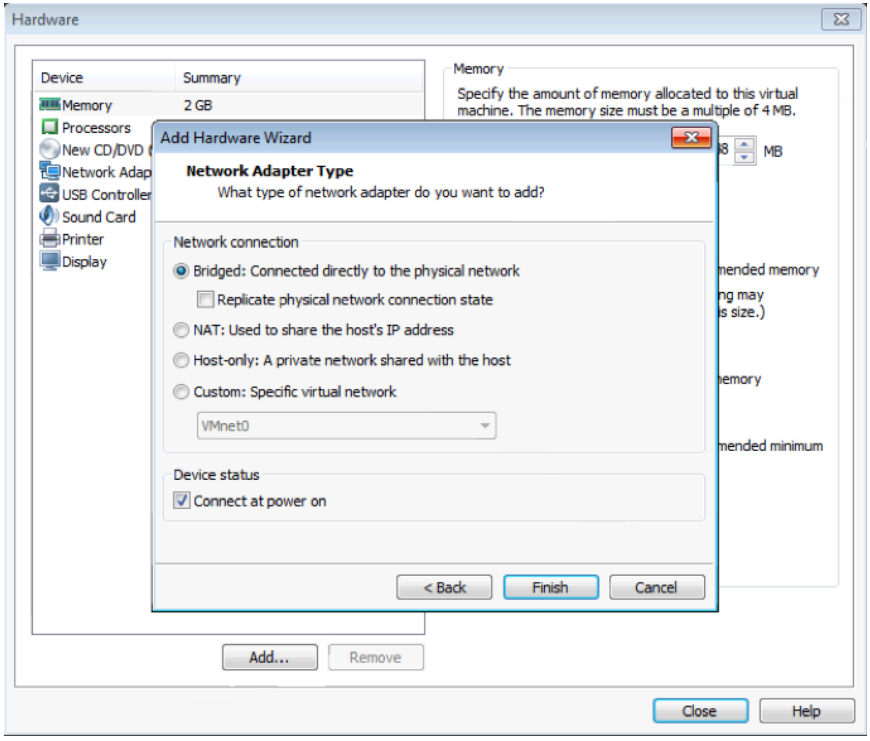


FIGURE 4-3. Configure network adapter type

23. Click **Finish** on the **Network Adapter Type** screen and then click **Close** on the **Hardware** screen.

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

24. Click **Finish**.

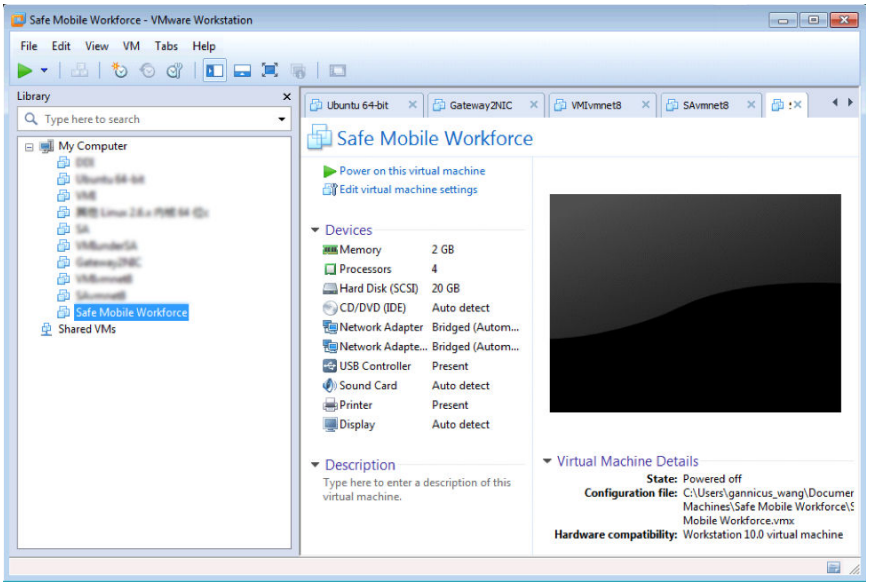


FIGURE 4-4. Virtual machines in VMware Workstation

The virtual machine you have just created appears in the left resource tree under **My Computer**.

25. Skip this step if you are using Workstation 9.0. If you are using Workstation 10.0, do the following:

    a. Open the .vmx configuration file for the virtual machine. The configuration file exists in the folder where you have saved your virtual machine.

    b. Make sure the following keys exist in the configuration file.

        i. ethernet0.virtualDev = "e1000"

        ii. ethernet1.virtualDev = "e1000"

        If they do not exist, or have the wrong values, add the keys at the botton of the file or update their values to the correct ones.

26. In the left resource tree, right-click the virtual machine you have just created, and click **Settings**.

The **Virtual Machine Settings** screen appears.

27. On the **Hardware** tab, click **CD/DVD (IDE)**.

    The CD/DVD settings appear on the right pane.

28. In the CD/DVD settings, do the following:

    a. Under **Connection** section, select **Use ISO image file**, and click **Browse**, and then select the Safe Mobile Workforce Server iso setup image file.

    b. Under **Device status** section, select **Connect at power on**.

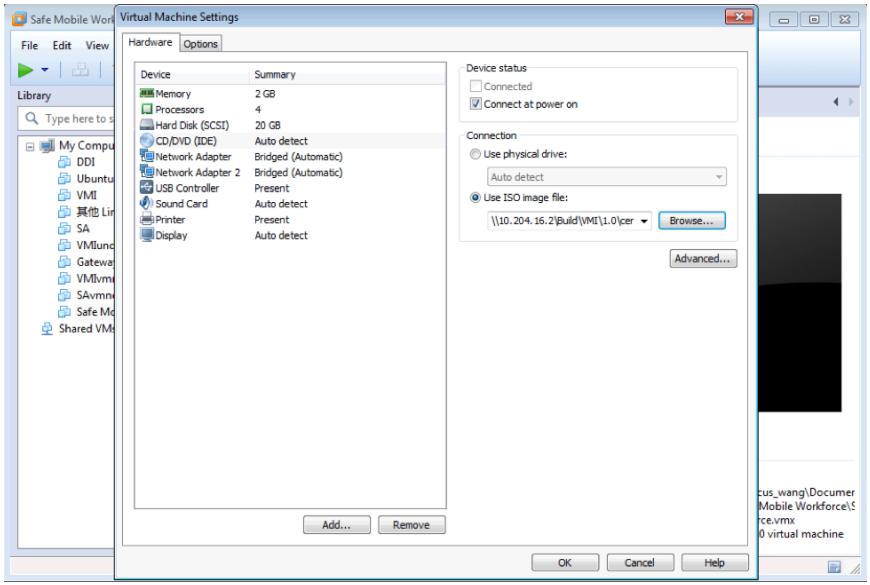


FIGURE 4-5. Browse and select Safe Mobile Workforce Server ISO image file

29. Click **OK** to complete the virtual machine configuration and close the window.

Step 2: Installing Safe Mobile Workforce on VMware Workstation

Context for the current task

Procedure

1. Start VMware Workstation and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 4-2*.
2. Click the **Console** tab on the virtual machine.

   The Safe Mobile Workforce installation menu appears.
3. Follow *step 3 on page 2-2* to *step 11 on page 2-3* of the topic *Installing Safe Mobile Workforce Server on a Bare Metal Server on page 2-2* to complete Safe Mobile Workforce installation.

Installing Safe Mobile Workforce Secure Access

Installing Safe Mobile Workforce Secure Access on VMware Workstation involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 4-9*).
2. Installing Safe Mobile Workforce Secure Access (See *Step 2: Installing Safe Mobile Workforce Secure Access on VMware Workstation on page 4-15*).

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the VM Workstation hard drive, or any other location that can be accessed from the computer where VM Workstation is installed.

2. Start VMware Workstation.
3. Click **File** > **New** > **Virtual Machine** from the menu.

   The **New Virtual Machine Wizard** screen appears.
4. Select **Custom (Advanced)** and click **Next**.

   The **Choose the Virtual Machine Hardware Compatibility** screen appears.
5. Select an appropriate option from the Hardware compatibility drop-down list.

   Note

   This document uses Workstation 10.0 hardware compatibility.

   The **Guest Operating System Installation** screen appears.
6. Select **I will install the operating system later**, and click **Next**.

   The **Select a Guest Operating System** screen appears.
7. On the **Select a Guest Operating System** screen, configure the following settings:
   a. **Guest operating system**: Linux
   b. **Version**: Other Linux 2.6.x kernel 64-bit

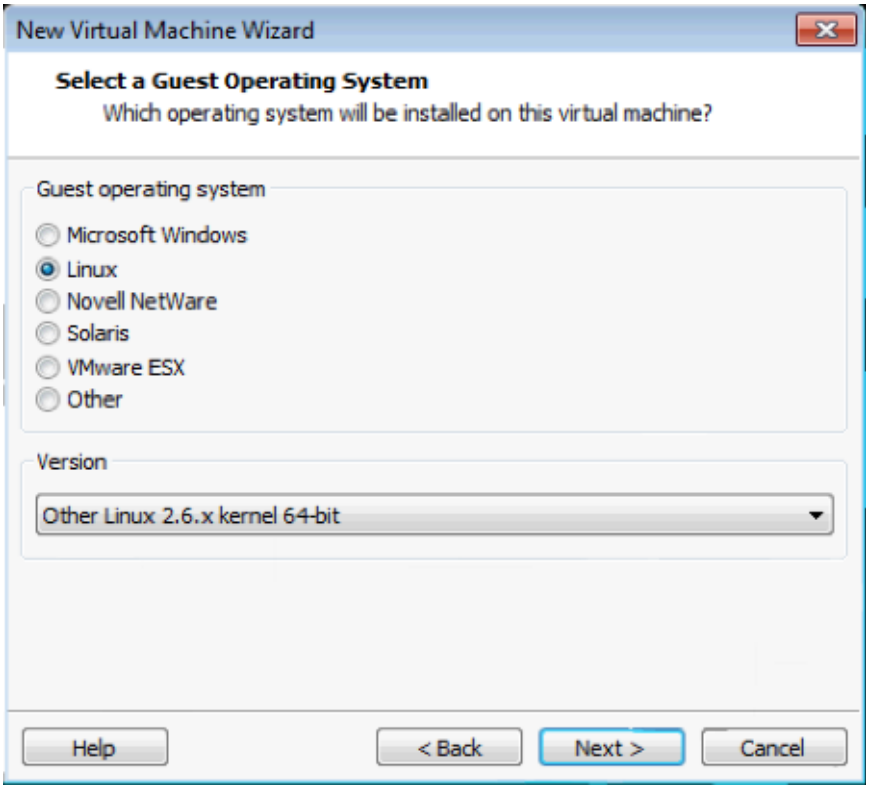


FIGURE 4-6. Select a guest operating system

8. Click **Next**.

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

9. Type a name for the virtual machine, and click **Next**.

   The **Processor Configuration** screen appears.

10. Under the **Processor** section, do the following:

    - In the **Number of processors** drop-down list, select **2**.
    - In the **Number of cores per processor** drop-down list, select **1**.

11. Click **Next**.

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

12. In the **Memory for the virtual machine** field, select at least **1024-MB**, and click **Next**.

    The **Network Type** screen appears.

13. Select **Use bridged networking**, and click **Next**.

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

14. From the **SCSI Controller** list, select the recommended type: **LSI Logic**, and click **Next**.

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

15. Select the recommended disk type: **SCSI**, and click **Next**.

    The **Select a Disk** screen appears.

16. Select **Create a new virtual disk** and click **Next**.

    The **Specify Disk Capacity** screen appears.

17. Do the following:

    - Select **30-GB** for the **Maximum disk size**.
    - Select **Split virtual disk into multiple files**.

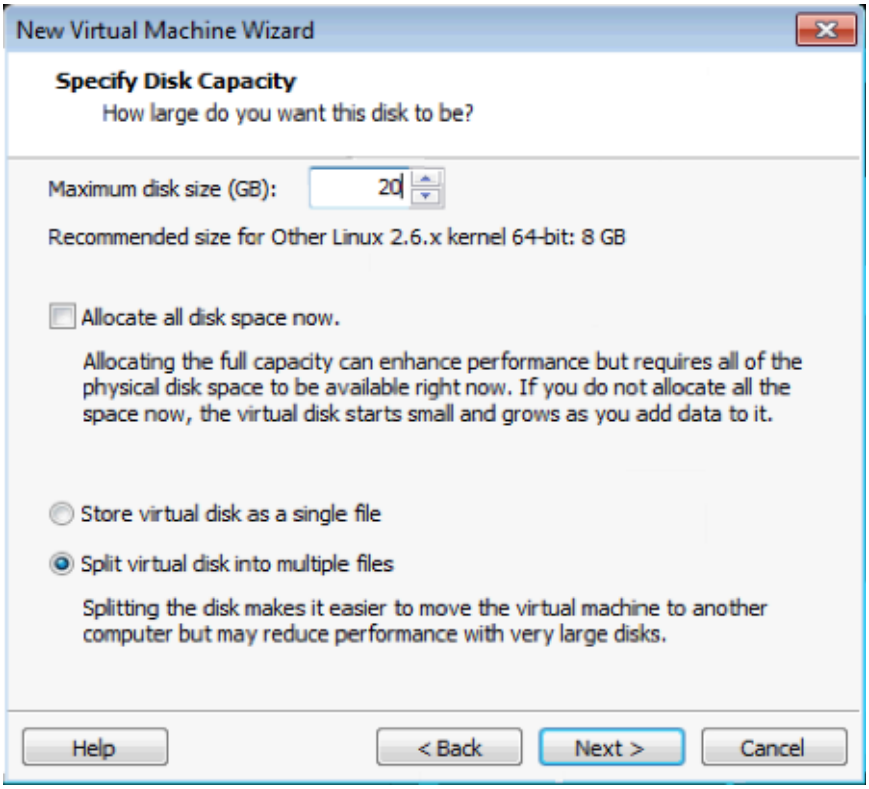


FIGURE 4-7. Specify disk capacity

18. Click **Next**.

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

19. Click **Finish** on the **New Virtual Machine Wizard** screen.

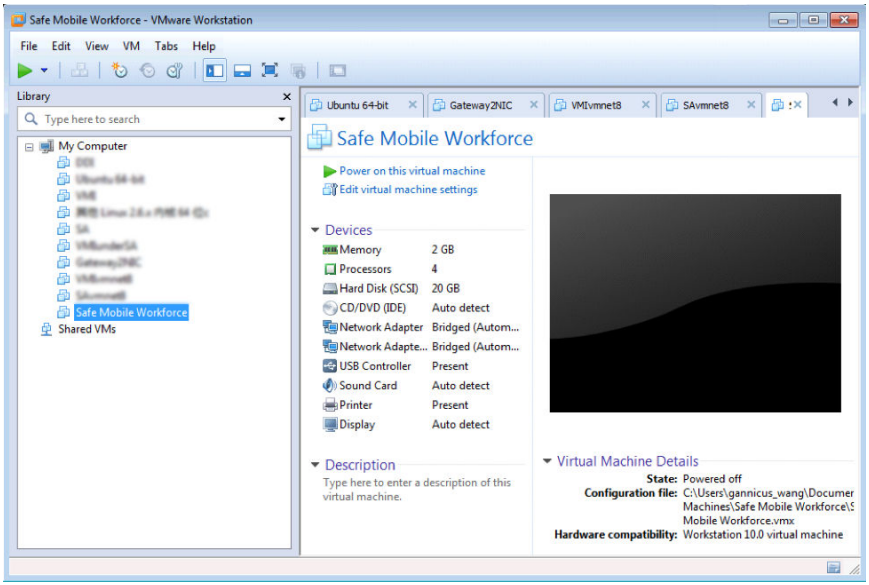


FIGURE 4-8. Virtual machines in VMware Workstation

The virtual machine you have just created appears in the left resource tree under **My Computer**.

20. In the left resource tree, right-click the virtual machine you have just created, and click **Settings**.

    The **Virtual Machine Settings** screen appears.

21. On the **Hardware** tab, click **CD/DVD (IDE)**.

    The CD/DVD settings appear on the right pane.

22. In the CD/DVD settings, do the following:

    a. Under **Connection** section, select **Use ISO image file**, and click **Browse**, and then select the Safe Mobile Workforce Secure Access iso setup image file.

    b. Under **Device status** section, select **Connect at power on**.

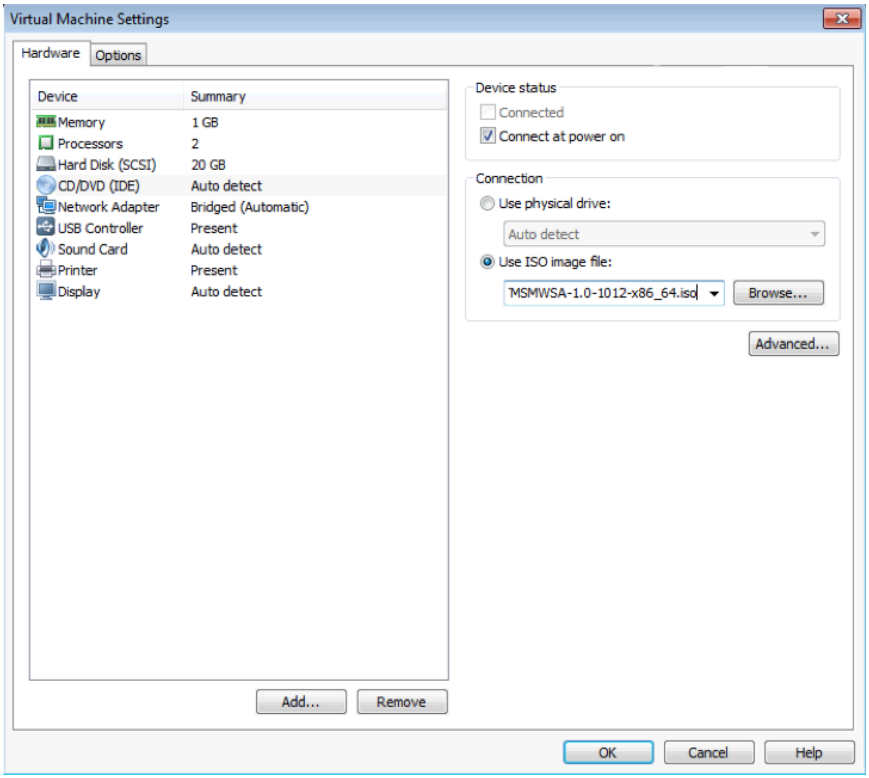


FIGURE 4-9. Browse and select Safe Mobile Workforce Secure Access ISO image file

23. Click **OK** to complete the virtual machine configuration and close the window.

Step 2: Installing Safe Mobile Workforce Secure Access on VMware Workstation

Procedure

1. Start VMware Workstation and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 3-17*.

2. Click the **Console** tab on the virtual machine.

   The Safe Mobile Workforce installation menu appears.

3. Follow *step 3 on page 2-4* to *step 13 on page 2-6* of the topic *Installing Safe Mobile Workforce Secure Access on a Bare Metal Server on page 2-4* to complete Secure Access installation.

Chapter 5

Installing on Microsoft Hyper-V

This chapter provides the information that you will need to create and configure a virtual machine on Microsoft Hyper-V and install Trend Micro Safe Mobile Workforce.

This chapter contains the following sections:

Installing Safe Mobile Workforce Server

Installing Safe Mobile Workforce on Microsoft Hyper-V involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 5-2*).
2. Installing Safe Mobile Workforce (See *Step 2: Installing Safe Mobile Workforce Server on Microsoft Hyper-V on page 5-6*).

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the Microsoft Hyper-V computer hard drive, or any other location that can be accessed from the computer where Microsoft Hyper-V is installed.
2. Copy the iso image setup file on the Microsoft Hyper-V computer hard drive.
3. Start **Microsoft Hyper-V**. Click **File** > **New** > **Virtual Machine** from the menu.

   The **New Virtual Machine Wizard** screen appears.
4. On the **Before You Begin** screen, click **Next**.

   The **Specify Name and Location** screen appears.
5. Type a name for the Safe Mobile Workforce server, and click **Next**.

   The **Specify Generation** screen appears.
6. Select **Generation 1**, and click **Next**.

   The **Assign Memory** screen appears.
7. In the **Startup memory** field, type `4096` MB, and click **Next**.

   The **Configure Networking** screen appears.
8. Select a virtual switch from the drop-down list that you want to use for the Safe Mobile Workforce Server, and click **Next**.

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

9. Check the virtual hard disk name, location and size, and make the changes if necessary, and then click **Next**.

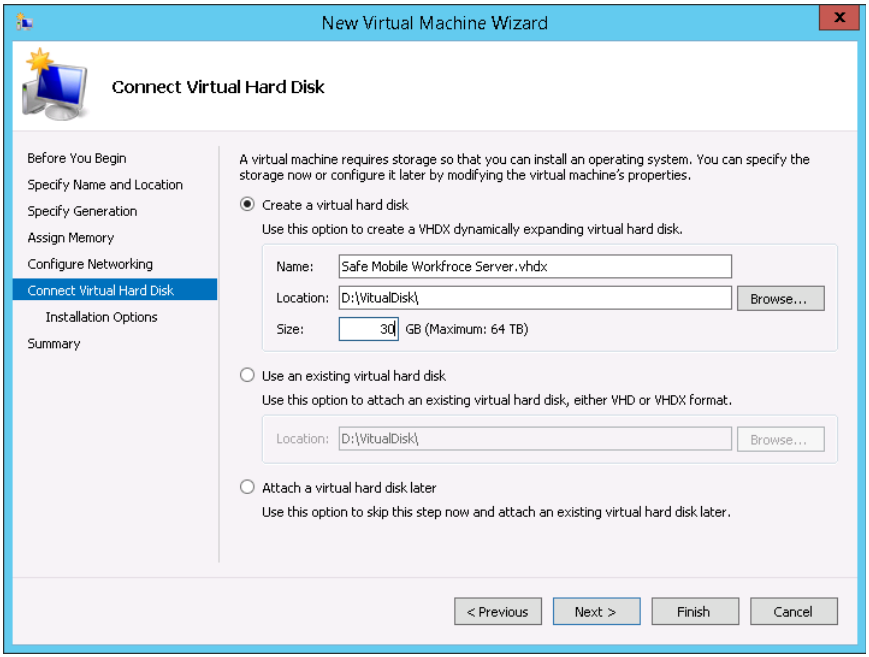


FIGURE 5-1. Create Virtual Hard Disk screen

The **Installation Options** screen appears.

10. Select **Install an operating system later** and then click **Next**.

The **Summary** screen appears.

11. Verify the virtual hard disk settings on the **Summary** screen, and click **Finish**. Click **Previous** to go back to any previous screen and change settings, if required.

The virtual machine setup completes, and the **Settings** screen appears.

12. On the left side of the **Settings** screen, click **Processor** under **Hardware** section, and then in the **Number of virtual processors** field, type 4.

13. On the left side of the **Settings** screen, click **Add Hardware** under **Hardware** section.

14. On the right side of the screen, select **Network Adapter** and then click **Add**.

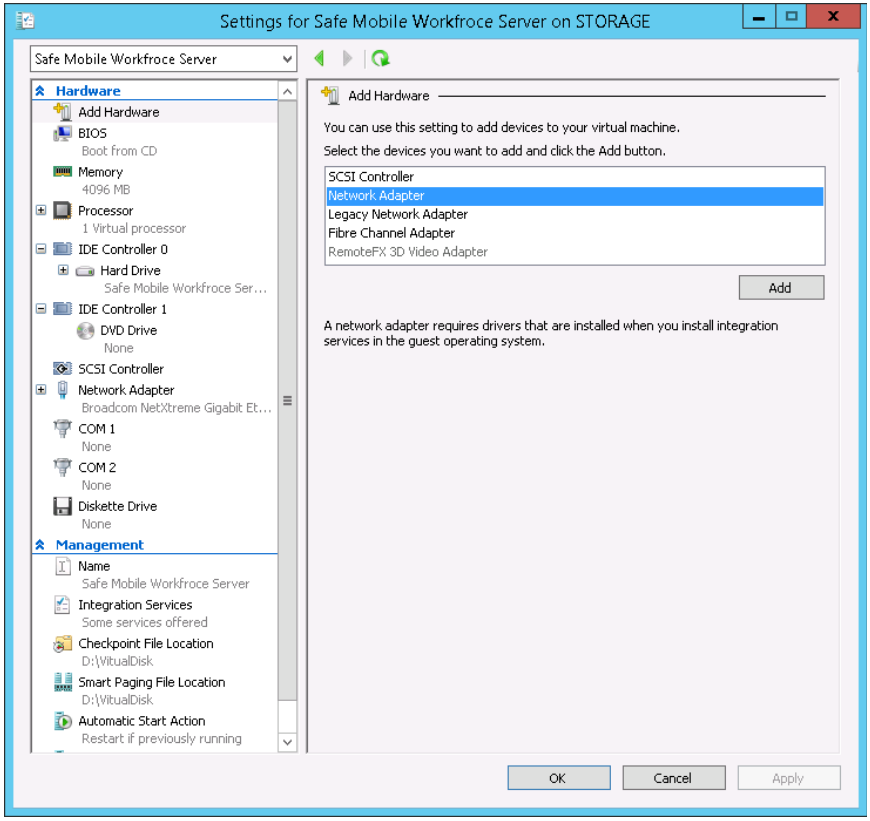


FIGURE 5-2. Add network adapter to the virtual machine

15. On the left side of the screen, click **Network Adapter**, and then select the network switch from the drop down list.

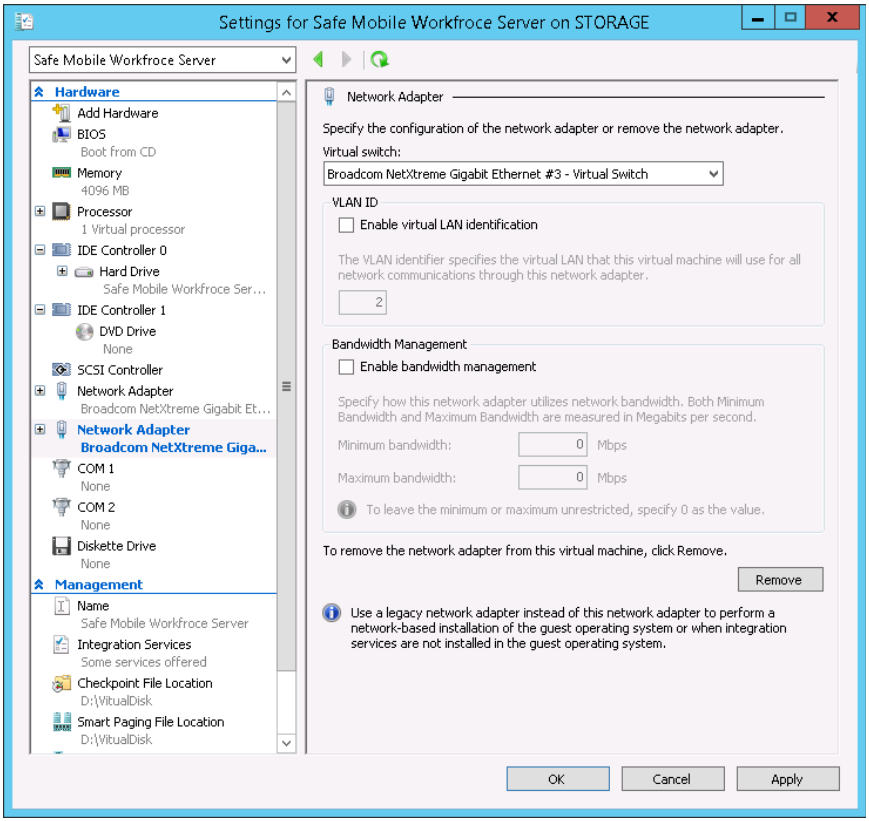


FIGURE 5-3. Select a network switch

16. On the left side of the screen, click **DVD Drive**, and then click **Image file**, and select the Safe Mobile Workforce Server installation setup file.

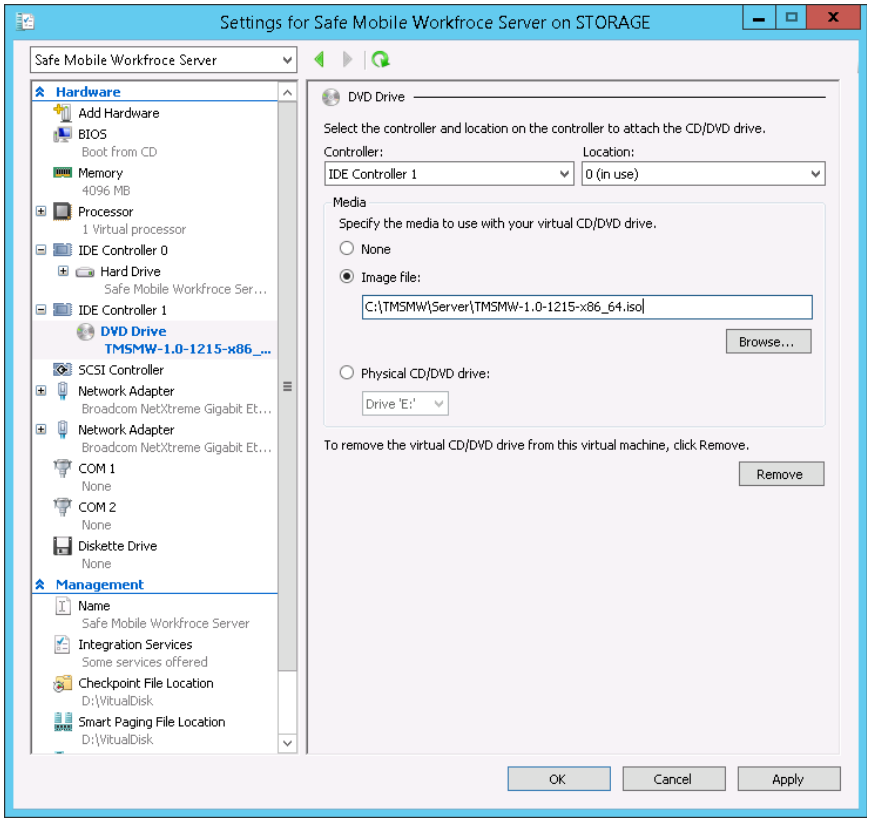


FIGURE 5-4. Select the Safe Mobile Workforce server installation file

17. Click **OK** to finish setting up the virtual machine.

Step 2: Installing Safe Mobile Workforce Server on Microsoft Hyper-V

Procedure

1. Start Microsoft Hyper-V and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 5-2*.

2. Click the **Console** tab on the virtual machine.

   The Safe Mobile Workforce installation menu appears.

3. Follow *step 3 on page 2-2* to *step 11 on page 2-3* of the topic *Installing Safe Mobile Workforce Server on a Bare Metal Server on page 2-2* to complete Safe Mobile Workforce installation.

Installing Safe Mobile Workforce Secure Access

Installing Safe Mobile Workforce Secure Access on Microsoft Hyper-V involves the following steps:

1. Creating a virtual machine (See *Step 1: Creating a Virtual Machine on page 5-7*).
2. Installing Safe Mobile Workforce Secure Access (See *Step 2: Installing Safe Mobile Workforce Secure Access on Microsoft Hyper-V on page 5-10*).

Step 1: Creating a Virtual Machine

Procedure

1. Copy the iso image setup file on the Microsoft Hyper-V computer hard drive, or any other location that can be accessed from the computer where Microsoft Hyper-V is installed.
2. Copy the iso image setup file on the Microsoft Hyper-V computer hard drive.
3. Start **Microsoft Hyper-V**. Click **File** > **New** > **Virtual Machine** from the menu.

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

4. On the **Before You Begin** screen, click **Next**.

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

5. Type a name for the Safe Mobile Workforce Secure Access, and click **Next**.

The **Specify Generation** screen appears.

6. Select **Generation 1**, and click **Next**.

   The **Assign Memory** screen appears.

7. In the **Startup memory** field, type `4096` MB, and click **Next**.

   The **Configure Networking** screen appears.

8. Select a virtual switch from the drop-down list that you want to use for the Safe Mobile Workforce Secure Access, and click **Next**.

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

9. Check the virtual hard disk name, location and size, and make the changes if necessary, and then click **Next**.

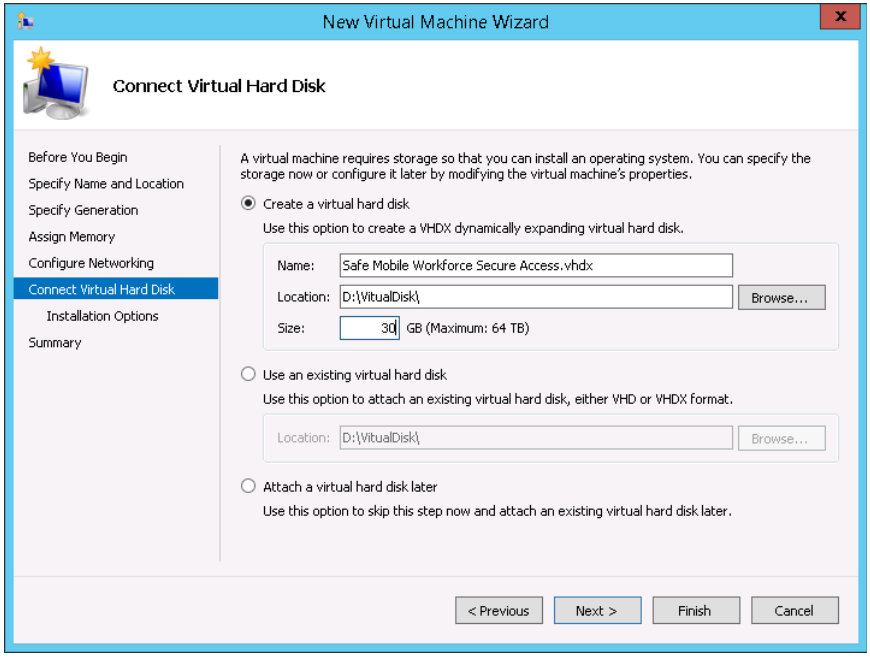


FIGURE 5-5. Create Virtual Hard Disk screen

The **Installation Options** screen appears.

10. Select **Install an operating system later** and then click **Next**.

    The **Summary** screen appears.

11. Verify the virtual hard disk settings on the **Summary** screen, and click **Finish**. Click **Previous** to go back to any previous screen and change settings, if required.

    The virtual machine setup completes, and the **Settings** screen appears.

12. On the left side of the **Settings** screen, click **Processor** under **Hardware** section, and then in the **Number of virtual processors** field, type `4`.

13. On the left side of the screen, click **DVD Drive**, and then click **Image file**, and select the Safe Mobile Workforce Secure Access installation setup file.

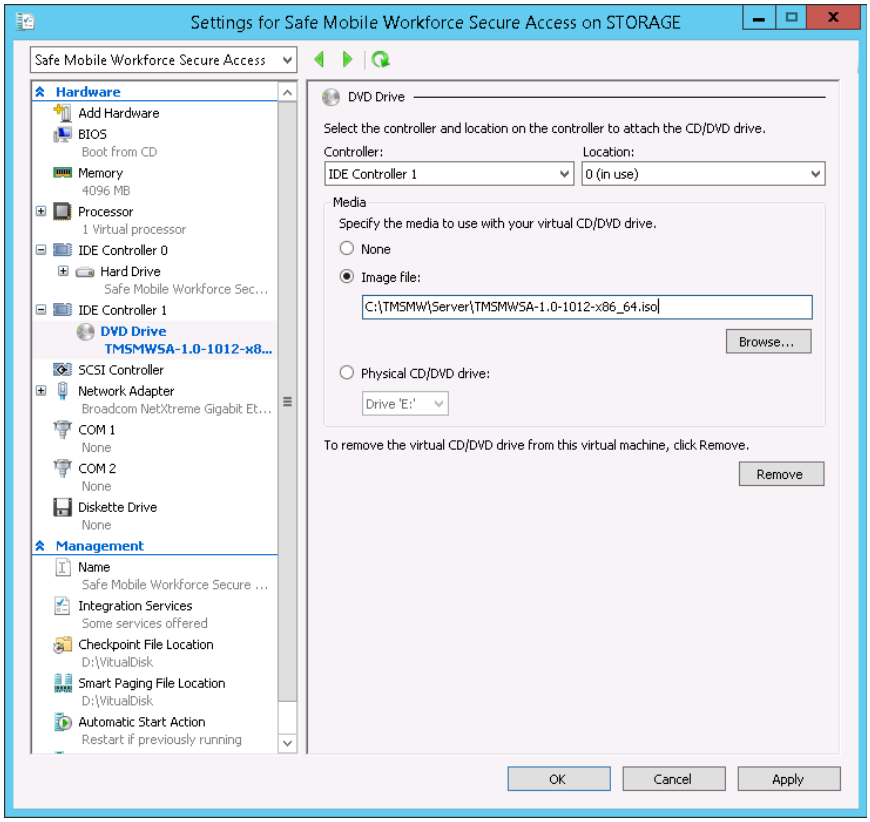


FIGURE 5-6. Select the Safe Mobile Workforce Secure Access installation file

14. Click **OK** to finish setting up the virtual machine.

Step 2: Installing Safe Mobile Workforce Secure Access on Microsoft Hyper-V

Procedure

1. Start VMware Workstation and power on the virtual machine that you created in *Step 1: Creating a Virtual Machine on page 5-7*.

2. Click the **Console** tab on the virtual machine.

   The Safe Mobile Workforce Secure Access installation menu appears.

3. Follow *step 3 on page 2-4* to *step 13 on page 2-6* of the topic *Installing Safe Mobile Workforce Secure Access on a Bare Metal Server on page 2-4* to complete Secure Access installation.

Chapter 6

Installing on Citrix XenServer

This chapter provides the information that you will need to create and configure a virtual machine on Citrix XenServer and install Trend Micro Safe Mobile Workforce.

This chapter contains the following sections:

Installing Safe Mobile Workforce Server

Installing Safe Mobile Workforce server on Citrix XenServer involves the following steps:

1. Installing a VNC viewer application. (See *Step 1: Installing a VNC Viewer Application on page 6-2*.)
2. Creating a virtual machine and installing Safe Mobile Workforce Server. (See *Step 2: Creating a Virtual Machine and Installing Safe Mobile Workforce Server on page 6-2*.)

Step 1: Installing a VNC Viewer Application

The Safe Mobile Workforce server installation requires a VNC viewer to complete the installation. Before you begin installing Safe Mobile Workforce server, install a VNC viewer application on the computer.

This document uses TightVNC viewer application for this procedure.

Step 2: Creating a Virtual Machine and Installing Safe Mobile Workforce Server

Procedure

1. Start **Citrix XenCenter**.
2. Click **Add New Server** button on the toolbar.

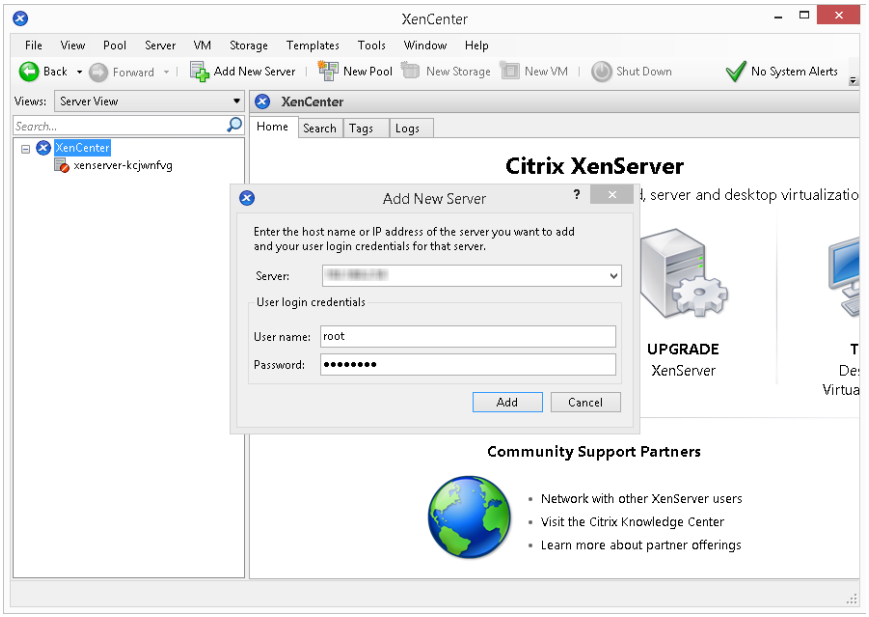


FIGURE 6-1. Add New Server dialog box

The **Add New Server** dialog box appears.

3. Type the server name, user name and password, and then click **Add**.

   XenCenter connects to XenServer and adds it to the server tree on the left side of the screen.

4. On the server tree on the left side of the screen, right-click the server name, then click **New VM**.

   The **New VM** screen appears.

5. From the list of operating systems, select **CentOS 6 (64-bit)**, and click **Next**.

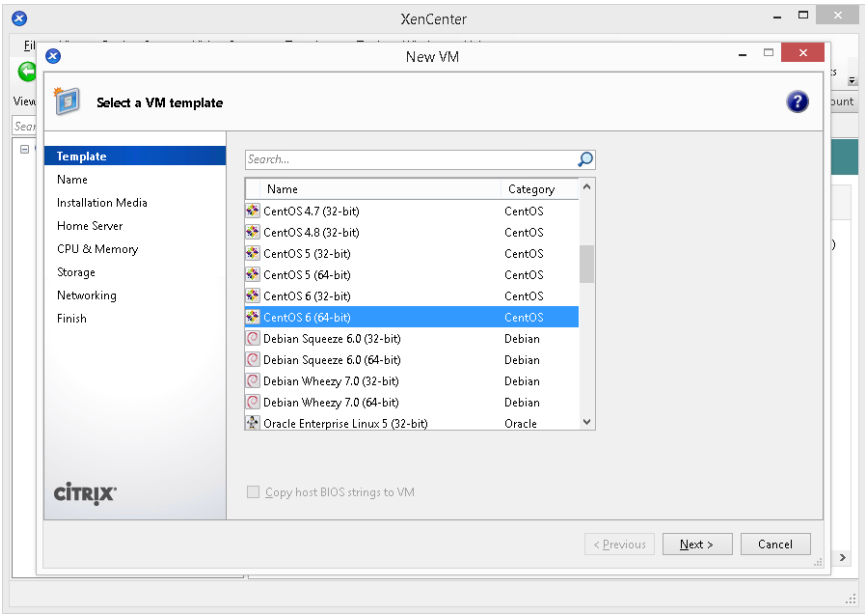


FIGURE 6-2. Select a VM template screen

6. Type a server name and description and then click **Next**.

   The **Installation Media** screen appears.

7. Do the following:

   a. Select an installation media.

      If you want to install Safe Mobile Workforce server from a network location, click **New ISO library**, select **Windows File Sharing (CIFS)**, and then follow the instructions on the screen.

   b. Under **Advanced OS boot parameters** section, type `graphical utf8 vnc`.

8. Click **Next**.

9. Select a server computer from the list, where you want to install Safe Mobile Workforce, and click **Next**.

10. On the **CPU & Memory** screen, type the following:

a. **Number of vCPUs**: `4`

b. **Memory**: `4096` MB

11. Click **Next**.

    The **Storage** screen appears.

12. Click **Properties**, and in the **Size** field, type `30` GB, and then click **OK**.

13. Click **Next** on the **Storage** screen.

    The **Networking** screen appears.

14. Click **Add** to add a new network interface.

    The **Add Virtual Interface** screen appears.

15. Without changing any configuration, click **Add**.

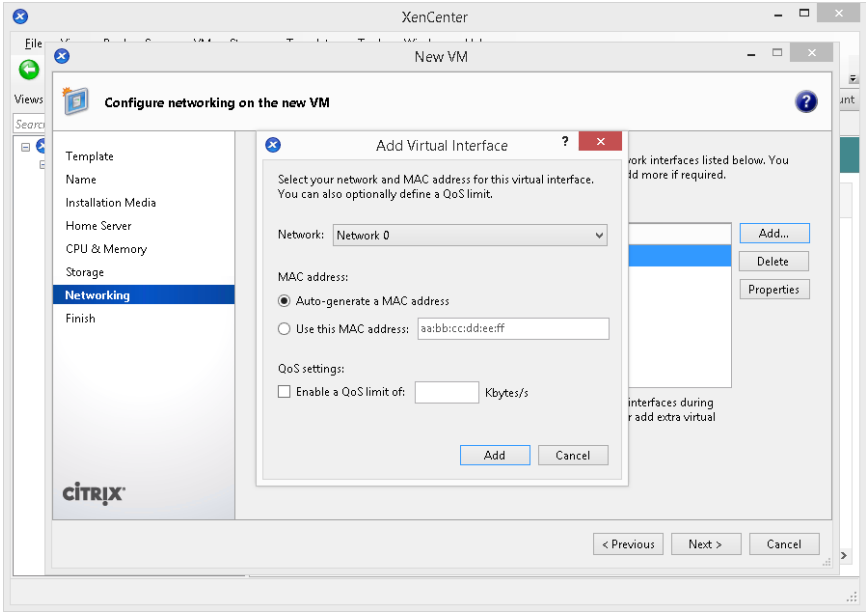


FIGURE 6-3. Add Virtual Interface screen

16. Click **Next** on the **Networking** screen.

    The **Finish** screen appears displaying the summary of settings for the new virtual machine.

17. Make sure that **Start the new VM automatically** is selected, then click **Create Now**.

    The wizard creates the virtual machine and adds it to the tree on the left side of the screen.

18. Select the virtual machine you have just created, and click the **Console** tab.

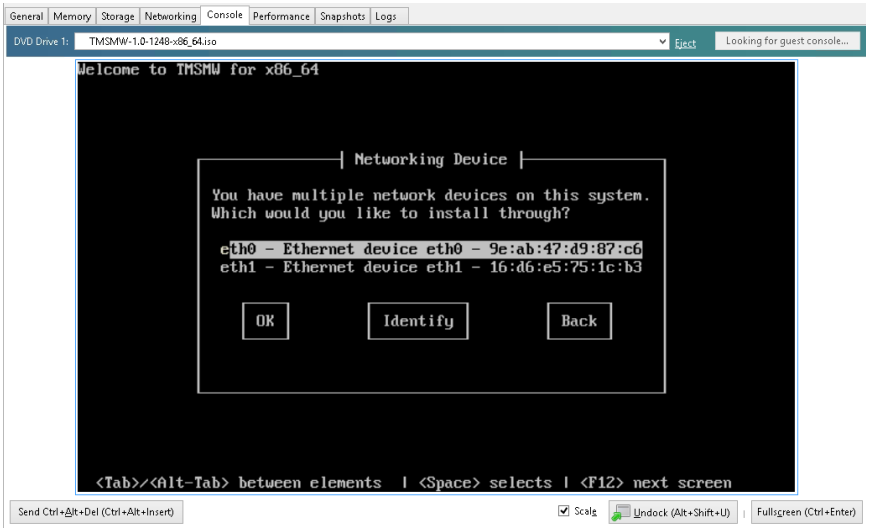


FIGURE 6-4. Select a network device for the installation

The screen displays the options to select a network device.

19. Select a network device and then select **OK**.

    The **Disc Found** screen appears.

20. Select **OK** to start the media test or **Skip** to skip it and start the installation.

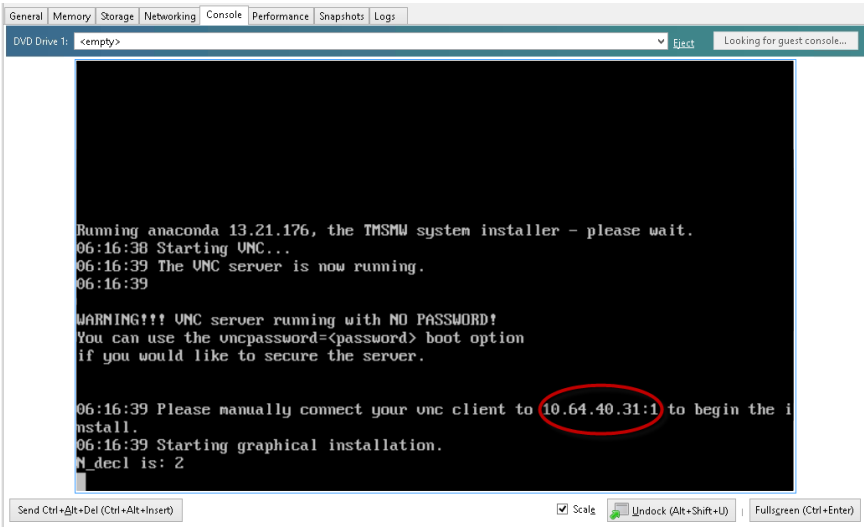


FIGURE 6-5. Screen displaying the VNC server IP address

The Safe Mobile Workforce starts the VNC server for the installation and a screen displays, showing the IP address of the VNC server.

21. Start TightVNC Viewer application and connect to the VNC server using the IP address shown on the screen.

    The Safe Mobile Workforce installation menu appears.

22. Follow *step 3 on page 2-2* to *step 11 on page 2-3* of the topic *Installing Safe Mobile Workforce Server on a Bare Metal Server on page 2-2* to complete Safe Mobile Workforce installation.

Installing Safe Mobile Workforce Secure Access

Installing Safe Mobile Workforce Secure Access on Citrix XenServer involves the following steps:

1. Installing a VNC viewer application. (See *Step 1: Installing a VNC Viewer Application on page 6-8*.)
2. Creating a virtual machine and installing Safe Mobile Workforce Secure Access. (See *Step 2: Creating a Virtual Machine and Installing Safe Mobile Workforce Secure Access on page 6-8*.)

Step 1: Installing a VNC Viewer Application

The Safe Mobile Workforce server installation requires a VNC viewer to complete the installation. Before you begin installing Safe Mobile Workforce server, install a VNC viewer application on the computer.

This document uses TightVNC viewer application for this procedure.

Step 2: Creating a Virtual Machine and Installing Safe Mobile Workforce Secure Access

Procedure

1. Start **Citrix XenCenter**.
2. Click **Add New Server** button on the toolbar.

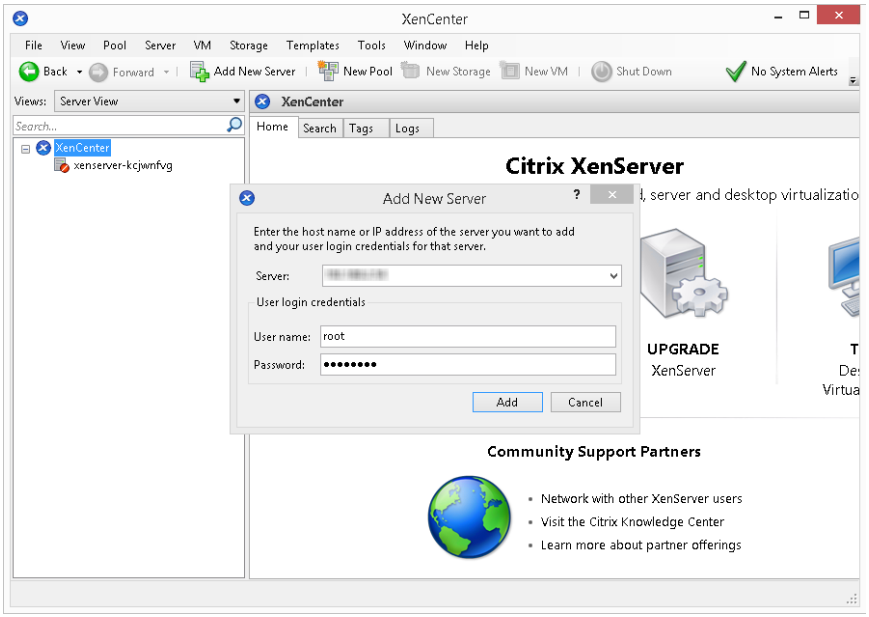


FIGURE 6-6. Add New Server dialog box

The **Add New Server** dialog box appears.

3. Type the server name, user name and password, and then click **Add**.

   XenCenter connects to XenServer and adds it to the server tree on the left side of the screen.

4. On the server tree on the left side of the screen, right-click the server name, then click **New VM**.

   The **New VM** screen appears.

5. From the list of operating systems, select **CentOS 6 (64-bit)**, and click **Next**.

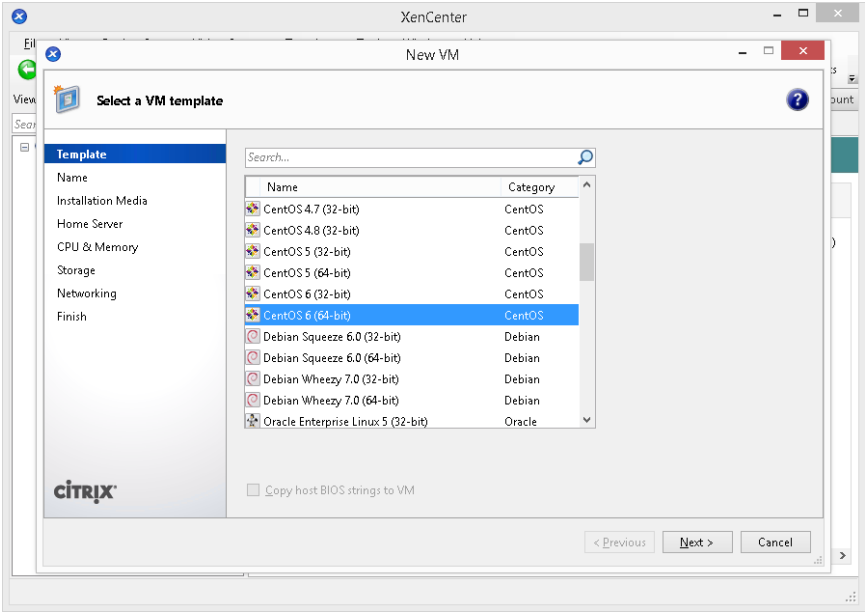


FIGURE 6-7. Select a VM template screen

6. Type a server name and description and then click **Next**.

   The **Installation Media** screen appears.

7. Do the following:

   a. Select an installation media.

      If you want to install Safe Mobile Workforce server from a network location, click **New ISO library**, select **Windows File Sharing (CIFS)**, and then follow the instructions on the screen.

   b. Under **Advanced OS boot parameters** section, type `graphical utf8 vnc`.

8. Click **Next**.

9. Select a server computer from the list, where you want to install Safe Mobile Workforce Secure Access, and click **Next**.

10. On the **CPU & Memory** screen, type the following:

a. **Number of vCPUs**: `4`

b. **Memory**: `4096` MB

11. Click **Next**.

    The **Storage** screen appears.

12. Click **Properties**, and in the **Size** field, type `30` GB, and then click **OK**.

13. Click **Next** on the **Storage** screen.

    The **Networking** screen appears.

14. Click **Next**.

    The **Finish** screen appears displaying the summary of settings for the new virtual machine.

15. Make sure that **Start the new VM automatically** is selected, then click **Create Now**.

    The wizard creates the virtual machine and adds it to the tree on the left side of the screen.

16. Select the virtual machine you have just created, and click the **Console** tab.

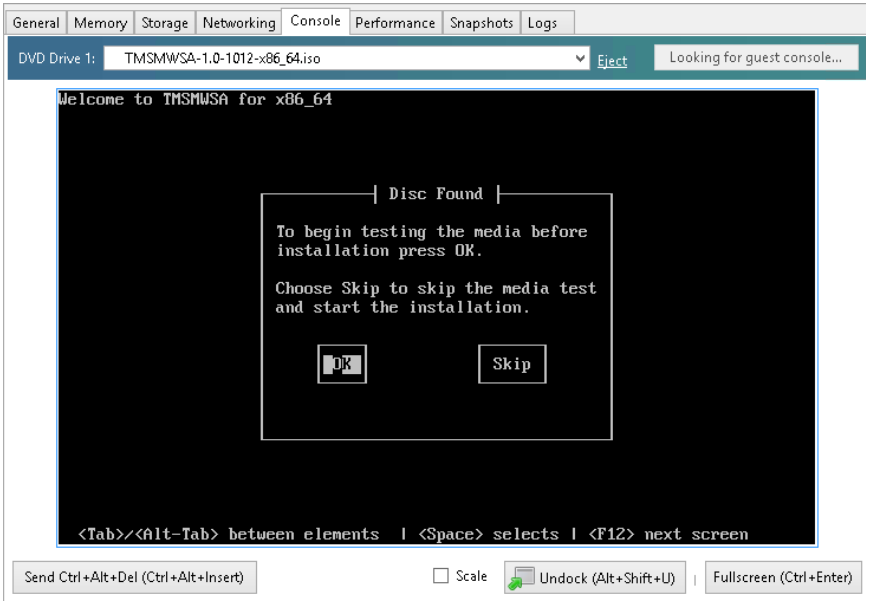


FIGURE 6-8. Select a network device for the installation

The screen displays the options to select a network device.

17. Select a network device and then select **OK**.

    The **Disc Found** screen appears.

18. Select **OK** to start the media test or **Skip** to skip it and start the installation.

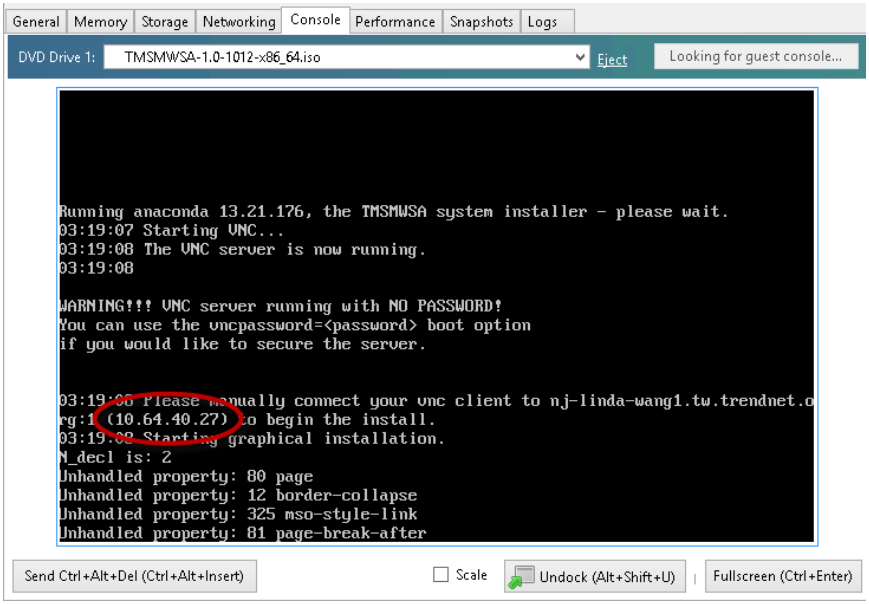


FIGURE 6-9. Screen displaying the VNC server IP address

The Safe Mobile Workforce starts the VNC server for the installation and a screen displays, showing the IP address of the VNC server.

19. Start TightVNC Viewer application and connect to the VNC server using the IP address shown on the screen.

    The Safe Mobile Workforce Secure Access installation menu appears.

20. Follow *step 3 on page 2-4* to *step 13 on page 2-6* of the topic *Installing Safe Mobile Workforce Secure Access on a Bare Metal Server on page 2-4* to complete Secure Access installation.

Chapter 7

Post-Installation Configuration

Trend Micro recommends performing all tasks in this chapter before using Safe Mobile Workforce.

This chapter contains the following sections:

Accessing Safe Mobile Workforce Administration Web Console

To access Safe Mobile Workforce Web console:

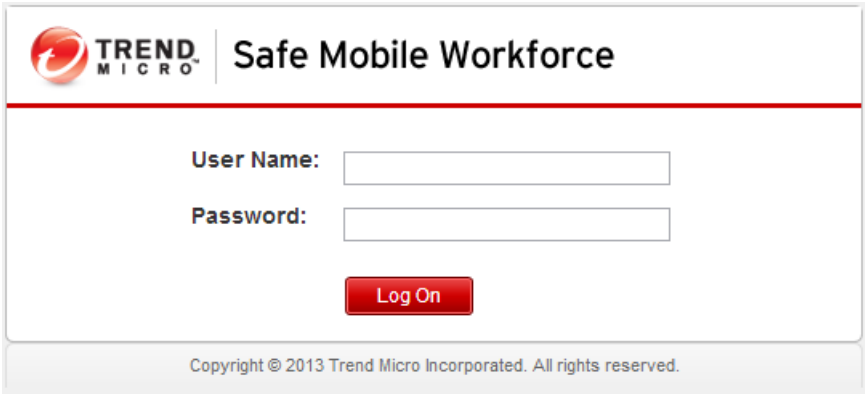
Procedure

1. Using a Web browser, open the following URL:

   https://<Safe Mobile Workforce_domain_name_or_IP_address>

   The following screen appears.

FIGURE 7-1. Safe Mobile Workforce Web console logon screen



2. Type a user name and password in the fields provided and click **Log On**.

Note

The default **User Name** for Safe Mobile Workforce Web console is `admin` and the Password is `admin`.

Make sure that you change the administrator password after your first sign in. Refer to the topic *Changing Administrator Account Password on page 7-4* for the procedure.

Activating Your Product

Safe Mobile Workforce displays a **Product License** screen on logging on to the administration Web console for the first time.

Use the **Product License** screen to activate your product.

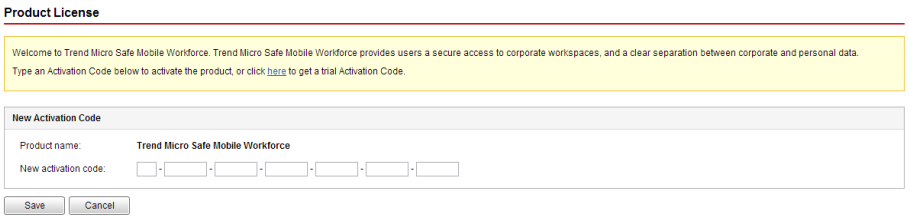


FIGURE 7-2. Product License screen

Procedure

1. If you do not have a license, click on **here** in **Click here to get trial Activation Code**, and follow the instructions on the Web page that appears.
2. Type your **Activation Code** that you have received in your email in the field provided.
3. Click **Save**.

Changing Administrator Account Password

Use the **My Account** screen to modify the administrator's account password in Safe Mobile Workforce.

Attention

Trend Micro recommends changing the administrator's account password every 30 to 90 days.

Procedure

1. Under **Account Information** section, click **Change password**.

   The **Change Password** dialog box pops up.

2. Use the following fields:

   - **Old password**–type the current administrator password.
   - **New password and Confirm password**–type the new administrator password.

3. Click **Save** on the pop-up dialog box.

4. Click **Save** on the **My Account** screen.

Configuring Server Network Interface (Optional)

Safe Mobile Workforce provides the following two options for configuring network interfaces for mobile devices to connect to the server:

- **IP Range**–this option enables you to assign individual IP address to each workspace.
- **Network Address Translator (NAT)**–this option enables you to share the server's IP address with the workspaces.

Procedure

1. Log on to the server Web console.
2. Click **Servers**.
3. Click the server name whose details you want to edit.

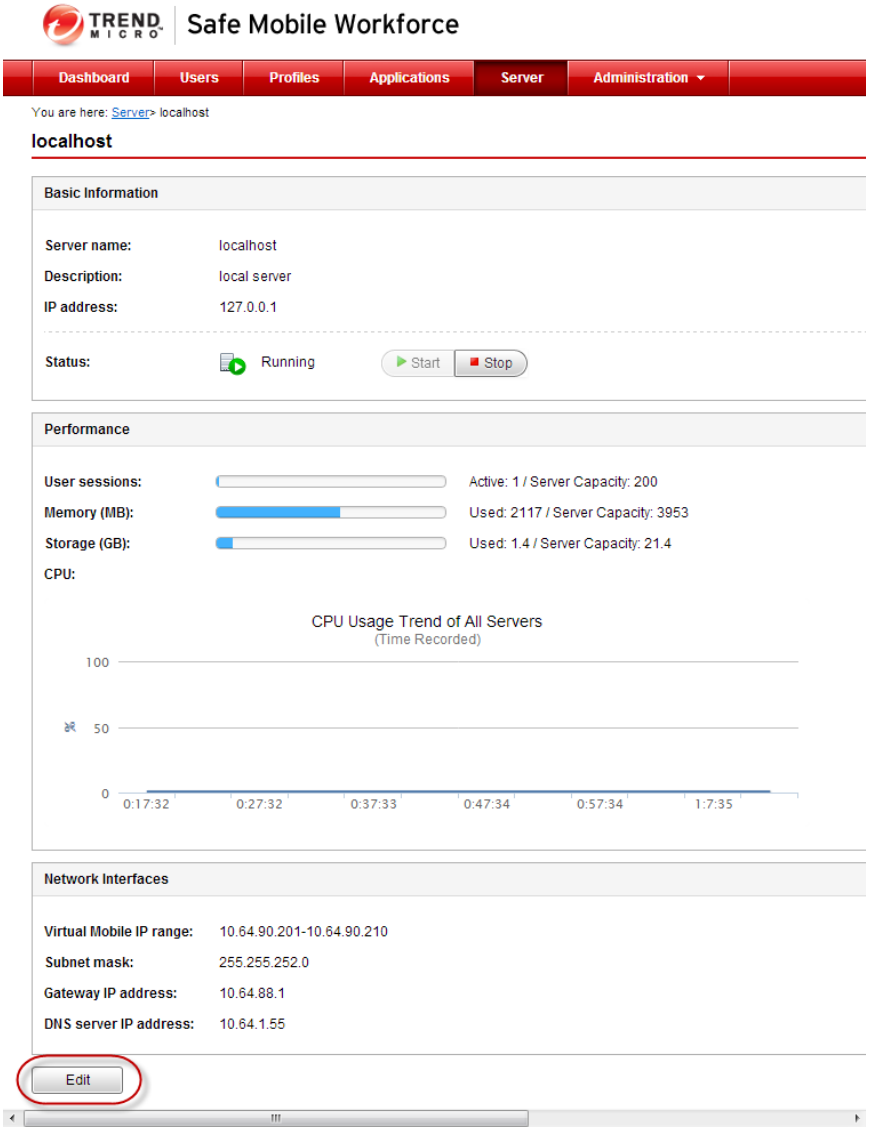


FIGURE 7-3. Server details screen

4. If the server is running, click **Stop** to stop the server, and then click **OK** to confirm.
5. Click **Edit**.
6. Update the following fields as required:
    - **Basic Information**
        - **Server name**
        - **Description**
    - **Workspace Network Connection**
        - **NAT: Workspaces share the server's IP address**–select this option if you want to share the server's IP address with the workspaces.
        - **IP Range**: Assign IP address to workspaces–select this option if you want to assign individual IP address to each workspace.
            - **Workspace IP range**–type a range of IP addresses that will used by the workspaces.

        > **Note**
        > The IP range should include at least two IP addresses. For example: 10.0.0.55-10.0.0.56.

    - **Subnet mask**
    - **Gateway IP address**
    - **DNS server IP address**
7. Click **Save**.

Configuring Active Directory Settings (Optional)

Safe Mobile Workforce provides optional integration with Microsoft Active Directory to manage users and groups more efficiently.

Use the **Active Directory** tab in **System Settings** to enable and configure the Active Directory settings.

If you do not want to import users and groups from Active Directory, or want to manage users locally on the Safe Mobile Workforce server, then you will need to disable the Active Directory integration.

Procedure

1. On the **System Settings** screen, click the **Active Directory** tab.
2. Select **Use Active Directory** to enable the feature
3. Configure the following:
   - **Server IP address**
   - **Server port**
   - **Base DN**–select a Base DN from the drop down list.
   - **User name and Password**–a user name and password to access the Active Directory server.
   - **Update frequency**–select a time from the list to determine how often to synchronize content with the Active Directory server.
4. Click **Save**.

   The server tests the connection with the Active Directory server and saves System Settings.

Disabling Active Directory

Use the **Active Directory** tab in **System Settings** to disable the Active Directory settings.

Procedure

1. Click the **Active Directory** tab.
2. Clear **Use Active Directory** checkbox to disable the feature.
3. Click **Save**.

Configuring Mobile Client Settings

The Safe Mobile Workforce mobile client provides access to the user workspace from a mobile device.

Use the **Mobile Client** tab on the **System Settings** screen to configure mobile clients for Safe Mobile Workforce.

Procedure

1. On the **System Settings** screen, click the **Mobile Client** tab.
2. Under the **Remember Password** section, if you want to allow users to save their passwords on their mobile devices, select **Allow users to save password on mobile device**.
3. Under the **Unsuccessful Signin Restriction Settings** section, if you want users to wait for a certain time before retrying after typing in a wrong password, select **Enable unsuccessful signin restrictions for Active Directory users**, and then select the number of attempts and the waiting time from the drop-down lists.
4. Under the **User Idle Time Setting** section, configure the time in minutes for the server, after which the server changes the user status from idle to offline.
5. Under the **Secure Access Settings**, configure the following:
   - **Domain name or IP address**

Note

If the server is connected to Secure Access or an external router, type the IP address of Secure Access or the router instead of the IP address of the server.

- **Port number**

6. Click **Save**.

Configuring SafeSync Integration Settings (Optional)

The SafeSync integration enables Safe Mobile Workforce to provide cloud based file storage to all users.

If you have already set up SafeSync in your enterprise environment, you can integrate Safe Mobile Workforce with SafeSync to provide file storage for all users.

Note

You can only integrate Safe Mobile Workforce with SafeSync if you are using Active Directory to manage user and group permissions in Safe Mobile Workforce.

Use the **SafeSync Integration** tab on **System Settings** screen to configure SafeSync integration settings.

Procedure

1. On the **System Settings** screen, click the **Active Directory** tab.
2. Make sure that the **Use Active Directory** checkbox is selected and the **Active Directory** settings are configured.
3. Click the **SafeSync Integration** tab.
4. Select **Enable users to access SafeSync account from workspace**, and then type the SafeSync server URL in the SafeSync server field.

5. Click **Save**.

Configuring Microsoft Exchange Server Settings (Optional)

If you have already set up an Exchange server in your enterprise environment, you can configure Safe Mobile Workforce to automatically configure Exchange server settings for all the users on their workspace.

Note

You can only configure Safe Mobile Workforce to use an Exchange server if you are using Active Directory server to manage user and group permissions in Safe Mobile Workforce.

Use the **Exchange Server** tab on **System Settings** screen to configure Microsoft Exchange Server settings.

Procedure

1. On the **System Settings** screen, click the **Active Directory** tab.
2. Make sure that the **Use Active Directory** checkbox is selected, and the Active Directory settings are configured.
3. Click the **Exchange Server** tab.
4. Select **Use automatic configuration for Exchange Server on workspace**, and then type the server name in the **Exchange server** field.
5. Click **Save**.

Configuring External Storage (Optional)

Safe Mobile Workforce enables you to use external storage to store user data. External storage is also required if you want to use multiple servers with Safe Mobile Workforce.

Safe Mobile Workforce uses network interface **eth0** for control and management information. Therefore, Trend Micro recommends connecting the external storage to network interface **eth0**.

Use the **External Storage** tab in **System Settings** to configure external storage for Safe Mobile Workforce server.

Procedure

1. On the **System Settings** screen, click the External Storage tab.
2. Select **Enable external storage**, and configure the following:
   - **Host name or IP address**
   - **Path**–type the location where you want to save the user data on the specified host or IP address.
3. Click **Test Connection** and then click **OK** on the pop-up dialog box.
4. Click **Save**.

   The server tests the connection with the external storage and saves **System Settings**.

Configuring Email Notifications

You must set up an email server and then configure the email notification settings to send the invitation or reset password emails to the users.

Use **Email Notifications** screen to configure email notifications in Safe Mobile Workforce.

Procedure

1. On the **Email Notifications** screen, under the **Email Settings** section, configure the following:
   - **From**–type the address from which you want to send the email notification. SMTP

- **SMTP Server**–type the SMTP server name or IP address.
- **Port**–type the SMTP server port number.
- **Authentication**–if the SMTP address requires authentication, select this option and type the following information:
  - **User name**
  - **Password**
- **Use TLS protocol for authentication**–if the SMTP server requires TLS protocol for authentication, select this option.

2. Click **Test Connection** to verify SMTP server address and port number.

> **Note**
>
> This test does not verify the user name and password configured to access the SMTP server.

3. Under **Invitation Email Template**, type the following:
   - **Subject**–the subject of the email message.
   - **Message**–the body of the email message.

> **Note**
>
> While editing the **Message** field, make sure to include the token variables %(name)s, %(username)s and %(password)s, which will be replaced by the actual values in the email message.

4. Under **Reset Password Template**, type the following:
   - **Subject**–the subject of the email message.
   - **Message**–the body of the email message.

Note

While editing the **Message** field, make sure to include the token variables %(name)s, %(username)s, %(password)s, which will be replaced by the actual values in the email message.

5. Click **Save** to save settings.

Managing Groups and Users

Safe Mobile Workforce enables you to add users and groups manually or import them from the Active Directory (AD). On importing a group from AD, Safe Mobile Workforce inherits all user account information from the Active Directory Domain Controller.

Note

User accounts imported from the Active Directory cannot be modified from the Safe Mobile Workforce server.

Importing Groups or Users from Active Directory

Before importing groups or users from Active Directory, make sure that you have already configured the Active Directory settings. See *Configuring Active Directory Settings (Optional) on page 7-8* for the procedure.

Use the **User Management** screen to import groups or users from Active Directory.

Procedure

1. Click **Import**.

   The **Import Group or User from Active Directory** screen appears.

2. Type the group or user information in the search field provided, and click **Search**.

3. Select the groups or users that you want to import from the search result, and then click **Import**.

Safe Mobile Workforce server sends an invitation email to all users in the imported group. The invitation email includes the user account information to log on to server.

Creating a User Account Locally

Safe Mobile Workforce allows you to add a local user account to the server. However, you cannot use Active Directory in conjunction with the local users. This means, you will need to disable Active Directory to add a local user.

Before you can create a local user account, make sure that you have disabled the Active Directory integration. See *Disabling Active Directory on page 7-9* for the procedure.

Use the **User Management** screen to create a user account locally.

Procedure

1. Click **Add User**.

   Add A New User screen appears.

2. Configure the following:

   - **User name**
   - **First name**
   - **Last name**
   - **Email address**
   - **Group**—select a group from the drop-down menu for the user.
   - **Profile**—select a profile from the drop-down menu for the user.

3. Click **Add**.

Safe Mobile Workforce server sends an invitation email to the user. The invitation email includes the user account information to log on to server.

Deploying Safe Mobile Workforce to Mobile Devices

Trend Micro recommends configuring Notification Settings to send an invitation email to the users. When you import users or groups from Active Directory, or add users locally, the Safe Mobile Workforce server sends an invitation email to the users that includes the account information to log on to the server. Users can download the client application from Google Play store or Apple App Store.

See *Configuring Email Notifications on page 7-12* for the procedure of creating and configuring system notifications.

Installing Android Client for Safe Mobile Workforce

Download the Android client application for Safe Mobile Workforce from Google Play store.

Procedure

1. Open Google Play store on an Android mobile device and search for `Safe Mobile Workforce`.
2. In the search results, look for **Trend Micro Safe Mobile Workforce** and tap **Install**.
3. Tap **Install** on the access permissions screen that appears and wait while the app downloads and installs, then tap **Open**.
4. Type **User name**, **Password** and **Server address** as mentioned in the email, and tap **Sign In**.
5. If a dialog box appears requiring you to enable GPS on the mobile device, tap **OK** and then enable GPS satellites.

Note

Safe Mobile Workforce requires to use the mobile device location information for any application installed in the user workspace. If you tap **Cancel**, Safe Mobile Workforce will display this pop-up dialog box again the next time you start the application.

You can now access the user workspace and use the applications installed.

Installing iOS Client for Safe Mobile Workforce

Download the iOS client app for Safe Mobile Workforce from Apple App Store.

Procedure

1. Open App Store on an iOS mobile device and search for `Safe Mobile Workforce`.
2. In the search results, look for **Trend Micro Safe Mobile Workforce** and tap **Free**, and then tap **Install**.
3. If required, type your password for the Apple account, and wait while the app downloads and installs, then tap **Open**.

   The Safe Mobile Workforce client app **Sign In** screen appears.
4. Type **User name**, **Password** and **Server Address** as mentioned in the email, and tap **Sign In**.

   A notification appears requiring you to allow the application to use the location.
5. Tap **OK**.

Note

Safe Mobile Workforce requires to use the mobile device location information for any application installed in the user workspace. If you tap **Don't Allow**, Safe Mobile Workforce will NOT display this pop-up dialog box again. You will need to enable this setting manually. To enable Safe Mobile Workforce to use the mobile device location information, tap **iOS Settings** > **Privacy** > **Location Services**, and enable Safe Mobile.

You can now access the user workspace and use the applications installed.

Installing Windows Client for Safe Mobile Workforce

Download the Windows client from the Windows Store.

Procedure

1. Open the Store on a Windows mobile device and search for `Safe Mobile Workforce`.
2. In the search results, look for **Trend Micro Safe Mobile Workforce** and tap **Install**.
3. If required, type your password for your Microsoft account, and wait while the app downloads and installs.
4. To start the app, go to the Apps screen and tap the app icon.

   The Safe Mobile Workforce client app **Sign In** screen appears.
5. Type **User name**, **Password** and **Server Address** as mentioned in the email, and tap **Sign In**.

   A notification appears requiring you to allow the application to use the location.
6. Tap **OK**.

Note

Safe Mobile Workforce requires to use the mobile device location information for any application installed in the user workspace. If you tap **Cancel**, Safe Mobile Workforce will display this pop-up dialog box again the next time you start the application.

You can now access the user workspace and use the applications installed.

Appendix A

Network Port Configurations

This appendix provides all the network ports configurations that you need while installing Safe Mobile Workforce.

This appendix contains the following sections:

Network Port Configuration for Safe Mobile Workforce Server

Configure the following network ports for Safe Mobile Workforce server:

Component	Network Ports	Details	Required or Optional	Direction
Management Web console	HTTPS port **443**	Used to access Safe Mobile Workforce management Web console.	Required	Inbound
Mobile client enrollment	HTTPS port **443**	Used to enroll mobile client to the server.	Required	Inbound
Mobile client access	TCP port **5901**	Used by mobile client to access Safe Mobile Workforce server.	Required	Inbound
	TCP port **5902** to **6923**	Used by mobile client to access Safe Mobile Workforce server.	Required if using NAT. Optional if using IP range.	Inbound
Workspace Management	TCP port **16509** TCP port **16514**	If you are using multiple servers, configure this port for accessing workspaces on secondary servers. If you are using only one server, this port is not required.	Optional	Inbound

Component	Network Ports	Details	Required or Optional	Direction
Active Directory	TCP port **389** (Domain Controller) for Management console TCP port **3268** (Global Category) for Management console	Used for user authentication using Active Directory. If you are not using Active Directory to authenticate or import users, these ports are not required.	Optional	Outbound
SMTP server	TCP port **25**	Used to access email server. If you are not using SMTP server to send emails, this port is not required.	Optional	Outbound
SafeSync port	HTTPS port **443**	Used to connect to the SafeSync server. If you are not using SafeSync as file storage, this port is not required.	Optional	Outbound

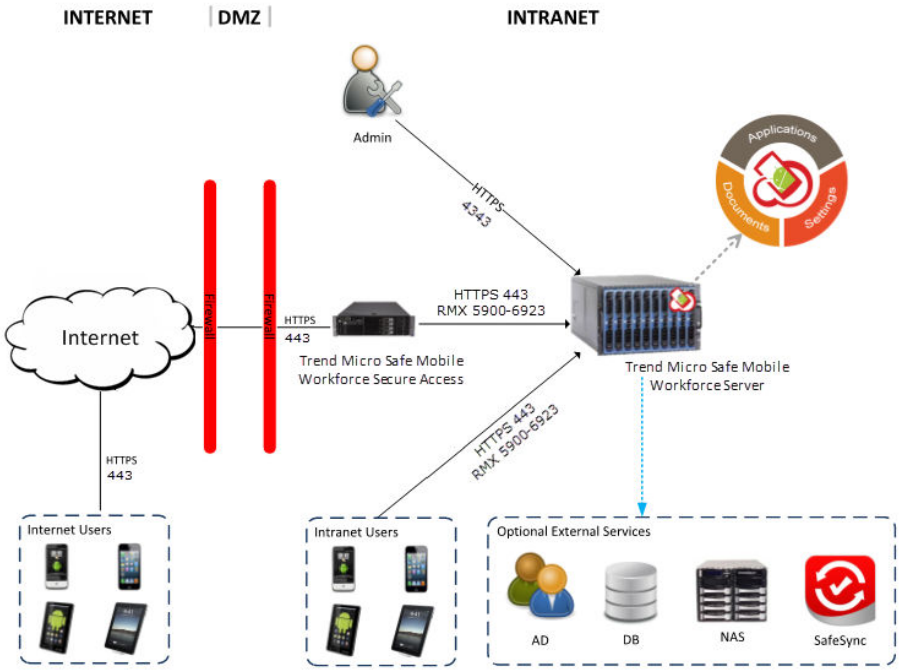
Network Port Configuration for Safe Mobile Workforce Secure Access

Configure the following network ports for Safe Mobile Workforce Secure Access:

Component	Network Ports	Details	Required or Optional	Direction
Mobile client enrollment	HTTPS Port 443	Used to enroll mobile client to the server.	Required	Inbound
Connection to Safe Mobile Workforce Server	HTTPS Port 443 TCP Port 5900 to 6923	Used by Secure Access to communicate with Safe Mobile Workforce server.	Required	Outbound
OAuth 2.0 authentication	8443	Used for user authentication using OAuth 2.0.	Optional	Inbound

Network Ports in Safe Mobile Workforce Architecture

The following figure shows the network ports used in Safe Mobile Workforce architecture.



Remote Mobile Experience (RMX) *is an intelligent remote access protocol.*

FIGURE A-1. Network Ports in Safe Mobile Workforce Architecture

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: MWEM26892/150318